



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>

IRONICALLY, SOME TARGETS ARE HARDER THAN OTHERS

Michael Clarkson - GCFA Practical v1.3

© SANS Institute 2003, Author retains full rights.

Table of Contents

Table of Contents		2
Abstract, and list of conventions		3
Part 1: Analysis of an unknown binary		
Binary Details		4
Program Description		8
Forensic Details		14
Program Identification		18
Legal Implications		22
Interview Questions		23
Additional Information		25
Part 2: Forensic Analysis of a Computer System		
Synopsis of Case Facts		26
Describe of system to be Analysed		26
Hardware Details		26
Image Media		27
Media Analysis of System		30
Timeline Analysis		49
Deleted File Examination	55	
String Search		55
Conclusions		57
Part 3: Legal Issues of Incident Handling		
Question A		59
Question B.	61	
Question C.	61	
Question D.	62	
Question E.		62
Endnotes		64

Abstract

IN THIS PAPER , A BINARY FILE OF UNKNOWN PURPOSE AND FUNCTIONALITY WILL BE EXAMINED . THIS WILL BE PERFORMED USING COMMONLY AVAILABLE TOOLS AND WILL SEEK TO DETERMINE THE PURPOSE OF THE BINARY AND THE REASON IT WAS ON THE SYSTEM . ANY OTHER DETAILS AVAILABLE ABOUT THE BINARY WILL ALSO BE DISCUSSED .

IN PART 2 OF THIS PAPER , A HARD DISK DRIVE WILL BE EXAMINED . THIS DISK DRIVE IS TAKEN FROM A COMPUTER IN AN UNKNOWN STATE , AND THE OPERATING SYSTEM 'S SECURITY MAY HAVE BEEN COMPROMISED . AN IMAGE OF THE DRIVE WILL BE TAKEN , AND PROVED TO BE FORENSICALLY SOUND . THIS IMAGE WILL THEN BE EXAMINED USING VARIOUS TOOLS , THE GOAL BEING TO DISCOVER AS MUCH INFORMATION ABOUT THE POTENTIAL COMPROMISE AS POSSIBLE , HOPEFULLY INCLUDING THE IDENTITY OF THE INTRUDER .

PART 3 WILL EXAMINE SOME LEGAL ASPECTS OF A HYPOTHETICAL SCENARIO . THIS SCENARIO INVOLVES A LAW ENFORCEMENT OFFICIAL SEEKING ASSISTANCE FROM THE SYSTEM ADMINISTRATOR OF AN INTERNET SERVICE PROVIDER (ISP) . THE ISP NETWORK MAY HAVE BEEN USED TO ATTACK A GOVERNMENT NETWORK . THIS SECTION OF THE PAPER WILL DISCUSS WHAT HELP THE SYSTEM ADMINISTRATOR IS ALLOWED TO GIVE THE LAW ENFORCEMENT OFFICIAL . THIS DISCUSSION WILL FOCUS ON THE LAW OF NEW ZEALAND , AS IT STOOD ON JULY 17TH , 2003 .

IN THIS ASSIGNMENT , THE FOLLOWING CONVENTIONS HAVE BEEN USED .

Section headings are in Times New Roman (12) Bold Underline

The investigator's comments are in Times New Roman (12).

Commands entered into a command line or shell are in Arial (8) Bold

The computer's responses to the command are in Arial(8)

Code listings are in Arial(8)

Document Listings are in Arial(8)

0.1 A blank line in

0.2 A continuous code or document listing

0.8 Indicates that for brevity, irrelevant or repetitive lines have been omitted from the listing

THE OUTPUT FROM THE SYSINTERNAL'S PROCESS EXPLORER IS IN ARIAL (6)

The printout of the Autopsy Time Line is in Arial(7)

LEGAL CASE NAMES ARE IN TIMES NEW ROMAN (12) ITALIC

Legislation is in Times New Roman (12) Underline

Analysis of an unknown binary

The following is an analysis of a binary of unknown functionality and purpose, which may be malicious. Accordingly, some security precautions are required, as will be later explained in more depth. Although the binary did not include an md5 checksum to assure us of its forensic accuracy, there is currently no reason to suspect that the file may be corrupted.

Binary Details

The details of the zip file containing the binary are as follows.

```
delta> ls
total 8
drwxr-xr-x  2 michael root    512 Jun 19 13:05 .
drwxr-xr-x  5 michael root    512 Jun 19 12:42 ..
-rw-r--r--  1 michael root   5687 Jun 17 14:28 binary_v1.3.zip
delta>
```

AS CAN BE SEEN , THE NAME OF THE ZIP FILE IS "BINARY_V1.3.ZIP". THE FILE IS (APPROX) 6KB IN ITS COMPRESSED FORM. THE NAME OF THE COMPUTER ON WHICH THIS STAGE OF THE INVESTIGATION IS BEING PERFORMED IS "DELTA." THIS MACHINE IS A SUNBLADE , RUNNING SOLARIS V 8. THE OWNER OF THE FILE IS "MICHAEL ", AS THIS IS THE USER WHO DOWNLOADED THE FILE (THIS CAN EASILY BE CONFIRMED BY LOGGING INTO THE MACHINE AS ANOTHER USER , AND DOWNLOADING THE FILE AGAIN .) ACCORDINGLY , BOTH THE USER AND GROUP INFORMATION , AS WELL AS THE ATTRIBUTES OF THE ZIP FILE CAN BE DISREGARDED . THE TIME STAMP ON THE FILE IS THE TIME THAT THE ZIP FILE WAS DOWNLOADED AND WRITTEN TO THE DISK ON THE LOCAL MACHINE . THIS ALSO HAS NO EVIDENTIAL VALUE , AS ALL THE TIME INFORMATION HAS BEEN LOST , DURING THE TRANSIT FROM THE MACHINE ON WHICH THE BINARY WAS FOUND .

USEFUL INFORMATION CAN BE GAINED FROM THE ZIP FILE HOWEVER .

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

This shows that the file's original size was 27kb. This high compression ratio (27:6, approx 80% compression) suggests that the file may contain large amounts of text, which is more easily compressed than binary data.

This output also shows us that the file was zipped up from a "File Allocation System". This is the file and directory system commonly used by Windows Operating System (OS). The file name is displayed as "target2.exe". The "exe" extension is used on DOS (Disk Operating System) systems to identify EXEcutable files. This accords with our hypothesis that the file was created in a Windows OS. Zipinfo displays the correct filename case, as stored in the file. As MS -DOS PKZIP always uses uppercase file names, this file may have been compressed from a Windows machine using the "Long File Name" system, which allows for lowercase file names.

The attributes on the stored file indicate that it is -Rwxa-- readable (always true), -rWxa-- writable, -rwXa-- executable (a guess based on the file name extension), and -rwxA-- archivable. The file is not a directory, hidden or a system file. The 2.0 indicates that the program used to zip the file was version 2.0 of that program. The defN indicates that the compression scheme used was "deflation", with a "Normal" compression ratio. Finally, the file was last modified at 12:45pm on Thursday the 20th of February, 2003. This is the DOS time, which is rounded to the nearest 2 seconds.

```
delta> zipinfo -v binary_v1.3.zip
Archive: binary_v1.3.zip 5687 bytes 1 file
```

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

```
-----
Actual offset of end-of-central-dir record: 5665 (00001621h)
Expected offset of end-of-central-dir record: 5665 (00001621h)
(based on the length of the central directory and its expected offset)
```

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

```
There is no zipfile comment.
```

```
Central directory entry #0:
```

```
-----
target2.exe
```

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

```
There is no file comment.
```

```
delta>
```

This file was apparently zipped up from a MS-DOS based system. MS-DOS does not store user information as part of a file's metadata. Accordingly, the zip file does not contain any information about the user or group who originally owned the binary in question.

Comments can be associated with the entire zip file when compressing. This zip file

had no such comment. Comments can also be associated with individual files contained in the zip file. The “target2.exe” compressed file also had no comments.

List file

```
delta> unzip -l binary_v1.3.zip
Archive: binary_v1.3.zip
Length Date Time Name
-----
26793 02-20-03 12:45 target2.exe
-----
26793          1 file
```

Verbose listing of file

```
delta> unzip -lv binary_v1.3.zip
Archive: binary_v1.3.zip
Length Method Size Ratio Date Time CRC-32 Name
-----
26793 Defl:N 5567 79% 02-20-03 12:45 d185fd18 target2.exe
-----
26793      5567 79%          1 file
```

Test file

```
delta> unzip -t binary_v1.3.zip
Archive: binary_v1.3.zip
testing: target2.exe OK
No errors detected in compressed data of binary_v1.3.zip.
```

UNZIP FILE

```
DELTA:> UNZIP BINARY_V1.3.ZIP
ARCHIVE: BINARY_V1.3.ZIP
INFLATING: TARGET2.EXE
DELTA:> LS -AL
TOTAL 35
DRWXR-XR-X 2 MICHAEL ROOT 512 JUN 27 10:13 .
DRWXR-XR-X 5 MICHAEL ROOT 512 JUN 27 10:10 ..
-RW-R--R-- 1 MICHAEL ROOT 5687 JUN 20 14:48 BINARY_V1.3.ZIP
-RW-R--R-- 1 MICHAEL ROOT 26793 FEB 20 12:45 TARGET2.EXE
DELTA:>
```

FILE LAST MODIFIED

```
DELTA:> LS -AL
TOTAL 35
DRWXR-XR-X 2 MICHAEL ROOT 512 JUN 27 10:13 .
DRWXR-XR-X 5 MICHAEL ROOT 512 JUN 27 10:10 ..
-RW-R--R-- 1 MICHAEL ROOT 5687 JUN 20 14:48 BINARY_V1.3.ZIP
-RW-R--R-- 1 MICHAEL ROOT 26793 FEB 20 12:45 TARGET2.EXE
```

FILE LAST CHANGED (iNODE INFORMATION)

```
DELTA:> LS -ALC
TOTAL 35
DRWXR-XR-X 2 MICHAEL ROOT 512 JUN 27 10:13 .
DRWXR-XR-X 5 MICHAEL ROOT 512 JUN 27 10:10 ..
-RW-R--R-- 1 MICHAEL ROOT 5687 JUN 27 06:05 BINARY_V1.3.ZIP
-RW-R--R-- 1 MICHAEL ROOT 26793 JUN 27 10:13 TARGET2.EXE
```

FILE LAST ACCESSED

```
DELTA:> LS -ALU
TOTAL 35
DRWXR-XR-X 2 MICHAEL ROOT 512 JUN 27 10:52 .
DRWXR-XR-X 5 MICHAEL ROOT 512 JUN 27 10:52 ..
-RW-R--R-- 1 MICHAEL ROOT 5687 JUN 27 10:13 BINARY_V1.3.ZIP
-RW-R--R-- 1 MICHAEL ROOT 26793 FEB 20 12:45 TARGET2.EXE
DELTA:>
```

ON A UNIX SYSTEM, THREE SEPARATE TIMES ARE SAVED FOR EACH FILE. THESE TIMES REPRESENT THE TIME THE FILE WAS LAST MODIFIED (M-TIME), LAST ACCESSED (A-TIME), OR HAD ITS METADATA CHANGED (C-TIME). COLLECTIVELY THESE ARE KNOWN AS THE MAC TIMES. FROM THE MAC TIMES OF THIS FILE ONCE EXPANDED, IT WAS CREATED ON FEBRUARY 20TH, AT 12:45. THE FILE'S METADATA WAS LAST CHANGED AT 10:13, JUNE 27 (THE TIME THE FILE WAS EXTRACTED) BUT THE FILE WAS LAST ACCESSED ALSO ON FEB 20TH AT 12:45. IT IS LIKELY THAT THE FILE WAS CREATED ON THE SYSTEM IN QUESTION ON THE 20TH OF FEBRUARY, AND EITHER NEVER RUN, OR RUN ONCE IMMEDIATELY AFTER IT WAS CREATED. THE LAST CHANGED TIME IS OF NO USE, AS THIS INCLUDES THE TIME THE INODE (PORTION OF THE DISK DRIVE) CONTAINING THE FILE WAS MODIFIED. AS THE CURRENT INODE ON THE TEST SYSTEM DID NOT CONTAIN ANY INFORMATION ABOUT THE FILE, IT WAS UPDATED WHEN THE FILE WAS EXTRACTED. 10:13 AM WAS IN FACT THE TIME THE UNZIP COMMAND WAS RUN.

THE FILE IS 26,793B, AS COULD BE SEEN FROM THE ZIP FILE. THE MD5 HASH OF THE BINARY IS "848903A92843895F3BA7FB77F02F9BF1", AS SHOWN IN THIS SCREEN-SHOT OF THE MD5 HASH BEING TAKEN.



The current owner and group information of the binary are those that the file was extracted onto the test system using. In this case, that is "michael" and "root".

```
DELTA:> FILE TARGET2.EXE
TARGET2.EXE: DOS EXECUTABLE (EXE)
DELTA:>
```

THE UNIX "FILE" COMMAND (USED TO IDENTIFY DIFFERENT FILE TYPES) IDENTIFIES THE FILE AS AN MS-DOS TYPE BINARY EXECUTABLE.

Program Description

EXECUTABLE FILES OFTEN CONTAIN READABLE TEXT, AS WELL AS BINARY DATA. THIS TEXT CAN REVEAL USEFUL INFORMATION ABOUT THE EXECUTABLE FILE, SUCH AS MENU OPTIONS, HELP STRINGS, OR USAGE STATEMENTS. THESE STRINGS ARE DISPLAYED USING THE "STRINGS" COMMAND. THE -A OPTION DISPLAYS ALL THE STRINGS IN THE FILE, INCLUDING THOSE OCCURRING AT THE BEGINNING AND END OF THE FILE.

DELTA:> STRINGS -A TARGET2.EXE

!THIS PROGRAM CANNOT BE RUN IN DOS MODE.

```
RICH
.TEXT
`.RDATA
@.DATA
.RSRC
HL@@
SUVW
D$,QPR
|4,3
D$J'P
T$,J'RP
L$,J
T$,VRS
D$J'P
T$,J'RP
|S H
L$0H
L$,J'Q
D$"J
D$,J'PQ
SUVW
D$0QPR
D$$J'P
T$0J'RP
L$0J
T$0URV
D$$J'P
T$0J'RP
_ ^I
T$H
D$J'PQ
D$(H
L$(Q
H(@@
T$$QRJ
D$$PW
5@@
5,@@
5@@@
5,@@@
5,@@@
5,@@@
HQA@
VPPP
5@@
5,@@
IRQH
5H0@
SPHXD@
H|D@
SQHPD@
HTD@
|$,H'D@
D$J
D$@SPS
D$TD
=D0@
5P0@
-T0@
T$H
```

T\$|RP
USSSP3
-@@@
-@@@
-^j3
SUVW
D\$(PQ
5D0@
-@@@
-@@@
;EUI
X!XU\
X"iUV
X#TUP
IQH@A@
-@@@
-@@@
-^j3
-^I
U WJ
HHA@
HPA@
5LD@
5PD@
5TD@
5XD@
T1H@D@
5TD@
5XD@
HT HT
H@D@
5LD@
5TD@
5XD@
5D@@
VWH?
HPA@
=@0@
HPA@
HPA@
U@H'B@
PH<B@
H(B@
T\$(QR
HPA@
L\$0PQ
=\$0@
HPA@
PH0C@
5\$0@
HPA@
HXC@
HXC@
H8C@
%|0@
%x0@
H '@
%p0@
%L0@
H(1@
SVW
= D@
SLEEP
HEAPALLOC
GETPROCESSHEAP
TERMINATEPROCESS
READFILE
PEEKNAMEPIPE
CLOSEHANDLE
CREATEPROCESSA
CREATEPIPE
WRITEFILE
GETLASTERROR
LOCALALLOC

© SANS Institute 2003, Author retains full rights.

```

KERNEL32.DLL
STARTSERVICECTRLDISPATCHERA
SETSERVICESTATUS
REGISTERSERVICECTRLHANDLERA
CLOSESERVICEHANDLE
CONTROLSERVICE
QUERYSERVICESTATUS
OPENSERVICEA
CREATESERVICEA
OPENSCTMANAGERA
DELETESERVICE
STARTSERVICEA
CHANGESERVICECONFIGA
QUERYSERVICECONFIGA
ADVAPI32.DLL
WSAIOCTL
WSASOCKETA
WS2_32.DLL
MFC42.DLL
MEMMOVE
EXIT
FP RINTF
_JOB
SP RINTF
PERROR
STRSTR
TIME
PRINTF
MSVCRT.DLL
__DLLONEXIT
__ONEXIT
__EXIT
__XCPTFILTER
__P__INITENV
__GETMAINARGS
__INITTERM
__SETUSERMATHERR
__ADJUST_FDIV
__P__COMMODE
__P__FMODE
__SET_APP_TYPE
__EXCEPT_HANDLER3
__CONTROLFP
??0INIT@IOS_BASE@STD@@@QAE@XZ
??1INIT@IOS_BASE@STD@@@QAE@XZ
??0_WINIT@STD@@@QAE@XZ
??1_WINIT@STD@@@QAE@XZ
MSVCP60.DLL
ERROR 3
ERROR 2
ERROR 1
IMPOSSIBLE CREARE RAW ICMP SOCKET
RAW ICMP SENDTO:
=====ICMP BACKDOOR V0.1=====
=====CODE BY SPOOF. ENJOY YOURSELF!
YOUR PASSWORD:
LOKI
CMD.EXE
EXIT OK!
LOCAL PARTNERS ACCESS
ERROR UNINSTALLING SERVICE
SERVICE UNINSTALLED SUCESSFULLY
ERROR INSTALLING SERVICE
SERVICE INSTALLED SUCESSFULLY
CREATE SERVICE %S OK!
CREATESERVICE FAILED:%D
SERVICE STOPPED
FORCE SERVICE STOPPED FAILED%D
THE SERVICE IS RUNNIN G OR STARTING!
QUERY SERVICE STATUS FAILED!
OPEN SERVICE FAILED!
SERVICE %S ALREADY EXISTS
LOCAL PRINTER MANAGER SERVICE
SMSSSES.EXE

```

```
OPEN SERVICE CONTROL MANAGE FAILED:%D
START SERVICE SUCCESSFULLY!
STARTING THE SERVICE FAILED!
STARTING THE SERVICE <%S>...
SUCCESSFULLY!
FAILED!
TRY TO CHANGE THE SERVICE'S START TYPE...
THE SERVICE IS DISABLED!
QUERY SERVICE CONFIG FAILED!
SMB2
SMB2
SMB2
SMBQ
SMBU
?????
SMB2
SMB2
SMB2
SMB/
DELTA:>
```

THE OUTPUT OF THE STRINGS COMMAND CLEARLY ALSO SHOWS THAT THIS IS AN MS-DOS BINARY. THE FIRST PART OF THE STRINGS OUTPUT IS FROM THE "DOS STUB" – THE PORTION OF THE CODE THAT WILL BE EXECUTED IF THE PROGRAM IS RUN IN DOS. HERE, THE PROGRAM WILL LIKELY DISPLAY "THIS PROGRAM CANNOT BE RUN IN DOS MODE" AND THEN EXIT. THIS IS AN INDICATION THAT THE PROGRAM IS WRITTEN FOR WINDOWS. IN EITHER CASE, AS THE FILE IS NOT A UNIX BINARY, FURTHER ASSESSMENT WILL NEED TO BE CONDUCTED ON A WINDOWS BOX.

THE FOLLOWING STRINGS MAY GIVE US AN IDEA WHAT THIS PROGRAM WILL DO WHEN EXECUTED.

```
Sleep
HeapAlloc
GetProcessHeap
This is standard Windows program functionality
```

```
TerminateProcess
This is a little suspicious. Generally programs only need to kill processes that they have started, so we might expect to see a fork or spawn call later on.
```

```
ReadFile
WriteFile
THE PROGRAM MAY HAVE THE ABILITY TO READ AND WRITE TO THE DISK DRIVE.
```

```
PEEKNAMEDPIPE
CLOSEHANDLE
CREATEPROCESSA
CREATEPIPE
These function calls are for creating a new process, and associating it with a data stream. This suggests network functionality.
```

```
GetLastError
LocalAlloc
KERNEL32.dll
More regular Windows system calls.
```

```
StartServiceCtrlDispatcherA
SetServiceStatus
RegisterServiceCtrlHandlerA
CloseServiceHandle
ControlService
```

QueryServiceStatus
OpenServiceA
CreateServiceA
OpenSCManagerA
DeleteService
StartServiceA
ChangeServiceConfigA
QueryServiceConfigA

These calls are associated with service control. This allows programs to start and stop windows services, ie spawning other programs.

ADVAPI32.dll
WSAloctl
WSASocketA
WS2_32.dll

THIS IS SOCKET FUNCTIONALITY, FOR COMMUNICATING WITH OTHER MACHINES .

MFC42.DLL
MEMMOVE
EXIT
FPRINTF
_JOB
SPRINTF
PERROR
STRSTR
TIME
PRINTF

These look like C functions, which may suggest that the program was written in C or a variant.

MSVCRT.dll
__dllonexit
_onexit
_exit
_XcptFilter
_p__initenv
__getmainargs
_initterm
__setusematherr
_adjust_fdiv
_p__commode
_p__fmode
__set_app_type
_except_handler3
_controlfp

Some more Windows strings

??0Init@ios_base@std@@@QAE@XZ
??1Init@ios_base@std@@@QAE@XZ
??0_Winit@std@@@QAE@XZ
??1_Winit@std@@@QAE@XZ
MSVCP60.dll
ERROR 3
ERROR 2
ERROR 1

UNKNOWN WINDOWS FUNCTIONS

IMPOSSIBILE CREARE RAW ICMP SOCKET

RAW ICMP SENDTO:

===== ICMP BACKDOOR V0.1 =====

===== CODE BY SPOOF. ENJOY YOURSELF!

YOUR PASSWORD:

LOKI

CMD.EXE

THIS SECTION APPEARS TO BE INTENDED TO BE READ. THESE STRINGS MAY BE STARTUP OR HELP MESSAGES . "ICMP BACKDOOR ." THIS MIGHT BE WHAT THE PROGRAM IS – ALL THE

OTHER STRINGS WOULD BE APPROPRIATE IF THIS IS IN FACT WHAT IT DOES, BUT WE NEED MORE INFORMATION TO CONFIRM THIS HYPOTHESIS.

```
EXIT OK!
LOCAL PARTNERS ACCESS
ERROR UNINSTALLING SERVICE
SERVICE UNINSTALLED SUCCESSFULLY
ERROR INSTALLING SERVICE
SERVICE INSTALLED SUCCESSFULLY
CREATE SERVICE %S OK!
CREATE SERVICE FAILED:%D
SERVICE STOPPED
FORCE SERVICE STOPPED FAILED%D
THE SERVICE IS RUNNING OR STARTING!
QUERY SERVICE STATUS FAILED!
OPEN SERVICE FAILED!
SERVICE %S ALREADY EXISTS
LOCAL PRINTER MANAGER SERVICE
SMSSSES.EXE
OPEN SERVICE CONTROL MANAGE FAILED:%D
START SERVICE SUCCESSFULLY!
STARTING THE SERVICE FAILED!
STARTING THE SERVICE <%S>...
SUCCESSFULLY!
FAILED!
TRY TO CHANGE THE SERVICE'S START TYPE...
THE SERVICE IS DISABLED!
QUERY SERVICE CONFIG FAILED!
MORE SERVICE MANIPULATION STRINGS, STARTING THE "SERVICE CONTROL MANAGER"
AND FOR CONTROLLING PROGRAMS.
```

QUICKVIEW PLUS IS A PROGRAM THAT PROVIDES INFORMATION ABOUT DIFFERENT FILE TYPES. EXAMINING THE BINARY IN THIS PROGRAM REVEALS THAT IT USES THE FOLLOWING WINDOWS SYSTEM DLL FILES.

```
kemel32.dll
advapi32.dll
ws2_32.dll
mfc42.dll
msvcrt.dll
msvc60.dll
```

SOME OF THESE ARE STANDARD FUNCTIONS REQUIRED FOR A WINDOWS BINARY. A BINARY CAN BE COMPILED IN TWO WAYS – STATICALLY AND DYNAMICALLY. A STATICALLY COMPILED BINARY CONTAINS ALL THE FUNCTIONS IN ITS OWN FILE THAT IT NEEDS TO EXECUTE. A DYNAMICALLY LINKED BINARY REFERS TO AND CALLS OTHER SYSTEM FILES TO USE SOME OF THEIR SERVICES. CLEARLY THIS BINARY HAS BEEN COMPILED IN A DYNAMICALLY LINKED FASHION, AS IT REQUIRES OTHER SYSTEM FILES TO FUNCTION. MSVCRT.DLL CONTAINS STANDARD C LIBRARY FUNCTIONS SUCH AS PRINTF, MEMCPY, AND COS. OTHER REFERENCES FROM THE FILE PROVIDE MORE INFORMATION. WS2_32.DLL IS THE WINSOCK DYNAMIC LINK LIBRARY. THIS CONTAINS THE WINDOWS SOCKETS API USED BY INTERNET AND NETWORK APPLICATIONS TO HANDLE NETWORK CONNECTIONS. AN API IS AN "APPLICATION PROGRAMMING INTERFACE" I.E. A SET OF STANDARDS THAT DEFINE HOW PROGRAMMERS ACCESS CERTAIN FUNCTIONS WRITTEN BY OTHER PROGRAMMERS. CLEARLY THE PROGRAM IS INTENDED TO COMMUNICATE OVER THE NETWORK.

FROM THE STRINGS LISTING

```
impossible create raw ICMP socket
RAW ICMP SendTo:
===== Icmp BackDoor V0.1 =====
===== Code by SpooF. Enjoy Yourself!
YourPassWord:
```

THE BINARY APPEARS TO BE AN ICMP BACKDOOR. THE STRING "IMPOSSIBILE CREARE RA W ICMP SOCKET" IS TRANSLATED BY GOOGLE TRANSLATION (FROM ITALIAN TO ENGLISH) AS "IMPOSSIBLE TO CREATE RA W ICMP SOCKET" (THIS WOULD TYPICALLY BE PHRASED "COULD NOT CREATE " IN AN ENGLISH PROGRAM). THIS IS CONSISTENT WITH THE ICMP HYPOTHESIS. THE PROGRAM ALSO CONTAINS VARIOUS OTHER STRINGS THAT APPEAR TO BE ERROR OR RESPONSE MESSAGES. SOME OF THE STRINGS INDICATE THAT THE PROGRAM IS STARTING OR STOPPING SERVICES, WHICH MAY MEAN THAT IT INCLUDES SOME TRICKY CONTROL OVER THE SYSTEM.

TO FURTHER ATTEMPT TO IDENTIFY WHAT THE PROGRAM DOES, IT WAS INSTALLED ON A WINDOWS MACHINE. THIS COMPUTER WAS RUNNING WINDOWS 2000 (PROFESSIONAL), AND WAS NOT PHYSICALLY CONNECTED TO ANY OTHER COMPUTERS. IT WAS RUNNING VMWARE 4.0.0 (BUILD 4460), WITH WINDOWS 2000 PROFESSIONAL INSTALLED AS THE "GUEST" OPERATING SYSTEM. FURTHER ANALYSIS OF THE BINARY WAS DONE UNDER THE VMWARE SYSTEM. THIS ALLOWED THE BINARY TO BE RUN WITHOUT FEAR OF COMPROMISING THE SYSTEM ITSELF. AFTER RUNNING THE BINARY IT WAS POSSIBLE TO EASILY RESTORE THE SYSTEM TO A KNOWN STATE BY "REVERT"ING THE VMWARE IMAGE TO ONE SAVED EARLIER. THIS ALLOWED FOR RELATIVELY FREE EXAMINATION OF THE BINARY. FIRST THE BINARY WAS RUN IN ITS DEFAULT MODE. WHEN EXECUTED, THE PROGRAM COMPLAINED ABOUT BEING UNABLE TO FIND A SYSTEM DYNAMIC LINK LIBRARY ("MSVCP60.DLL"). THIS SYSTEM BINARY WAS COPIED INTO THE VMWARE OPERATING SPACE VIA A FLOPPY DISK, AND THE UNKNOWN BINARY EXECUTED AGAIN. ONCE STARTED, THE PROGRAM PAUSED FOR 15 SECONDS, THEN RETURNED BACK TO THE OPERATING SYSTEM. IT DID NOT DISPLAY ANY ERROR MESSAGES, OR USER INFORMATION. IF RUN WITH A COMMAND LINE SWITCH (IE TARGET2.EXE /?, -I, -D ETC) THE PROGRAM IMMEDIATELY RETURNED TO THE OPERATING SYSTEM, WITHOUT PAUSING FOR THE 15 SECONDS.

PROGRAM EXECUTION

THE PROGRAM MAY EXPECT SOME PARAMETERS TO BE PASSED TO IT. THESE COULD INDICATE THE MODE THE PROGRAM SHOULD EXECUTE IN. THE PROGRAM SETS UP VARIOUS VARIABLES, AND THEN EXECUTES SOME SERVICE CONTROL FUNCTIONS. THIS SETS UP THE FUNCTIONALITY REQUIRED FOR THE PROGRAM TO CHECK TO SEE IF A CERTAIN SERVICE IS RUNNING ON THE COMPUTER. THE PROGRAM THEN MAKES SOME REGISTRY CALLS. SYSINTERNALS "REGISTRY MONITOR" SHOWS THESE REGISTRY CALLS AS BEING TO "HKLM (HKEY LOCAL MACHINE)\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon", "LeakTrack", and "Diagnostics". Calls are also made to "CurrentControlSet\Control\Error Message Instrument", "Compatibility2", and "AppInit_DLLs". These may be standard calls made from a Windows application with these included DLL files. However, calls are also made to "Microsoft\Cryptography\ RNG\Seed". These suspicious calls may indicate that the program is opening an encrypted communications channel.

FORENSIC DETAILS

SOME OF THE CALLS MADE BY THE PROGRAM RETURN FAIL RESULTS. THIS MAY INDICATE THAT THE PROGRAM NEEDS TO BE INSTALLED IN SOME FASHION BEFORE IT CAN BE RUN SUCCESSFULLY. THE PROGRAM CODE ITSELF ALSO CONTAINS CALLS TO THE PROGRAM

"\\WINNT\SYSTEM32\SMSSSES.EXE". THIS STRING FIRST OCCURS AT THE HEXADECIMAL LOCATION 60F3. UNFORTUNATELY THE DISASSEMBLER USED IN EXAMINING THIS BINARY, IDA PRO (INTERACTIVE DISASSEMBLER VERSION 4.5.0.762) WOULD ONLY DISASSEMBLE THE PROGRAM TO THE HEXADECIMAL LOCATION 5FFF. THIS MAY BE DUE TO A LIMITATION IN THE DISASSEMBLER, OR THE PROGRAM MAY CONTAIN SOME KIND OF "END OF FILE" MARKER. IT DOES CONTAIN THE HEX CODE 1A EARLY ON IN THE FILE. THIS IS THE CODE USED IN DOS FILES TO INDICATE THE END OF FILE. THE CODE IS NOT UNUSUAL IN THIS LOCATION HOWEVER, AS IT MARKS THE END OF THE "DOS-STUB", THE PORTION OF THE PROGRAM THAT EXECUTES WHEN THE PROGRAM IS RUN IN DOS (HERE IT DISPLAYS "THIS PROGRAM CANNOT BE RUN IN DOS MODE"). DUE TO IDA PRO'S FAILURE TO DISASSEMBLE THE COMPLETE BINARY, IT WAS IMPOSSIBLE TO TRACE BACK INTO THESE STRINGS TO FIND OUT WHAT THEY WERE USED FOR. IT IS POSSIBLE (ALTHOUGH UNLIKELY) THAT THEY WERE SIMPLY APPENDED TO THE END OF THE EXECUTABLE TO MAKE DISASSEMBLY MORE DIFFICULT. HOWEVER, IF THAT WAS THE AUTHOR'S INTENTION, THEN THERE WOULD BE FAR BETTER WAYS TO DO THIS E.G. PACKING THE EXECUTABLE IN AN ENCRYPTED FASHION WITH A PRODUCT SUCH AS NEOLITE!. ALTERNATIVELY IT MAY BE THAT THE COMPILER USED IS SIMPLY NOT ONE IDA PRO RECOGNISES, AND IS UNABLE TO UNDERSTAND ITS INTERNAL FORMAT. IT MAY BE THAT IDA PRO DOES NOT DISASSEMBLE THIS PORTION BY DEFAULT, AND THERE IS AN OPTION TO PERFORM A MORE COMPLETE ANALYSIS. EITHER WAY, THIS MADE UNDERSTANDING THE BINARY'S FUNCTION MORE DIFFICULT.

THE STRING REFERS TO "\\WINNT\SYSTEM32\SMSSSES.EXE". THIS PROGRAM DOES NOT APPEAR TO BE A STANDARD WINDOWS EXECUTABLE, NOR DID IT APPEAR IN ANY SEARCH ENGINE RESULTS. THIS MAY BE AN EXECUTABLE THAT THE BINARY DROPS WHEN IT IS INITIALLY INSTALLED. THE BINARY ALSO REFERENCEES "\\WINNT\SYSTEM32\REG.EXE". THIS FILE ALSO DOES NOT EXIST, BUT MAY BE INSTALLED AS PART OF THE WINDOWS RESOURCE KIT. THE DEFAULT VERSION OF THE FILE IS USED TO READ AND WRITE THE WINDOWS REGISTRY, BUT THE VERSION REFERRED TO BY THE BINARY MIGHT HAVE OTHER FUNCTIONALITY. WITHOUT THE BINARY BEING INSTALLED CORRECTLY, IT IS IMPOSSIBLE TO TELL WHAT PURPOSE AND OUTCOME THE FILES THAT THE BINARY LINKS TO MIGHT HAVE.

THE BINARY WAS EXECUTED WITH A PACKET SNIFFER RUNNING. THE COMPUTER USED TO EXECUTE THE BINARY WAS A WINDOWS 2000 MACHINE, RUNNING SERVICE PACK 2. THE COMPUTER HAD THE TCP/IP, "CLIENT FOR MICROSOFT NETWORKS", AND "FILE AND PRINTER SHARING FOR MICROSOFT NETWORKS" NETWORK PROTOCOLS INSTALLED. THE PACKET SNIFFER USED WAS ETHEREAL (0.9.2) WITH THE WINPCAP 3.0 PACKET CAPTURE LIBRARIES INSTALLED. THE NETWORK CARD USED WAS THE ASUS P4PE MOTHERBOARD ONBOARD NETWORK CARD. THE COMPUTER WAS CONNECTED BY AN ETHERNET CABLE, TO A NETGEAR EN103(TP) HUB. THIS HUB WAS ONLY CONNECTED TO THE INVESTIGATION COMPUTER.

WHEN THE BINARY WAS EXECUTED, NO NETWORK PACKETS WERE DETECTED. THE BINARY MAY BE SEARCHING FOR A LOCAL FILE THAT IS NOT INSTALLED, OR IT MAY BE ACTING IN A "LISTENER" MODE, IE ACTIVATE FOR 15 SECONDS, AND FIRE OFF A SHELL IF IT DETECTS CERTAIN INCOMING PACKET DURING THAT TIME. ALTERNATIVELY, IT MIGHT NOT INCLUDE NETWORK FUNCTIONS AT ALL, AND JUST LINK TO THE WINSOCK FILES TO CONFUSE EXAMINERS.

THE BINARY WAS THEN EXAMINED USING "PROCESS EXPLORER" FROM SYSINTERNALS. THIS

PROGRAM WAS RUN , FOLLOWED BY THE BINARY. THIS SHOWED THAT THE BINARY EXECUTED , AND THEN EXITED , WITHOUT LEAVING ANY PROGRAMS RUNNING IN MEMORY. THE "HANDLES" LISTED FOR THE BINARY WERE :

```
Process: target2.exe Pid: 632

Handle Type      Access      Name
0x14 Directory    0x00000003 \KnownDlls
0x18 File         0x00100020 C:\Documents and Settings\Administrator\Desktop\binary_v1.3
0x20 Directory    0x00F000F  \Windows
0x28 Mutant      0x00000001 \NlsCacheMutant
0x30 Key          0x00F003F  HKLM
0x38 WindowStation 0x00F037F  \Windows\WindowStations\WInSta0
0x44 WindowStation 0x00F037F  \Windows\WindowStations\WInSta0
0x48 Desktop     0x00F01FF  \Default
0x4C File         0x00100080 \Device\NamedPipe\
```

THE FINAL ENTRY HERE , "\DEVICE\NAMEDPIPE" WAS DESCRIBED BY THE PROGRAM AS "A DISK FILE , COMMUNICATIONS ENDP OINT, OR DRIVER INTERFACE " WITH 3 REFERENCES . THIS MAYBE A NETWORK LISTENER , AS NO SPECIFIC FILE WAS LISTED .

THE DLL VIEW FROM THE SAME PROGRAM SHOWED :

```
Process: target2.exe Pid: 632

Base Size MM Description Version Time Path
0x240000 0x16000 * 8/05/2001 12:00 p.m. C:\WINNT\system32\unicode.nls
0x260000 0x2F000 * 8/05/2001 12:00 p.m. C:\WINNT\system32\locale.nls
0x290000 0x41000 * 8/05/2001 12:00 p.m. C:\WINNT\system32\sortkey.nls
0x2E0000 0x4000 * 8/05/2001 12:00 p.m. C:\WINNT\system32\sorttbls.nls
0x300000 0x2000 * 8/05/2001 12:00 p.m. C:\WINNT\system32\ctype.nls
0x400000 0x6000 20/02/2003 12:45 p.m. C:\Documents and
Settings\Administrator\Desktop\binary_v1.3\target2.exe
0x6C370000 0xF2000 MFCDLL Shared Library - Retail Version 6.00.8665.0000 8/05/2001 12:00 p.m. C:\WINNT\system32\mf42.dll
0x75020000 0x8000 Windows Socket 2.0 Helper for Windows NT 5.00.2134.0001 8/05/2001 12:00 p.m. C:\WINNT\system32\ws2help.dll
0x75030000 0x13000 Windows Socket 2.0 32 -Bit DLL 5.00.2195.2780 8/05/2001 12:00 p.m. C:\WINNT\system32\ws2_32.dll
0x76080000 0x61000 Microsoft (R) C++ Runtime Library 6.00.8972.0000 23/08/2001 5:00 p.m. C:\Documents and
Settings\Administrator\Desktop\binary_v1.3\msvcp60.dll
0x77D40000 0x70000 Remote Procedure Call Runtime 5.00.2195.2832 8/05/2001 12:00 p.m. C:\WINNT\system32\rpcrt4.dll
0x77DB0000 0xB5000 Advanced Windows 32 Base API 5.00.2195.2867 8/05/2001 12:00 p.m. C:\WINNT\system32\advapi32.dll
0x77E10000 0x84000 Windows 2000 USER API Client DLL 5.00.2195.2821 8/05/2001 12:00 p.m. C:\WINNT\system32\user32.dll
0x77E80000 0xB5000 Windows NT BASE API Client DLL 5.00.2195.2778 8/05/2001 12:00 p.m. C:\WINNT\system32\kernel32.dll
0x77F40000 0x3C000 GDI Client DLL 5.00.2195.2778 8/05/2001 12:00 p.m. C:\WINNT\system32\gdi32.dll
0x77F80000 0x7B000 NTLayer DLL 5.00.2195.2779 8/05/2001 12:00 p.m. C:\WINNT\system32\ntdll.dll
0x78000000 0x46000 Microsoft (R) C Runtime Library 6.01.8924.0000 8/05/2001 12:00 p.m. C:\WINNT\system32\msvrt.dll
```

The windows socket functionality shows that the binary uses network services. There is no keyboard hook call, so the program is probably not looking for user input. The only functions seem to be standard windows functions, C functions, and socket functions, as well as possible remote procedure calls.

THERE IS NO REASON TO SUSPECT THAT THE BINARY IS ANYTHING OTHER THAN WHAT IT CLAIMS TO BE - AN ICMP BACKDOOR. THE INTERNAL FUNCTIONALITY SUPPORTS THIS HYPOTHESIS , AS DOES THE LIST OF OTHER SYSTEM DLLS THAT THE BINARY USES. THE BINARY REFERS TO "CMD.EXE". WHAT THE BINARY MAY DO IS , OPEN A REVERSE COMMAND AND SHELL , TUNNELED THROUGH ICMP PACKETS . THE TIMING FUNCTIONS IN THE BINARY AND THE SERVICE CALLS COULD POTENTIALLY ALLOW THE BINARY TO EXECUTE THE SHELL AT A KNOWN TIME , ALLOWING A REMOTE ATTACKER ACCESS TO THE SYSTEM. THE SHELL WOULD HAVE THEN BEEN OPENED FROM INSIDE THE NETWORK , AND BE RUNNING THROUGH ICMP (WHICH IS NOT TYPICALLY USED FOR TELNET TYPE COMMANDS) SO IT MAYBE ALLOWED THROUGH THE FIREWALL WHERE OTHER PROGRAMS WOULD BE BLOCKED .

THE BINARY ALSO CONTAINS A STRING (IN UNICODE) REFERRING TO "\199.107.97.191\C\$". THIS MAYBE THE SITE THAT THE BINARY TRIES TO CONNECT TO WITH THE REVERSE SHELL. THE BINARY DOES CONTAIN SOME CODE FOR OPENING FILES , SO IT MAY USE THESE FILES TO ALLOW IT TO CONNECT TO OTHER SITES , AND JUST USE THIS IP

ADDRESS AS A DEFAULT , OR A "RED HERRING . "

IT ALSO REFERS TO "YOUR PASSWORD." IT MAY BE DESIGNED TO PREVENT USE OF THE BINARY WITHOUT A CERTAIN PASSWORD . THIS STRING IS FOUND CLOSE TO THE STRING "LOKI", WHICH MAY BE THE REQUIRED PASSWORD , OR MAY SIMPLY REFER TO THE ORIGINAL PROGRAM .

LOKI IS ANOTHER ICMP BACKDOOR PROGRAM , NAMED AFTER THE NORSE GOD OF TRICKERY AND DECEPTION. THE FOLLOWING DESCRIPTION IS TAKEN FROM "PHRACK " MAGAZINEⁱⁱ .

"THE CONCEPT OF THE LOKI PROJECT IS SIMPLE: ARBITRARY INFORMATION TUNNELING IN THE DATA PORTION OF ICMP_ECHO AND ICMP_ECHOREPLY PACKETS. LOKI EXPLOITS THE COVERT CHANNEL THAT EXISTS INSIDE OF ICMP_ECHO TRAFFIC. THIS CHANNEL EXISTS BECAUSE NETWORK DEVICES DO NOT FILTER THE CONTENTS OF ICMP_ECHO TRAFFIC. THEY SIMPLY PASS THEM, DROP THEM, OR RETURN THEM. THE TROJAN PACKETS THEMSELVES ARE MASQUERADED AS COMMON ICMP_ECHO TRAFFIC. WE CAN ENCAPSULATE (TUNNEL) ANY INFORMATION WE WANT. FROM HERE ON OUT, LOKI TRAFFIC WILL REFER TO ICMP_ECHO TRAFFIC THAT TUNNELS INFORMATION. (ASTUTE READERS WILL NOTE THAT LOKI IS SIMPLY A FORM OF STEGANOGRAPHY)."

THE BINARY RUNS FOR 15 SECONDS, WITHOUT SENDING OUT ANY NETWORK DATA . IT MAY BE WAITING FOR A CERTAIN NETWORK INPUT , (A PING PACKET OR SIMILAR, PERHAPS CONTAINING THE PASSWORD) TO ACTIVATE THE REVERSE ICMP SHELL. THIS HYPOTHESIS IS UNLIKELY, AS NO LISTENING CONNECTIONS SHOW UP UNDER "NETSTAT -A". TRACING INTO THE BINARY USING IDA PRO, THE START PROCEDURE CALLS THE "MAIN" PROCEDURE . THIS SETS UP SOME VARIABLES, AND THEN CALLS THE "STARTSERVICECTRLDISPATCHER A" FUNCTION OF ADVAPI32.DLL. THIS FUNCTION THEN CALLS "WAITNAMEDPIPE W" FROM THE KERNEL32.DLL. THIS FUNCTION WAITS UNTIL A TIME-OUT OCCURS , OR THE NAMED PIPE IS AVAILABLE FOR A CONNECTION . THE BINARY IS NOT WAITING FOR A NETWORK CONNECTION , BUT RATHER A RESPONSE FROM THE LOCAL MACHINE . IT APPEARS TO TRY TO SET UP A CONNECTION TO A SERVICE , WAIT 15 SECONDS FOR THAT SERVICE TO CONNECT , AND THEN FAIL BACK TO THE OPERATING SYSTEM. THIS MAY BE DUE TO THE FACT THAT THE BINARY WAS NOT FULLY INSTALLED ON THE INVESTIGATION COMPUTER.

The IP address listed (199.107.97.191) is listed in SamSpade.org as belonging to

Azusa Pacific University
PO Box 7000
Azusa, CA 91702-7000
UNITED STATES

This program may have been written by a student at that university. In circumstances different from those in which this binary was encountered, more information could be gathered by contacting the appropriate people at that university to obtain further information about the user in control of that IP address.

Another string in the binary also identifies it as being written by "Spoof." Searching through various sites did not reveal any other code written by this author. There is also a string in the code "Hello from MFC." This may represent a cracker group, or it could refer to the Microsoft Foundation Classes. This is a group of classes used in programming that could have been included when the program was compiled. The string might simply show which compiler was used to compile the binary.

Binary footprints

This binary uses other system files. These system files are commonly used by other applications, and so their existence on the system alone should not be considered suspicious. The binary refers to the \winnt\system32\smsses.exe and \winnt\system32\reg.exe files. These files do not exist in a standard windows installation. Although their existence on a system would be suspicious, (reg.exe would not be a cause for concern if the resource kit had been installed) the binary could be modified to use files with other names or locations. As no more information about these files is available, they alone cannot be used to identify the binary.

Ultimately, the binary (in this form) can only reliably be detected through searching for a file with the md5sum 848903a92843895f3ba7fb77f02f9bf1. If the binary had been hex edited to use other executables, then this test would also fail, the MD5 being dependent on every byte in the file. Possibly a script could be constructed that would extract the first portion of the program that does not contain modifiable strings, and run an md5sum on that extracted portion, but that is outside the focus of this analysis.

Program Identification

THE SPECIFIC PROGRAM CODE FOR THIS PROGRAM WAS NOT ABLE TO BE LOCATED ON THE INTERNET. A SEARCH FOR "CODE BY SPOOF" DID NOT RETURN ANY USABLE RESULTS, USING ANY OF THE MAJOR SEARCH ENGINES (GOOGLE, ALTAVISTA, YAHOO AND INFOSEEK.) ALTHOUGH SEARCHING FOR "COMMENT-LIKE" STRINGS CAN OFTEN HAVE GOOD RESULTS, THESE STRINGS ARE ALSO VERY EASY FOR AN INEXPERIENCED PROGRAMMER TO CHANGE. THE CURRENT BINARY MAY BE A MODIFIED FORM OF ANOTHER PROGRAM THAT IS MORE AVAILABLE. A SEARCH FOR "\WINNT\SYSTEM32\SMSSSES.EXE" ALSO DID NOT YIELD ANY USEFUL RESULTS. SEARCHING FOR "\SYSTEM32\REG.EXE" RETURNED MANY RESULTS, BUT AS THIS IS A STANDARD MICROSOFT PROGRAM THIS IS NOT SURPRISING. NONE OF THE RESULTS APPEARED TO REFER TO ANY KIND OF MALICIOUS INSTALLATION OR USE. A SEARCH FOR THE ITALIAN ERROR MESSAGE "IMPOSSIBILE CREARE R AWICMP SOCKET" RETURNED A SINGLE PAGEⁱⁱⁱ. THIS CONTAINED THE CLOSEST SOURCE CODE AVAILABLE YET, ALTHOUGH NOT EXACTLY THE SAME. THIS PROGRAM USES SOME OF THE SAME SYSTEM DLL FILES, SUCH AS WS2_32.DLL, AND APPEARS TO HAVE SIMILAR FUNCTIONALITY TO THE UNKNOWN BINARY.

THIS PAGE WAS TRANSLATED BY WWW.GOOGLE.COM, AND BY WWW.T-MAIL.COM. NEITHER OF THESE GAVE THE BEST TRANSLATION IN ALL AREAS, SO A COMBINATION OF THE TWO TRANSLATIONS APPEARS BELOW. FOR READABILITY THE WHITESPACE FROM THE ORIGINAL CODE HAS BEEN MODIFIED. PORTIONS OF THE C CODE HAVE ALSO BEEN TRANSLATED, WHICH MEANS THAT THE CODE WILL NOT COMPILE AS WRITTEN. FOR EXAMPLE, A VARIABLE NAME THAT REQUIRES ONE WORD IN THE ORIGINAL ITALIAN MAY HAVE BEEN TRANSLATED AS 3 ENGLISH WORDS, SEPARATED BY SPACES. AS C DOES NOT ALLOW SPACES IN VARIABLE NAMES, THIS WILL BREAK THE COMPILATION, BUT SERVES TO GIVE MORE OF AN IDEA WHAT THE CODE IS INTENDED TO DO.

“
-----[PREVIOUS]--[INDEX]--[NEXT]-----
=====

-----[BFI NUMBER 7, YEAR 2 - 25/12/1999 - ROWS 13 OF]-----

=====
-[22 HACKING]-----

--[UNDERCOVER WORK -DASHIE EMPLOYED TIME : MANY HOURS TO READ TO THE MICRO SUX DOCUMENTATION AND 10 MINUTEREN TO WRITE THE CODE...

INGESTED FOOD: HALF LITER OF SKIFOSA GATORADE TO THE RED ORANGE TONS OF ICE CREAM 1,5 LITERS OF COKE LENGTHENED WITH THE FANTA.... WARM GOD THAT!!!

DEDICATED TO: MIKY, THE GIRL WHO HAS UPSET ME THE BENARES LIFE, ITS PUTS INTO EFFECT THEM BOY NONCHE' MY PRECIOUS FRIEND 'SPIRIT', PERCHE' ITS VACCATE SUMMERY ME FAN ALWAYS TO SQUARTARE PIGPEN, PERCHE' OTHERWISE WOULD BE FORGOTTEN ABOUT THE EXISTENCE OF UNIX THE FUSYS, IN ORDER TO HAVE ITSELF MADE TO COME WANTS TO READ ALL THE TCP/IP ILLUSTRATED MICROSOFT, GOD BIT PARDONS THEM PERCHE' DOES NOT KNOW WHAT THEY MAKE...

ECCOMI HERE! THE DARK ANNIHILATOR, THE ADAM OF THE OSCURITA ONE', THE SALVATORE OF THE RETURNED 'INFERI E!' EHEH... AFTER MONTHS OF GIOVAGARE IN PIU' THE DEEP RECESSES OF THE ABYSS THEY ARE MAGICALLY REAPPEARED CARRYING WITH ME SOMETHING OF PRETTY... AN INTERESTING CUE FOR ALL THOSE THAT WILL HAVE READ THE ARTICLE OF FUSYS ON THE ICMP TUNNELING... IN LITTLE WORDS THIS E' A BOOKCASE, EXACTLY LIKE THAT PROPOSAL FROM FUSYS, THAT IT SUPPLIES FUNCTIONS FOR THE ENCAPSULATION OF GIVE TO YOU IN PACKAGES ICMP. THE ONLY DIFFERENCE E' THAT THE AFORESAID BOOKCASE E' RED-ADAPT IN ORDER TO BE COMPILED ALSO UNDER WINSOZZZ. THE FREE WILL CONCURS TO YOU TO MAKE OF CIO' THAT YOU WANT, AND SICCOME OF CUES VE IT HAS SOME THEY GIVE GIA' FUSYS TO YOU TO SUFFICIENZA, SAID THAT E' THE CASE YOU WATCH THE CODE AND YOU TRY TO WRITE SOMETHING TO US...

ICMP_TUNNEL.H SNP

/* COVERT TUNNELING IN ICMP 0x00 ECHO REPLY MESSAGES

MANY THANKS TO FUSYS AND RICHARD STEVENS ^_^ DARK SCHNEIDER X1999 */

INCLUDES < WINSOCK2.H >

INCLUDES < WS2TCP/IP.H >

INCLUDES < STDIO.H >

DEFINE ICMP_ECHOREPLY 0

8 DEFINE ICMP_ECHO

// DEFINITION OF SOME CONSTANTS

DEFINE IP_HDR 20

DEFINE ICMP_HDR 8

DEFINE ICMP_MINLEN 8

DEFINE MAXMSG 4096

DEFINE MAXPACKET 5004

DEFINE LAST 1

DEFINE REPLY 1

DEFINE ECHO_TAG 0xF001

DEFINE ECHO_LAST 0xF002

// STRUCTURES AND VARIABLE

// LAUNCH A RIGHT PORKO LIBERATORIO D*IO... AFTER HOURS I HAVE FOUND LIKE MAKING

// TO REMOVE TO ME FROM THE BALLS THE FOTTUTA ICMP.DLL (WINSOCK CURSED)

// IP HEADER

STRUCT IP

{

 UNSIGNED CHAR HLEN:4;

 UNSIGNED CHAR VERSION:4;

 UNSIGNED CHAR TOS;

 UNSIGNED SHORT LUNGTOT;

 UNSIGNED SHORT ID;

 UNSIGNED SHORT FLAGS;

 UNSIGNED CHAR TTL;

 UNSIGNED CHAR PROTO;

 UNSIGNED SHORT CHECKSUM;

 UNSIGNED INT SOURCEIP;

 UNSIGNED INT DESTIP;

};

ICMP HEADER STRUCT ICMP

{

 TYPE BYTE;

 BYTE TAILS;

 USHORT CHECKSUM;

 USHORT ID;

 USHORT SEQ;

 ULONG GIVE TO YOU;

```

};

SOCKET SOCKFD;
U_INT ICMP_INIT = 1;
STRUCT SOCKADDR_IN CLISRC;

FUNCTION OF CHECKSUM USHORT CHECKSUM(USHORT *BUFFER, INT SIZE)
{
    UNSIGNED LONG CKSUM=0;
    WHILE(SIZE > 1)
    {
        CKSUM+=*BUFFER++;
        SIZE -=SIZEOF(USHORT);
    }
    IF(SIZE)
    {
        CKSUM += *(UCHAR*)BUFFER;
    }
    CKSUM = (CKSUM >> 16) + (CKSUM & 0XFFFF);
    CKSUM += (CKSUM >> 16);
    RETURN (USHORT)(~CKSUM);
}

//REIMPLEMENTO BCOPY AND BZERO... BUT PERCHE' CABBAGE WINDOWS
//DOES NOT MAKE AVAILABLE?
VOID BZERO(CHAR *PNT, INT DIM_PNT)
{
    MEMSET((CHAR *)&PNT, 0, DIM_PNT);
};

VOID BCOPY(CHAR *SRC, CHAR *DEST, INT DIM_SRC)
{
    MEMMOVE((CHAR *)&DEST, (CHAR *)&SRC, DIM_SRC);
};

//MICRO$OFT SUCKS
//FUNCTIONS OF MANAGEMEN T OF PACKAGES ICMP
//FANKULO TO THOSE CURSED STRONTIUMS THAT THEY ARE INVENTS ICMP.DLL
//THE UGLY BASTARDS TO YOU PIECES OF MERDA, THE COMPATIBILITA' VE IS FICCATA IT ON
//FOR THE CULO?
//MICRO$OFT SUCKS

VOID ICMP_INIT(VOID)
{
    IF(ICMP_INIT)
    {
        IF((SOCKFD = SOCKET(AF_INET, SOCK_RAW, IPPROTO_ICMP)) == INVALID_SOCKET)
        {
            FPRINTF(STDERR, "IMPOSSIBLE TO CREATE RAW ICMP SOCKET");
            EXIT(0);
        }
    }
    ICMP_INIT = 0;
};

VOID ICMP_RESET(VOID)
{
    CLOSESOCKET(SOCKFD);
    ICMP_INIT = 1;
};

INT ICMP_SEND(CHAR *SEND_MESG, SIZE_T MESGLEN, ULONG DEST_IP, INT ECHO, INT LAST)
{
    INT TALKED NONSENSE;
    STRUCT TUNNEL
    {
        STRUCT ICMP ICMP;
        UCHAR DATA[MAXMESG];
    } ICMP_PK;
    INT ICMPLEN = SIZEOF(STRUCT ICMP);
    INT PACK_DIM;
    STRUCT SOCKADDR_IN DEST;

```

```

INT DESTLEN;
IF(MESGLEN > MAXMESG) RETURN(-1);
IF(ICMP_INIT) ICMP_INIT();
DESTLEN = SIZEOF(DEST);
BZERO((CHAR *)&DEST, DESTLEN);
DEST.SIN_FAMILY = AF_INET;
DEST.SIN_ADDR.S_ADDR = DEST_IP;
PACK_DIM = MESGLEN + SIZEOF(STRUCT ICMP);
MEMSET(&ICMP_PK, 0, PACK_DIM);
ICMP_PK.ICMP.TYPE = ICMP_ECHOREPLY;
BCOPY(SEND_MESG, (CHAR *)&ICMP_PK.ICMP.DATI, MESGLEN);
ICMP_PK.ICMP.CHECKSUM = CHECKSUM((USHORT *) &ICMP_PK.ICMP, (SIZEOF(STRUCT ICMP) + MESGLEN));
IF(ECHO) ICMP_PK.ICMP.SEQ = ECHO_TAG;
IF(LAST) ICMP_PK.ICMP.SEQ = ECHO_LAST;
IF(SPAPATO = SENDTO(SOCKFD, (CHAR *)&ICMP_PK, PACK_DIM, 0, (STRUCT SOCKADDR *)&DEST, DESTLEN) < 0)
{
    PERROR("RAW ICMP SENDTO:");
    RETURN(-1);
}
ELSE IF(SPAPATO != PACK_DIM)
{
    PERROR("DIMENSIONIWRONG PACKAGE IP: RETURN(-1);");
}
RETURN(SPAPATO);
};

INT ICMP_RECV(CHAR *RCV_MESG, SIZE_T MESGLEN, INT ECHO)
{
    STRUCT RCV
    {
        STRUCT IP IP;
        STRUCT ICMP ICMP;
        CHAR DATA[MAXMESG];
    } RCV_PK;
    INT PACK_DIM;
    INT RECEIVED;
    INT IPHDRLEN;
    INT CLILEN = SIZEOF(CLISRC);
    IF(!ICMP_INIT) ICMP_INIT();
    WHILE(1)
    {
        PACK_DIM = MESGLEN + SIZEOF(STRUCT IP) + SIZEOF(STRUCT ICMP);
        MEMSET(&RCV_PK, 0, PACK_DIM);
        IF((ACCOLTO = RECVFROM(SOCKFD, (CHAR *)&RCV_PK, PACK_DIM, 0, (STRUCT SOCKADDR *)&CLISRC,
        &CLILEN)) < 0) CONTINUOUS ONES;
        IPHDRLEN = RCV_PK.IP.HLEN < < 2;
        IF(ACCOLTO < (IPHDRLEN + ICMP_MINLEN)) CONTINUOUS;
        RECEIVED -= IPHDRLEN;
        IF(!ECHO)
        {
            IF(!RCV_PK.ICMP.ID &&!RCV_PK.ICMP.CODE && RCV_PK.ICMP.TYPE == ICMP_ECHOREPLY &&
            RCV_PK.ICMP.SEQ != ECHO_TAG && RCV_PK.ICMP.SEQ != ECHO_LAST)
            BREAK;
        }
        IF(ECHO)
        {
            IF(!RCV_PK.ICMP.ID &&!RCV_PK.ICMP.CODE && RCV_PK.ICMP.TYPE == ICMP_ECHOREPLY &&
            (RCV_PK.ICMP.SEQ == ECHO_TAG || RCV_PK.ICMP.SEQ == ECHO_LAST))
            BREAK;
        }
    }
    IF(!ECHO)
    {
        RECEIVED -= ICMP_HDR;
        BCOPY((CHAR *)&RCV_PK.ICMP.DATI, RCV_MESG, RECEIVED);
        RETURN(ACCOLTO);
    }
    IF(ECHO)
    {
        IF(RCV_PK.ICMP.SEQ == ECHO_TAG)
        {
            RECEIVED -= ICMP_HDR;
            BZERO(RCV_MESG, SIZEOF(RCV_MESG));
        }
    }
}

```

```

        BCOPY((CHAR *)&RCV_PK.ICMP.DATI, RECV_MESG, RECEIVED);
        RETURN(ACCOLTO);
    }
    RETURN(-666);
}
};

```

HERE THE CODE OF THE BOOKCASE ENDS. IN ORDER TO WRITE PROGRAMS E' MOREOVER ABSOLUTELY NECESSARY TO INSERT SOME LINES OF CODE IN THE MAIN: VOID MAIN(INT ARGV, CHAR **ARGV)

```

{
WSADATA ws;
INT STATUS;
INITIALIZATION OF THE WINSOCK IF(STATUS = WSASTARTUP(0x101, &ws) != 0)
{
FPRINTF(STDERR, "IMPOSSIBLE TO INIZIALIZARE WINSOCK");
EXIT(0);
}
}

```

```

// THE TRUE CODE GOES US HERE AND JUST, BUT I MUST SAY THAT IT PASSES TO ME WANTS IT OF
// WRITING IT AFTER THE MADONNE THAT I HAVE PULLED IN ORDER TO MAKE TO TURN CODE ICMP...
CLOSING AND DEALLOCAZIONE
WSACLEANUP();
}

```

THIS E' WHICH HAD TO THE FACT THAT THE WINSOCK HAS THE NECESSITA' OF BEING INIZIALIZATE: IN PRACTICAL E' A PO' LIKE IF EYE HAD TO BE SAID TO THE SYSTEM "THAT GIVES HERE IN THEN USE THE WINSOCK AND THEREFORE IT PREPARES ALL OF THE SORT THE INTERFACES" OR ONE ROBA... I KNOW THAT NOT E' MUCH TECHNICIAN, BUT I HAVE NOT FOUND NO DEFINITION RIGOROUS OF THE PERCHE' IS NECESSARY ONE EXPLICIT DECLARATION OF INITIALIZATION... IMPERSCRUTABILI MYSTERIES OF MICIOSOFT MOTHER...

```

=====
-----[ EOF 13/22 ]-----
=====
-----[ PREVIOUS ]--[ INDEX ]--[ NEXT ]-----
..

```

THIS CODE IS NOT COMPLETE AS ORIGINALLY WRITTEN EITHER. FOR EXAMPLE, AT ONE POINT THE TRANSLATION READS "// THE TRUE CODE GOES US HERE". THIS MAY INDICATE THAT TO AVOID HAVING "SCRIPT KIDDIES" USE HIS CODE, THE AUTHOR HAS DELIBERATELY LEFT IT CRIPPLED. THIS MAY BE WHY SOME STRINGS APPEARING IN THE BINARY DO NOT APPEAR IN THIS CODE - THAT IT HAS BEEN COMBINED WITH ANOTHER PROGRAM OF SIMILAR FUNCTIONALITY. ALSO, THIS PROGRAM CODE DOES NOT USE ALL THE SAME SYSTEM DLL FILES AS THE ORIGINAL FILE. NOR DOES IT APPEAR TO READ OR WRITE WINDOWS REGISTRY SETTINGS, OR FILES FROM THE HARD DISK AS THE ORIGINAL BINARY DID. THIS MAY MEAN THAT ALTHOUGH THIS CODE HAS BEEN USED AS THE SHELL FOR THE COMMUNICATIONS CHANNEL, THE AUTHOR OF THE BINARY HAS COMBINED IT WITH CODE FOR A WINDOWS BACK DOOR PROGRAM.

THE WINDOWS SERVICE FUNCTIONALITY APPEARS TO BE QUITE SIMILAR TO A PROGRAM CALLED "HUC SERVICES TOOLS V0.4 BY LION, LION@CNHONKER.NET." THIS CODE CAN BE FOUND BY SEARCHING FOR "HSER.TXT" WITH GOOGLE. THE PAGE CONTAINING THE CODE APPEARS TO HAVE BEEN REMOVED, BUT (AS OF 06/07/03) THE GOOGLE CACHED COPY OF THE PAGE STILL EXISTS. IT MAY BE THAT THE AUTHOR OF THE BINARY HAS COMBINED FUNCTIONS FROM THESE PROGRAMS TO CREATE THE ULTIMATE BINARY. DUE TO THE NATURE OF THE COMBINATION CODE, WITH THE FULL SOURCE OF THE CURRENT BINARY BEING UNAVAILABLE, IT IS IMPOSSIBLE TO ACCURATELY DOWNLOAD AND COMPILE CODE THAT RESULTS IN THE EXACT BINARY FOUND. HOWEVER WE CAN BE REASONABLY CONFIDENT THAT WE HAVE IDENTIFIED SOURCE CODE THAT CONTAINS MUCH THE SAME FUNCTIONALITY

Legal Implications

It is impossible to determine whether or not the binary was executed on the machine it was found on. The zip file downloaded was created locally with the time and date that the download finished. This gives us no information about the time or date that the zip file or original binary were created. The zip file lists the modification time of the binary as being 12:45 on the 20th of February, 2003. The zip program used to compress the binary only stores the one time and date with the zip file. It is impossible to tell if the binary was created before that date, accessed (possibly executed) after that date, or even executed at all. The binary makes some Windows Registry calls. The Registry file from the machine on which the binary was found is unavailable. It is also impossible to tell whether the binary had been fully installed on the original system. If access to the system was available, checking whether the "\\winnt\system32\smsses.exe" file existed could give a clue as to whether the binary was fully installed, or simply copied onto the system. The binary requires such system DLLs as msvcp60.dll to run. If this file is unavailable to the binary then it prints an error message. If this file was not installed on the system that the binary was found on, then it could be assumed that the binary had not successfully executed there. What would have been helpful at this stage of the investigation would have been a full file listing (with file Modification, Creation and Access dates) from the system that the binary had been found on. With this extra information it may have been possible to determine whether, and when, the binary had been executed. With only the available information however, this is impossible to determine.

Even if the binary had been successfully installed and executed on the system, this may not necessarily be illegal. This would depend on who had control over the system. If the owner of the system chosen to download, compile and execute the binary on their own system, then clearly this would be perfectly legal. If the binary was found on a staff member's computer within a company, then this still may not be illegal. In this instance the legality would depend on the policies in place at the company. If part of the employment contract that the employee had (read and then) signed contained a clause that no unapproved software was to be used on the company systems (and the binary was unapproved) then this would breach the contract and may lead to liability for that employee. If the binary had been installed without the employee's knowledge, and it could be determined who had installed the binary, then potentially the person installing the binary could be charged with an offence. This might breach privacy legislation, or anti "hacking" laws. This would depend on the location that the compromised system was located in, as well as the location from which the binary was installed (as this may have been done remotely.) Which jurisdiction's laws would apply would depend on the circumstances of the case, as well as the particular laws in question.

INTERVIEW QUESTIONS

IF GIVEN THE OPPORTUNITY TO COMMUNICATE WITH THE PERSON ALLEGED TO HAVE

INSTALLED AND EXECUTED THE BINARY IN QUESTION, THERE ARE SEVERAL LINES OF QUESTIONING THAT COULD YIELD HELPFUL INFORMATION. THE PARTICULAR LINE CHOSEN WOULD DEPEND ON THE RESPONSES GIVEN BY THE SUSPECTED INSTALLER OF THE SOFTWARE, AS WELL AS THEIR LEVEL OF COMPUTER COMPETENCE.

APPROACH 1: TECHNICALLY NAIVE INVESTIGATOR

ASSUMING ALL THE STANDARD NAME, DATE ETC QUESTIONS HAVE BEEN ESTABLISHED. ALSO, IT WOULD PROBABLY BE WISE TO FIND A SUBTLE WAY TO READ THE SUSPECT THEIR "MIRANDA" RIGHTS, SO THAT THE RESULTS OF THE INTERVIEW COULD POTENTIALLY BE USED IN COURT.

Q0 (SETTING THE SCENE). LOOK, I WAS WONDERING IF YOU COULD HELP US OUT WITH SOMETHING. WE KNOW THAT YOU'RE GOOD WITH COMPUTERS, AND WE NEED SOME HELP. WE'VE FOUND THIS FILE ON A COMPUTER HERE, AND WE HAVE NO IDEA WHAT IT IS. I WAS JUST HOPING THAT YOU MIGHT HAVE A MINUTE TO HELP US OUT. CAN YOU GIVE US A HAND?

Q1. WELL, WE DID A [DIR\LS] ON THE COMPUTER WHERE THIS FILE IS. AND IT SHOWED US ALL THIS INFORMATION, BUT IT DOESN'T REALLY MEAN MUCH TO ME. IT SAYS THESE TIMES AND DATES AND THESE OTHER NUMBERS AND LETTERS AND STUFF. COULD YOU TALK US THROUGH WAS ALL THIS STUFFS ABOUT?

Q2. THE NAME OF THE FILE THAT WE DON'T KNOW ABOUT IS "TARGET2.EXE". DO YOU KNOW WHAT THIS MIGHT MEAN? DOES ANYTHING THERE MAKE SENSE TO YOU?

Q3. OH, OK IT'S AN EXECUTABLE FILE. WELL, WE DIDN'T KNOW THAT, SO WE OPENED IT UP AND PRINTED IT OUT IN MICROSOFT WORD. JUST QUIETLY, IT PRINTED OUT A WHOLE LOT OF RUBBISH. BUT, THERE'S ALSO SOME STUFF IN THERE THAT LOOKS LIKE IT MEAN SOMETHING, IF WE KNEW WHAT WE WERE LOOKING AT. FOR EXAMPLE, HERE IT SAYS "HELLO FROM MFC." THE ONLY MFC I KNOW OF IS THE MELBOURNE FOOTBALL CLUB, AND THEY DON'T REALLY DO COMPUTER STUFF. DO YOU HAVE ANY IDEA WHO/WHAT MFC MIGHT BE?

Q4. SOME MORE STUFF HERE GOES ON ABOUT SERVICES BEING STARTED, AND FAILURES AND STUFF. DO YOU HAVE ANY IDEA WHAT THAT MIGHT BE ABOUT?

Q5. OK, SO TOP OF YOUR HEAD, WHAT DO YOU THINK THAT THIS PROGRAM MIGHT BE DOING?

Q6. WELL, IT MIGHT BE COMMUNICATING WITH SOMEONE. THAT'S VERY HELPFUL. AND THERE'S THESE NUMBERS IN THE PRINTOUT AS WELL, 199.171 DOT SOMETHING. THEY LOOK KIND OF LIKE A TELEPHONE NUMBER TO ME. DO YOU HAVE ANY IDEA WHAT THEY MIGHT BE REFERRING TO?

Q7. THAT'S VERY USEFUL. BECAUSE WHEN WE LOOKED UP THAT IP IN THE FIREWALL LOGS, IT SEEMS THAT YOU WERE LOGGED IN AND COMMUNICATING WITH THE COMPROMISED COMPUTER THE LAST TIME THE BINARY EXECUTED. HOW DO YOU EXPLAIN THAT?

APPROACH 2: TECHNICALLY COMPETENT INVESTIGATOR

Q0 (SETTING THE SCENE). WE'VE FOUND THIS BINARY ON THE SYSTEM. WE KNOW THAT IT WAS EXECUTED AT THIS TIME. WE KNOW THAT YOU WERE LOGGED IN AT THAT TIME, AND HAD ACCESS TO INSTALL THE BINARY ON THE COMPUTER IN QUESTION. WE KNOW THAT YOU DID IT, WE JUST NEED TO KNOW HOW, SO THAT WE CAN PREVENT IT HAPPENING AGAIN. THERE WILL BE NEGATIVE REPERCUSSIONS OF THIS INCIDENT, CERTAINLY. BUT, IF YOU HELP ME UNDERSTAND HOW OUR SYSTEMS AND PROCEDURES ALLOWED IT TO HAPPEN, THEN I'LL GO TO BAT FOR YOU AND TRY TO HELP KEEP YOU OUT OF TROUBLE AS MUCH AS I CAN. OK?

Q1. HOW DID YOU GAIN THE LOGIN CREDENTIALS FOR THE COMPROMISED MACHINE?

Q2. HOW DID YOU GAIN PHYSICAL ACCESS TO THE ROOM WHERE THE COMPROMISED COMPUTER WAS LOCATED?

Q3. WHEN DID YOU INSTALL THIS SOFTWARE ON THE COMPUTER IN QUESTION?

Q4. DID YOU COMPILE THIS BINARY?

Q5. DID YOU WRITE THE SOURCE CODE?

Q6. DO YOU STILL HAVE A COPY OF THE SOURCE CODE?

Q7. WHAT COMPILER DID YOU USE?

Q8. WHAT MACHINE WAS THE PROGRAM COMPILED ON?

Q9. WHAT MACHINE WERE THE COMMUNICATIONS WITH?

Q10. WHO CONTROLS THE MACHINE THAT THE BINARY WAS COMMUNICATING WITH?

ADDITIONAL INFORMATION

POSSIBLE SOURCES FOR THE SOURCE CODE

ICMP TUNNELLING SOURCE CODE III

WINDOWS SERVICE CONTROL SOURCE CODE^{iv}

PROJECT LOKI OVERVIEW II

PROJECT LOKI SOURCE CODE^v

SAMSPADE LOOKUP ON 199.107.97.191^{vi}

GENERAL INFORMATION ON WINDOWS DLL FILES^{vii}

MORE DETAILED INFORMATION ON THE WINDOWS WINSOCK DLL FILE^{viii}

© SANS Institute 2003, Author retains full rights.

GCFA PART 2 : OPTION 1

PERFORM FORENSIC ANALYSIS ON A SYSTEM

SYNOPSIS OF CASE FACTS

DURING RESEARCH INTO A NON-RELATED TOPIC , A CO-WORKER DISCOVERED A VULNERABILITY IN A COMMONLY USED LINUX SERVICE . TO FACILITATE RESEARCH INTO THIS VULNERABILITY , A COMPUTER WAS SET UP AS A TESTING UNIT . THE SUSPECTED VULNERABILITY WAS EXPLORED ON THIS MACHINE . THE INTENTION WAS THAT HAVING GAINED ACCESS TO THE COMPUTER , THE OPPORTUNITY WOULD BE TAKEN TO EXPLORE AND GAIN FAMILIARITY WITH OTHER "HACKER " TOOLS AND TRICKS , ON A SYSTEM WITH NO OPERATIONAL REQUIREMENT . THIS POTENTIALLY COMPROMISED MACHINE PRESENTED AN IDEAL LEARNING EXPERIENCE . WHEN MY COLLEAGUE HAD FINISHED EXPLORING THE TEST SYSTEM , I TOOK THE OPPORTUNITY TO INVESTIGATE IT . DURING THE INITIAL RESEARCH , I DELIBERATELY AVOIDED COMING INTO CONTACT WITH ANYTHING BEING DONE TO THE SYSTEM , SUCH THAT WHEN COMMENCING THE INVESTIGATION INTO THE SYSTEM I HAD NO INFORMATION ABOUT THE COMPUTER OTHER THAN THE INITIAL OPERATING SYSTEM INSTALLED . FOR THE REST OF THIS INVESTIGATION IT WILL BE ASSUMED THAT NO THING IS KNOWN ABOUT THE ATTACKER OR ATTACK USED , OTHER THAN THE FACTS FOUND FROM THE COMPUTER .

DESCRIBE THE SYSTEM (S) YOU WILL BE ANALYZING

THE COMPROMISED COMPUTER WAS ACQUIRED FROM THE TEST LAB AT WORK . THE SYSTEM HAD BEEN USED FOR TESTING PURPOSES , AND CONTINUES TO BE USED FOR THAT PURPOSE . THE SYSTEM WAS INSTALLED WITH REDHAT LINUX (6.2) . IT HAD A STANDARD (DISK SMITH ELECTRONICS) NE2000 COMPATIBLE NETWORK CARD , CONNECTED TO AN ETHERNET HUB . NO INFORMATION IS AVAILABLE AS TO THE OTHER SYSTEMS THAT MAY HAVE BEEN CONNECTED TO THE HUB AT THE SAME TIME AS THE POTENTIALLY COMPROMISED SYSTEM .

HARDWARE

Case #1. Tag #1

Computer Main Processing Unit, unmarked brand. Beige

Serial #: 11XX96

Pentium (1), 133 MHz.

128 MB RAM.

ATAPI DiamondData CD-ROM (Read Only) drive. 40x.

Serial #: 9128D 3722XXXX02910 PCL 000

Seagate 1.6 GB HDD (Removed.)

Internal PCI Network Card

Internal PCI Video Card
Internal 3.5" High Density Floppy Disk Drive

15" LCD Visual Display Unit.

Keyboard, Mouse
Network Cable (1.5m)
Network Hub OfficeConnect Ethernet Hub 4C

Case #1. Tag #2

Hard Disk Drive from Suspect Computer.

Seagate ST31621A Hard Disk Drive . 1620 MB. Serial #: FJbSG9G

IMAGE MEDIA

TO OBTAIN THE IMAGE FROM THE SUSPECT SYSTEM, THE SUSPECT HARD DISK DRIVE WAS EXTRACTED FROM THE COMPUTER. A CLEAN COMPUTER WAS SET UP, AND THE HARD DISK DRIVE ZEROED OUT USING BCWIPE. THE IMAGING COMPUTER WAS POWERED DOWN, AND THEN BOOTED INTO THE BIOS. FROM THE BIOS, THE BOOT ORDER WAS CHANGED SO THAT THE FLOPPY DISK (A) WAS THE FIRST BOOT DEVICE. A SYSTEM DISK (FROM A WINDOWS 98 OPERATING SYSTEM) WAS CREATED. THIS DISK INCLUDED THE ENCASE FOR DOS EXECUTABLE (V4.13). THE IMAGING COMPUTER WAS POWERED DOWN AT THIS POINT, AND THE SUSPECT HARD DISK DRIVE INSTALLED ON THE SECONDARY IDE CHANNEL. THE COMPUTER WAS BOOTED UP WITH THE FLOPPY DISK IN THE DRIVE, TO PREVENT ANY READS OR WRITES FROM THE SUSPECT HARD DISK DRIVE. AFTER BOOTING FROM THE SYSTEM FLOPPY, ENCASE WAS EXECUTED. THE "HASH" OPTION WAS CHOSEN BEFORE IMAGING THE SUSPECT DRIVE, TO GET A RESULT TO COMPARE THE IMAGED COPY TO. THE RESULT FROM THIS OPERATION WAS SAVED TO THE FLOPPY DISK (A).

Hard disk (0) was unlocked at this point to allow the image to be written to it. The "Acquire" option was then chosen. The hard drive to be acquired was HDD (1), and HDD (0) was the chosen target drive. This imaged the suspect hard disk onto the forensic computer drive. Compression was not used when imaging, and the Hash option was not selected. Once the image acquisition had completed, an MD5 hash was taken of the image obtained, and also saved to the floppy disk. These hash values were identical, confirming the forensic integrity of the acquired image. At this stage I exited from the Encase tool, removed the floppy disk from the disk drive, and rebooted the computer into Windows for image analysis. Once in Windows, Encase for Windows was started, and a new case created. The Image files were moved into the \Program Files\Encase4 directory, so that Encase could refer to them there. Encase was started, and a new case created. The image.e01 file was added to this case, and a hash performed. This hash accorded to the hashes obtained from DOS.

As the main investigation was to be performed under Redhat (9), the images now needed to be transferred to the RedHat system. It was also helpful to create a more transportable (and less writable) copy of the image than the original. For this purpose, the original EnCase acquire files were first independently MD5 summed. This was done using the md5sum.exe executable from CygWin. The output of this command was piped to a DOS text file, using the commands

```
"DOCUME~1\ADMINI~1\DESKTOP\UTILS\MD5SUME\IMG_1_2.E01 > c:\img_1_21.md5"  
"DOCUME~1\ADMINI~1\DESKTOP\UTILS\MD5SUME\IMG_1_2.E02 > c:\img_1_22.md5"  
"DOCUME~1\ADMINI~1\DESKTOP\UTILS\MD5SUME\IMG_1_2.E03 > c:\img_1_23.md5"
```

RESPECTIVELY. THESE IMAGES WERE THEN BURNED ONTO CDS, ALONG WITH THE TEXT FILES CONTAINING THEIR MD5 SUMS. THIS ALLOWED FOR THE IMAGES TO BE COMPARED AFTER THEY WERE COPIED ONTO THE INVESTIGATION SYSTEM, BY RE-MD5 SUMMING THE COPIES ON THE HARD DRIVE, AND COMPARING THESE RESULTS WITH THE MD5 SUMS STORED ON THE CD. THIS ENSURED THAT THE DATA WAS THE SAME AS THAT FROM THE ORIGINAL HARD DISK DRIVE, AND THEREFORE ACCEPTABLE IN COURT ACCORDING TO THE "BEST EVIDENCE" RULE. AT THIS POINT THE FILES WERE COMBINED, USING "cat img_1_2.e01 > COMPLETEIMAGE.IMG" ETC. THIS DONE, I ATTEMPTED TO MOUNT THE IMAGE USING THE LOOPBACK DEVICE. THIS ATTEMPT FAILED, AS THE IMAGE HAD BEEN OBTAINED FROM A DISK, RATHER THAN A SPECIFIC PARTITION. TO FIND THE START OF THE EXT 2 PARTITION ON THE DRIVE, THE IMAGE FILE WAS OPENED IN A HEX EDITOR. THIS WAS USED TO SEARCH FOR "LOST+FOUND", BEING AN EARLY ENTRY ON THE DRIVE. THIS FOUND, THE HEXIDECIMAL VALUE "53 EF" (THIS IS THE "MAGIC" NUMBER USED TO IDENTIFY THE FILE SYSTEM TYPE, AND THE BYTES ARE REVERSED FOR INTEL BIG-ENDIAN COMPUTERS) WAS SEARCHED FOR IN REVERSE. (HEX) 438 WAS SUBTRACTED FROM THIS NUMBER TO FIND THE START OF THE PARTITION. THIS VALUE WAS THEN USED IN THE MOUNT COMMAND, WITH "mount -offset 345381". THIS ALSO FAILED. FURTHER RESEARCH ON THIS FAILURE SHOWED THAT ENCASE USES A PROPRIETARY IMAGE FORMAT, RATHER THAN A FLAT /RAW IMAGE FORMAT. THE ENCASE IMAGE FORMAT IS INCOMPATIBLE WITH UNIX UTILITIES. THEREFORE, A "RAWER" DD IMAGE WAS REQUIRED.

ACCORDINGLY, THE SUSPECT HARD DISK WAS INSTALLED IN THE SECOND DRIVE BAY IN THE FORENSIC COMPUTER. WINDOWS TENDS TO WRITE TO DRIVES THAT IT DETECTS, SO THE IMAGE WAS NECESSARILY TAKEN THROUGH DOS. A BOOT FLOPPY DISK WOULD HAVE BEEN ANOTHER OPTION, ALTHOUGH A DOS VERSION OF THE DD TOOL COULD NOT BE LOCATED AT THE TIME OF ACQUISITION. THEREFORE THE IMAGE HAD TO BE TAKEN FROM LINUX. THE INVESTIGATIVE DRIVE WAS INSTALLED IN THE FIRST DRIVE BAY. THE COMPUTER WAS BOOTED INTO LINUX. THE SECOND IDE DRIVE APPEARED UNDER LINUX AS "HDC" AS IT WAS THE MASTER DRIVE ON THE SECONDARY IDE CONTROLLER. A DD IMAGE OF THE DRIVE WAS TAKEN, USING THE COMMAND

```
"dd if=/dev/hdc of=image.dd ibs=1 conv=no trunc,noerror".
```

This image was verified using by a comparison of "md5sum /dev/hdc" and "md5sum image.dd". The md5 sums also matched those obtained through the EnCase tool.

```
[root@localhost root]# md5sum /dev/hdc  
172e559fa3ccd2835dcf267f74ca7d2f /dev/hdc  
[root@localhost root]# dd if=/dev/hdc of=RH_1_2.dd ibs=1 conv=no trunc,noerror  
1623690240+0 records in  
3171270+0 records out  
[root@localhost root]# md5sum RH_1_2.dd
```

172e559fa3cod2835dcf267f74ca7d2f RH_1_2.dd

Although the dd image was made using the "root" user, it was then copied into the directory of the user "michael" for a analysis. This properties of this image were altered using "chmod 604 RH_1_2.dd" to ensure that anyone (specifically "michael") could read this file. The resulting properties allowed only root to read and write the file, and anyone to read the file. Although it might be a cause for concern on a multi-user system, on the standalone forensic system there was no risk in a world readable file containing this kind of information. User "michael" had no permission to write to this file, as it was owned by root. We could therefore be certain that none of the unix tools (as long as they were executed from the "michael" user account) would modify the data. At any stage an md5sum could be taken of the image to verify this, but the only one taken in this instance was as the final step of the analysis to prove that none of the tools had changed anything.

A slice of the file then needed to be copied out in order to mount the file, or examine it under Autopsy. To gather the partition information the command "sbin/fdisk -lu" (List details, output information in sectors) was used.

```
[MICHAEL@LOCALHOST MORGUE]$ /sbin/fdisk -lu RH_1_2.dd
YOU MUST SET CYLINDERS.
YOU CAN DO THIS FROM THE EXTRA FUNCTIONS MENU.
```

```
DISK RH_1_2.DD: 0 MB, 0 BYTES
64 HEADS, 63 SECTORS/TRACK, 0 CYLINDERS, TOTAL 0 SECTORS
UNITS = SECTORS OF 1 * 512 = 512 BYTES
```

```
DEVICE BOOT START END BLOCKS ID SYSTEM
RH_1_2.DD1 * 63 3072383 1536160+ 83 LINUX
RH_1_2.DD2 3072384 3169151 48384 5 EXTENDED
RH_1_2.DD5 3072447 3169151 48352+ 82 LINUX SWAP
YOU MUST SET CYLINDERS.
YOU CAN DO THIS FROM THE EXTRA FUNCTIONS MENU.
```

To extract the necessary section, dd was used. The start sector was sector 63 (being the first of the main Linux Partition), and the stop sector 3072383. Subtracting the start sector (63) from the stop sector (3072383) gives the number of sectors to copy (3072320).

```
[michael@localhost morgue]$ dd if=RH_1_2.dd of=RH_Partition_1.dd ibs=512 skip=63 count=3072320
3072320+0 records in
3072320+0 records out
```

This command left the RH_Partition_1.dd file containing only the valid ext2 partition, and therefore examinable under Autopsy. An md5sum of this new file was taken using the command "md5sum RH_Partition_1.dd > RH_Partition_1.md5". This md5 sum was also saved to a floppy disk to later compare with the file, ensuring that it had not been modified by any of the tools used. The file containing the single linux partition was then mounted for examination. This used the command

```
"mount -t ext2 -o ro,loop,noexec,noatime /home/michael/temp/morgue/RH_Partition_1.dd /mnt/hack/root:"
```

This mounts the specified file (RH_Partition_1.dd) onto the directory listed (/mnt/hack/root). It treats it as being of the file system (" -t" is specify file system type) "ext2" - being the standard linux file system. This means that the file structure contained in the file can be examined, and treated like a live file system. The other options to the command, (specified with " -o), are Read Only ("ro"), mount using the LoopBack device ("loop" - this means treating a local file as an external file -system),

do not allow any files from the file to be executed (“noexec”), and do not update the access times of any of the files when they are displayed (“noatime”). This ensures that the file will not be changed by an investigator exploring and running commands on the mounted file-system.

MEDIA ANALYSIS OF SYSTEM

THE FIRST STEP TO EXAMINING THE SYSTEM WAS TO MAKE SURE THAT NONE OF THE SYSTEM BINARIES HAD BEEN MODIFIED. THIS WAS NOT TO EXECUTE THEM, AS OF COURSE ALL TOOLS WERE USING KNOWN GOOD COPIED FROM A CD. HOWEVER, IF THE /BIN/LOGIN OR SIMILAR FILE HAD BEEN MODIFIED ON THE SYSTEM, THEN THIS WOULD BE EXTREMELY SUSPICIOUS. CHECKING THE SYSTEM FILES WAS MADE EASIER BY THE OPERATING SYSTEM INVESTIGATED BEING REDHAT LINUX (6.2). THIS OPERATING SYSTEM USES THE RPM (OR REDHAT PACKAGE MANAGER) THAT INSTALLS PRECOMPILED EXECUTABLE FILES. ACCORDINGLY AN INVESTIGATOR CAN USE MD5 HASHES FROM A SYSTEM KNOWN TO BE FREE FROM COMPROMISE TO COMPARE WITH THE SUSPECT SYSTEM. THIS WOULD NOT BE THE CASE WHERE THE OPEN SOURCE SYSTEM HAD COMPILED THE EXECUTABLES ON THE MACHINE IN QUESTION, AS EACH DIFFERING COMPILATION WOULD HAVE DIFFERING MD5 HASHES.

TO COMPARE THE SYSTEM BINARIES, A LIST OF KNOWN GOOD MD5 HASHES WAS DOWNLOADED FROM KNOWNGOODS^{ix}. THIS FILE, LINUX-REDHAT-6.2-1386.TXT WAS LISTED AS HAVING THE MD5 HASH OF 5450D78784364D0B1A66476A5B2E81E7. THIS WAS COMPARED WITH THE MD5 SUM OF THE FILE ONCE COPIED ONTO THE INVESTIGATION MACHINE, AND FOUND TO BE IDENTICAL. POTENTIALLY A HACKER COULD HAVE COMPROMISED THE KNOWNGOODS.ORG WEBSITE, AND UPDATED BOTH THE FILE AND THE MD5-SUM LISTED, BUT WE HAVE NO INFORMATION TO THIS EFFECT. A TOOL TO COMPARE FILES WITH THEIR EXPECTED HASHES, "KG-REPORT-0.1.1" WAS THEN DOWNLOADED AND INSTALLED ONTO THE INVESTIGATION MACHINE. THE ONLY REQUIRED FILE FROM THIS TOOL WAS THE SCRIPT "CHECK-FILES.SH". THIS IS A SHELL SCRIPT THAT GOES THROUGH A SPECIFIED DIRECTORY (HERE THE MOUNTED VERSION OF THE DD COPY OF THE PARTITION FROM THE SUSPECT DRIVE) AND COMPARES THE MD5 RESULTS WITH THOSE FROM A SPECIFIED FILE. THE SCRIPT WAS FIRST VIEWED IN EMACS TO ENSURE THAT THERE WOULD BE NO UNEXPECTED FUNCTIONALITY, AND ALSO TO DISCOVER THE EXPECTED SYNTAX.

```
BEGIN SCRIPT"
#!/BIN/SH
# CHECKFILES.SH - CHECKS FOR MODIFIED FILES AND DISPLAYS A STATUS REPORT.
#
# COPYRIGHT (C) 2002 ANDREAS HOCHSTEGER <E9625392@STUDENT.TUWIEN.AC.AT>
#
# THIS PROGRAM IS FREE SOFTWARE; YOU CAN REDISTRIBUTE IT AND/OR MODIFY
# IT UNDER THE TERMS OF THE GNU GENERAL PUBLIC LICENSE AS PUBLISHED BY
# THE FREE SOFTWARE FOUNDATION; EITHER VERSION 2 OF THE LICENSE, OR
# (AT YOUR OPTION) ANY LATER VERSION.
#
# THIS PROGRAM IS DISTRIBUTED IN THE HOPE THAT IT WILL BE USEFUL,
# BUT WITHOUT ANY WARRANTY; WITHOUT EVEN THE IMPLIED WARRANTY OF
# MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SEE THE
# GNU GENERAL PUBLIC LICENSE FOR MORE DETAILS.
#
# YOU SHOULD HAVE RECEIVED A COPY OF THE GNU GENERAL PUBLIC LICENSE
# ALONG WITH THIS PROGRAM; IF NOT, WRITE TO THE FREE SOFTWARE
# FOUNDATION, INC., 675 MASS AVE, CAMBRIDGE, MA 02139, USA.
```

```

IF [ "$#" -lt "1" -o "$#" -gt "2" ]; THEN
    ECHO "USAGE: $0 REFERENCE [PATH]"
    ECHO " REFERENCE IS A FILE WITH CHECKSUMS FROM HTTP://WWW.KNOWNGOODS.ORG/"
    ECHO " PATH IS THE PATH YOU WANT TO CHECK"
    EXIT 1
FI

FOR LIN `CAT $1 | GREP ",$2"; DO
    F=`ECHO "$L" | AWK -F ',' '{PRINT $2}'`
    MD5REF=`ECHO "$L" | AWK -F ',' '{PRINT $3}'`
    ECHO -N "$F"
    IF [-E $F]; THEN
        MD5=`MD5SUM $F | AWK '{PRINT $1}'`
        IF [ "$MD5REF" == "$MD5" ]; THEN
            STAT="OK (MD5:$MD5)";
        ELSE
            STAT="ERROR (MD5:$MD5, MD5REF:$MD5REF)";
        FI
    ELSE
        STAT="MISSING"
    FI
    ECHO " $STAT";
DONE

EXIT 0
"

```

THIS SCRIPT WAS EXECUTED WITH THE COMMAND `./CHECK-FILES.SH ./LINUX-REDHAT-6.2-386.TXT /mnt/hack/root`. THIS SCRIPT RETURNED NO RESULTS. THE SCRIPT WAS THEN RUN USING THE COMMAND `./CHECK-FILES.SH ./LINUX-REDHAT-6.2-386.TXT /` TO ENSURE THAT IT WAS ACTUALLY RETURNING VALID RESULTS. THIS RETURNED PAGES OF RESULTS, AS THE INVESTIGATIVE SYSTEM IS RUNNING REDHAT 9. AFTER THIS RESULT, WE KNOW THAT NONE OF THE STANDARD SYSTEM BINARIES HAD BEEN MODIFIED SINCE INSTALLATION.

IN ORDER TO CHECK THE SYSTEM FOR SETUID OR SETGID FILES, A FIND COMMAND WAS USED. THIS WAS TOLD TO LOOK FOR EITHER FILES WITH THE SETUID BIT SET (4000), OR THE SETGID BIT SET (2000). FIND WAS INSTRUCTED ONLY TO RETURN FILES OF TYPE "REGULAR FILE" TO AVOID DIRECTORIES OR LINKS ETC. THE -LS OPTION OUTPUTS THE RESULTS IN LS -DLS FORMAT.

```

[root@localhost hack]# find /mnt/hack/root/ \( -perm -004000 -o -perm -002000 \) -type f -ls
65098 16 -rwxr-sr-x 1 root mail 15280 Feb 22 2000 /mnt/hack/root/usr/lib/emacs/20.5/i386-redhat-linux-gnu/movemail
144505 36 -rwsr-xr-x 1 root root 35168 Feb 17 2000 /mnt/hack/root/usr/bin/chage
144512 36 -rwsr-xr-x 1 root root 36756 Feb 17 2000 /mnt/hack/root/usr/bin/gpasswd
144543 8 -r-xr-sr-x 1 root tty 6128 Mar 7 2000 /mnt/hack/root/usr/bin/wall
144676 36 -rwsr-xr-x 1 root root 33288 Mar 2 2000 /mnt/hack/root/usr/bin/at
144973 76 -r-xr-sr-x 1 news news 73144 Mar 3 2000 /mnt/hack/root/usr/bin/inews
145052 44 -r-sr-x-- 1 root news 43132 Mar 3 2000 /mnt/hack/root/usr/bin/inndstart
145077 92 -r-sr-x-- 1 uucp news 89792 Mar 3 2000 /mnt/hack/root/usr/bin/mews
145089 40 -r-sr-x-- 1 root news 40540 Mar 3 2000 /mnt/hack/root/usr/bin/startinnfeed
145245 524 -rws--x-x 2 root root 531516 Feb 3 2000 /mnt/hack/root/usr/bin/suidperl
145245 524 -rws--x-x 2 root root 531516 Feb 3 2000 /mnt/hack/root/usr/bin/sperl5.00503
145256 20 -r-sr-sf-x 1 root lp 16872 Feb 15 2000 /mnt/hack/root/usr/bin/lpq
145257 20 -r-sr-sf-x 1 root lp 18568 Feb 15 2000 /mnt/hack/root/usr/bin/lpr
145258 20 -r-sr-sf-x 1 root lp 17208 Feb 15 2000 /mnt/hack/root/usr/bin/lprm
145274 36 -rwxr-sr-x 1 root man 36192 Mar 1 2000 /mnt/hack/root/usr/bin/man
145312 172 -rwxr-sr-x 1 root uucp 168080 Mar 8 2000 /mnt/hack/root/usr/bin/minicpm
145369 48 -rwsr-xr-x 1 root root 46600 Feb 4 2000 /mnt/hack/root/usr/bin/nwsfind
145459 12 -r-s--x-x 1 root root 12244 Feb 8 2000 /mnt/hack/root/usr/bin/passwd
145508 12 -rwxr-sr-x 1 root mail 11620 Feb 8 2000 /mnt/hack/root/usr/bin/lockfile
145510 80 -rwsr-sr-x 1 root mail 76432 Feb 8 2000 /mnt/hack/root/usr/bin/procmail
145560 16 -rwsr-xr-x 1 root root 14352 Mar 7 2000 /mnt/hack/root/usr/bin/rcp
145562 12 -rwsr-xr-x 1 root root 10256 Mar 7 2000 /mnt/hack/root/usr/bin/rlogin
145563 8 -rwsr-xr-x 1 root root 7436 Mar 7 2000 /mnt/hack/root/usr/bin/rsh
145634 24 -rwxr-sr-x 1 root slocate 24272 Feb 4 2000 /mnt/hack/root/usr/bin/slocate
145730 16 -rws--x-x 1 root root 14056 Mar 7 2000 /mnt/hack/root/usr/bin/chfn

```

```

145731 16 -rws--x--x 1 root root 13832 Mar 7 2000 /mnt/hack/root/usr/bin/chsh
145748 8 -rws--x--x 1 root root 5640 Mar 7 2000 /mnt/hack/root/usr/bin/newgrp
145759 12 -rwxr-sr-x 1 root tty 8328 Mar 7 2000 /mnt/hack/root/usr/bin/write
145787 132 -r-sr-sr-x 1 uucp uucp 127924 Mar 7 2000 /mnt/hack/root/usr/bin/cu
145788 96 -r-sr-xr-x 1 uucp uucp 92852 Mar 7 2000 /mnt/hack/root/usr/bin/uucp
145790 40 -r-sr-sr-x 1 uucp uucp 39364 Mar 7 2000 /mnt/hack/root/usr/bin/uuname
145792 104 -r-sr-xr-x 1 uucp uucp 101024 Mar 7 2000 /mnt/hack/root/usr/bin/uustat
145794 96 -r-sr-xr-x 1 uucp uucp 93920 Mar 7 2000 /mnt/hack/root/usr/bin/uux
145804 24 -rwsr-xr-x 1 root root 21816 Feb 4 2000 /mnt/hack/root/usr/bin/crontab
17020 8 -rwsr-xr-x 1 root root 5896 Mar 9 2000 /mnt/hack/root/usr/sbin/usernetctl
17826 28 -rwxr-sr-x 1 root lp 25064 Feb 15 2000 /mnt/hack/root/usr/sbin/lpc
18227 320 -rwsr-sr-x 1 root root 320516 Feb 18 2000 /mnt/hack/root/usr/sbin/sendmail
18256 20 -rwsr-xr-x 1 root bin 16488 Feb 8 2000 /mnt/hack/root/usr/sbin/traceroute
18294 8 -rwxr-sr-x 1 root utmp 6096 Feb 25 2000 /mnt/hack/root/usr/sbin/utempter
18319 224 -r-sr-sr-x 1 uucp uucp 225008 Mar 7 2000 /mnt/hack/root/usr/sbin/uucico
18322 108 -r-sr-sr-x 1 uucp uucp 103164 Mar 7 2000 /mnt/hack/root/usr/sbin/uuxqt
64144 36 -rwsr-xr-x 1 root root 34751 Mar 1 2000 /mnt/hack/root/usr/libexec/pt_chown
145001 16 -rwsr-xr-x 1 root root 14188 Mar 8 2000 /mnt/hack/root/bin/su
145142 20 -rwsr-xr-x 1 root root 17968 Mar 7 2000 /mnt/hack/root/bin/ping
145325 60 -rwsr-xr-x 1 root root 56208 Feb 4 2000 /mnt/hack/root/bin/mount
145326 28 -rwsr-xr-x 1 root root 26608 Feb 4 2000 /mnt/hack/root/bin/umount
112774 48 -rwsr-sr-x 1 root tty 45388 Mar 3 2000 /mnt/hack/root/sbin/dump
112776 72 -rwsr-sr-x 1 root tty 67788 Mar 3 2000 /mnt/hack/root/sbin/restore
113164 4 -rwxr-sr-x 1 root root 3860 Mar 9 2000 /mnt/hack/root/sbin/netreport
113170 28 -r-sr-xr-x 1 root root 26126 Feb 6 2000 /mnt/hack/root/sbin/pwdb_chkpwd
113171 28 -r-sr-xr-x 1 root root 27114 Feb 6 2000 /mnt/hack/root/sbin/unix_chkpwd

```

ALTHOUGH SOME OF THESE FILES LOOK SUSPICIOUS, AND DID NOT RETURN A MAN PAGE ON THE INVESTIGATION MACHINE, THEY WERE ALL SIMPLY FROM THE EARLIER VERSION OF REDHAT. NONE OF THESE BINARIES IS UNUSUAL FOR A REDHAT 6.2 INSTALLATION.

THE USER LIST COULD ALSO CONTAIN SIGNS OF AN INTRUSION. THIS IS CONTAINED IN "/etc/passwd." MALICIOUS INTRUDERS APPARENTLY OFTEN LEAVE THEMSELVES ACCESS PRIVILEGES ON COMPROMISED MACHINES, SO THAT THEY CAN GET BACK INTO THOSE MACHINES. THE PASSWD FILE WAS OBTAINED WITH THE COMMAND "cat /mnt/hack/root/etc/passwd".

```

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody/
xfs:x:43:43:X Font Server:/etc/X11/fs/bin/false
named:x:25:25:Named:/var/named:/bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql/bin/bash
wayne:x:500:500:wayne:/home/wayne:/bin/bash
wroot:x:0:0:/root:/bin/bash
wruser:666:666:/root:/bin/bash
wruser:x:666:666:/root:/bin/bash

```

Most of the users are as expected, until we get down to wroot. This user has a User Identifier (uid) of 0. The operating system uses the uid to control user access, to files and folders etc. UID 0 is that of root, which has full access to the system. A user having a uid of 0 is an extremely bad sign. Another curious sign is that the "wruser" has two entries in the passwd file. The entries only differ by an "x" in the second

field. This "x" is used to indicate that the users password is stored in the "shadow" file. A user not having a shadowed password would be bad enough, but a double -up in the passwd file clearly shows us that something is amiss.

The system was next examined for unusual directory entries. A common trick is to create a directory containing malicious code, and to name this directory starting with a full stop ("."). This is the character Unix uses to define hidden directories, and if a directory starts with this character it will not be displayed using a default "ls" command. It can still be displayed by "ls -a", or using the "find" command. To find any hidden directories, the 'find /mnt/hack/root/ -name ".*"' command was used. This command was run as an "su" to root, to prevent access error messages.

```
[MICHAEL@LOCALHOST ROOT]$ SU
PASSWORD:
[ROOT@LOCALHOST ROOT]# FIND /MNT/HACK/ROOT/ -NAME ".*"
/MNT/HACK/ROOT/VAR/LIB/NEWS/NEWS.DAILY
/MNT/HACK/ROOT/VAR/SPOOL/AT/SEQ
/MNT/HACK/ROOT/TMP/FONT-UNIX
/MNT/HACK/ROOT/TMP/...
/MNT/HACK/ROOT/TMP/.../LRK4/PROCPS-1.01/PROC.DEPEND
/MNT/HACK/ROOT/USR/DOC/BIND-8.2.2_P5/BOG/CVSIGNORE
/MNT/HACK/ROOT/USR/DOC/PM/MAKE-2.1.34/TESTS/PURIFY
/MNT/HACK/ROOT/USR/DOC/SAMBA-2.0.6/DOCS/YOYDLDOCS/CVSIGNORE
/MNT/HACK/ROOT/USR/DOC/UCD-SNMP-4.1.1/LOCAL/CVSIGNORE
/MNT/HACK/ROOT/USR/LIB/PERL5/5.00503/1386-LINUX/PACKLIST
/MNT/HACK/ROOT/USR/LIB/PERL5/SITE_PERL/5.005/1386-LINUX/AUTO/MD5/PACKLIST
/MNT/HACK/ROOT/USR/LIB/PERL5/SITE_PERL/5.005/1386-LINUX/AUTO/MOD_PERL/PACKLIST
/MNT/HACK/ROOT/USR/LIB/LINUXCONF/INSTALL/GNOME/DIRECTORY
/MNT/HACK/ROOT/USR/LIB/LINUXCONF/INSTALL/GNOME/ORDER
/MNT/HACK/ROOT/USR/MAN/MAN1/..1.GZ
/MNT/HACK/ROOT/USR/BIN/GITACTION
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.AIXTERM
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.COMMON
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.HFT
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.HPTERM
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.HP
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.IRIS-ANSI-NET
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.ANSI
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.IRIS-ANSI
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.LINUX
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.CONSOLE
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.MACH
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.MINIX
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.SUN-CMD
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.ETERM
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.GENERIC
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.PC3
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.SUN
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.THX
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.VT102
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.VT420
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.SCREEN
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.VT100
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.VT125
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.VT200
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.VT201
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.VT220
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.VT240
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.VT300
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.VT320
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.VT400
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.XTERM-DEBIAN
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.DTTERM
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.RXVT
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.XTERM-COLOR
/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.XTERMS
```

```

/MNT/HACK/ROOT/USR/SHARE/GIT/GITRC.XTERM
/MNT/HACK/ROOT/ETC/PWD.LOCK
/MNT/HACK/ROOT/ETC/SKEL/EMACS
/MNT/HACK/ROOT/ETC/SKEL/BASH_LOGOUT
/MNT/HACK/ROOT/ETC/SKEL/BASH_PROFILE
/MNT/HACK/ROOT/ETC/SKEL/BASHRC
/MNT/HACK/ROOT/ETC/SKEL/SCREENRC
/MNT/HACK/ROOT/HOME/WAYNE/EMACS
/MNT/HACK/ROOT/HOME/WAYNE/BASH_LOGOUT
/MNT/HACK/ROOT/HOME/WAYNE/BASH_PROFILE
/MNT/HACK/ROOT/HOME/WAYNE/BASHRC
/MNT/HACK/ROOT/HOME/WAYNE/SCREENRC
/MNT/HACK/ROOT/HOME/WAYNE/BASH_HISTORY
/MNT/HACK/ROOT/LIB/MODULES/2.2.14-5.0/RHKMNTAG
/MNT/HACK/ROOT/ROOT/XDEFAULTS
/MNT/HACK/ROOT/ROOT/BASH_LOGOUT
/MNT/HACK/ROOT/ROOT/BASH_PROFILE
/MNT/HACK/ROOT/ROOT/BASHRC
/MNT/HACK/ROOT/ROOT/CSHRC
/MNT/HACK/ROOT/ROOT/TCSHRC
/MNT/HACK/ROOT/ROOT/BASH_HISTORY
[ROOT@LOCALHOST ROOT]#

```

THE EARLY "GIT" ENTRIES LOOKED SUSPICIOUS, BUT ARE IN FACT THE "GNU INTERACTIVE TOOLS" AND PERFECTLY LEGITIMATE. ANOTHER POSSIBLY SUSPECT ENTRY IS "SKEL" BUT THIS ALSO IS A STANDARD FILESET. THE DIRECTORY THAT IS NOT SO BENIGN IS THE "/TMP/..." DIRECTORY. THIS DIRECTORY NAME DOES NOT OCCUR IN ANY STANDARD LINUX INSTALLATION, BUT IS COMMONLY USED TO HIDE FILES BY AN INTRUDER. THE "/TMP" DIRECTORY CONTAINS THE FOLLOWING.

```

[ROOT@LOCALHOST TMP]# LS -AL
TOTAL 148
DRwxRwxrwt 6 root root 4096 Jul 5 19:43.
DRwxr-xr-x 17 root root 4096 Jul 5 15:21 ..
DRwxr-xr-x 7 30 root 4096 Jul 5 19:31 ...
DRwxr-xr-x 2 root root 4096 Jul 3 14:18 FAKEIDENTD-1.2
DRwxRwxrwt 2 xfs xfs 4096 Jul 5 14:04 .FONT-UNIX
-rw----- 1 root root 456 Jul 2 14:09 FSTAB.OFC7U8
-rw-r--r-- 1 root root 24 Jul 5 12:20 IDENTDV
-rw-r--r-- 1 root root 63 Jul 5 17:27 IDENTDV
-rw-r--r-- 1 root root 5659 Jul 3 01:59 INSTALL.LOG
-rw-r--r-- 1 root root 95547 Jul 2 17:12 LAME1
DR-xr-xr-x 5 root root 4096 Jul 5 15:24 LINUX_x86
-rw-r--r-- 1 root root 2239 Jul 2 14:12 UPGRADE.LOG
[ROOT@LOCALHOST TMP]#

```

FAKE IDENTD IS A STANDARD INSTALLATION OF THE FAKE IDENT SERVICE. ".FONT-UNIX" CONTAINS ONLY A SINGLE SYMBOLIC LINK. THE "LINUX_x86" DIRECTORY CONTAINS THE INSTALL FILES FOR "TRIPWIRE FOR SERVERS VERSION 3.0 FOR UNIX OPERATING SYSTEMS." THE "LAME1" FILE CONTAINS THE FOLLOWING.

```

[ROOT@LOCALHOST TMP]# HEAD -10 LAME1
15.51:08.116009 ETH0 < 192.168.210.7.32837 > 192.168.210.6.AUTH: S 4232921198:4232921198(0)WIN 5840 <MSS
1460,SACKOK,TIMESTAMP 432968 0,NOP,WSCALE 0>
(D F)
  4500 003C DB26 4000 4006 3A 36 C0A8 D207
  C0A8 D206 8045 0071 FC4D 406E 0000 0000
  A002 16D0 B316 0000 0204 05B4 0402 080A
  0006 9B48 0000 0000 0103 0300
15.51:08.116154 ETH0 > 192.168.210.6.AUTH > 192.168.210.7.32837: S 4232627424:4232627424(0)ACK
4232921199 WIN 32120 <MSS 1460,SACK OK,TIMESTAMP 431310
432968,NOP,WSCALE 0> (DF)
  4500 003C 0963 4000 4006 0BFA C0A8 D206
  C0A8 D207 0071 8045 FC48 C4E0 FC4D 406F
  A012 7D78 F65E 0000 0204 05B4 0402 080A
  0006 94CE 0006 9B48 0103 0300

[ROOT@LOCALHOST TMP]# TAIL -10 LAME1
5004 0000 D65B 0000

```

```

15:51:11.006448 ETH0 < 192.168.210.7.32840 > 192.168.210.6.AUTH: F 31:31(0) ACK 33 WIN 5840
<NOP,NOP,TIMESTAMP 433258 431597> (DF)
    4500 0034 EE4C 4000 4006 2718 C0A8 D207
    C0A8 D206 8048 0071 FC51 724E FC7C 36EF
    8011 16D0 E562 0000 0101 080A 0006 9C6A
    0006 95ED
15:51:11.006614 ETH0 > 192.168.210.6.AUTH > 192.168.210.7.32840:R 4235998959:4235998959(0) WIN 0
    4500 0028 09FE 0000 FF06 8C72 C0A8 D206
    C0A8 D207 0071 8048 FC7C 36EF 0000 0000
    5004 0000 D65B 0000
[ROOT@LOCALHOST TMP]#

```

THIS APPEARS TO BE A 3 SECOND PACKET TRACE FILE. THE IP ADDRESSES USED ARE NON-ROUTABLE, BUT MAY REFER TO THE LOCAL MACHINE WHICH WAS NOT CONNECTED TO THE INTERNET. TO CHECK THIS, THE NIC CONFIGURATION FILE WAS CHECKED.

```

[ROOT@LOCALHOST NETWORK-SCRIPTS]# cd /mnt/hack/root/etc/sysconfig/network-scripts
[ROOT@LOCALHOST NETWORK-SCRIPTS]# cat ifcfg-eth0
DEVICE=eth0
BOOTPROTO=static
IPADDR=192.168.210.6
NETMASK=255.255.255.0
GATEWAY=192.168.210.33
[ROOT@LOCALHOST NETWORK-SCRIPTS]#

```

This shows that the local address was in fact 192.168.210.6, which was referenced in the "lame1" file. All of the packets contained in the "lame1" file were between 192.168.210.6 and 192.168.210.7. Is it therefore likely that a sniffer of some sort was running, either on this system or the machine at the far end of the connections.

NB: In the following file listings, some files are shown as belonging to the user "michael". Unix uses the UID to identify who files belong to. On the investigation computer, user 500 was "michael". On the suspect computer, user 500 was "wayne". Therefore in the following file listings, files shown as belonging to "michael" actually belong to "wayne".

```

[ROOT@LOCALHOST TMP]# cd "."
[ROOT@LOCALHOST ...]# ls -al
TOTAL 7948
drwxr-xr-x 7 30 root 4096 Jul 5 19:31 .
drwxrwxrwt 6 root root 4096 Jul 5 19:43 ..
drwxr-xr-x 3 30 root 4096 Jul 5 19:35 ADORE
drwxrwxrwx 3 michael michael 4096 Jul 5 19:16 KIS_CLIENT-0.9
-rw-r--r-- 1 1001 1001 256000 Jul 20 2001 KIS_CLIENT-0.9.TAR
-rw-r--r-- 1 1001 1001 28998 Jul 20 2001 KIS_SERVER-0.9.TAR.GZ
drwxr-xr-x 3 root root 4096 Jul 5 18:47 KNARK-0.50
drwxr-xr-x 3 root root 4096 Jul 5 18:37 KNARK-0.59
-rw-r--r-- 1 michael michael 61440 Jul 5 18:45 KNARK.TAR
drwxr-xr-x 18 root root 4096 Jul 5 19:28 LRK4
-rw-r--r-- 1 michael michael 92160 Jul 5 19:03 TOOLS2.TAR
-rw-r--r-- 1 michael michael 3788800 Jul 5 19:26 TOOLS3.TAR
-rw-r--r-- 1 michael michael 51200 Jul 5 19:30 TOOLS4.TAR
-rw-r--r-- 1 michael michael 3788800 Jul 5 19:03 TOOLS.TAR
-rw-r--r-- 1 1001 1001 4217 Jul 20 2001 USAGE.TXT
[ROOT@LOCALHOST ...]#

```

ADORE AND KNARK ARE WELL KNOWN LINUX LOADABLE KERNEL MODULE (LKM) ROOTKITS. FURTHER "GOOGLE" RESEARCH SHOWED THAT "KIS" IS THE "KERNEL INTRUSION SYSTEM", AN LKM ROOTKIT, AND "LRK4" IS VERSION 4 OF THE "LINUX ROOT KIT." THIS PROGRAM IS ANOTHER LINUX ROOT KIT, WHICH REPLACES SYSTEM BINARIES. REPLACED FILES INCLUDE PS, NETSTAT, LOGIN AND PASSWD. THE EARLIER RESULTS FROM THE KNOWN - GOODS REPORTING TOOL SHOWED THAT ALL SYSTEM BINARIES HAD THE EXPECTED

MD5HASH. THIS MEANS THAT ALTHOUGH THIS PARTICULAR ROOTKIT MAY HAVE BEEN COPIED ONTO THE SYSTEM, IT WAS NOT PROPERLY INSTALLED ON THAT SYSTEM. THE UNKNOWN TAR FILES WE'RE NOW EXAMINING.

```
[root@localhost ...]# tar -tvf tools.tar |head -10
drwxr-xr-x root/root      0 1998-11-26 10:49:24 lrk4/
-rw-r--r-- root/root     716 1998-11-24 17:27:03 lrk4/MCONFIG
-rw-r--r-- root/root    4755 1998-11-26 08:51:53 lrk4/MAKEFILE
-rw-r--r-- root/root    9488 1998-11-26 19:01:22 lrk4/README
drwxr-xr-x root/root      0 1998-11-26 09:28:23 lrk4/bin/
-rw-r--r-- root/root    1661 1998-11-24 17:27:03 lrk4/BINDSHELL.C
drwxr--r-- root/root      0 1998-11-26 09:28:24 lrk4/chfn/
-rw----- root/root    11493 1998-11-24 17:27:03 lrk4/chfn/chfn.c
-rw----- root/root     109 1998-11-24 17:27:03 lrk4/chfn/MAKEFILE
-rw----- root/root    5283 1998-11-24 17:27:03 lrk4/chfn/SETPWNAM.C
[root@localhost ...]# tar -tvf tools.tar |tail -10
-rw-r--r-- root/root      753 1998-11-24 17:27:16 lrk4/FINDUTILS/TESTSUITE/XARGS.SYSV/L2.XO
-rw-r--r-- root/root     1203 1998-11-24 17:27:17 lrk4/FINDUTILS/TESTSUITE/MAKEFILE.AM
-rw-r--r-- root/root     3634 1998-11-24 17:27:17 lrk4/FINDUTILS/TESTSUITE/MAKEFILE.IN
-rw-r--r-- root/root     3644 1998-11-24 17:27:17 lrk4/FINDUTILS/TESTSUITE/MAKEFILE
-rw-r--r-- root/root      462 1998-11-24 17:27:17 lrk4/FINDUTILS/CONFIG.LOG
-rw-r--r-- root/root     4535 1998-11-24 17:27:17 lrk4/FINDUTILS/MAKEFILE
-rw-r--r-- root/root     2370 1998-11-24 17:27:17 lrk4/FINDUTILS/CONFIG.CACHE
-rwxr-xr-x root/root      9519 1998-11-24 17:27:17 lrk4/FINDUTILS/CONFIG.STATUS
-rw-r--r-- root/root     5056 1998-11-24 17:27:17 lrk4/FINDUTILS/CONFIG.H
-rw-r--r-- root/root       29 1998-11-24 17:27:17 lrk4/FINDUTILS/STAMP.H

[root@localhost ...]# tar -tvf tools.tar |grep -v lrk
[root@localhost ...]#
```

This file contains the lrk4 program.

```
[root@localhost ...]# tar -tvf tools2.tar
-rw-r--r-- packet/packet 56295 2001-07-20 11:52:59 kis_client-0.9.tar.gz
-rw-r--r-- packet/packet 28998 2001-07-20 11:53:05 kis_server-0.9.tar.gz
-rw-r--r-- packet/packet 4217 2001-07-20 11:53:13 USAGE.TXT
[root@localhost ...]#
```

The tools2.tar file contains the compressed installation files for "KIS".

```
[root@localhost ...]# tar -tvf tools3.tar |head -10
drwxr-xr-x root/root      0 1998-11-26 10:49:24 lrk4/
-rw-r--r-- root/root     716 1998-11-24 17:27:03 lrk4/MCONFIG
-rw-r--r-- root/root    4755 1998-11-26 08:51:53 lrk4/Makefile
-rw-r--r-- root/root    9488 1998-11-26 19:01:22 lrk4/README
drwxr-xr-x root/root      0 1998-11-26 09:28:23 lrk4/bin/
-rw-r--r-- root/root    1661 1998-11-24 17:27:03 lrk4/bindshell.c
drwxr--r-- root/root      0 1998-11-26 09:28:24 lrk4/chfn/
-rw----- root/root    11493 1998-11-24 17:27:03 lrk4/chfn/chfn.c
-rw----- root/root     109 1998-11-24 17:27:03 lrk4/chfn/Makefile
-rw----- root/root    5283 1998-11-24 17:27:03 lrk4/chfn/setpwnam.c
[root@localhost ...]# tar -tvf tools3.tar |tail -10
-rw-r--r-- root/root      753 1998-11-24 17:27:16 lrk4/findutils/testsuite/xargs.sysv/l2.xo
-rw-r--r-- root/root     1203 1998-11-24 17:27:17 lrk4/findutils/testsuite/Makefile.am
-rw-r--r-- root/root     3634 1998-11-24 17:27:17 lrk4/findutils/testsuite/Makefile.in
-rw-r--r-- root/root     3644 1998-11-24 17:27:17 lrk4/findutils/testsuite/Makefile
-rw-r--r-- root/root      462 1998-11-24 17:27:17 lrk4/findutils/config.log
-rw-r--r-- root/root     4535 1998-11-24 17:27:17 lrk4/findutils/Makefile
-rw-r--r-- root/root     2370 1998-11-24 17:27:17 lrk4/findutils/config.cache
-rwxr-xr-x root/root      9519 1998-11-24 17:27:17 lrk4/findutils/config.status
-rw-r--r-- root/root     5056 1998-11-24 17:27:17 lrk4/findutils/config.h
-rw-r--r-- root/root       29 1998-11-24 17:27:17 lrk4/findutils/stamp-h
[root@localhost ...]#
```

Tools3.tar appears to be the same as tools.tar. To make certain of this md5sums of both files were taken.

```
[root@localhost ...]# md5sum tools.tar
4d988511ea00a49e1450b7de490db614 tools.tar
```

```
[root@localhost ...]# md5sum tools3.tar
4d988511ea00a49e1450b7de490db614 tools3.tar
[root@localhost ...]#
```

These files are identical.

```
[root@localhost ...]# tar -tvf tools4.tar
drwxr-xr-x stealth/stealth 0 2000-12-24 05:03:29 adore/
drwxr-xr-x stealth/stealth 0 2000-12-24 05:03:29 adore/CVS/
-rw-r--r-- stealth/stealth 5 2000-12-24 05:03:29 adore/CVS/Root
-rw-r--r-- stealth/stealth 6 2000-12-24 05:03:29 adore/CVS/Repository
-rw-r--r-- stealth/stealth 616 2000-12-24 05:03:29 adore/CVS/Entries
-rw-r--r-- stealth/stealth 10 2000-12-24 05:03:29 adore/CVS/Tag
-rw-r--r-- stealth/stealth 1660 2000-06-26 07:03:05 adore/LICENSE
-rw-r--r-- stealth/stealth 738 2000-12-24 04:46:53 adore/Makefile.gen
-rw-r--r-- stealth/stealth 2632 2000-12-24 04:55:59 adore/README
-rw-r--r-- stealth/stealth 21 2000-12-24 04:55:59 adore/TODO
-rw-r--r-- stealth/stealth 10757 2000-12-24 04:55:59 adore/adore.c
-rw-r--r-- stealth/stealth 4179 2000-12-22 03:54:05 adore/ava.c
-rw-r--r-- stealth/stealth 1979 2000-12-24 04:57:23 adore/cleaner.c
-rwxr-xr-x stealth/stealth 2810 2000-12-24 04:57:23 adore/configure
-rw-r--r-- stealth/stealth 1904 2000-09-20 01:47:24 adore/dummy.c
-rw-r--r-- stealth/stealth 3262 2000-12-22 03:54:05 adore/libinvisible.c
-rw-r--r-- stealth/stealth 2527 2000-12-22 03:54:05 adore/libinvisible.h
-rwxr-xr-x stealth/stealth 199 2000-12-24 04:46:53 adore/startadore
[root@localhost ...]#
```

TOOLS4.TAR CONTAINS THE ADORE INSTALLATION FILES.

THE TIMES LISTED ON THE STANDARD "LS -AL" ARE THE TIMES THAT THE FILES WERE CREATED. HOWEVER, SOME COMPRESSION PROGRAMS STORE THE TIME THAT A FILE WAS CREATED IN THE COMPRESSED FILE, AND CAN EXTRACT THIS CREATION TIME WHEN THE FILE IS RESTORED. THIS IS THE EXPLANATION FOR THE MISLEADING FILE CREATION TIMES IN THE TEMP DIRECTORY.

```
-rw-r--r-- 1 1001 1001 28998 Jul 20 2001 kis_server-0.9.tar.gz
```

The kis_server gzip file has a creation time of 2001, years before this system was installed. To gain a more accurate picture of the time the files were copied onto the system, the C time must be used. This represents the last time the metadata of the file was altered. This could include be a file being moved, "chmod"ed (change mode), or "chown"ed (change owner).

```
[root@localhost ...]# ls -lc
total 7940
drwxr-xr-x 3 30 root 4096 Jul 5 19:35 adore
drwxrwxrwx 3 michael michael 4096 Jul 5 19:16 kis_client-0.9
-rw-r--r-- 1 1001 1001 256000 Jul 5 19:14 kis_client-0.9.tar
-rw-r--r-- 1 1001 1001 28998 Jul 5 19:05 kis_server-0.9.tar.gz
drwxr-xr-x 3 root root 4096 Jul 5 18:47 knark-0.50
drwxr-xr-x 3 root root 4096 Jul 5 18:37 knark-0.59
-rw-r--r-- 1 michael michael 61440 Jul 5 18:46 knark.tar
drwxr-xr-x 18 root root 4096 Jul 5 19:28 lrk4
-rw-r--r-- 1 michael michael 92160 Jul 5 19:04 tools2.tar
-rw-r--r-- 1 michael michael 3788800 Jul 5 19:28 tools3.tar
-rw-r--r-- 1 michael michael 51200 Jul 5 19:31 tools4.tar
-rw-r--r-- 1 michael michael 3788800 Jul 5 19:04 tools.tar
-rw-r--r-- 1 1001 1001 4217 Jul 5 19:05 USAGE.TXT
[root@localhost ...]#
```

ALL THE FILES WERE INSTALLED ONTO THE SYSTEM WITHIN AN HOUR OF 7PM, JULY 5TH. TO DISCOVER WHAT ELSE HAPPENED WITHIN THIS TIME PERIOD, THE SYSTEM LOGS WERE EXAMINED.

THE /VAR/LOG/MAILLOG CONTAINS THE FOLLOWING LINES

```
Jul 3 15:35:17 redhat6 sendmail[773]: NOQUEUE: Null connection from charlie [192.168.210.33]
Jul 3 15:35:17 redhat6 sendmail[775]: NOQUEUE: Authentication-Warning: localhost.localdomain: charlie
[192.168.210.33] didn't use HELO protocol
Jul 3 15:35:17 redhat6 sendmail[775]: PAA00775: lost input channel from charlie [192.168.210.33]
Jul 3 15:35:17 redhat6 sendmail[775]: PAA00775: from=nessus720696718@hotmail.com, size=0, class=0, pri=0,
nrpts=0, proto=SMTP, relay=charlie
[192.168.210.33]
Jul 3 15:35:17 redhat6 sendmail[776]: NOQUEUE: Null connection from charlie [192.168.210.33]

Jul 3 15:35:28 redhat6 sendmail[822]: PAA00822: /tmp/nessus_test.. Cannot mail directly to files
Jul 3 15:35:28 redhat6 sendmail[822]: PAA00822: lost input channel from charlie [192.168.210.33]

Jul 3 15:35:38 redhat6 sendmail[855]: PAA00855: from=<test_1@nessus.org>, size=0, class=0, pri=0, nrpts=0,
proto=SMTP, relay=charlie [192.168.210.33]
Jul 3 15:35:42 redhat6 sendmail[866]: PAA00866: ruleset=check_rcpt, arg 1=<test_2@nessus.org>, relay=charlie
[192.168.210.33], reject=550
<test_2@nessus.org>... Relaying denied
```

Clearly someone on 192.168.210.33 ran a Nessus^x scan against this machine at 3:35pm on July 3rd. Nessus is a widely available tool that is used to test computers for security vulnerabilities and related issues.

The nessus scan also appears in the "/var/log/messages" file.

```
Jul 3 15:17:54 redhat6 login: FAILED LOGIN 1 FROM (null) FOR root, User not known to the underlying
authentication module
Jul 3 15:17:59 redhat6 PAM_pwdb[615]: authentication failure; LOGIN(uid=0)-> root for login service
Jul 3 15:18:00 redhat6 login[615]: FAILED LOGIN 2 FROM (null) FOR root, Authentication failure
Jul 3 15:18:04 redhat6 PAM_pwdb[615]: (login) session opened for user root by LOGIN(uid=0)
Jul 3 15:18:39 redhat6 identd: cannot bind() server socket: Permission denied.
Jul 3 15:18:39 redhat6 inetd[478]: /sbin/identd (pid 659): exit status 255

Jul 3 15:18:41 redhat6 inetd[478]: /sbin/identd (pid 697): exit status 255
Jul 3 15:18:41 redhat6 inetd[478]: ident/tcp server failing (looping or being flooded), service terminated for 10 min
Jul 3 15:23:24 redhat6 inetd[478]: pid 704: exit signal 13
Jul 3 15:23:24 redhat6 inetd[478]: pid 706: exit signal 13
Jul 3 15:23:25 redhat6 ftpd[703]: getpeername (in.ftpd): Transport endpoint is not connected
Jul 3 15:23:25 redhat6 inetd[478]: pid 703: exit status 1
Jul 3 15:28:41 redhat6 inetd[478]: ident/tcp: bind: Address already in use
Jul 3 15:30:52 redhat6 ftpd[711]: lost connection to charlie [192.168.210.33]
Jul 3 15:30:52 redhat6 ftpd[711]: FTP session closed

Jul 3 03:35:13 redhat6 ftpd[753]: ANONYMOUS FTP LOGIN FROM charlie [192.168.210.33], nessus@nessus.org
Jul 3 03:35:13 redhat6 ftpd[753]: FTP session closed
```

Other suspicious activity also appears in the "/var/log/messages" log file that records kernel messages

```
Jul 3 16:50:37 redhat6 PAM_pwdb[615]: authentication failure; LOGIN(uid=0)-> root for login service
Jul 3 16:50:38 redhat6 login[615]: FAILED LOGIN 1 FROM (null) FOR root, Authentication failure
Jul 3 16:50:50 redhat6 PAM_pwdb[615]: (login) session opened for user root by LOGIN(uid=0)

Jul 5 12:21:23 redhat6 inetd[477]: ident/tcp server failing (looping or being flooded), service terminated for 10 min
Jul 5 12:29:51 redhat6 identd: cannot bind() server socket: Address already in use.
Jul 5 12:33:44 redhat6 PAM_pwdb[614]: (login) session closed for user root
Jul 5 12:33:48 redhat6 PAM_pwdb[707]: get passwd; pwdb: request not recognized
Jul 5 12:33:49 redhat6 login[707]: FAILED LOGIN 1 FROM (null) FOR wroot, Authentication service cannot retrieve
authentication info.
Jul 5 12:34:01 redhat6 PAM_pwdb[707]: get passwd; pwdb: request not recognized
Jul 5 12:34:01 redhat6 login[707]: FAILED LOGIN 2 FROM (null) FOR wroot, Authentication service cannot retrieve
authentication info.
Jul 5 12:36:21 redhat6 PAM_pwdb[708]: get passwd; pwdb: request not recognized
Jul 5 12:36:22 redhat6 login[708]: FAILED LOGIN 1 FROM (null) FOR wroot, Authentication service cannot retrieve
authentication info.
```

```

Jul 5 12:36:39 redhat6 PAM_pwdb[708]: (login) session opened for user root by LOGIN(uid=0)
Jul 5 12:38:02 redhat6 PAM_pwdb[732]: (su) session opened for user wroot by root(uid=0)
Jul 5 12:38:31 redhat6 PAM_pwdb[732]: (su) session closed for user wroot
Jul 5 12:38:33 redhat6 PAM_pwdb[708]: (login) session closed for user root
Jul 5 12:38:39 redhat6 PAM_pwdb[745]: get passwd; pwdb: request not recognized
Jul 5 12:38:40 redhat6 login[745]: FAILED LOGIN 1 FROM (null) FOR wroot, Authentication service cannot retrieve authentication info.
Jul 5 12:39:05 redhat6 pam_rhosts_auth[746]: denied to wayne@192.168.210.7 as wayne: access not allowed
Jul 5 12:39:07 redhat6 PAM_pwdb[746]: authentication failure; (uid=0)-> wayne for rlogin service
Jul 5 12:39:08 redhat6 in.rlogind[746]: PAM authentication failed for in.rlogind
Jul 5 12:39:13 redhat6 PAM_pwdb[747]: (login) session opened for user wayne by (uid=0)
Jul 5 12:39:42 redhat6 PAM_pwdb[747]: (login) session closed for user wayne
Jul 5 12:40:26 redhat6 pam_rhosts_auth[772]: denied to wayne@192.168.210.7 as wroot: access not allowed
Jul 5 12:40:27 redhat6 PAM_pwdb[772]: get passwd; pwdb: request not recognized
Jul 5 12:40:27 redhat6 in.rlogind[772]: PAM authentication failed for in.rlogind
Jul 5 12:41:13 redhat6 PAM_pwdb[773]: get passwd; pwdb: request not recognized
Jul 5 12:41:14 redhat6 login[773]: FAILED LOGIN 1 FROM 192.168.210.7 FOR wroot, Authentication failure
Jul 5 12:41:17 redhat6 login[773]: FAILED LOGIN 2 FROM 192.168.210.7 FOR , User not known to the underlying authentication module
Jul 5 12:41:20 redhat6 login[773]: FAILED LOGIN 3 FROM 192.168.210.7 FOR , User not known to the underlying authentication module
Jul 5 12:41:22 redhat6 PAM_pwdb[773]: check pass; user unknown
Jul 5 12:41:23 redhat6 login[773]: FAILED LOGIN SESSION FROM 192.168.210.7 FOR rew, User not known to the underlying authentication module
Jul 5 12:41:52 redhat6 PAM_pwdb[768]: (login) session opened for user root by LOGIN(uid=0)

Jul 5 12:56:56 redhat6 inetd[477]: ident/tcp server failing (looping or being flooded), service terminated for 10 min
Jul 5 12:57:03 redhat6 identd: cannot bind() server socket: Address already in use.
Jul 5 12:59:49 redhat6 PAM_pwdb[958]: password for (wayne/500) changed by (root/0)
Jul 5 13:00:23 redhat6 PAM_pwdb[959]: password for (wroot0) changed by ((null)/0)
Jul 5 13:00:34 redhat6 PAM_pwdb[882]: (login) session closed for user root
Jul 5 13:00:40 redhat6 PAM_pwdb[963]: (login) session opened for user wroot by LOGIN(uid=0)
Jul 5 13:02:29 redhat6 identd: cannot bind() server socket: Address already in use.
Jul 5 13:03:21 redhat6 PAM_pwdb[995]: password for (wroot0) changed by ((null)/0)
Jul 5 13:04:31 redhat6 pam_rhosts_auth[996]: denied to wayne@192.168.210.7 as wroot: access not allowed
Jul 5 13:04:32 redhat6 PAM_pwdb[996]: authentication failure; (uid=0)-> wroot for rlogin service
Jul 5 13:04:32 redhat6 in.rlogind[996]: PAM authentication failed for in.rlogind
Jul 5 13:04:39 redhat6 login: FAILED LOGIN 1 FROM 192.168.210.7 FOR wroot, Authentication failure
Jul 5 13:04:50 redhat6 login: FAILED LOGIN 2 FROM 192.168.210.7 FOR wroot, Authentication failure
Jul 5 13:10:08 redhat6 pam_rhosts_auth[1002]: denied to wayne@192.168.210.7 as wroot: access not allowed
Jul 5 13:10:13 redhat6 in.rlogind[1002]: PAM authentication failed for in.rlogind
Jul 5 13:10:18 redhat6 login: FAILED LOGIN 1 FROM 192.168.210.7 FOR wroot, Authentication failure
Jul 5 13:10:25 redhat6 login: FAILED LOGIN 2 FROM 192.168.210.7 FOR root, Authentication failure
Jul 5 13:10:30 redhat6 PAM_pwdb[1003]: (login) session opened for user wayne by (uid=0)
Jul 5 13:10:51 redhat6 PAM_pwdb[1024]: (su) session opened for user wroot by wayne(uid=500)
Jul 5 13:11:39 redhat6 identd: cannot bind() server socket: Address already in use.
Jul 5 13:11:39 redhat6 identd: cannot bind() server socket: Address already in use.
Jul 5 13:11:46 redhat6 PAM_pwdb[1024]: (su) session closed for user wroot
Jul 5 13:11:51 redhat6 PAM_pwdb[1003]: (login) session closed for user wayne
Jul 5 13:12:38 redhat6 identd: cannot bind() server socket: Permission denied.

Jul 5 14:11:10 redhat6 PAM_pwdb[614]: check pass; user unknown
Jul 5 14:11:11 redhat6 login[614]: FAILED LOGIN 1 FROM (null) FOR rooty, User not known to the underlying authentication module
Jul 5 14:11:16 redhat6 PAM_pwdb[614]: (login) session opened for user root by LOGIN(uid=0)
Jul 5 14:11:21 redhat6 identd: cannot bind() server socket: Address already in use.

Jul 5 18:42:51 redhat6 ftpd[1473]: PAM-istfile: Refused user root for service ftp
Jul 5 18:42:51 redhat6 PAM_pwdb[1473]: authentication failure; (uid=0)-> root for ftp service
Jul 5 18:42:52 redhat6 ftpd: 192.168.210.7: connected: IDLE
[1473]: failed login from 192.168.210.7 [192.168.210.7]
Jul 5 18:43:04 redhat6 PAM_pwdb[1473]: authentication failure; (uid=0)-> wruser for ftp service
Jul 5 18:43:05 redhat6 ftpd: 192.168.210.7: connected: IDLE
[1473]: failed login from 192.168.210.7 [192.168.210.7]
Jul 5 18:43:15 redhat6 ftpd: 192.168.210.7: wayne
[1473]: FTP LOGIN FROM 192.168.210.7 [192.168.210.7], wayne
Jul 5 18:45:21 redhat6 ftpd: 192.168.210.7: wayne: QUIT
[1473]: FTP session closed
Jul 5 19:01:10 redhat6 ftpd[1540]: failed login from 192.168.210.7 [192.168.210.7]
Jul 5 19:01:21 redhat6 ftpd[1540]: FTP LOGIN FROM 192.168.210.7 [192.168.210.7], wayne
Jul 5 19:17:16 redhat6 ftpd[1540]: FTP session closed
Jul 5 19:25:05 redhat6 ftpd[1834]: PAM-istfile: Refused user root for service ftp
Jul 5 19:25:05 redhat6 PAM_pwdb[1834]: authentication failure; (uid=0)-> root for ftp service
Jul 5 19:25:06 redhat6 ftpd: 192.168.210.7: connected: IDLE

```

```

[1834]: failed login from 192.168.210.7 [192.168.210.7]
Jul  5 19:25:14 redhat6 ftpd: 192.168.210.7: wayne
[1834]: FTP LOGIN FROM 192.168.210.7 [192.168.210.7], wayne
Jul  5 19:26:48 redhat6 ftpd: 192.168.210.7: wayne: QUIT
[1834]: FTP session closed
Jul  5 19:30:04 redhat6 ftpd[1842]: PAM-histfile: Refused user root for service ftp
Jul  5 19:30:04 redhat6 PAM_pwd[1842]: authentication failure; (uid=0)-> root for ftp service
Jul  5 19:30:04 redhat6 ftpd: 192.168.210.7: connected: IDLE
[1842]: failed login from 192.168.210.7 [192.168.210.7]
Jul  5 19:30:12 redhat6 ftpd: 192.168.210.7: wayne
[1842]: FTP LOGIN FROM 192.168.210.7 [192.168.210.7], wayne
Jul  5 19:45:39 redhat6 ftpd: 192.168.210.7: wayne: IDLE
[1842]: User wayne timed out after 900 seconds at Sat Jul  5 19:45:39 2003
Jul  5 19:45:39 redhat6 ftpd: 192.168.210.7: wayne: IDLE
[1842]: FTP session closed
Jul  5 19:45:39 redhat6 inetd[477]: pid 1842: exit status 1

```

THE "/VAR/LOG/SECURE" FILE THAT DEALS WITH LOGIN FAILURES AND SUCH CONTAINS THE FOLLOWING

```

JUL  5 12:36:39 REDHAT6 LOGIN: ROOT LOGIN ON TTY1
JUL  5 12:39:04 REDHAT6 IN.RLOGIND[746]: CONNECT FROM 192.168.210.7
JUL  5 12:39:13 REDHAT6 LOGIN: LOGIN ON 0 BY WAYNE FROM 192.168.210.7
JUL  5 12:40:26 REDHAT6 IN.RLOGIND[772]: CONNECT FROM 192.168.210.7
JUL  5 12:41:52 REDHAT6 LOGIN: ROOT LOGIN ON TTY1
JUL  5 12:52:30 REDHAT6 LAST MESSAGE REPEATED 2 TIMES
JUL  5 13:00:40 REDHAT6 LOGIN: ROOT LOGIN ON TTY1
JUL  5 13:04:31 REDHAT6 IN.RLOGIND[996]: CONNECT FROM 192.168.210.7
JUL  5 13:10:08 REDHAT6 IN.RLOGIND[1002]: CONNECT FROM 192.168.210.7
JUL  5 13:10:30 REDHAT6 LOGIN: LOGIN ON 0 BY WAYNE FROM 192.168.210.7
JUL  5 13:16:36 REDHAT6 IN.RLOGIND[1089]: CONNECT FROM 192.168.210.7
JUL  5 13:18:01 REDHAT6 LOGIN: ROOT LOGIN ON TTY1
JUL  5 13:21:46 REDHAT6 IN.RLOGIND[1127]: CONNECT FROM 192.168.210.7
JUL  5 13:21:50 REDHAT6 LOGIN: LOGIN ON 0 BY WRUSER FROM 192.168.210.7
JUL  5 14:11:16 REDHAT6 LOGIN: ROOT LOGIN ON TTY1
JUL  5 14:14:16 REDHAT6 IN.RLOGIND[692]: CONNECT FROM 192.168.210.7
JUL  5 14:14:28 REDHAT6 LOGIN: LOGIN ON 0 BY WRUSER FROM 192.168.210.7

```

AND FINALLY, THE "/VAR/LOG/XFERLOG" FILE (WHICH RECORDS FILE TRANSFERS TO AND FROM THE SYSTEM) CONTAINS

```

SAT JUL  5 17:46:19 2003 1 192.168.210.7 15169 /TMP/KNARK.TAR.GZ B_IR WAYNE FTP 0 *C
SAT JUL  5 18:45:17 2003 3 192.168.210.7 12856 /TMP/KNARK B_IR WAYNE FTP 0 *C
SAT JUL  5 19:02:17 2003 4 192.168.210.7 87860 /TMP/TOOLS A_IR WAYNE FTP 0 *C
SAT JUL  5 19:02:26 2003 1 192.168.210.7 87860 /TMP/TOOLS B_IR WAYNE FTP 0 *C
SAT JUL  5 19:03:18 2003 34 192.168.210.7 900450 /TMP/TOOLS B_IR WAYNE FTP 0 *C
SAT JUL  5 19:03:29 2003 1 192.168.210.7 87860 /TMP/TOOLS2 B_IR WAYNE FTP 0 *C
SAT JUL  5 19:26:25 2003 36 192.168.210.7 900450 /TMP/TOOLS3.TAR.GZ A_IR WAYNE FTP 0 *C
SAT JUL  5 19:26:31 2003 1 192.168.210.7 900450 /TMP/TOOLS3.TAR.GZ B_IR WAYNE FTP 0 *C
SAT JUL  5 19:30:33 2003 1 192.168.210.7 9738 /TMP/TOOLS4.TAR.GZ A_IR WAYNE FTP 0 *C
SAT JUL  5 19:30:39 2003 1 192.168.210.7 9738 /TMP/TOOLS4.TAR.GZ B_IR WAYNE FTP 0 *C

```

Unfortunately, the system was seized in a powered down state. The system usually stores information about running processes in the "/proc" directory. This can be useful information for an investigator as it helps identify what the system was doing. The system was turned off however, which made it impossible to get any information from the /proc directory. In fact, the /proc directory was completely empty.

```

[root@localhost root]# cd /mnt/hack/root/var/proc
[root@localhost proc]# ls -al
total 8
drwxr-xr-x  2 root  root   4096 Jul 3 01:47 .
drwxr-xr-x 17 root  root   4096 Jul 5 15:21 ..
[root@localhost proc]#

```

ANOTHER OPTION WAS TO SEARCH FOR THE LOADABLE KERNEL MODULES FOUND ON THE

HARD DISK DRIVE . THIS WAS DONE USING THE "CHKROOTKIT " PROGRAM . THIS PROGRAM RECOGNISES KNOWN ROOTKIT SIGNATURES , AND WARNS IF ANY HAVE BEEN INSTALLED . IT WAS EXECUTED WITH THE COMMAND LINE "/CHKROOTKIT -R /MNT/HACK/ROOT". IT DETECTED NO INSTALLED ROOTKITS . THIS MEANS THAT ANY ROOTKITS FOUND ON THE SYSTEM HAD SIMPLY BEEN COPIED THERE AND EXPANDED , RATHER THAN PROPERLY INSTALLED . ALTHOUGH THE "/BOOT/SYSTEM.MAP" FILE WAS ALSO EXAMINED , THIS FILE IS DIFFERENT FROM MACHINE TO MACHINE . THERE WAS NO KNOWN GOOD COPY AVAILABLE , BUT NOTHING OUT OF PLACE COULD BE SEEN IN THIS FILE .

SYSTEM STARTUP FILES COULD ALSO SHOW EVIDENCE OF A COMPROMISE . THESE ARE LOCATED IN THE "/ETC/INIT" AND "RC.D" DIRECTORIES . FILES SET TO START AUTOMATICALLY BEGIN WITH AN "S" , AND FILES SET TO NOT START BEGIN WITH A "K" . ALTHOUGH ALL THESE DIRECTORIES WERE EXAMINED , FOR BREVITY ONLY EXAMPLES ARE SHOWN .

```
[root@localhost init.d]# cd /etc/init.d
```

```
[root@localhost init.d]# ls -al
```

```
TOTAL 188
```

```
drwxr-xr-x 2 root root 4096 Jul 3 14:18 .
drwxr-xr-x 10 root root 4096 Jul 2 14:09 ..
-rwxr-xr-x 1 root root 525 Mar 4 2000 anacron
-rwxr-xr-x 1 root root 1367 Oct 27 1999 apmd
-rwxr-xr-x 1 root root 827 Feb 18 2000 arpwatc
-rwxr-xr-x 1 root root 989 Mar 2 2000 atd
-rwxr-xr-x 1 root root 1031 Feb 4 2000 crond
-rwxr-xr-x 1 root root 405 Jul 3 14:18 fakeidentd
-rwxr-xr-x 1 root root 7349 Jan 21 2000 functions
-rwxr-xr-x 1 root root 1261 Mar 1 2000 gpm
-rwxr-xr-x 1 root root 3260 Mar 9 2000 halt
-rwxr-xr-x 1 root root 865 Mar 2 2000 httpd
-rwxr-xr-x 1 root root 1151 Feb 23 2000 identd
-rwxr-xr-x 1 root root 1463 Feb 1 2000 inet
-rwxr-xr-x 1 root root 1890 Mar 3 2000 innd
-rwxr-xr-x 1 root root 2448 Feb 17 2000 ipchains
-rwxr-xr-x 1 root root 1065 Mar 9 2000 kdcrotate
-rwxr-xr-x 1 root root 1203 Mar 7 2000 keytable
-rwxr-xr-x 1 root root 449 Oct 1 1999 killall
-rwxr-xr-x 1 root root 1179 Mar 5 2000 kudzu
lrwxrwxrwx 1 root root 43 Jul 2 14:11 linuxconf -> /usr/lib/linuxconf/redhat/scripts/linuxconf
-rwxr-xr-x 1 root root 1176 Feb 15 2000 lpd
-rwxr-xr-x 1 root root 1104 Feb 25 2000 mars-nwe
-rwxr-xr-x 1 root root 1340 Feb 29 2000 named
-rwxr-xr-x 1 root root 3217 Sep 21 1999 netfs
-rwxr-xr-x 1 root root 5094 Mar 8 2000 network
-rwxr-xr-x 1 root root 2257 Feb 10 2000 nfs
-rwxr-xr-x 1 root root 1722 Feb 10 2000 nfslock
-r-xr-xr-x 1 root root 4481 Mar 8 2000 pcmcia
-rwxr-xr-x 1 root root 1086 Feb 8 2000 portmap
-rwxr-xr-x 1 root root 2431 Feb 13 2000 postgresql
-rwxr-xr-x 1 root root 1542 Feb 5 2000 random
-rwxr-xr-x 1 root root 780 Feb 10 2000 rstatd
-rwxr-xr-x 1 root root 976 Feb 10 2000 rusersd
-rwxr-xr-x 1 root root 941 Feb 12 2000 rwalld
-rwxr-xr-x 1 root root 882 Feb 8 2000 rwhod
-rwxr-xr-x 1 root root 1549 Feb 18 2000 sendmail
-rwxr-xr-x 1 root root 1504 Feb 5 2000 single
-rwxr-xr-x 1 root root 1177 Feb 26 2000 smb
-rwxr-xr-x 1 root root 851 Feb 28 2000 snmpd
-rwxr-xr-x 1 root root 1024 Feb 4 2000 syslog
-rwxr-xr-x 1 root root 1956 Mar 7 2000 xfs
-rwxr-xr-x 1 root root 1712 Feb 6 2000 ypbind
-rwxr-xr-x 1 root root 1084 Mar 7 2000 yppasswdd
-rwxr-xr-x 1 root root 1137 Mar 7 2000 ypserv
```

```
[root@localhost init.d]#
```

An interesting entry here is "fakeidentd" - the Fake Ident Daemon.

```
[root@localhost rc.d]# cd rc0.d/
[root@localhost rc0.d]# ls -al
total 8
drwxr-xr-x  2 root  root   4096 Jul 3 14:18 .
drwxr-xr-x 10 root  root   4096 Jul 2 14:09 ..
lrwxrwxrwx  1 root  root    19 Jul 3 01:55 K00linuxconf-> ../init.d/linuxconf
lrwxrwxrwx  1 root  root    14 Jul 3 01:53 K05innnd-> ../init.d/innnd
lrwxrwxrwx  1 root  root    18 Jul 3 01:49 K05keytable-> ../init.d/keytable
lrwxrwxrwx  1 root  root    13 Jul 3 01:49 K10xfs-> ../init.d/xfs
lrwxrwxrwx  1 root  root    13 Jul 3 01:52 K15gpm-> ../init.d/gpm
lrwxrwxrwx  1 root  root    15 Jul 3 01:49 K15httpd-> ../init.d/httpd
lrwxrwxrwx  1 root  root    13 Jul 3 01:57 K20nfs-> ../init.d/nfs
lrwxrwxrwx  1 root  root    16 Jul 3 01:58 K20rstatd-> ../init.d/rstatd
lrwxrwxrwx  1 root  root    17 Jul 3 01:58 K20rusersd-> ../init.d/rusersd
lrwxrwxrwx  1 root  root    16 Jul 3 01:58 K20rwalld-> ../init.d/rwalld
lrwxrwxrwx  1 root  root    15 Jul 3 01:58 K20rwhod-> ../init.d/rwhod
lrwxrwxrwx  1 root  root    18 Jul 3 01:58 K30sendmail-> ../init.d/sendmail
lrwxrwxrwx  1 root  root    19 Jul 3 01:59 K34ypasswdd-> ../init.d/ypasswdd
lrwxrwxrwx  1 root  root    13 Jul 3 01:58 K35smb-> ../init.d/smb
lrwxrwxrwx  1 root  root    27 Jul 3 14:18 K45fakeidentd-> /etc/rc.d/init.d/fakeidentd
lrwxrwxrwx  1 root  root    15 Jul 3 01:49 K45named-> ../init.d/named
lrwxrwxrwx  1 root  root    14 Jul 3 01:52 K50inet-> ../init.d/inet
lrwxrwxrwx  1 root  root    15 Jul 3 01:59 K50snmpd-> ../init.d/snmpd
lrwxrwxrwx  1 root  root    13 Jul 3 01:49 K60atd-> ../init.d/atd
lrwxrwxrwx  1 root  root    15 Jul 3 01:59 K60crond-> ../init.d/crond
lrwxrwxrwx  1 root  root    13 Jul 3 01:56 K60lpd-> ../init.d/lpd
lrwxrwxrwx  1 root  root    18 Jul 3 01:56 K60mars-nwe-> ../init.d/mars-nwe
lrwxrwxrwx  1 root  root    16 Jul 3 01:57 K65identd-> ../init.d/identd
lrwxrwxrwx  1 root  root    17 Jul 3 01:57 K70nfslock-> ../init.d/nfslock
lrwxrwxrwx  1 root  root    15 Jul 3 01:52 K75netfs-> ../init.d/netfs
lrwxrwxrwx  1 root  root    16 Jul 3 01:52 K80random-> ../init.d/random
lrwxrwxrwx  1 root  root    14 Jul 3 01:49 K84apmd-> ../init.d/apmd
lrwxrwxrwx  1 root  root    16 Jul 3 01:59 K84ypserv-> ../init.d/ypserv
lrwxrwxrwx  1 root  root    17 Jul 3 01:57 K89portmap-> ../init.d/portmap
lrwxrwxrwx  1 root  root    17 Jul 3 01:52 K90network-> ../init.d/network
lrwxrwxrwx  1 root  root    18 Jul 3 01:53 K92ipchains-> ../init.d/ipchains
lrwxrwxrwx  1 root  root    15 Jul 3 01:54 K95kudzu-> ../init.d/kudzu
lrwxrwxrwx  1 root  root    16 Jul 3 01:54 K96pcmcia-> ../init.d/pcmcia
lrwxrwxrwx  1 root  root    16 Jul 3 01:58 K99syslog-> ../init.d/syslog
lrwxrwxrwx  1 root  root    17 Jul 3 01:52 S00killall-> ../init.d/killall
lrwxrwxrwx  1 root  root    14 Jul 3 01:52 S01halt-> ../init.d/halt
[root@localhost rc0.d]# cd ..
```

```
[root@localhost rc.d]# cd rc6.d/
[root@localhost rc6.d]# ls -al
total 8
drwxr-xr-x  2 root  root   4096 Jul 3 14:18 .
drwxr-xr-x 10 root  root   4096 Jul 2 14:09 ..
lrwxrwxrwx  1 root  root    19 Jul 3 01:55 K00linuxconf-> ../init.d/linuxconf
lrwxrwxrwx  1 root  root    14 Jul 3 01:53 K05innnd-> ../init.d/innnd
lrwxrwxrwx  1 root  root    18 Jul 3 01:49 K05keytable-> ../init.d/keytable
lrwxrwxrwx  1 root  root    13 Jul 3 01:49 K10xfs-> ../init.d/xfs
lrwxrwxrwx  1 root  root    13 Jul 3 01:52 K15gpm-> ../init.d/gpm
lrwxrwxrwx  1 root  root    15 Jul 3 01:49 K15httpd-> ../init.d/httpd
lrwxrwxrwx  1 root  root    13 Jul 3 01:57 K20nfs-> ../init.d/nfs
lrwxrwxrwx  1 root  root    16 Jul 3 01:58 K20rstatd-> ../init.d/rstatd
lrwxrwxrwx  1 root  root    17 Jul 3 01:58 K20rusersd-> ../init.d/rusersd
lrwxrwxrwx  1 root  root    16 Jul 3 01:58 K20rwalld-> ../init.d/rwalld
lrwxrwxrwx  1 root  root    15 Jul 3 01:58 K20rwhod-> ../init.d/rwhod
lrwxrwxrwx  1 root  root    18 Jul 3 01:58 K30sendmail-> ../init.d/sendmail
lrwxrwxrwx  1 root  root    19 Jul 3 01:59 K34ypasswdd-> ../init.d/ypasswdd
lrwxrwxrwx  1 root  root    13 Jul 3 01:58 K35smb-> ../init.d/smb
lrwxrwxrwx  1 root  root    27 Jul 3 14:18 K45fakeidentd-> /etc/rc.d/init.d/fakeidentd
lrwxrwxrwx  1 root  root    15 Jul 3 01:49 K45named-> ../init.d/named
lrwxrwxrwx  1 root  root    14 Jul 3 01:52 K50inet-> ../init.d/inet
lrwxrwxrwx  1 root  root    15 Jul 3 01:59 K50snmpd-> ../init.d/snmpd
lrwxrwxrwx  1 root  root    13 Jul 3 01:49 K60atd-> ../init.d/atd
lrwxrwxrwx  1 root  root    15 Jul 3 01:59 K60crond-> ../init.d/crond
lrwxrwxrwx  1 root  root    13 Jul 3 01:56 K60lpd-> ../init.d/lpd
lrwxrwxrwx  1 root  root    18 Jul 3 01:56 K60mars-nwe-> ../init.d/mars-nwe
lrwxrwxrwx  1 root  root    16 Jul 3 01:57 K65identd-> ../init.d/identd
```

```

lrwxrwxrwx 1 root root 17 Jul 3 01:57 K70nfslock-> ../init.d/nfslock
lrwxrwxrwx 1 root root 15 Jul 3 01:52 K75netfs-> ../init.d/netfs
lrwxrwxrwx 1 root root 16 Jul 3 01:52 K80random-> ../init.d/random
lrwxrwxrwx 1 root root 14 Jul 3 01:49 K84apmd-> ../init.d/apmd
lrwxrwxrwx 1 root root 16 Jul 3 01:59 K84ypserv-> ../init.d/ypserv
lrwxrwxrwx 1 root root 17 Jul 3 01:57 K89portmap-> ../init.d/portmap
lrwxrwxrwx 1 root root 17 Jul 3 01:52 K90network-> ../init.d/network
lrwxrwxrwx 1 root root 18 Jul 3 01:53 K92ipchains-> ../init.d/ipchains
lrwxrwxrwx 1 root root 15 Jul 3 01:54 K95kudzu-> ../init.d/kudzu
lrwxrwxrwx 1 root root 16 Jul 3 01:54 K96pcmcia-> ../init.d/pcmcia
lrwxrwxrwx 1 root root 16 Jul 3 01:58 K99syslog-> ../init.d/syslog
lrwxrwxrwx 1 root root 17 Jul 3 01:52 S00killall-> ../init.d/killall
lrwxrwxrwx 1 root root 14 Jul 3 01:52 S01reboot-> ../init.d/halt

```

```
[root@localhost rc6.d]# cd ..
```

```
[root@localhost rc.d]# ls -al
```

```

total 68
drwxr-xr-x 10 root root 4096 Jul 2 14:09 .
drwxr-xr-x 29 root root 4096 Jul 5 18:13 ..
drwxr-xr-x 2 root root 4096 Jul 3 14:18 init.d
-rwxr-xr-x 1 root root 2889 Nov 9 1999 rc
drwxr-xr-x 2 root root 4096 Jul 3 14:18 rc0.d
drwxr-xr-x 2 root root 4096 Jul 3 13:10 rc1.d
drwxr-xr-x 2 root root 4096 Jul 3 14:18 rc2.d
drwxr-xr-x 2 root root 4096 Jul 3 13:10 rc3.d
drwxr-xr-x 2 root root 4096 Jul 3 13:10 rc4.d
drwxr-xr-x 2 root root 4096 Jul 3 13:10 rc5.d
drwxr-xr-x 2 root root 4096 Jul 3 14:18 rc6.d
-rwxr-xr-x 1 root root 933 Oct 1 1999 rc.local
-r-xr-x-- 1 news news 2964 Mar 3 2000 rc.news
-rwxr-xr-x 1 root root 13679 Feb 24 2000 rc.sysinit
[root@localhost rc.d]#

```

These are all much as you would expect on this type of system. The rc.local, news, and sysinit files were also examined, using "emacs rc.local", "emacs rc.news", or "emacs rc.sysinit" respectively. No anomalies were found in these files.

User's startup files were also examined at this point. Only one user had a home directory, "/home/wayne".

```

[ROOT@LOCALHOST WAYNE]# LS -AL
TOTAL 32
DRWX----- 2 MICHAEL MICHAEL 4096 JUL 5 12:39 .
DRWXR-XR-X 5 ROOT ROOT 4096 FEB 7 1996 ..
-RW----- 1 MICHAEL MICHAEL 19 JUL 5 13:11 .BASH_HISTORY
-RW-R--R-- 1 MICHAEL MICHAEL 24 JUL 3 01:59 .BASH_LOGOUT
-RW-R--R-- 1 MICHAEL MICHAEL 230 JUL 3 01:59 .BASH_PROFILE
-RW-R--R-- 1 MICHAEL MICHAEL 124 JUL 3 01:59 .BASHRC
-RWXR-XR-X 1 MICHAEL MICHAEL 333 JUL 3 01:59 .EMACS
-RW-R--R-- 1 MICHAEL MICHAEL 3394 JUL 3 01:59 .SCREENRC

```

```
[ROOT@LOCALHOST WAYNE]# CAT .BASH_HISTORY
```

```
EXIT
```

```
SU WROOT
```

```
EXIT
```

```
[ROOT@LOCALHOST WAYNE]#
```

THE OTHER FILES (".BASH_LOGOUT", ".BASH_PROFILE", ".EMACS" AND ".SCREENRC") WERE UNMODIFIED FROM THE STANDARD RED HAT INSTALLATION. AS THE ".BASH_HISTORY" FILE ONLY CONTAINED THREE COMMANDS (EXIT, SU WROOT, AND EXIT) IT IS LIKELY THAT AFTER OBTAINING A LOGIN AND PASSWORD FOR WROOT THAT THE INTRUDER USED THIS ACCOUNT, RATHER THAN "WAYNE". AFTER OBTAINING THIS LOGIN/PASSWORD COMBINATION HE MAY IN FACT HAVE CLEANED OUT THE ".BASH_HISTORY" FILE TO COVER HIS TRACKS.

THE ONLY OTHER USER ON THE SYSTEM IS "ROOT". "/ROOT/.BASH_HISTORY" WAS NEXT EXAMINED. THIS FILE INCLUDING THE FOLLOWING COMMANDS.

CHECKING THE SYSTEM I NSTALLED SUCCESSFULL Y

```
EXIT
MOUNT /DEV/FD0 /MNT/FLOPPY
DF -K
CD /MNT/FLOPPY
LS
CP */TMP/
CD /TMP
LS
```

ADDING SOME PACKAGES

```
PACKAGEADD
RPMADD
ADDPACKAGE
ADDRPM
CLEAR
LS
RPM
LS
```

Installing the fake ident service from an RPM

```
rpm -U fakeident*.rpm
```

Checking the fakeident service installed success fully

```
telnet localhost 113
/usr/sbin/identd -V
/usr/sbin/fakeidentd -version
```

Setting up network connectivity

```
reboot
ping 192.168.210.33
ifconfig
ping 192.168.210.33
ps -ef
ping 192.168.210.33
```

```
reboot
cd /etc
ls
vi inetd.conf
ping 192.168.210.7
```

Using TCPDump (likely to check the Fakeident service) and creating the lame l file

```
man tcpdump
tcpdump -X > /tmp/lame1
```

```
cd /etc
ls
more hosts
vi hosts
more hosts.allow
wq
ping charlie
```

Installing a different version of fakeident, this time from the source code.

```
cd fakeidentd-1.2orig/
ls
make
make install
```

IT IS LIKELY THAT THE ROOT ACCOUNT IS COM PROMISED BY THIS TIME. HERE THE ROOT USER DIRECTLY EDITS THE "/ETC/PASSWD" AND "/ETC/SHADOW" FILES.

```
VI /ETC/SHADOW
EXIT
VI /ETC/PASSWD
EXIT
MORE /ETC/PASSWD
MAN PASSWD
MORE /ETC/PASSWD
VI /ETC/PASSWD
EXIT
```

REMOVING THE TRIPWIRE INSTALLATION DIRECTORY

RM JONTY

INSTALLING TRIPWIRE FROM A CD-ROM

```
SHOWMOUNT
MORE /ETC/FSTAB
MOUNT -T ISO9660 /DEV/CDROM /MNT/CDROM
MOUNT -T ISO9660 /DEV/CDROM /MNT/CDROM
CD /MNT/CDROM
LS
CP -R LINUX_x86 /TMP
CD /TMP
LS
CD LINUX *
LS
MORE RE*
LS
MORE INSTALL.CFG

./INSTALL.SH
LS
PWD
CD /MNT/CDROM
LD
LS
CD POL *
LS
CD LINUX *
LS
CD RED *
LS
CD 6.2
LS
PWD
CD /USR/LOCAL/BIN/TRIPWIRE
CD /USR/LOCAL
LS
CD TRIPWIRE
LS
CD TFS
LS
CD POLICY
LS
CP /MNT/CDROM/POLICYFILES/LINUX/REDHAT/6.2/TWPOL.TXT .
LS
CD ../BIN
```

Creating the tripwire files

```
./twadmin --create-polfile twpol.txt
./twadmin --create-polfile ./policy/twpol.txt
ls
```

Running tripwire (interactively)

```
./tripwire --hit
./tripwire --check --interactive
umount /dev/cdrom
eject
```

RUNNING TRIPWIRE (NON-INTERACTIVELY)

```
CD TRIPWIRE/TFS
LS
CD BIN
LS
./TRIPWIRE --CHECK
/sbin/identd
```

It is likely that the intruder has again gained root access at this point. Here they install knark.

```
cd /tmp
ls
gunzip knark.tar.gz
ls
tar xvf knark.tar
ls
cd knark*
ls -al
more README
ls
```

```
mount /dev/fd0 /mnt/floppy
ls
cd README /mnt/floppy
cp README /mnt/floppy
cd /tmp
```

And move it from the original directory (/tmp) to the target directory (/tmp/.../)

```
umount /dev/fd0
cd knark*
ls
make
ls
pwd
cd ...
cd ..
ls
ls -al
cp kna* ...
ls
cp -r kn*/tmp/...
ls
rm kna*
ls
rm -r ka*
rm kna*
rm -r kna*
ls
cd ...
ls
cd ka*
cd kn*
ls
```

Knark install is attempted

```
insmod knark
make instmod knark
find /-name insmod
find /-name insmod
/sbin/insmod knark
/sbin/insmod /tmp/.../knark
make
```

Knark is apparently running at this time

```
cd /proc
ls
cd knark
ls -al
```

INSTALL ANOTHER VERSION OF KNARK

```
MV KNARK KNARK.TAR.GZ
GUNZIP *.GZ
LS
TAR XVPF *.TAR
LS
CD *.50
LS
MORE RE*
MAKE
MAKE INSTALL
LS
```

RENAME THE TOOLS FILES FOR UNZIPPING, THEN UNZIP THEM.

```
MV TOOLS TOOLS.TAR.GZ
MV TOOLS2 TOOLS2.TAR.GZ
GUNZIP *.GZ
LS
TAR XVF T*.TAR
TAR XVF TOOLS.TAR
LS
TAR XVF TOOLS2.TAR
LS
```

OPEN AN LRK4 README FILE (USAGE).*

```
MORE USAGE*
LS
CD LRK4
LS
MORE README
LS
```

Attempt to install “lrk4”

```
make
more Makefile
vi Makefile
ls
make
more linsniffer.c
ls
make
vi l*.c
ls
cd ..
ls
more USAGE
more US*
```

ATTEMPT TO INSTALL “KIS”

```
LS
GUNZIP KIS_C*.GZ
LS
TAR XVF KIS *TAR
LS
CD KIS
CD KIS*
LS
MORE README
MORE README
MORE INSTALL
LS
./CONFIGURE
FIND / -NAME GTK
```

Move more tools to “/tmp/...”.

```
mv tool* .../
cd .../
ls
gunzip tools4.tar.gz
ls
tar xvf tools4.tar
ls
```

Install “adore”.

```
cd adore
ls
more README
ls
configure
./configure
ls
more Makefile
make
ls
make install
more README

ls
make clean; make
ls
ls -al
```

Start adore

```
./ava
./startadore
./ava h /tmp/.../
ls
more README
ls
./ava
./startadore
find / -name rmmmod
echo $PATH
path=$PATH:/sbin
path=$PATH:/sbin
export PATH
./startadore
echo $PATH
PATH=$PATH:/sbin
export PATH
echo $PATH
./startadore
./ava
```

```
.java h /tmp/.../
cd /tmp
ls -al
cd ...
.java
ls
```

FINALLY, POWER DOWN THE SYSTEM.

HALT

THE CRON (RUN REGULARLY) FILES COULD ALSO BE MALICIOUS FUNCTIONALITY.

```
[MICHAEL@LOCALHOST ETC]$ LS -AL CRON*
```

```
-RW-R--R-- 1 ROOT ROOT 255 AUG 28 1999 CRONTAB
```

CRON.D:

TOTAL 12

```
DRWXR-XR-X 2 ROOT ROOT 4096 FEB 4 2000 .
```

```
DRWXR-XR-X 29 ROOT ROOT 4096 JUL 5 18:13 ..
```

```
-RW-R--R-- 1 ROOT ROOT 86 FEB 18 2000 KMOD
```

CRON.DAILY:

TOTAL 36

```
DRWXR-XR-X 2 ROOT ROOT 4096 JUL 2 14:11 .
```

```
DRWXR-XR-X 29 ROOT ROOT 4096 JUL 5 18:13 ..
```

```
-RWXR-XR-X 1 ROOT ROOT 276 MAR 4 2000 0ANACRON
```

```
-RWXR-XR-X 1 ROOT ROOT 77 MAR 3 2000 INN-CRON-EXPIRE
```

```
-RWXR-XR-X 1 ROOT ROOT 53 MAR 3 2000 INN-CRON-RNEWS
```

```
-RWXR-XR-X 1 ROOT ROOT 51 FEB 25 2000 LOGROTATE
```

```
-RWXR-XR-X 1 ROOT ROOT 402 MAR 1 2000 MAKEWHATIS.CRON
```

```
-RWXR-XR-X 1 ROOT ROOT 102 FEB 4 2000 SLOCATE.CRON
```

```
-RWXR-XR-X 1 ROOT ROOT 104 FEB 15 2000 TMPWATCH
```

CRON.HOURLY:

TOTAL 12

```
DRWXR-XR-X 2 ROOT ROOT 4096 AUG 28 1999 .
```

```
DRWXR-XR-X 29 ROOT ROOT 4096 JUL 5 18:13 ..
```

```
-RWXR-XR-X 1 ROOT ROOT 65 MAR 3 2000 INN-CRON-NNTPSEND
```

CRON.MONTHLY:

TOTAL 12

```
DRWXR-XR-X 2 ROOT ROOT 4096 AUG 28 1999 .
```

```
DRWXR-XR-X 29 ROOT ROOT 4096 JUL 5 18:13 ..
```

```
-RWXR-XR-X 1 ROOT ROOT 278 MAR 4 2000 0ANACRON
```

CRON.WEEKLY:

TOTAL 16

```
DRWXR-XR-X 2 ROOT ROOT 4096 JUL 2 14:11 .
```

```
DRWXR-XR-X 29 ROOT ROOT 4096 JUL 5 18:13 ..
```

```
-RWXR-XR-X 1 ROOT ROOT 277 MAR 4 2000 0ANACRON
```

```
-RWXR-XR-X 1 ROOT ROOT 399 MAR 1 2000 MAKEWHATIS.CRON
```

```
[MICHAEL@LOCALHOST ETC]$
```

ALL THESE FILES ARE EXPECTED VERSIONS.

TIME-LINE ANALYSIS

NOTE: DUE TO A DISCREPANCY BETWEEN THE TIMEZONE ON THE ANALYSIS COMPUTER AND THE DISK IMAGE, ALL TIMES LISTED ARE 12 HOURS SLOW. FOR THE LOCAL TIMES THAT THE LISTED TIMES RELATE TO, ADD 12 HOURS TO EACH TIME.

eg. TimeLine listing

```
Sat Jul 05 2003 07:05:07 3788800 .a. -r-w-r--r-- wayne wayne 162927 /tmp/.../tools.tar
```

Vs.

Mount file listing

```

[root@localhost ...]# ls -lu
total 7940
drwxr-xr-x  3 30   root    4096 Jul 5 19:38 adore
drwxrwxrwx  3 michael michael 4096 Jul 5 19:38 kis_client-0.9
-rw-r--r--  1 1001 1001   256000 Jul 5 19:15 kis_client-0.9.tar
-rw-r--r--  1 1001 1001   28998 Jul 5 19:05 kis_server-0.9.tar.gz
drwxr-xr-x  3 root   root    4096 Jul 5 19:38 knark-0.50
drwxr-xr-x  3 root   root    4096 Jul 5 19:38 knark-0.59
-rw-r--r--  1 michael michael 61440 Jul 5 18:46 knark.tar
drwxr-xr-x  18 root   root    4096 Jul 5 19:38 lrk4
-rw-r--r--  1 michael michael 92160 Jul 5 19:05 tools2.tar
-rw-r--r--  1 michael michael 3788800 Jul 5 19:28 tools3.tar
-rw-r--r--  1 michael michael 51200 Jul 5 19:31 tools4.tar
-rw-r--r--  1 michael michael 3788800 Jul 5 19:05 tools.tar
-rw-r--r--  1 1001 1001   4217 Jul 5 19:14 USAGE.TXT
[root@localhost ...]#

```

THIS TIMELINE WAS CREATED FROM THE TIME RANGE JAN 1ST, 2002 - JAN 1ST, 2004. SOME OF THE FILES ARE DISPLAYED WITH THEIR ORIGINAL CREATION DATE S. THIS OCCURS WHERE THEY ARE COMPRESSED ALONG WITH THEIR ORIGINAL DATES , AND THE PROGRAM USED TO DECOMPRESS THEM ALSO EXTRACTS THE DATES AND USES THEM ON THE NEW SYSTEM . FOR EXAMPLE , THE TRIPWIRE FILES ARE LISTED AS BEING FROM MAY, WHICH IS KNOWN TO BE BEFORE THE SYSTEM WAS INSTALLED .

```

Tue May 14 2002 10:00:00 5554608 m.. -f-x---- root/wroot root 145959 /usr/local/tripwire/tfs/bin/tripwire
552231 m.. -f-r--r-- root/wroot root 145975 /usr/local/tripwire/tfs/documents/tfs_userguide.pdf
6355 m.. -f-r--r-- root/wroot root 145969 /usr/local/tripwire/tfs/man/man8/twagent8

```

THE OPERATING SYSTEM INSTALLATION WAS STARTED

```

TUE JUL 01 2003 22:53:36 237 M.C -f-RW-R--R-- ROOT/WROOT ROOT 48757 /BOOT/KERNEL.H
TUE JUL 01 2003 22:53:37 2635 A. -f-RW-R--R-- ROOT/WROOT ROOT 114836 /VAR/LOG/DMESG
TUE JUL 01 2003 22:53:53 4096 M.C D/DRWX----- ROOT/WROOT ROOT 177690 /VAR/LIB/NFS/SM.BAK
0 MAC C/CRW----- ROOT/WROOT ROOT 35342 /DEV/APM_BIOS
4096 M.C D/DRWX----- ROOT/WROOT ROOT 177689 /VAR/LIB/NFS/SM
0 MAC L/CRW----- ROOT/WROOT ROOT 35342 /ETC/RC.D/RC1.D/K83YPBIND (DELETED-REALLOC)
4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 1819 /VAR/LIB/NFS
TUE JUL 01 2003 22:53:55 56333 A. -f-RW-R--R-- ROOT/WROOT ROOT 114837 /VAR/LOG/BOOT.LOG
TUE JUL 01 2003 22:53:59 14394 A. -f-RW----- ROOT/WROOT ROOT 114838 /VAR/LOG/CRON
TUE JUL 01 2003 22:54:01 4 A. -f-RW-R--R-- ROOT/WROOT ROOT 50470 /VAR/SPOOL/LPD/LPD.LOCK
4096 M.C D/DRWXR-XR-X ROOT/WROOT DAEMON 49827 /VAR/SPOOL/LPD
TUE JUL 01 2003 22:54:12 4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 96793 /USR/SHARE/FONTS/DEFAULT/GHOSTSCRIPT
4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 50327 /USR/SHARE/FONTS/DEFAULT/TTYPE1

```

A delay caused the install to pause for 3 hours, possibly requiring user input.

```

Wed Jul 02 2003 01:22:59 20 ma. l/rwxrwxrwx root/wroot root 35347 /etc/rc.d/rc6.d/K83ypbind -> ../init.d/fakeidentd (deleted)
20 ma. l/rwxrwxrwx root/wroot root 35367 /etc/rc.d/rc4.d/K25fakeidentd -> ../init.d/fakeidentd fs (deleted)
20 ma. l/rwxrwxrwx root/wroot root 35347 /etc/rc.d/rc5.d/S80fakeidentd -> ../init.d/fakeidentd daytable (deleted)
20 ma. l/rwxrwxrwx root/wroot root 35367 <RH_Partition_1.dd-dead-35367>
20 m.. l/rwxrwxrwx root/wroot root 35365 <RH_Partition_1.dd-dead-35365>
20 ma. l/rwxrwxrwx root/wroot root 35347 <RH_Partition_1.dd-dead-35347>

```

THE MAIN FILE INSTALL PROCESS BEGINS

```

Wed Jul 02 2003 02:05:22 2239 A. -f-RW-R--R-- ROOT/WROOT ROOT 162688 /TMP/UPGRADE.LOG
Wed Jul 02 2003 02:06:27 161 ..C -f-RW-R--R-- ROOT/WROOT ROOT 80168 /ETC/HOSTS.ALLOW
547 ..C -f-RW-R--R-- ROOT/WROOT ROOT 80174 /ETC/PROFILE

```

VARIOUS SYSTEM BINARIES ARE INSTALLED

```

Wed Jul 02 2003 02:11:15 6 ..C L/LRwxrwxrwx ROOT/WROOT ROOT 114051 /SBIN/SWAPOFF -> SWAPON B
1606 ..C -f-RW-R--R-- ROOT/WROOT ROOT 145330 /USR/MAN/MAN8/LMOUNT.8.GZ
26608 ..C -f-RWSR-XR-X ROOT/WROOT ROOT 145326 /BIN/UMOUNT
12599 ..C -f-RW-R--R-- ROOT/WROOT ROOT 145327 /USR/MAN/MAN8/MOUNT.8.GZ
56208 ..C -f-RWSR-XR-X ROOT/WROOT ROOT 145325 /BIN/MOUNT
6200 ..C -f-RWXR-XR-X ROOT/WROOT ROOT 114048 /SBIN/SWAPON

```

The RedHat Package Manager is installed

```

Wed Jul 02 2003 02:11:36 4096 ..c d/dnwxr-xr-x root/wroot root 50209 /etc/rpm
222 ..c -f-rwxr-xr-x root/wroot root 145555 /usr/bin/gendiff
886424 ..c -f-rwxr-xr-x root/wroot root 145541 /bin/rpm
Wed Jul 02 2003 02:11:37 695192 ..c -f-rwxr-xr-x root/wroot root 145556 /usr/bin/rpm2cpio
Wed Jul 02 2003 02:11:38 1288 ..c -f-rwxr-xr-x root/wroot root 176862 /usr/lib/rpm/brp-compress
1212 ..c -f-rwxr-xr-x root/wroot root 176872 /usr/lib/rpm/find-requires

```

OTHER DELAYS OCCUR DURING THE INSTALL PROCESS

```
Wed Jul 02 2003 02:12:26 160 ..c-/-rw-r--r- root/wroot root 82665 /ETC/LILO.CONF.RPMSAVE
Wed Jul 02 2003 02:12:27 160 M.C-/-RW-R--R- ROOT/WROOT ROOT 82400 /ETC/LILO.CO NF
160 M.C-/-RW-R--R- ROOT/WROOT ROOT 82400 /USR/SHARE/LOCALE/SK/LC_MESSAGES/TIMECONFIG.MO-RPMDDELETE
(DELETED-REALLOC)
Wed Jul 02 2003 02:12:31 10240 M.C-/-RW----- ROOT/WROOT ROOT 50674 /BOOT/MAP
10240 M.C-/-RW----- ROOT/WROOT ROOT 50674 /BOOT/MAP~ (DELETED-REALLOC)
Wed Jul 02 2003 02:14:33 34 ..c-/-RW-R--R- ROOT/WROOT ROOT 82662 /ETC/CONF.MODULES~
51 M.C-/-RW-R--R- ROOT/WROOT ROOT 82739 /ETC/CONF.MODULES
Wed Jul 02 2003 02:14:58 95 M.C-/-RW-R--R- ROOT/WROOT ROOT 98809 /ETC/SYSCONFIG/NETWORK-SCRIPTS/IFCFG-ETH0
4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 97079 /ETC/SYSCONFIG/NETWORK-SCRIPTS
Wed Jul 02 2003 02:38:03 26736 ..c-/-RWXR-XR-X ROOT/WROOT ROOT 18091 /USR/SBIN/IDENTD.O.Orig
Wed Jul 02 2003 03:43:06 18424 M.C-/-R--RW-R-- ROOT/WROOT MAN 177691 /VAR/CATMAN/CAT8/TCPDUMP.8.GZ
Wed Jul 02 2003 03:51:58 18424 .A.-/R--RW-R-- ROOT/WROOT MAN 177691 /VAR/CATMAN/CAT8/TCPDUMP.8.GZ
Wed Jul 02 2003 04:00:32 16384 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 160325 /USR/MAN/MAN1
Wed Jul 02 2003 04:04:55 11092 M.C-/-RWXR-XR-X ROOT/WROOT ROOT 18728 /USR/SBIN/CIDENTD
3004 M.C-/-RWXR-XR-X ROOT/WROOT ROOT 162904 /USR/MAN/MAN1/CIDENTD.1
Wed Jul 02 2003 05:12:13 95547 M.C-/-RW-R--R- ROOT/WROOT ROOT 162903 /TMP/LAME1
Wed Jul 02 2003 05:24:27 20 .A.LRWXRWXRX ROOT/WROOT ROOT 35365 <RH_PARTITION_1.DD-DEAD-35365>
Wed Jul 02 2003 05:26:20 0 MA.SRW-RW-RW- ROOT/WROOT ROOT 35360 <RH_PARTITION_1.DD-DEAD-35360>
0 MA.-/SRW-RW-RW- ROOT/WROOT ROOT 35360 /USR/LIB/LIBZ.SO.1.1.3-RPMDDELETE (DELETED)
```

The "lame1" file is created, at the same size as the current version.

```
Wed Jul 02 2003 04:04:55 11092 m.c-/-rwxr-xr-x root/wroot root 18728 /usr/sbin/cidentd
3004 m.c-/-rwxr-xr-x root/wroot root 162904 /usr/man/man1/cidentd.1
Wed Jul 02 2003 05:12:13 95547 m.c-/-rw-r--r- root/wroot root 162903 /tmp/lame1
Wed Jul 02 2003 05:24:27 20 a.lrwxrwxrx root/wroot root 35365 <RH_Partition_1.dd-dead-35365>
```

THE INSTALLATION PROC ESS CONTINUES

```
Wed Jul 02 2003 13:47:08 16384 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 11 /LOST+FOUND
0 MAC----- ROOT/WROOT ROOT 1 <RH_PARTITION_1.DD-ALIVE-1>
Wed Jul 02 2003 13:47:41 4096 MAC D/DRWXR-XR-X ROOT/WROOT ROOT 32065 /PROC
Wed Jul 02 2003 13:47:44 5659 .A.-/RW-R--R- ROOT/WROOT ROOT 160322 /TMP/INSTALL.LOG
Wed Jul 02 2003 13:48:00 9748 ..c-/-RW-R--R- ROOT/WROOT ROOT 32069 /USR/LIB/LIBEFENCE.A
1574 ..c-/-RW-R--R- ROOT/WROOT ROOT 16036 /USR/DOC/ELECTRICFENCE-2.1/README
5591 ..c-/-RW-R--R- ROOT/WROOT ROOT 64133 /USR/MAN/MAN3/LIBEFENCE.3.GZ
17976 ..c-/-RW-R--R- ROOT/WROOT ROOT 16035 /USR/DOC/ELECTRICFENCE-2.1/COPYING
940 ..c-/-RW-R--R- ROOT/WROOT ROOT 16034 /USR/DOC/ELECTRICFENCE-2.1/CHANGES
4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 16033 /USR/DOC/ELECTRICFENCE-2.1
50 ..c-/-RW-R--R- ROOT/WROOT ROOT 64132 /USR/MAN/MAN3/EFENCE.3.GZ
```

THE MANUAL "MAN" PAGES ARE INSTALLED

```
Wed Jul 02 2003 13:56:04 59568 ..c-/-RWXR-XR-X ROOT/WROOT ROOT 145264 /USR/BIN/SB
55504 ..c-/-RWXR-XR-X ROOT/WROOT ROOT 145263 /USR/BIN/RZ
16872 ..c-/-R-SR-SR-X ROOT/WROOT LP 145256 /USR/BIN/LPQ
59568 ..c-/-RWXR-XR-X ROOT/WROOT ROOT 145264 /USR/BIN/SZ
2239 ..c-/-RW-R--R- ROOT/WROOT ROOT 162069 /USR/MAN/MAN1/LPRM.1.GZ
1176 ..c-/-RWXR-XR-X ROOT/WROOT ROOT 162065 /ETC/RC.D/INIT.D/LPD
59568 ..c-/-RWXR-XR-X ROOT/WROOT ROOT 145264 /USR/BIN/SX
3435 ..c-/-RW-R--R- ROOT/WROOT ROOT 97938 /USR/MAN/MAN5/PRINTCAP.5.GZ
51696 ..c-/-RWXR--R- ROOT/WROOT ROOT 17827 /USR/SBIN/LPD
25064 ..c-/-RWXR-SR-X ROOT/WROOT LP 17826 /USR/SBIN/LPC
3261 ..c-/-RW-R--R- ROOT/WROOT ROOT T 162068 /USR/MAN/MAN1/LPR.1.GZ
1875 ..c-/-RW-R--R- ROOT/WROOT ROOT 145262 /USR/MAN/MAN8/PAC.8.GZ
```

The man pages are extracted

```
Wed Jul 02 2003 13:56:10 8 m..l/lrwxrwxrx root/wroot root 162082 /usr/man/man1/manpath.1.gz-> man.1.gz
3 m..l/lrwxrwxrx root/wroot root 145276 /usr/bin/manpath-> man
Wed Jul 02 2003 13:56:13 2873 ..c-/-rw-r--r- root/wroot root 1761 /usr/doc/man-pages-1.28/COPYING
4096 m.c d/drwxr-xr-x root/wroot root 1760 /usr/doc/man-pages-1.28
1124 ..c-/-rw-r--r- root/wroot root 1762 /usr/doc/man-pages-1.28/README
Wed Jul 02 2003 13:56:25 2840 ..c-/-rw-r--r- root/wroot man 17860 /usr/man/man2/execute.2.gz
1850 ..c-/-rw-r--r- root/wroot man 17958 /usr/man/man2/readv.2.gz
1878 ..c-/-rw-r--r- root/wroot man 17896 /usr/man/man2/getsockname.2.gz
1504 ..c-/-rw-r--r- root/wroot man 17839 /usr/man/man2/auct.2.gz
48 ..c-/-rw-r--r- root/wroot man 17836 /usr/man/man2/_sysctl.2.gz
```

THE PLUGGABLE AUTHENTICATION MODULE IS INSTALLED

```
Wed Jul 02 2003 13:59:40 250 M.C-/-RW-R--R- ROOT/WROOT ROOT 82323 /ETC/PAM.D/PASSWD
372 M..-/-RW----- ROOT/WROOT ROOT 82661 /ETC/GSHADOW-
437 M.C-/-RW-R--R- ROOT/WROOT ROOT 80179 /ETC/PAM.D/LOGIN
446 M..-/-RW----- ROOT/WROOT ROOT 80419 /ETC/GROUP-
443 M.C-/-RW-R--R- ROOT/WROOT ROOT 82447 /ETC/PAM.D/RLOGIN
361 M.C-/-RW-R--R- ROOT/WROOT ROOT 82658 /ETC/YP.CONF
32 M.C-/-RW-R--R- ROOT/WROOT ROOT 82657 /ETC/SYSCONFIG/NETWORK
```

USER ACCOUNTS ARE SET UP

```
Wed Jul 02 2003 13:59:43 333 MAC -/RWXR-XR-X WAYNE WAYNE 50450 /HOME/WAYNE/.EMACS
Wed Jul 02 2003 13:59:44 230 M.C -/RW-R-R- WAYNE WAYNE 50452 /HOME/WAYNE/.BASH_PROFILE
446 ..C -/RW- - - - - ROOT/WROOT ROOT 80419 /ETC/GROUP-
372 ..C -/RW- - - - - ROOT/WROOT ROOT 82661 /ETC/GSHADOW-
3394 MAC -/RW-R-R- WAYNE WAYNE 50454 /HOME/WAYNE/.SCREENRC
124 M.C -/RW-R-R- WAYNE WAYNE 50453 /HOME/WAYNE/.BASHRC
382 M.C -/R- - - - - ROOT/WROOT ROOT 82666 /ETC/GSHADOW
459 M.C -/RW-R-R- ROOT/WROOT ROOT 82648 /ETC/GROUP
24 M.C -/RW-R-R- WAYNE WAYNE 50451 /HOME/WAYNE/.BASH_LOGOUT
700 M.C -/RW-R-R- ROOT/WROOT ROOT 82664 /ETC/PASSWD.OLD
Wed Jul 02 2003 13:59:45 0 M.C -/RW-R-R- ROOT/WROOT ROOT 82660 /ETC/SYSCONF/DESKTOP
870 M.C -/RW-R-R- ROOT/WROOT ROOT 80178 /ETC/LOCALTIME
44 M.C -/RW-R-R- ROOT/WROOT ROOT 82103 /ETC/SYSCONF/CLOCK
Wed Jul 02 2003 13:59:48 34 M. -/RW-R-R- ROOT/WROOT ROOT 82662 /ETC/CONF/MODULES~
38 M.C -/RW-R-R- ROOT/WROOT ROOT 81639 /ETC/SYSCONF/PCMCIA
Wed Jul 02 2003 14:00:03 160 M. -/RW-R-R- ROOT/WROOT ROOT 82665 /ETC/LILO.CONF.RPMSAVE
Wed Jul 02 2003 14:00:04 512 M.C -/RW-R-R- ROOT/WROOT ROOT 50456 /BOOT/BOOT.0300
```

THE INSTALLATION CONT INUES

```
Wed Jul 02 2003 16:02:00 9 MAC -/RW- - - - - ROOT/WROOT ROOT 145916 /VAR/SPOOL/ANACRON/CRON.DAILY
4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 144586 /VAR/SPOOL/ANACRON
Wed Jul 02 2003 16:02:01 380 MAC -/RW-R-R- ROOT/WROOT ROOT 98810 /VAR/LIB/LOGROTATE.STATUS
4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 96193 /VAR/LB
Wed Jul 02 2003 16:02:02 6057 .A -/RW-R-R- ROOT/WROOT ROOT 160534 /USR/MAN/MAN1/TACK.1.GZ
2145 .A -/RW-R-R- ROOT/WROOT ROOT 160522 /USR/MAN/MAN1/MKTEMP.1.GZ
1480 .A -/RW-R-R- ROOT/WROOT ROOT 160533 /USR/MAN/MAN1/INFOTOCAP.1M.GZ
```

THE INSTALLATION COMP LETES

```
Wed Jul 02 2003 16:04:42 261409 M.C -/RW-R- - - - ROOT/WROOT SLOCATE 82741 /VAR/LIB/SLOCATE/SLOCATE.DB
261409 M.C -/RW-R- - - - ROOT/WROOT SLOCATE 82741 /VAR/LIB/SLOCATE/SLOCATE.DB.TMP (DELETED-REALLOC)
4096 M.C D/DRWXR-X- - - ROOT/WROOT SLOCATE 80600 /VAR/LIB/SLOCATE
```

THE FAKE IDENT SERVICE IS INST ALLED

```
Thu Jul 03 2003 01:08:48 405 M.C -/RWXR-XR-X ROOT/WROOT ROOT 66712 /TMP/FAKEIDENTD-1.2/FAKEIDENTD
12412 M.C -/RWXR-XR-X ROOT/WROOT ROOT 66711 /TMP/FAKEIDENTD-1.2/IDENTD.C
Thu Jul 03 2003 01:08:49 1771 M.C -/RWXR-XR-X ROOT/WROOT ROOT 66713 /TMP/FAKEIDENTD-1.2/MAKEFILE
19027 .A -/RWXR-XR-X ROOT/WROOT ROOT 66714 /TMP/FAKEIDENTD-1.2/COPYING
Thu Jul 03 2003 01:08:50 1761 MAC -/RWXR-XR-X ROOT/WROOT ROOT 66717 /TMP/FAKEIDENTD-1.2/MAKEFILE~
246 MAC -/RWXR-XR-X ROOT/WROOT ROOT 66715 /TMP/FAKEIDENTD-1.2/INSTALL
19027 M.C -/RWXR-XR-X ROOT/WROOT ROOT 66714 /TMP/FAKEIDENTD-1.2/COPYING
1905 MAC -/RWXR-XR-X ROOT/WROOT ROOT 66716 /TMP/FAKEIDENTD-1.2/README
Thu Jul 03 2003 01:09:09 7086 .A -/RW-R-R- ROOT/WROOT ROOT 145557 /USR/MAN/MAN8/RPM.8.GZ
4096 M.C D/DRWXRWXR-X ROOT/WROOT MAN 176760 /VAR/CATMAN/CAT8
Thu Jul 03 2003 01:09:12 8783 MAC -/R-R-RW-R- ROOT/WROOT MAN 178936 /VAR/CATMAN/CAT8/RPM.8.GZ
Thu Jul 03 2003 01:10:44 20 ..C/L/RWXRWXRX ROOT/WROOT ROOT 35367 /ETC/RC.D/RC4.D/K25FAKEIDENTD ->
./INIT.D/FAKEIDENTDFS (DELETED)
4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 32357 /ETC/RC.D/RC1.D
49152 MAC -/RW-R-R- ROOT/WROOT ROOT 177697 /VAR/LIB/RPM/PROVIDESINDEX.RPM
16384 MAC -/RW-R-R- ROOT/WROOT ROOT 177699 /VAR/LIB/RPM/CONFLICTSINDEX.RPM
16384 MAC -/RW-R-R- ROOT/WROOT ROOT 177695 /VAR/LIB/RPM/NAMEINDEX.RPM
4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 32359 /ETC/RC.D/RC3.D
4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 16040 /USR/SBIN
20 ..C/LRWXRWXRX ROOT/WROOT ROOT 35365 <RH_PARTITION_1.DD-DEAD-35365>
16384 MAC -/RW-R-R- ROOT/WROOT ROOT 177700 /VAR/LIB/RPM/GROUPINDEX.RPM
20 ..C/LRWXRWXRX ROOT/WROOT ROOT 35347 <RH_PARTITION_1.DD-DEAD-35347>
4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 32360 /ETC/RC.D/RC4.D
20 ..C/LRWXRWXRX ROOT/WROOT ROOT 35367 <RH_PARTITION_1.DD-DEAD-35367>
56 MAC -/RW-R-R- ROOT/WROOT ROOT 35366 /VAR/TMP/RPM-TMP.82031 (DELETED)
4096 M.C D/DRWXRWXRWX ROOT/WROOT ROOT 32077 /VAR/TMP
4136456 MAC -/RW-R-R- ROOT/WROOT ROOT 177694 /VAR/LIB/RPM/PACKAGES.RPM
16384 MAC -/RW-R-R- ROOT/WROOT ROOT 177701 /VAR/LIB/RPM/TRIGGERINDEX.RPM
56 MAC -/RW-R-R- ROOT/WROOT ROOT 35366 <RH_PARTITION_1.DD-DEAD-35366>
4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 32361 /ETC/RC.D/RC5.D
49152 MAC -/RW-R-R- ROOT/WROOT ROOT 177698 /VAR/LIB/RPM/REQUIREDBY.RPM
1343488 MAC -/RW-R-R- ROOT/WROOT ROOT 177696 /VAR/LIB/RPM/FILEINDEX.RPM
20 ..C/LRWXRWXRXRX ROOT/WROOT ROOT 35347 /ETC/RC.D/RC5.D/S80FAKEIDENTD -> ./INIT.D/FAKEIDENTDEYTABLE
(DELETED)
20 ..C/LRWXRWXRXRX ROOT/WROOT ROOT 35347 /ETC/RC.D/RC6.D/K83YPBIND -> ./INIT.D/FAKEIDENTD (DELETED)
Thu Jul 03 2003 01:12:38 4096 M.C D/DRWXR-XR-X ROOT/WROOT ROOT 112229 /SBIN
3078 M.C -/RW-R-R- ROOT/WROOT ROOT 81436 /ETC/INETD.CONF
Thu Jul 03 2003 01:39:44 96 M.C -/RW-R-R- ROOT/WROOT ROOT 82656 /ETC/HOSTS
Thu Jul 03 2003 01:51:21 0 ..C/SRW-RW-RW- ROOT/WROOT ROOT 35360 <RH_PARTITION_1.DD-DEAD-35360>
0 ..C/SRW-RW-RW- ROOT/WROOT ROOT 35360 /USR/LIB/LIBZ.SO.1.1.3-RPMDELETE (DELETED)
Thu Jul 03 2003 02:18:55 1771 .A -/RWXR-XR-X ROOT/WROOT ROOT 66713 /TMP/FAKEIDENTD-1.2/MAKEFILE
12412 .A -/RWXR-XR-X ROOT/WROOT ROOT 66711 /TMP/FAKEIDENTD-1.2/IDENTD.C
Thu Jul 03 2003 02:18:57 4096 M. D/DRWXR-XR-X ROOT/WROOT ROOT 66708 /TMP/FAKEIDENTD-1.2
4096 M. -/DRWXR-XR-X ROOT/WROOT ROOT 66708 /USR/MAN/MAN6/BANNER.6.GZ-RPMDELETE (DELETED-REALLOC)
Thu Jul 03 2003 02:18:58 20113 M.C -/RWXR-XR-X ROOT/WROOT ROOT 114842 /SBIN/IDENT
```

```

27 M.C./LRWXRWXRWX ROOT/WROOT ROOT 35346 /ETC/RC.D/RC5.D/K83YPBIND -> /ETC/RC.D/INIT.D/FAKEIDENTD
(DELETED-REALLOC)
405 M.C./-RWXR-XR-X ROOT/WROOT ROOT 162686 /ETC/RC.D/INIT.D/FAKEIDENTD
20113 MAC -/RWXR-XR-X ROOT/WROOT ROOT 66718 /TMP/FAKEIDENTD-1.2/IDENTD
405 A.-/RWXR-XR-X ROOT/WROOT ROOT 66712 /TMP/FAKEIDENTD-1.2/FAKEIDENTD
9 M.C./-RW-R-R- ROOT/WROOT ROOT 82742 /ETC/IDENTUSER
9 MAC -/RW-R-R- ROOT/WROOT ROOT 66719 /TMP/FAKEIDENTD-1.2/IDENTUSER
4096 M.C.D/DRWXR-XR-X ROOT/WROOT ROOT 160653 /ETC/RC.D/RC0.D
4096 M.C.D/DRWXR-XR-X ROOT/WROOT ROOT 32362 /ETC/RC.D/RC6.D
4096 M.C.D/DRWXR-XR-X ROOT/WROOT ROOT 32358 /ETC/RC.D/RC2.D
27 M.C./LRWXRWXRWX ROOT/WROOT ROOT 35346 /ETC/RC.D/RC3.D/S80FAKEIDENTD -> /ETC/RC.D/INIT.D/FAKEIDENTDNA
(DELETED-REALLOC)
4096 M.C.D/DRWXR-XR-X ROOT/WROOT ROOT 160652 /ETC/RC.D/INIT.D
27 M.C./LRWXRWXRWX ROOT/WROOT ROOT 162687 /ETC/RC.D/RC0.D/K45FAKEIDENTD -> /ETC/RC.D/INIT.D/FAKEIDENTD
27 M.C./LRWXRWXRWX ROOT/WROOT ROOT 35346 /ETC/RC.D/RC6.D/K45FAKEIDENTD -> /ETC/RC.D/INIT.D/FAKEIDENTD
M.C. 35345 /ETC/RC.D/RC2.D/S45FAKEIDENTD -> /ETC/RC.D/INIT.D/FAKEIDENTDN.A
27 M.C./LRWXRWXRWX ROOT/WROOT ROOT 35345 /ETC/RC.D/RC4.D/K83YPBIND -> /ETC/RC.D/INIT.D/FAKEIDENTD
(DELETED-REALLOC)

```

USER "WAYNE"'S SETTINGS ARE MODIFIED

```

SAT JUL 05 2003 01:10:31 124 A.-/RW-R-R- WAYNE WAYNE 50453 /HOME/WAYNE/.BASHRC
230 A.-/RW-R-R- WAYNE WAYNE 50452 /HOME/WAYNE/.BASH_PROFILE
19 A.-/RW----- WAYNE WAYNE 50690 /VAR/SPOOL/MQ/QUEUE/Q/PAA00987 (DELETED-REALLOC)
19 A.-/RW----- WAYNE WAYNE 50690 /HOME/WAYNE/.BASH_HISTORY
194394 A.-/RW-R-R- ROOT/WROOT ROOT 50690 /VAR/LOCK/SUBSYS/XFS (DELETED-REALLOC)
SAT JUL 05 2003 01:11:27 4096 M.C.D/DRWXR-X- ROOT/WROOT ROOT 96198 /ROOT
SAT JUL 05 2003 01:11:51 19 M.C./-RW----- WAYNE WAYNE 50690 /HOME/WAYNE/.BASH_HISTORY
19 M.C./-RW----- WAYNE WAYNE 50690 /VAR/SPOOL/MQ/QUEUE/Q/PAA00987 (DELETED-REALLOC)
24 A.-/RW-R-R- WAYNE WAYNE 50451 /HOME/WAYNE/.BASH_LOGOUT
194394 M.C./-RW-R-R- ROOT/WROOT ROOT 50690 /VAR/LOCK/SUBSYS/XFS (DELETED-REALLOC)

```

Someone accesses and modifies the passwd and shadow files (possibly using vi or a similar editor – “shadow~” and “passwd~” are created)

```

Sat Jul 05 2003 01:15:35 717 m.-/r----- root/wroot root 82321 /etc/shadow-
Sat Jul 05 2003 01:17:47 24 a.-/r-r-r-- root/wroot root 98337 /root/bash_logout
Sat Jul 05 2003 01:19:54 799 m.-/r-r-r-- root/wroot root 80509 /etc/passwd-
Sat Jul 05 2003 01:20:34 775 m.c.-/r----- root/wroot root 82745 /etc/shadow
799 ac-/r-r-r-- root/wroot root 80509 /etc/passwd-
799 m.c.-/r-r-r-- root/wroot root 82655 /etc/passwd
717 .c-/r----- root/wroot root 82321 /etc/shadow-
Sat Jul 05 2003 02:03:34 8 m.c.-/r-r-r-- root/wroot root 82667 /etc/HOSTNAME

```

TRIPWIRE IS INSTALLED

```

SAT JUL 05 2003 03:23:57 14031 M.C./-R-R-R- ROOT/WROOT ROOT 2583 /TMP/LINUX_X86/LICENSE.TXT
29648 M.C./-R-R-R- ROOT/WROOT ROOT 2585 /TMP/LINUX_X86/RELEASE_NOTES
3778320 A.-/R-XR-XR-X ROOT/WROOT ROOT 145926 /TMP/LINUX_X86/BIN/SIGGEN
8337 M.C./-R-R-R- ROOT/WROOT ROOT 2584 /TMP/LINUX_X86/README

```

Various files including "lame1" are accessed.

```

Sat Jul 05 2003 06:12:09 3460 a.-/r-r-r-- root/wroot root 97239 /lib/modules/2.2.14-5.0/fs/nls_iso8859-1.o
45405 a.-/r-r-r-- root/wroot root 97214 /lib/modules/2.2.14-5.0/fs/fat.o
5172 a.-/r-r-r-- root/wroot root 97223 /lib/modules/2.2.14-5.0/fs/nls_cp437.o
15741 a.-/r-r-r-- root/wroot root 97256 /lib/modules/2.2.14-5.0/fs/fat.o
28633 a.-/r-r-r-- root/wroot root 82668 /lib/modules/2.2.14-5.0/modules.dep
Sat Jul 05 2003 06:12:46 95547 a.-/r-r-r-- root/wroot root 162903 /tmp/lame1
Sat Jul 05 2003 06:13:08 63 a.-/r-r-r-- root/wroot root 162683 /tmp/identIV
Sat Jul 05 2003 06:13:25 90 mac-/r-r-r-- root/wroot root 82766 /etc/mtab
4096 m.c.d/drwxr-xr-x root/wroot root 80161 /etc
90 mac-/r-r-r-- root/wroot root 82766 /etc/mtab.tmp (deleted-realloc)

```

THE KNARK ROOTKIT IS EXTRACTED .

```

SAT JUL 05 2003 06:23:21 14975 MAC -/RWXR-XR-X ROOT/WROOT ROOT 66729 /TMP/.../KNARK-0.59/REXEC
1644 MAC -/RW-R-R- ROOT/WROOT ROOT 2604 /TMP/.../KNARK-0.59/SRC/ROOTME.O
3530 MAC -/RW-R-R- ROOT/WROOT ROOT 2600 /TMP/.../KNARK-0.59/SRC/REXEC.C
4096 M.C.D/DRWXR-XR-X ROOT/WROOT ROOT 2592 /TMP/.../KNARK-0.59/SRC

```

The tools.tar and tools2.tar files are copied onto the system .

```

Sat Jul 05 2003 06:47:39 1427 a.-/r-r-r-- root/wroot root 178933 /tmp/.../knark-0.50/Makefile
Sat Jul 05 2003 07:03:18 3788800 m.-/r-r-r-- wayne wayne 162927 /tmp/.../tools.tar
Sat Jul 05 2003 07:03:29 92160 m.-/r-r-r-- wayne wayne 162920 /tmp/.../tools2.tar
Sat Jul 05 2003 07:04:24 92160 .c-/r-r-r-- wayne wayne 162920 /tmp/.../tools2.tar
3788800 .c-/r-r-r-- wayne wayne 162927 /tmp/.../tools.tar

```

The files are extracted (from the lack of time between the completion of the “kis”

extraction, and “tools2.tar” being extracted, these were likely done with a single command.)

```
Sat Jul 05 2003 07:05:07 3788800 .a. -/rw-r--r-- wayne wayne 162927 /tmp/.../tools.tar
Sat Jul 05 2003 07:05:24 4217 ..c -/rw-r--r-- 1001 1001 162970 /tmp/.../USAGE.TXT
28998 .ac -/rw-r--r-- 1001 1001 162969 /tmp/.../kis_server-0.9.tar.gz
92160 .a. -/rw-r--r-- wayne wayne 162920 /tmp/.../tools2.tar
```

LRK IS EXTRACTED FROM TOOLS2.TAR

```
SAT JUL 05 2003 07:12:03 18571 MAC -/RWXR-XR-X ROOT/WROOT ROOT 130940 /TMP/.../LRK4/FIX
SAT JUL 05 2003 07:12:04 13496 MAC -/RWXR-XR-X ROOT/WROOT ROOT 130941 /TMP/.../LRK4/Z2
SAT JUL 05 2003 07:12:05 15608 MAC -/RWXR-XR-X ROOT/WROOT ROOT 130942 /TMP/.../LRK4/WTED
SAT JUL 05 2003 07:12:21 0 MAC -/RW----- ROOT/WROOT ROOT 130944 /TMP/.../LRK4/LINSNIFFER.C.SWX (DELETED)
```

The kis tar file is extracted

```
Sat Jul 05 2003 07:14:45 256000 ..c -/rw-r--r-- 1001 1001 162971 /tmp/.../kis_client-0.9.tar
Sat Jul 05 2003 07:15:01 17992 .a. -/rw-r--r-- wayne wayne 179003 /tmp/.../kis_client-0.9/COPYING
0 .a. -/rw-r--r-- wayne wayne 179002 /tmp/.../kis_client-0.9/AUTHORS
528 .a. -/rw-r--r-- wayne wayne 179012 /tmp/.../kis_client-0.9/config.h.in
```

TOOLS3.TAR IS UPLOADED ONTO THE SYSTEM .

```
SAT JUL 05 2003 07:26:31 3788800 M.. -/RW-R--R-- WAYNE WAYNE 162968 /TMP/.../TOOLS3.TAR
```

TOOLS3.TAR IS CHANGED , POSSIBLY MOVED INTO THE CURRENT DIRECTORY, AND THEN EXTRACTED .

```
SAT JUL 05 2003 07:28:29 3788800 ..c -/RW-R--R-- WAYNE WAYNE 162968 /TMP/.../TOOLS3.TAR
SAT JUL 05 2003 07:28:41 1732 .A. -/RW----- ROOT/WROOT ROOT 178982 /TMP/.../LRK4/NET-TOOLS-1.32-ALPHA/LIB/IPX_GR.C
6240 .A. -/RW-R--R-- ROOT/WROOT ROOT 50711 /TMP/.../LRK4/FILEUTILS-3.13/INL/CAT-COMPAT.C
```

THE TIMELINE ONLY REFLECTS THE MOST RECENT TIME CHANGE FOR EACH FILE . THE SECURE AND XFERLOG WERE UPDATED WITH EACH UPLOAD , AND THIS IS SIMPLY THE MOST RECENT . HERE THE SECURE AND XFERLOG ARE UPDATED , FROM THE UPLOAD OF TOOLS4.TAR .

```
SAT JUL 05 2003 07:29:59 31062 M.C -/RW----- ROOT/WROOT ROOT 114780 /VAR/LOG/SECURE
SAT JUL 05 2003 07:30:39 863 M.C -/RW----- ROOT/WROOT ROOT 114834 /VAR/LOG/XFERLOG
51200 M.. -/RW-R--R-- WAYNE WAYNE 162973 /TMP/.../TOOLS4.TAR
SAT JUL 05 2003 07:31:15 51200 ..c -/RW-R--R-- WAYNE WAYNE 162973 /TMP/.../TOOLS4.TAR
```

Tools4.tar is extracted. Although the tar access appears fourth in this list, they all occur in the same second.

```
Sat Jul 05 2003 07:31:30 616 .ac -/rw-r--r-- wayne wayne 146101 /tmp/.../adore/CVS/Entries
199 ..c -/rwx-x-x wayne wayne 82822 /tmp/.../adore/startadore
6 .ac -/rw-r--r-- wayne wayne 146100 /tmp/.../adore/CVS/Repository
51200 .a. -/rw-r--r-- wayne wayne 162973 /tmp/.../tools4.tar
4179 ..c -/rw-r--r-- wayne wayne 82816 /tmp/.../adore/ava.c
4096 ..c d/rwxr-x-x wayne wayne 146098 /tmp/.../adore/CVS
1979 ..c -/rw-r--r-- wayne wayne 82817 /tmp/.../adore/cleaner.c
21 .ac -/rw-r--r-- wayne wayne 82814 /tmp/.../adore/TODO
4096 m.. d/rwxr-x-x 30 root 162678 /tmp/...
738 .ac -/rw-r--r-- wayne wayne 82812 /tmp/.../adore/Makefile.gen
2527 ..c -/rw-r--r-- wayne wayne 82821 /tmp/.../adore/lib/invisible.h
2810 ..c -/rwx-x-x wayne wayne 82818 /tmp/.../adore/configure
10 .ac -/rw-r--r-- wayne wayne 146102 /tmp/.../adore/CVS/Tag
1904 .ac -/rw-r--r-- wayne wayne 82819 /tmp/.../adore/dummy.c
2632 ..c -/rw-r--r-- wayne wayne 82813 /tmp/.../adore/README
5 .ac -/rw-r--r-- wayne wayne 146099 /tmp/.../adore/CVS/Root
10757 ..c -/rw-r--r-- wayne wayne 82815 /tmp/.../adore/adore.c
1660 .ac -/rw-r--r-- wayne wayne 82811 /tmp/.../adore/LICENCE
3262 ..c -/rw-r--r-- wayne wayne 82820 /tmp/.../adore/lib/invisible.c
4096 m.. l/dwxr-x-x 30 root 162678 /etc/rc.d/rc0.d/K83ypbind (deleted-reallo)
```

THE ADORE ROOTKIT IS COMPILED

```
SAT JUL 05 2003 07:32:46 516 M.C -/RW-R--R-- ROOT/WROOT ROOT 82823 /TMP/.../ADORE/MAKEFILE
2810 .A. -/RWXR-XR-X WAYNE WAYNE 82818 /TMP/.../ADORE/CONFIGURE
SAT JUL 05 2003 07:35:08 10757 .A. -/RW-R--R-- WAYNE WAYNE 82815 /TMP/.../ADORE/ADORE.C
516 .A. -/RW-R--R-- ROOT/WROOT ROOT 82823 /TMP/.../ADORE/MAKEFILE
SAT JUL 05 2003 07:35:13 5132 M.C -/RW-R--R-- ROOT/WROOT ROOT 82824 /TMP/.../ADORE/ADORE.O
4179 .A. -/RW-R--R-- WAYNE WAYNE 82816 /TMP/.../ADORE/AVA.C
```

And cleans up after itself

```

Sat Jul 05 2003 07:35:16 0..c-rw----- root/wroot root 162978 <RH_Partition_1.dd-dead-162978>
0..c-rw----- root/wroot root 162977 <RH_Partition_1.dd-dead-162977>
1979 a.-/rw-r--r-- wayne wayne 82817 /tmp/./adore/cleaner.c
1572 .ac-rw-r--r-- root/wroot root 162976 <RH_Partition_1.dd-dead-162976>
0 .ac-rw-r--r-- root/wroot root 162979 /tmp/cc4EAWgS.ld (deleted)
3516 .ac-rw-r--r-- root/wroot root 162975 /tmp/cchVzP.X0.o (deleted)
14755 m.c-/rwx-r-x root/wroot root 82825 /tmp/./adore/ava
0..c-/rw----- root/wroot root 162977 /tmp/cc4cOvd4.c (deleted)
3516 .ac-rw-r--r-- root/wroot root 162975 <RH_Partition_1.dd-dead-162975>
1572 .ac-rw-r--r-- root/wroot root 162976 /tmp/ccw7Y6RP.o (deleted)
4096 m.c/d/rwx-r-x 30 root 82810 /tmp/./adore
1084 m.c-/rw-r--r-- root/wroot root 82826 /tmp/./adore/cleaner.o
1002 mac-/rw----- root/wroot root 162974 /tmp/ccgkurtNs (deleted)
0 .ac-rw-r--r-- root/wroot root 162979 <RH_Partition_1.dd-dead-162979>
1002 mac-rw----- root/wroot root 162974 <RH_Partition_1.dd-dead-162974>
0..c-/rw----- root/wroot root 162978 /tmp/ccOSSJfY.o (deleted)

```

THE ADORE README FILE IS ACCESSED .

```
SAT JUL 05 2003 07:37:54 2632 A.-/RW-R--R-- WAYNE WAYNE 82813 /TMP/./ADORE/README
```

THE ENTIRE "/TMP/./" DIRECTORY IS ACCESS ED, POSSIBLY THRO UGH A "FIND ." OR SIMILAR COMMAND .

```

SAT JUL 05 2003 07:38:41 4096 A.D/DRWXR-XR-X WAYNE WAYNE 146098 /TMP/./ADORE/CVS
4096 A.D/DRWXR-XR-X ROOT/WROOT ROOT 50717 /TMP/./LRK4/CRO.N3.0PL1
4096 A.D/DRWXR-XR-X ROOT/WROOT ROOT 146071 /TMP/./LRK4/FINDUTILS/TESTSUITE/XARGS.SYSV
4096 A.-/DRWXR--R- ROOT/WROOT ROOT 82743 /ETC/MTAB~ (DELETED-REALLOC)
4096 A.D/DRWXR-XR-X ROOT/WROOT ROOT 146042 /TMP/./LRK4/FINDUTILS/TESTSUITE
4096 A.D/DRWXR-XR-X ROOT/WROOT ROOT 66730 /TMP/./LRK4/FILEUTILS-3.13/SRC
4096 A.D/DRWXRWXRWX WAYNE WAYNE 146087 /TMP/./KIS_CLIENT-0.9/SRC
4096 A.D/DRWXR-XR-X ROOT/WROOT ROOT 66740 /TMP/./LRK4/PRO.CPS-1.01
4096 A.D/DRWXR--R- ROOT/WROOT ROOT 145990 /TMP/./LRK4/RSHD
4096 A.D/DRWXR-XR-X ROOT/WROOT ROOT 145993 /TMP/./LRK4/SHADO.W-961025
4096 A.D/DRWXR-XR-X ROOT/WROOT ROOT 130850 /TMP/./LRK4
4096 A.D/DRWXR--R- ROOT/WROOT ROOT 145918 /TMP/./LRK4/CHFN
4096 A.D/DRWXR--R- ROOT/WROOT ROOT 82743 /TMP/./LRK4/INETD

```

CRON IS UPDATED .

```
SAT JUL 05 2003 07:40:00 14394 M.C-/RW----- ROOT/WROOT ROOT 114838 /VAR/LOG/CRON
```

ADORE IS STAR TED.

```

SAT JUL 05 2003 07:40:55 199 A.-/RWXR-XR-X WAYNE WAYNE 82822 /TMP/./ADORE/STARTADORE
1084 A.-/RW-R--R- ROOT/WROOT ROOT 82826 /TMP/./ADORE/CLEANER.O
5132 A.-/RW-R--R- ROOT/WROOT ROOT 82824 /TMP/./ADORE/ADORE.O

```

THE ADORE "AVA" FUNCTION IS USED , WHICH ACCESSES THE "/TMP/./" DIRECTORY , POSSIBLY TO HIDE IT FROM THE USER , WHICH IS PART OF AD ORE'S FUNCTIONALITY .

```

SAT JUL 05 2003 07:41:15 14755 A.-/RWXR-XR-X ROOT/WROOT ROOT 82825 /TMP/./ADORE/AVA
4096 ..CL/DRWXR-XR-X 30 ROOT 162678 /ETC/RC.D/RC0.D/K83YPBIND (DELETED-REALLOC)
4096 ..C.D/DRWXR-XR-X 30 ROOT 162678 /TMP/...
SAT JUL 05 2003 07:41:41 4096 A.L/DRWXR-XR-X 30 ROOT 162678 /ETC/RC.D/RC0.D/K83YPBIND (DELETED-REALLOC)
4096 A.D/DRWXR-XR-X 30 ROOT 162678 /TMP/...

```

TRIPWIRE IS EXECUTED , AND ACCESSES MU LTIIPLE FILES .

```

SAT JUL 05 2003 07:44:12 5554608 A.-/R-X----- ROOT/WROOT ROOT 145959 /USR/LOCAL/TRIPWIRE/TFS/BIN/TRIPWIRE
SAT JUL 05 2003 07:44:14 3778320 A.-/R-X----- ROOT/WROOT ROOT 145958 /USR/LOCAL/TRIPWIRE/TFS/BIN/SIGGEN
SAT JUL 05 2003 07:44:17 4971792 A.-/R-X----- ROOT/WROOT ROOT 145960 /USR/LOCAL/TRIPWIRE/TFS/BIN/TWADMIN
SAT JUL 05 2003 07:44:19 14 A.L/LRWXRWXRWX ROOT/WROOT ROOT 145269 /USR/BIN/MAIL -> ../BIN/MAIL
4096 A.D/DRWXR-X-- ROOT/WROOT ROOT 145955 /USR/LOCAL/TRIPWIRE/TFS/DB
16384 A.D/DRWXR-XR-X ROOT/WROOT ROOT 144293 /USR/BIN
12 A.L/LRWXRWXRWX ROOT/WROOT ROOT 144294 /USR/BIN/X11-> ./X11R6/BIN
4494064 A.-/R-X----- ROOT/WROOT ROOT 145961 /USR/LOCAL/TRIPWIRE/TFS/BIN/TWPRINT
6125 A.-/RWXR-XR-X ROOT/WROOT ROOT 145700 /USR/BIN/RNMAIL
4586 A.-/RW-R----- ROOT/WROOT ROOT 145979 /USR/LOCAL/TRIPWIRE/TFS/BIN/TW.CFG
12642 A.-/RWXR-XR-X ROOT/WROOT ROOT 145699 /USR/BIN/PNEWS
931 A.-/RW-R----- ROOT/WROOT ROOT 145976 /USR/LOCAL/TRIPWIRE/TFS/KEY/SITE.KEY
4096 A.D/DRWXR-X-- ROOT/WROOT ROOT 145956 /USR/LOCAL/TRIPWIRE/TFS/KEY
8287 A.-/RW-R--R- ROOT/WROOT ROOT 178943 /USR/LOCAL/TRIPWIRE/TFS/POLICY/TW.POL
4 A.L/LRWXRWXRWX ROOT/WROOT ROOT 145004 /USR/BIN/ -> TEST
4096 A.D/DRWXR-XR-X ROOT/WROOT ROOT 64136 /USR/LOCAL/BIN
931 A.-/RW-R----- ROOT/WROOT ROOT 145977 /USR/LOCAL/TRIPWIRE/TFS/KEY/REDHAT6-LOCAL.KEY
1260 A.-/RWXR-XR-X ROOT/WROOT ROOT 144907 /USR/BIN/.GITACTIO

```

The Tripwire report is created.

```

Sat Jul 05 2003 07:49:10 96 a.-/rw-r--r-- root/wroot root 82656 /etc/hosts
4096 m.c/d/rwx-r-x-- root/wroot root 145954 /usr/local/tripwire/tfs/report
8238 a.-/rw-r--r-- root/wroot root 146103 /usr/local/tripwire/tfs/report/redhat6-20030705-194328.twr
Sat Jul 05 2003 07:49:11 8238 m.c-/rw-r--r-- root/wroot root 146103 /usr/local/tripwire/tfs/report/redhat6-20030705-194328.twr

```

THE SYSTEM IS SHUTDOWN.

```
SAT JUL 05 2003 07:49:31 5 MAC -/RW-R--R-- ROOT/WROOT ROOT 18729 /VAR/RUN/SHUTDOWN.PID (DELETED)
25968 .A. -/RWXR-XR-X ROOT/WROOT ROOT 112446 /SBIN/INIT
14128 .A. -/RWXR-XR-X ROOT/WROOT ROOT 112452 /SBIN/SHUTDOWN
5 MAC -RW-R--R-- ROOT/WROOT ROOT 18729 <RH_PARTITION_1.DD-DEAD-18729>
0 M.C.F/FRW----- ROOT/WROOT ROOT 32307 /DEV/INITCTL
SAT JUL 05 2003 07:49:32 60 .A. -/RW----- ROOT/WROOT ROOT 82669 /ETC/IOCTL.SAVE
0 .A. F/FRW----- ROOT/WROOT ROOT 32307 /DEV/INITCTL
1756 .A. -/RW-R--R-- ROOT/WROOT ROOT 81443 /ETC/INITTAB

SAT JUL 05 2003 07:50:01 229248 M.C. -/RW-RW-R-- ROOT/WROOT UTMP 113169 /VAR/LOG/WTMP
340663 .A. -/RWXR-XR-X ROOT/WROOT ROOT 144301 /LIB/LD-2.1.3.SO
75600 .A. -/RWXR-XR-X ROOT/WROOT ROOT 144569 /BIN/GREP
6096 .A. -/R-XR-XR-X ROOT/WROOT ROOT 114744 /SBIN/QUOTAON
456 .A. -/RW-R--R-- ROOT/WROOT ROOT 82375 /ETC/ESTAB
8128 .A. -/RWXR-XR-X ROOT/WROOT ROOT 112447 /SBIN/KILLALL5
6 .A. L/LRWXRWXRWX ROOT/WROOT ROOT 114051 /SBIN/SWAPON B
4101324 .A. -/RWXR-XR-X ROOT/WROOT ROOT 144308 /LIB/LIBC-2.1.3.SO
3260 .A. -/RWXR-XR-X ROOT/WROOT ROOT 161660 /ETC/RC.D/INIT.D/HALT
527442 .A. -/RWXR-XR-X ROOT/WROOT ROOT 144319 /LIB/LIBM-2.1.3.SO
7 .A. L/LRWXRWXRWX ROOT/WROOT ROOT 114743 /SBIN/QUOTAOFF -> QUOTAON
56208 .A. -/RWSR-XR-X ROOT/WROOT ROOT 145325 /BIN/MOUNT
13 .A. L/LRWXRWXRWX ROOT/WROOT ROOT 144309 /LIB/LIBC.SO.6 -> LIBC-2.1.3.SO
148848 .A. -/RWXR-XR-X ROOT/WROOT ROOT 144861 /BIN/GAWK-3.0.4
11 .A. L/LRWXRWXRWX ROOT/WROOT ROOT 144302 /LIB/LD-LINUX.SO.2 -> LD-2.1.3.SO
4 .A. L/LRWXRWXRWX ROOT/WROOT ROOT 144873 /BIN/AWK -> GAWKH B
12247 .A. -/RW-R--R-- ROOT/WROOT ROOT 82738 /ETC/LD.SO.CACHE
13 .A. L/LRWXRWXRWX ROOT/WROOT ROOT 144320 /LIB/LIBM.SO.6 -> LIBM-2.1.3.SO
6896 .A. -/RWXR-XR-X ROOT/WROOT ROOT 112445 /SBIN/HALT
148848 .A. -/RWXR-XR-X ROOT/WROOT ROOT 144861 /BIN/GAWK
6200 .A. -/RWXR-XR-X ROOT/WROOT ROOT 114048 /SBIN/SWAPON
```

Recover Deleted Files

The search for deleted files was conducted in Autopsy Forensic Browser, version 1.62. The dd image file was still listed in the Autopsy "fsmorgue" file from earlier investigation. Autopsy was started, using the command ". /autopsy 8888 localhost &". The "File Browsing" option was selected once Autopsy was started. The RH_Partition_1.dd file was then selected, being the extract of partition 1 from the dd of the entire drive. "Begin analysis" was then chosen. From this file browser window, "All Deleted Files" was chosen. This lists all deleted files on the system, along with their MAC times, sizes, UID and GID, and the inode they occupy (or occupied if it has been reallocated.) No suspect deleted files were found on the system, although a directory, "/jon ty" was found. This directory turned out to contain files for "Tripwire for Servers 3.0".

String Search

Various groups of keywords were searched for. The Encase tool was used for this search, as it has a user friendly ability to search for multiple key words at once.

"hacker speak", ("r00t*", "h4x0r", "0wn*", "l33t", "gr33t*", "greet*", 666, 12345, 31337)

These are terms commonly used by malicious intruders. Vowels (and other letters) are commonly replaced by numbers. This may be to obfuscate the writing, so that people uninitiated into the practise will be unable to read the text. This is a rather weak explanation as the numbers are chosen to resemble their letter counterparts. They also have the advantage of being able to bypass some content checkers, that check for known text strings. "Greet" is commonly used in exploit code and viruses to

acknowledge other “black-hat” computer intruders. The number 666 is a biblical reference to the devil, and commonly used as a port number (or 6666 – being an ephemeral port ie one over 1024), but this would also be detected by the “666” string search. 12345 is another such number, used self consciously as it is so predictable. 31337 is more numbers replace by letters. The 3 is the letter “e”, the 1 is an “L”, and the 7 is a “t”. The word eleet is a deliberate misspelling of “elite”, being a skilled member of a small group of computer coders.

profanity, ("fuck", "shit")

Profanity is commonly used in malicious code, and infrequently used in open -source or production code. It is therefore useful and indicative of a computer being misused.

intrusion terms ("rootkit", "hack", "sniff", "adore", "LKM", "backdoor")

These are terms commonly associated with computer intrusion tools. The tools often contain README files that describe their functionality, and will likely contain these terms.

“r00t” was found in the lrk4 README file, as well as tools and tools3.tar (and various unallocated clusters.) These tools had already been located through a hidden directory search.

“OWN” WAS FOUND IN (/USR/LIB/) LIBSP.A, LIBSPGROVE.A, LIBSTYLE.A, (/USR/MAN/MAN1/) CREATE SEQUENCE.L.GZ, (/usr/info/) MAKE.INFO-5.GZ, (/usr/man/man1/) YPWHICH.1.GZ, and (/usr/doc/wu-ftpd-2.6.0) CONTRIBUTORS. These are all usual system files.

“133t” was found in unallocated clusters, that appear to have previously been part of the “bitchX” irc tool. This tool was not installed on the computer, and may have been installed previously and the hard disk since reformatted.

Although “gr33t” was not found, “greet” was found in 562 places, and not further investigated.

“666” was found in 19,243 places, and not further investigated.

“12345” was found in 4,953 places, and not further investigated.

“fuck” was found in (/usr/share/emacs/20.5/etc/) yow.lines, (/tmp/.../knark -0.59/src/) knarc.c, modhide.c, (/usr/lib/ispell/) americanmed+.hash, americanxlq.hash, britishmed+.hash, britishxlq.hash, (/tmp/linux_x86/libkit /TWagent-libkit/) config.a, (/usr/share/emacs/20.5/lisp/play) doctor.elc (along with a surprising amount of other profanity), (/tmp/.../lrk4/) linsniffer.c, (/tmp/...) knark.tar, tools.tar, tools3.tar, (/tmp/.../knark-0.50/src/) modhide.c, and (/usr/bin/filter/) filter_innd.pl

“shit” triggered in many of the same places as “fuck”, although also triggered on “hashit”, “Matsushita”, “Yamashita”, “RefreshItems”, “BashIt”, and “HIShitpos”, all of which occurred multiple times.

“rootkit” occurred in many “/tm p/.../” files.

“hack” occurred in (/usr/doc/cvs -1.10.7/) BUGS, FAQ, NEWS, README, TODO, and cvs.ps. It occurred in over 4000 other places also, and may be unsuitable for a search term due to its generic nature and various usage.

“sniff” was found in many places, including system files and /tmp/.../, as were “adore” and “LKM”.

“backdoor” was found in (/usr/share/emacs/20.5/lisp/progmodes/) cperl -mode.elc, (/tmp/lrk4/) README, (/tmp/.../lrk4/inted/) inetd.c, (/tmp/.../adore/) adore.c, libinvisible.c, (/tmp/...) tools.tar, tools3.tar, and tools4.tar, (/usr/bin/filter/) filter_innd.pl, and (/var/lib/rpm/packages.rpm).

CONCLUSIONS

HYPOTHESIS : THE INTRUDER SCANNED THE SYSTEM USING THE PORT SCANNING TOOL "NESSUS." THE INTRUDER THEN GAINED ACCESS TO THE MACHINE. THIS PROBABLY OCCURRED THROUGH A FLAW DISCOVERED BY THE NESSUS TOOL, POSSIBLY IN THE "FAKEIDENT" PROGRAM (THE VERSION INSTALLED ON THE COMPUTER IS 1.2, ALL VERSIONS PRIOR TO 1.5 ARE KNOWN TO BE VULNERABLE TO A BUFFER OVERFLOW ATTACK^{xi}.)

IT IS ALSO POSSIBLE THAT THE INTRUDER GUESSED THE USER ("WAYNE")'S PASSWORD. THE INTRUDER EXPLOITED THIS ACCESS TO GAIN ROOT ACCESS. THIS ROOT ACCESS WAS USED TO MODIFY THE PASSWD AND SHADOW FILES, TO INCLUDE NEW USER ACCOUNTS. THESE ACCOUNTS WERE "WRUSER", WITH A UID AND GID OF 666, AND "WROOT" WITH A UID OF 0. THE "WRUSER" ACCOUNT OCCURRED IN THE PASSWD FILE TWICE, ONCE WITH AND ONCE WITHOUT THE "X" INDICATING A SHADOWED PASSWORD. THIS MAY INDICATE THAT THE PASSWORD FILE WAS MANUALLY, AND INCORRECTLY, EDITED. TESTS PERFORMED ON OTHER SYSTEMS SHOWED THAT A DOUBLE-UP OF A USER ACCOUNT OF THIS TYPE, WHERE THE "NON-SHADOWED" VERSION OCCURS FIRST IN THE PASSWD FILE, LEFT THAT USER UNABLE TO LOG IN. THIS MAY SHOW THAT THE INTRUDER IS NOT OVERLY FAMILIAR WITH UNIX SYSTEM FILE STRUCTURES. THE INTRUDER THEN UPLOADED SEVERAL LINUX ROOT KITS. ALTHOUGH THESE WERE EXPANDED FROM THE ORIGINAL "TAR" ARCHIVES, ONLY ONE (ADORE) WAS SUCCESSFULLY EXECUTED. THE INTRUDER ATTEMPTED TO INSTALL THE OTHERS, BUT THE COMPILATION MAY HAVE FAILED. THE README FILE FOR "ADORE" WAS ACCESSED BEFORE THE PROGRAM WAS ITS ELF EXECUTED, WHICH MAY SHOW THAT THE INTRUDER IS UNFAMILIAR WITH THIS TOOL. THE "ADORE" ROOTKIT WAS NOT DETECTED BY THE "CHKROOTKIT" PROGRAM WHICH CHECKS FOR IT SPECIFICALLY, WHICH MAY SHOW THAT THE PROGRAM WAS NOT SET UP TO RUN ON REBOOT. AS THE COMPUTER WAS POWERED DOWN WHEN SEIZED, NO "PROC" INFORMATION WAS AVAILABLE TO TELL IF "ADORE" WAS RUNNING AT THE TIME.

FROM THIS, IT IS LIKELY THAT THE INTRUDER IS A NOVICE HACKER. NESSUS IS A NOISY TOOL, WHICH SHOWS MANY ENTRIES IN LOGS. A SOPHISTICATED HACKER WOULD NOT USE SUCH A TOOL IN THIS WAY. SIMILARLY, THE TOOL AND TOOL 3 ARCHIVE FILES UPLOADED BY THE INTRUDER CONTAINED THE SAME INFORMATION. THIS WAS A WASTE OF TIME AND BANDWIDTH WHICH MAY SUGGEST THAT THE INTRUDER WAS USING SOME ONE ELSE'S TOOLS, OR JUST RANDOMLY DOWNLOADING THINGS THEY THOUGHT MIGHT WORK. AS SHOWN BY

ACCESSING THE "ADORE" README FILE ON THE COMPROMISED SYSTEM , THE INTRUDER IS NOT FAMILIAR WITH THESE TOOLS ALREADY . AT THE VERY LEAST , A SKILLED INTRUDER WOULD KNOW TO VIEW THE README FILE ON THEIR OWN SYSTEM , IF NOT HAVING IT PRINTED OUT ALREADY .

© SANS Institute 2003, Author retains full rights.

Legal Issues of Incident Handling

What, if any, information can you provide to the law enforcement officer over the phone during the initial contact?

THE FIRST ISSUE TO CONSIDER IN THIS SITUATION IS ONE OF CONTRACT LAW. THE DETAILS OF THE CONTRACT SIGNED BETWEEN THE INTERNET USER AND THE ISP MAY LIMIT THE INFORMATION THAT THE ISP IS ALLOWED TO KEEP, OR PUBLISH (NOTE, ANY COMMUNICATION TO A THIRD PARTY IS CONSIDERED PUBLICATION, AS HELD IN GODFREY V. DEMON INTERNET LTD., CASE NO. 1998 G NO. 30 (26 MARCH 1999), REPORTED AT: [2000] 3 W.L.R. 1020.) THIS WOULD DEPEND ON THE CONTRACT BETWEEN THE SUBSCRIBER AND THE ISP IN QUESTION, ABOUT WHICH NO INFORMATION IS AVAILABLE HERE. POTENTIALLY THIS COULD RAISE ISSUES SUCH AS THOSE IN A RECENT CASE IN WHICH AN ISP WAS ACCUSED OF BREACHING CONFIDENTIALITY CLAUSES IN A CONTRACT BY INTERCEPTING THEIR CLIENTS' EMAILS^{xii}. THE JUDGE IN THAT CASE DECLINED TO UPHOLD AN INTERIM INJUNCTION REQUIRING THE CLIENT TO CONTINUE DEALING WITH THE ISP, DUE TO THE ISP'S CONTRACTUAL BREACH. THE ISP ARGUED THAT THE CONTRACT EXPRESSLY AUTHORISED MONITORING, BUT THE JUDGE RULED THAT INTERCEPTING AND USING EMAILS IS SO FAR REMOVED FROM THE PRIMARY CONTRACT THAT IT COULD NOT BE CONSIDERED AN IMPLIED TERM OF THAT CONTRACT. THE CASE HERE IS SLIGHTLY DIFFERENT, AS THE THIRD PARTY IS A LAW ENFORCEMENT OFFICIAL.

THE DISCLOSURE WILL ALSO BE LIMITED BY THE PRIVACY ACT 1993. THIS ACT REQUIRES ANYONE COLLECTING INFORMATION ABOUT SPECIFIC PEOPLE TO DETERMINE WHAT USES THAT INFORMATION WILL BE USED FOR, AND TO LIMIT THEMSELVES TO THOSE PURPOSES. IT SETS DOWN SOME INFORMATION PRIVACY PRINCIPLES THAT NEED TO BE APPLIED IN SOME CIRCUMSTANCES, BUT MOST OF THESE ARE NOT RELEVANT HERE. INFORMATION PRIVACY PRINCIPLE (IPP) 11 HOWEVER BEGINS

"

Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds -

(a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the

purposes

in connection with which the information was obtained; or

(b) That the source of the information is a publicly available publication; or

(c) That the disclosure is to the individual concerned; or

(d) That the disclosure is authorised by the individual concerned; or

(e) That non-compliance is necessary -

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, investigation, prosecution, and punishment

of

offences; or

(ii) For the enforcement of the law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or Tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

"

THIS IPP WOULD LIMIT THE DISCLOSURE OF THIS PERSONAL INFORMATION, BUT AS SUBSECTION (E)(1) IS MET, THE INFORMATION CAN BE DISCLOSED.

NOTABLE SECTIONS AN EXAMPLE "TERMS AND CONDITIONS" FROM A NEW ZEALAND ISP^{xiii} ARE

“

3.2 Your use of the Services

You will, at all times during the term of this Agreement:

* Comply with, and ensure that anyone else who uses the Services complies with, these terms and conditions for paradise.net customers and such system operating procedures, instructions and acceptable use requirements as we may notify you of from time to time;

* Ensure your use of the Services does not interfere with or disrupt TelstraClear's Network;

* Not use the Services for any unlawful or offensive act;

* Not use the Services to publish or distribute any information, software or other material, which is unlawful or which a reasonable person would consider offensive, abusive or defamatory (flaming);

* Not use the Services to distribute multiple unsolicited electronic mail to large numbers of persons including, but not limited to, electronic mail advertisements (spamming);

* Not use the Services to gain or attempt to gain unauthorised access to any computer systems or in a manner which infringes the rights of any person;

* Take all reasonable care (in accordance with industry accepted standards of best practice) to prevent the spread of viruses, or contamination by virus, of any software or hardware operated by any other person on the Internet, our system included;

* Be responsible and liable for any use (authorised or unauthorised) of the Services by any other person (including any charges associated with that use).

“

“

9. Privacy

9.1 You agree that paradise.net can collect information about you and the ways in which you are using the Services. Paradise.net will obtain this information directly from you, from our customer records and from the records that are generated within our equipment when you use our Services.

9.2 You agree that paradise.net may hold this information about you and may pass it on to our employees, contractors, agents and business partners for a range of lawful purposes connected with our business operations, which include:

* providing you with Services;

* administering your account;

* looking at ways in which we can improve the Services;

* keeping you informed as to the products and services (both existing and new) that are available to you from TelstraClear.

“

“

9.7 Pursuant to Privacy Principle 11, we may disclose information about you to law enforcement authorities (such as the Police or the Department of Internal Affairs) if we think that it is necessary to help maintain the law.

”

THESE TERMS AND CONDITIONS ARE RELATIVELY UNIFORM ACROSS THE INDUSTRY. AS 9.7 SPECIFICALLY ALLOWS THE ISP TO COMPLY WITH THE PRIVACY ACT (ALTHOUGH THIS WOULD BE UNNECESSARY ON THE PRESENT FACTS), ALL RELEVANT INFORMATION CAN BE PROVIDED TO THE LAW ENFORCEMENT OFFICER DURING THE INITIAL CALL.

NOTE ALSO THAT ALTHOUGH IT IS ILLEGAL TO HINDER AN OFFICER DURING THE COURSE OF HIS/HER INVESTIGATION, ONE IS NOT COMPELLED TO OFFER ANY POSITIVE HELP. THIS SITUATION WOULD OF COURSE BE DIFFERENT IF THE OFFICER HAD AN APPLICABLE SEARCH WARRANT FOR THE LOGS IN QUESTION.

AN EXAMPLE OF THE LACK OF LAW IN THIS AREA WAS RECENTLY DEMONSTRATED, IN A

CASENOTE FROM THE PRIVACY COMMISSIONER^{xiv} WHICH READS

“

COMPLAINTS

IN ONE COMPLAINT AN INDIVIDUAL REQUESTED ACCESS TO THE IDENTITY OF A PERSON WHO HAD REPEATEDLY ANONYMOUSLY EMAILED HER. WHILE THERE ARE CLEAR PROCEDURES FOR DEALING WITH MALICIOUS TELEPHONE CALLS THE SAME CANNOT NECESSARILY ALWAYS BE SAID FOR HARASSING EMAILS. NORMALLY AN ISP WILL ACT IF THREATS ARE MADE (ALTHOUGH A NEW ACCOUNT CAN EASILY BE OPENED TO REPLACE ONE THAT HAS BEEN CLOSED). IN THIS CASE THE MESSAGES, ALTHOUGH NOT OVERTLY THREATENING, WERE UNWELCOME AS THEY CONTAINED ANONYMOUS STATEMENTS OF AFFECTION (WITH A DISCONCERTING FEATURE THAT SUGGESTED THE SENDER KNEW WHERE THE COMPLAINANT LIVED). ALTHOUGH THE MESSAGES WERE DIRECTED FROM A US "HOTMAIL" ACCOUNT, THE EMAIL HEADER REVEALED THE SENDER'S NEW ZEALAND ISP AND HENCE THE COMPLAINANT'S ACCESS REQUEST COULD BE REVIEWED. THE LEGAL ISSUES INCLUDED WHETHER THE SENDER'S IDENTITY COULD BE SAID TO BE "ABOUT" THE RECIPIENT (AND HENCE "PERSONAL INFORMATION" TO WHICH THERE IS A RIGHT OF ACCESS) AND, IF SO, WHETHER THAT COULD BE PROPERLY WITHHELD TO AVOID AN "UNWARRANTED DISCLOSURE OF THE AFFAIRS" OF THE SENDER. THE COMPLAINT REMAINS UNDER REVIEW.

This was a 2000 case, however the law in this area remains as it was then. The fact that a privacy commission complaint was required shows that no law applied directly to the situation. If a private citizen could request this information from an ISP, then a law enforcement officer could not be in a weaker position to do so.

What must the law enforcement officer do to ensure you to preserve this evidence if there is a delay in obtaining any required legal authority?

What the law enforcement officer is required to do to ensure that you preserve the evidence will be covered by that law enforcement officer's internal policy and procedures. From the system administrator's point of view, assuming that they wish to co-operate, no legal authority is required for the officer to request that they store the relevant information in a more permanent fashion. In this regard the officer has no less rights than any member of the public, who could also call up and request logs to be saved. A law enforcement officer making the request would likely have more persuasive power however.

What legal authority, if any, does the law enforcement officer need to provide to you in order for you to send him your logs?

At present there is no law covering the officer requesting a copy of the logs. The Privacy Act (IPP 11) requires that information about an individual only be released to a law enforcement officer, but that is clearly the case here. The Crimes Act 1961 requires a warrant for an officer to intercept "private communications" but these are narrowly defined. The Act reads

“

216B. Prohibition on use of listening devices—

(1) Subject to subsections (2) [(to (4))], every one is liable to imprisonment for a term not exceeding 2 years who intentionally intercepts any private communication by means of a listening device.

“

THE ACT THEN CONTINUES

“

PART 11A - OBTAINING EVIDENCE BY LISTENING DEVICES

[INTERPRETATION

312A. INTERPRETATION—

(1) IN THIS PART, UNLESS THE CONTEXT OTHERWISE REQUIRES,—

"INTERCEPT", IN RELATION TO A PRIVATE COMMUNICATION, INCLUDES HEAR, LISTEN TO, RECORD, MONITOR, OR ACQUIRE THE COMMUNICATION WHILE IT IS TAKING PLACE:

"LISTENING DEVICE"--

(A) MEANS ANY ELECTRONIC, MECHANICAL, OR ELECTROMAGNETIC INSTRUMENT, APPARATUS, EQUIPMENT, OR OTHER DEVICE THAT IS USED OR IS CAPABLE OF BEING USED TO INTERCEPT A PRIVATE COMMUNICATION; BUT

"PRIVATE COMMUNICATION"--

(A) MEANS ANY ORAL COMMUNICATION MADE UNDER CIRCUMSTANCES THAT MAY REASONABLY BE TAKEN TO INDICATE THAT ANY PARTY TO THE COMMUNICATION DESIRES IT TO BE CONFINED TO THE PARTIES TO THE COMMUNICATION; BUT

(B) DOES NOT INCLUDE SUCH A COMMUNICATION OCCURRING IN CIRCUMSTANCES IN WHICH ANY PARTY OUGHT REASONABLY TO EXPECT THAT THE COMMUNICATION MAY BE INTERCEPTED BY SOME OTHER PERSON NOT HAVING THE EXPRESS OR IMPLIED CONSENT OF ANY PARTY TO DO SO:

THE LOGS IN THE PRESENT CASE ARE NOT "ORAL COMMUNICATIONS" AND THEIR 'INTERCEPTION' IS THEREFORE NOT COVERED BY THE CRIMES ACT 1961. A RECENT AMENDMENT TO THE CRIMES ACT, THE CRIMES AMENDMENT ACT (NO. 6) 2003 WILL CHANGE THIS POSITION .

THE RELEVANT PORTION OF THIS ACT READS

“

"private communication -

(a) means a communication (whether in oral or written form or otherwise) made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication; but

(b) does not include such a communication occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some other person not having the express or implied consent of any party to do so."

However, this Act does not come into force until October 1, 2003. In the interim, the law remains as it was. Once the Amendment Act comes into force, the law enforcement agent will require a valid warrant to obtain the records in question.

The Telecommunications (Interception Capability) Bill will compel the ISP to keep the logs, so that they can be used by law enforcement. However this Bill is still before Parliament, and therefore has no legal standing.

Although it is irrelevant to the issue of the ISP giving out information it already possesses, communications providers are already required to assist in the deployment of interception or phone listening devices, under the Telecommunications (Residual Powers) Act 1987.

What other "investigative" activity are you permitted to conduct at this time?

As the system administrator is in control of the system, they effectively own the information. Accordingly, as long as you do not intrude on other users' privacy, you are permitted to perform any investigative activity you choose. This position may be limited by the contract between the system administrator and the ISP. This contract will define the terms of reference of the system administrator's job, and these may be breached by the system administrator pursuing an investigation using the company's information. A prudent system administrator would check with the CEO or other official in the company to obtain approval before any further investigation. The Crimes Amendment Act (no. 6) 2003 makes it illegal to gain unauthorised access to computer systems. However, it does not cover elevating access, simply gaining it originally. As the system administrator already has authorised access to the system,

they would not be breaching this law by exploring the system beyond what they are authorised to do. As mentioned however, this would likely breach the contract with the ISP and lead to disciplinary actions.

How would your actions change if your logs disclosed a hacker gained unauthorized access to your system at some point, created an account for him/her to use, and used THAT account to hack into the government system?

The only difference in this scenario is that the ISP is no longer covered by the terms and conditions that users sign up with. As the terms and conditions allow the ISP to release information to law enforcement agents anyway, this release of information would not be any different. The "hacker" might not have been physically in the country when they accessed the system. This would change the situation and raise issues of international criminal law, and jurisdictional issues. The resolution to these issues would depend on where the "hacker" was located, as New Zealand has different relationships (treaties, customary law etc) with different countries around the world.

From a practical point of view, some extra actions would be required from the system administrator. A "hacker" gained unauthorised access to the system he or she was administering. Clearly, the situation that allowed this must not be allowed to continue. The flaw that allowed the "hacker" access to the system must be located, and that service hardened to prevent re-entry (or others exploiting the same flaw.) As this entry might break the law, the evidentiary value of the evidence should not be compromised. Therefore, the system administrator's first action should be to back up the evidence, so as to preserve it for the (possible) later prosecution of the intruder. This accomplished, the system should be hardened to prevent the flaw being re-exploited, by the same individual or another.

iNeoLite by NeoWorx, available at

URL: http://www.softpile.com/Utilities/Compression/Review_05102_index.html

ii“Daemon9”, “Project Loki”. August, 1996. URL: http://www.phrack.org/phrack/49/P49_-06

iii“Dashie”. “UNDERCOVER WORK” 25/12/1999. URL: http://www.softj.org/bfi/online/bfi7/bfi07_-13.html

iv“Lion”, “HUC Services tools V0.4”.

URL: <HTTP://WWW.GOOGLE.CO.NZ/SEARCH?O=CACHE:CXT8P4WLZ38J:SCANSPEACE.MYETANG.COM/HONKER/HSER.TXT+%22HSER.TXT%22&HL=EN&START=1&IE=UTF-8>

v“Daemon9”, “L O K I 2 (the implementation)”. August 1996.

URL: http://www.phrack.org/phrack/51/P51_-06

viSamSpade. URL: <http://www.samspace.org/t/lookat?a=199.107.97.191>

vii“LIUtilities”. “Windows DLL Library”.

URL: <http://www.liutilities.com/products/wintaskspro/dlllibrary/>

viiiQuinn, Bob. “WinSocket Version 2.0: Overview, Status and Pointers”. December 5, 1998.

URL: <http://www.sockets.com/winsock2.htm>

ix“The Shmoo Group”. KnownGoods Database. 2003. URL: <http://www.knowngoods.org>

xNessus. URL: <http://www.nessus.org/>

xi“BugTraq”, “Fake Identd - Remote root exploit”. July 29 2002.

URL: <http://www.securityfocus.com/archive/1/284953>

xii“Watson, David”. “Intercepted emails breached contract says court”. April 7, 2003.

URL: <http://www.computerworld.co.nz/webhome.nsf/0/B0B53EC3ED8DD934CC256CFA000EEA8C?opendocument>

xiiiParadise.net. “Paradise.net Terms and Conditions.”

URL: <http://www.paradise.net.nz/detect/frames/default/pages/main/terms.html>

xivPrivacy Commissioner. “27th Meeting of the International Working Group on Data Protection in Telecommunications Greece, 4/5 May 2000.”

URL: <http://www.privacy.org.nz/search97cgi/s97.cgi?action=View&VdkVgwKey=http%3A%2F%2Fwww%2Eprivacy%2Eorg%2Eenz%2Fpeople%2Fgreececr%2Ehtml&DocOffset=1&DocsFound=1&QueryZip=hotmail&Collection=privcoll&SearchUrl=http%3A%2F%2Fwww%2Eprivacy%2Eorg%2Eenz%2Fsearch97cgi%2Fs97%5Fcgi%3Faction%3Dsearch%26QueryZip%3Dhotmail%26ResultTemplate%3Ddefault%252Ehts%26QueryText%3Dhotmail%26Collection%3Dprivcoll%26ResultStart%3D1%26ResultCount%3D25&>

© SANS Institute 2003, Author retains full rights