



# Universidad Carlos III de Madrid

## Report for Linux Analysis

---

Juan Diego Llano Miraval

Fecha: 19/05/2024

### procedure

We validate the sha256:

```
a82c89650253f6b68fa26329d7f7c046bdb64183f2b5b4810e2a287b0718dde1 Horcrux.E01
7219e0e9a2e25b5b4dfce372cc1031f576aa3bb9b9c25b39c6d5ec5b1d6d1660 Horcrux.E01.txt
2a718bed8fa943f203eae28df38bdf65cfb3441b1280240789c218c7c690965a Horcrux.E02
6530df91d9a395962661a11e0a1b833742a839f39cd4de5b006f681524c83c2b Horcrux.E03
007426232694f9a93312e25d608e4f199814717ccce29674dab5f38ce2044663 Horcrux.E04
2e2f5bcf5155bc765129a0747151b05440de817ef4d469c56d752bf50f870188 Horcrux.E05
431b4e1769a0d0e797330cfb359519375d415346aef10c40085d7ff2264f2ffd Horcrux.E06
91c96ea50b53ec122085e71ed9f1eb507073b95db8c2b2610fc9d3cc8b8a6a10 Horcrux.E07
3a93aec6c549f035f69c3eae86b3b66ebbe566cce3b295477af12fa51c2f9e4 Horcrux.E08
b99a4715e7c38e251b1e42db680cf8f5769874803965835c1c9cdeaa2acda610 Horcrux.E09
361b92f03c2cc18dc7b5e793b2c657f4b98e191e8a036df77fcfdbffea91c863 Horcrux.E10
2a2ef6dbb3583da9f77733db02979dc4412f2316d8e1cffccbd86024ce34c331 Horcrux.E11
16a1f3daa4561f9c19d88e45ff5a69ed455b07f039079ca1061479eae8a93e79 Horcrux.E12
ed5135b941d24e2b45ab451a96c27b348e0b8676811458f76e1b1b00237620a4 Horcrux.E13
a4bbd61a1a816aa0d665e53eb49f5d892b2edc7f9697516075c2f2a786bef256 Horcrux.E14
```

1. What distribution of Linux is being used on this machine?

On the partition 5, on the boot folder we can see some kali files, so we can confirm this is a Kali Linux.

Name	Size	Type	Date Modified
grub	4	Directory	14/03/2019 3:31:54
config-4.13.0-kali1-amd64	193	Regular File	08/11/2017 8:32:46
initrd.img-4.13.0-kali1-amd64	27.032	Regular File	14/03/2019 3:33:44
System.map-4.13.0-kali1-amd64	2.928	Regular File	08/11/2017 8:32:46
vmlinuz-4.13.0-kali1-amd64	4.358	Regular File	08/11/2017 8:32:46

```

#
# Automatically generated file; DO NOT EDIT.
# Linux/x86 4.13.10 Kernel Configuration
#
CONFIG_64BIT=y
CONFIG_X86_64=y
CONFIG_X86=y
CONFIG_INSTRUCTION_DECODER=y
CONFIG_OUTPUT_FORMAT="elf64-x86-64"
CONFIG_ARCH_DEFCONFIG="arch/x86/configs/x86_64_defconfig"
CONFIG_LOCKDEP_SUPPORT=y
CONFIG_STACKTRACE_SUPPORT=y
CONFIG_MMU=y
CONFIG_ARCH_MMAP_RND_BITS_MIN=28
CONFIG_ARCH_MMAP_RND_BITS_MAX=32
CONFIG_ARCH_MMAP_RND_COMPAT_BITS_MIN=8
CONFIG_ARCH_MMAP_RND_COMPAT_BITS_MAX=16
CONFIG_NEED_DMA_MAP_STATE=y
CONFIG_NEED_SG_DMA_LENGTH=y

```

## 2. What is the MD5 hash of the apache access.log?

By looking at [/var/log/apache2/access.log](#) we can see the file, we right click and export hash list. The output is:

d41d8cd98f00b204e9800998ecf8427e

3. It is believed that a credential dumping tool was downloaded. What is the file name of the download?

Looking through the files leads me to the Download folder where I see [mimikatz\\_trunk.zip](#)

4. There was a super secret file created, what is the absolute path?

On the .bash\_history we can trace down the commands and found:

Name	Type	Date Modified
Music	Directory	14/03/2019 3:36:07
Pictures	Directory	22/03/2019 5:47:48
Public	Directory	14/03/2019 3:36:07
Templates	Directory	14/03/2019 3:36:07
Videos	Directory	14/03/2019 3:36:07
.bashrc	Regular File	09/11/2017 13:31:54
<b>.bash_history</b>	Regular File	22/03/2019 5:48:44
.ICEauthority	Regular File	22/03/2019 15:16:16
.profile	Regular File	30/10/2017 12:46:42
.rnd	Regular File	20/03/2019 21:26:21
.viminfo	Regular File	22/03/2019 4:12:59
irZLAohL.jpeg	Regular File	22/03/2019 5:39:18
snky	Regular File	22/03/2019 2:48:15

```

msfdb init
msfconsole
shutdown now
touch snky snky > /root/Desktop/SuperSecretFile.txt
cat snky snky > /root/Desktop/SuperSecretFile.txt
msfconsole
clear
history
clear
history
whoami

```

/root/Desktop/SuperSecretFile.txt

5. What program used "didyouthinkwedmakeiteeasy.jpg" during execution?

On the same .bash\_history we look for any command using "didyouthinkwedmakeiteeasy.jpg" and we found:

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree

File List

Name	Size	Type	Date Modified
Music	4	Directory	14/03/2019 3:36:07
Pictures	4	Directory	22/03/2019 5:47:48
Public	4	Directory	14/03/2019 3:36:07
Templates	4	Directory	14/03/2019 3:36:07
Videos	4	Directory	14/03/2019 3:36:07
.bashrc	4	Regular File	09/11/2017 13:31:54
.bash_history	2	Regular File	22/03/2019 5:48:44
.ICEauthority	3	Regular File	22/03/2019 15:16:16
.profile	1	Regular File	30/10/2017 12:46:42
.rnd	1	Regular File	20/03/2019 21:26:21
.viminfo	9	Regular File	22/03/2019 4:12:59
irZLAohL.jpeg	128	Regular File	22/03/2019 5:39:18
snky	0	Regular File	22/03/2019 2:48:15

```
wall yolo
ls
pwd
cd ..
ls
cd home/
ls
cd /root
ls
cd ../root
cd ../root/Documents/myfirsthack/../../../Desktop/
sl
ls
cd ../../Documents/myfirsthack/
netstat
echo bob.txt
touch bob.txt
echo "If you're still reading this file, scream cake."
echo "Seriously, we'll give you a hint to answer question if you scream cake."
sudo visudo
ls
sudo ifng
ifconfig
apt get moo
sudo apt get moo
sudo apt install moo
sudo apt-install moo
sudo apt-get install moo
lol Castro just failed at all these commands. Someone pat him on the back.
I tried okay
history > history.txt
binwalk didyouthinkwedmakeiteeasy.jpg
clear
history
exit
touch keys.txt
pwd
```

New Edit Remove Remove All Create Image

Properties Hex Value Inter... Custom Conte...

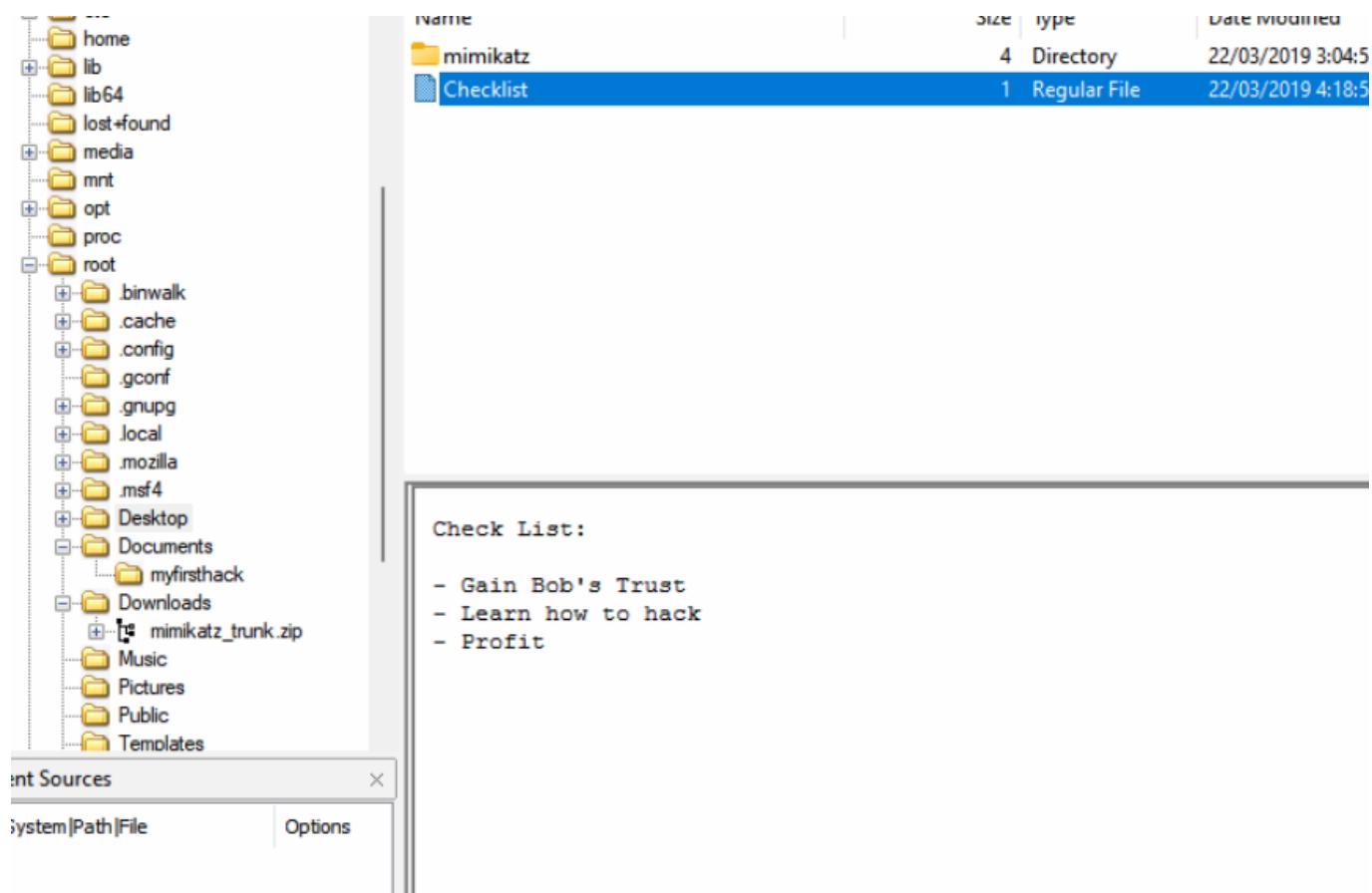
Listed: 24 Selected: 1 Horcrux.E01/Partition 5 [14304MB]/NONAME [ext4]/[root]/root/.bash\_history

007426232694f9a93312e25d608e4f19  
2e2f5bcf5155bc765129a0747151b054

binwalk

6. What is the third goal from the checklist Karen created?

As we saw previously, there was a secret file created on Desktop, so we take a look and found the check list:



the third goal is profit.

#### 7. How many times was apache run?

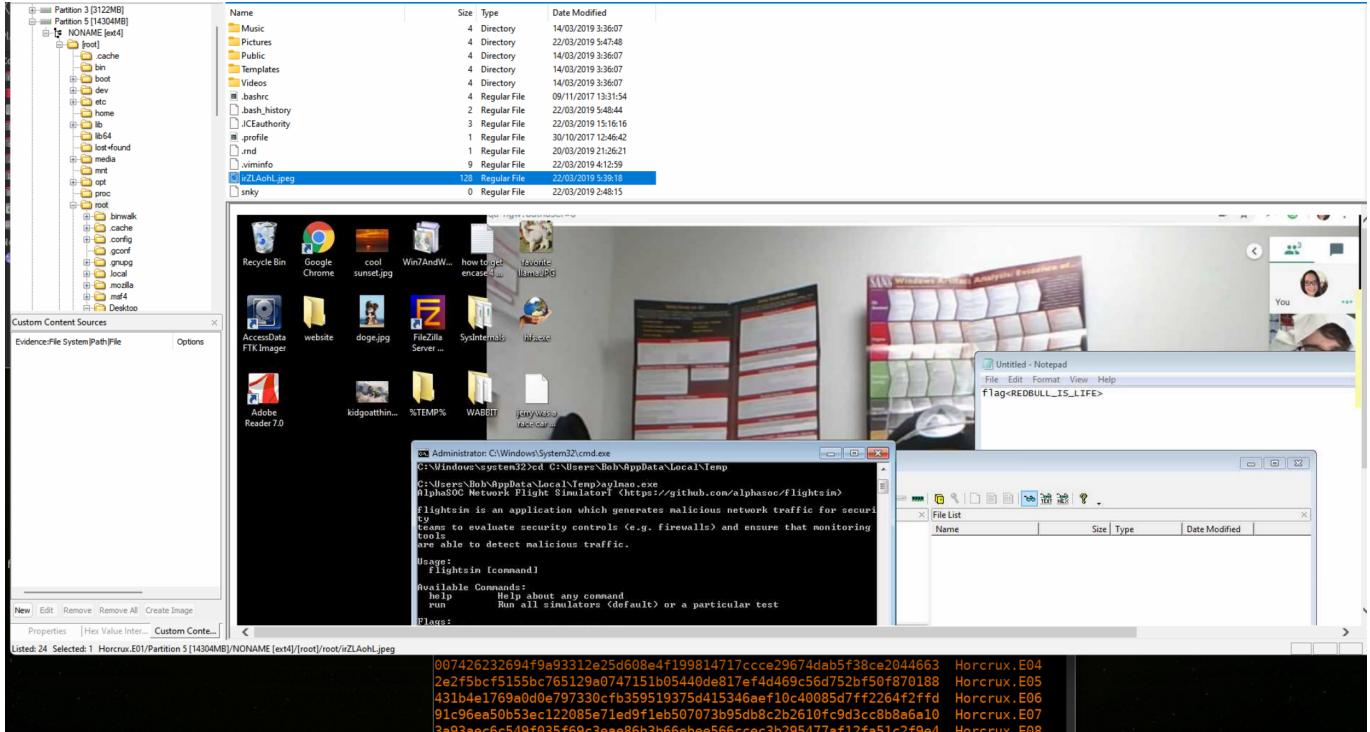
When looking at the logs for any time stamp, we realized that the logs have 0 bytes, they were ready to start but the service never started, so the time apache ran was 0.

The screenshot shows the AccessData FTK Imager 4.7.1.2 interface. On the left is the 'Evidence Tree' pane, which displays a file system structure with folders like cache, lib, local, log, apt, chkrootkit, couchdb, dradis, exim4, gdm3, glusterfs, and inetsim. Inside the 'log' folder, there is a subfolder named 'apache2'. In the main workspace, the 'File List' pane is visible, showing a table of files with their names, sizes, types, and dates modified. The table includes:

Name	Size	Type	Date Modified
access.log	0	Regular File	09/11/2017 13:41:05
error.log	0	Regular File	09/11/2017 13:41:05
other_vhosts_access.log	0	Regular File	09/11/2017 13:41:05

#### 8. It is believed this machine was used to attack another, what file proves this?"

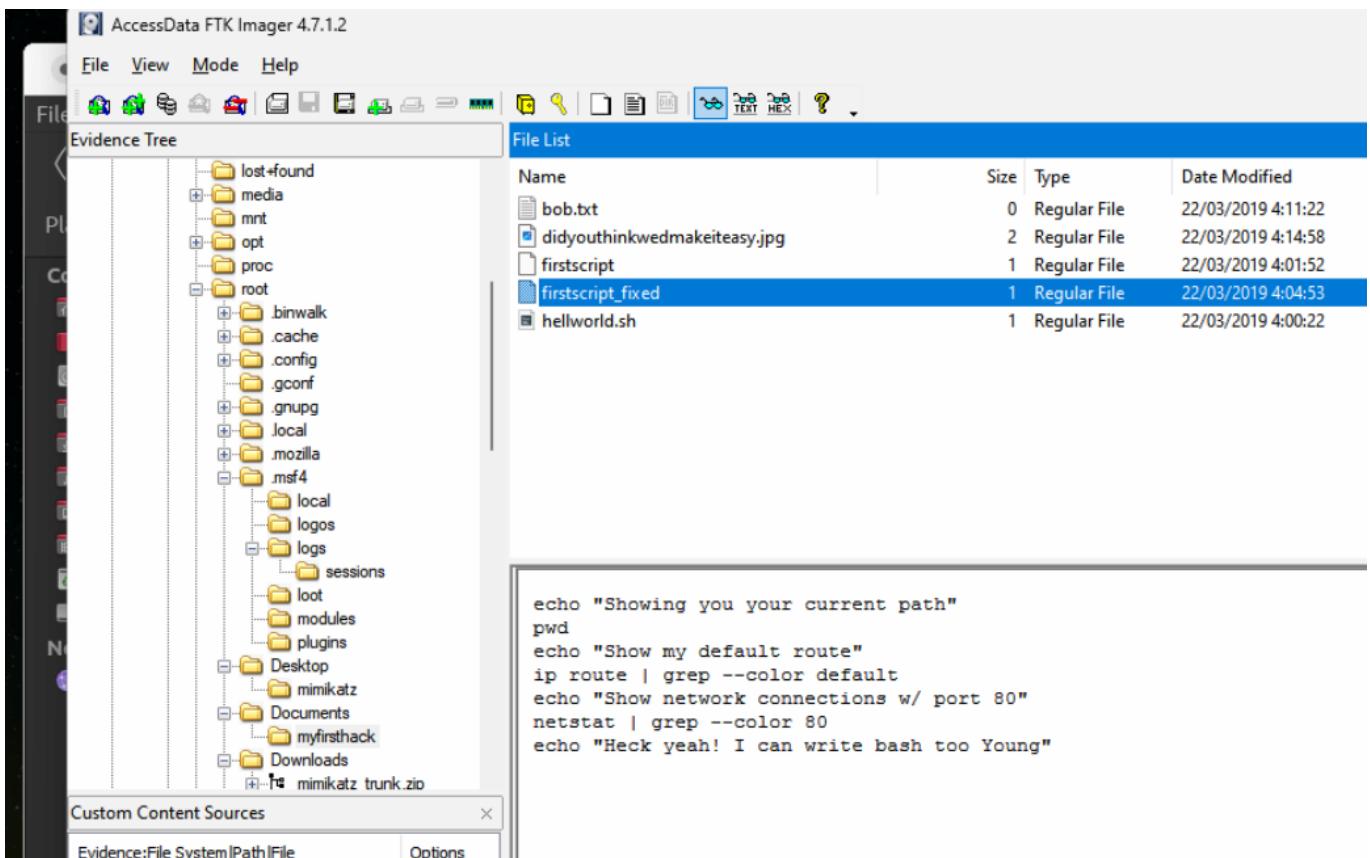
We know there ia a metsploit framework being used, but on the history we cant find evidence of an attack to someone. By expanding the view, we checked the images, and found:



this is a screenshot of a windows machine, but the image is from a Kali Linux, this might be taken from the victim.

- Within the Documents file path, it is believed that Karen was taunting a fellow computer expert through a bash script. Who was Karen taunting?

On the firstscript\_fixed we can found a message to Young:



she was taunting Young

## 10. A user su'd to root at 11:26 multiple times. Who was it?"

By looking at `/var/log/auth.log` we can look the requested time and found that it was postgres:

The screenshot shows the EnCase Evidence File System browser interface. The left pane displays a tree view of the file system, with the current path being /var/log/auth.log. The right pane shows a list of files in the auth.log directory, including auth.log, auth.log.1, bootstrap.log, btmp, daemon.log, daemon.log.1, and debug. The auth.log file is selected and highlighted in blue. Below the list is a large text area containing the log entries. The log entries show multiple instances of the 'postgres' user successfully switching to root ('su') at various times on March 20, 2019, between 11:23:45 and 11:26:22. The log entries are as follows:

```

Mar 20 11:23:45 KarenHacker polkitd(authority=local): Registered Authentication Agent for unix-session: 0
Mar 20 11:25:01 KarenHacker CRON[3910]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 20 11:25:01 KarenHacker CRON[3910]: pam_unix(cron:session): session closed for user root
Mar 20 11:26:22 KarenHacker su[4060]: Successful su for postgres by root
Mar 20 11:26:22 KarenHacker su[4060]: + ??? root:postgres
Mar 20 11:26:22 KarenHacker su[4060]: pam_unix(su:session): session opened for user postgres by (uid=0)
Mar 20 11:26:22 KarenHacker su[4060]: pam_systemd(su:session): Cannot create session: Already occupied
Mar 20 11:26:22 KarenHacker su[4060]: pam_unix(su:session): session closed for user postgres
Mar 20 11:26:22 KarenHacker su[4074]: Successful su for postgres by root
Mar 20 11:26:22 KarenHacker su[4074]: + ??? root:postgres
Mar 20 11:26:22 KarenHacker su[4074]: pam_unix(su:session): session opened for user postgres by (uid=0)
Mar 20 11:26:22 KarenHacker su[4074]: pam_systemd(su:session): Cannot create session: Already occupied
Mar 20 11:26:22 KarenHacker su[4074]: pam_unix(su:session): session closed for user postgres
Mar 20 11:26:22 KarenHacker su[4081]: Successful su for postgres by root
Mar 20 11:26:22 KarenHacker su[4081]: + /dev/pts/0 root:postgres
Mar 20 11:26:22 KarenHacker su[4081]: pam_unix(su:session): session opened for user postgres by (uid=0)
Mar 20 11:26:22 KarenHacker su[4081]: pam_systemd(su:session): Cannot create session: Already occupied
Mar 20 11:26:22 KarenHacker su[4081]: pam_unix(su:session): session closed for user postgres
Mar 20 11:26:22 KarenHacker su[4094]: Successful su for postgres by root
Mar 20 11:26:22 KarenHacker su[4094]: + /dev/pts/0 root:postgres
Mar 20 11:26:22 KarenHacker su[4094]: pam_unix(su:session): session opened for user postgres by (uid=0)
Mar 20 11:26:22 KarenHacker su[4094]: pam_systemd(su:session): Cannot create session: Already occupied
Mar 20 11:26:22 KarenHacker su[4094]: pam_unix(su:session): session closed for user postgres
Mar 20 11:26:22 KarenHacker su[4101]: Successful su for postgres by root
Mar 20 11:26:22 KarenHacker su[4101]: + /dev/pts/0 root:postgres
Mar 20 11:26:22 KarenHacker su[4101]: pam_unix(su:session): session opened for user postgres by (uid=0)
Mar 20 11:26:22 KarenHacker su[4101]: pam_systemd(su:session): Cannot create session: Already occupied
Mar 20 11:26:23 KarenHacker su[4101]: pam_unix(su:session): session closed for user postgres
Mar 20 11:26:23 KarenHacker su[4114]: Successful su for postgres by root
Mar 20 11:26:23 KarenHacker su[4114]: + /dev/pts/0 root:postgres
Mar 20 11:26:23 KarenHacker su[4114]: pam_unix(su:session): session opened for user postgres by (uid=0)
Mar 20 11:26:23 KarenHacker su[4114]: pam_systemd(su:session): Cannot create session: Already occupied
Mar 20 11:26:23 KarenHacker su[4114]: pam_unix(su:session): session closed for user postgres
Mar 20 11:35:01 KarenHacker CRON[4363]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 20 11:35:01 KarenHacker CRON[4363]: pam_unix(cron:session): session closed for user root
Mar 20 11:39:01 KarenHacker CRON[4379]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 20 11:39:01 KarenHacker CRON[4379]: pam_unix(cron:session): session closed for user root

```

Properties Hex Value Inter... Custom Conte...

Listed: 49 Selected: 1 Horcrux.E01/Partition 5 [14304MB]/NONAME [/root]/var/log/auth.log

007426232694f9a93312e25d608e4f199814717ccce29674da  
2e2f5bcf5155bc765129a0747151b05440de817ef4d469c56c  
431b4e1769a0d0e797330cfb359519375d415346aef10c4008

## 11. "Based on the bash history, what is the current working directory?"

the last directory change was to: `/root/Documents/myfirsthack`

Custom Content Sources

Evidence: File System | Path | File Options

New Edit Remove Remove All Create Image Properties | Hex Value Inter... Custom Conte...

Listed: 24 Selected: 1 Horcrux.E01/Partition 5 [14304MB]/NONAME [ext4]/[root]/root/.bash\_history 007426232694f9a93312e25d608e4f199814717c

4	Directory	14/05/2019 5:50:07/
4	Regular File	09/11/2017 13:31:54
2	Regular File	22/03/2019 5:48:44
3	Regular File	22/03/2019 15:16:16
1	Regular File	30/10/2017 12:46:42
1	Regular File	20/03/2019 21:26:21
9	Regular File	22/03/2019 4:12:59
128	Regular File	22/03/2019 5:39:18
0	Regular File	22/03/2019 2:48:15

```
wall yolo
ls
pwd
cd ..
ls
cd home/
ls
cd /root
ls
cd ../root
cd ../root/Documents/myfirsthack/.../Desktop/
sl
ls
cd ../Documents/myfirsthack/
netstat
echo bob.txt
touch bob.txt
echo "If you're still reading this file, scream cake."
echo "Seriously, we'll give you a hint to answer question if you scream cake."
sudo visudo
ls
sudo ifng
ifconfig
apt get moo
sudo apt get moo
sudo apt install moo
sudo apt-install moo
sudo apt-get install moo
lol Castro just failed at all these commands. Someone pat him on the back.
I tried okay
history > history.txt
binwalk didyouthinkwedmakeiteeasy.jpg
clear
history
exit
touch keys.txt
pwd
```