

What distribution of Linux is being used on this machine?

The screenshot shows the Evidence Tree on the left with the path: Forensic.ad1 > Custom Content Image(Multi) [AD1] > Horosx.E01:Partition 5 (14304MB) NONAME > [root] > boot > grub. The File List on the right shows the following files:

Name	Size	Type	Date Modified
grub	4	Directory	2019-03-14 3:3...
config-4.13.0-kali1-amd64	193	Regular File	2017-11-08 8:3...
initrd.img-4.13.0-kali1-amd64	27,632	Regular File	2019-03-14 3:3...
System.map-4.13.0-kali1-amd64	2,928	Regular File	2017-11-08 8:3...
vmlinuz-4.13.0-kali1-amd64	4,358	Regular File	2017-11-08 8:3...

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

The screenshot shows the Evidence Tree on the left with the path: var > log > apache2. The File List on the right shows the following files:

Name	Size	Type	Date Modified
access.log	0	Regular File	2017-11-09 1:4...
error.log	0	Regular File	2017-11-09 1:4...
other_vhosts_access.log	0	Regular File	2017-11-09 1:4...

The Properties window on the left shows the MD5 verification hash for access.log:

MD5 verification hash: d41d8cd98f00b204e9800998ecf8427e

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

The screenshot shows the Evidence Tree on the left with the path: Custom Content Image(Multi) [AD1] > Horosx.E01:Partition 5 (14304MB) NONAME [ext4] > [root] > Downloads > myfirsthack > credentials_tool.zip. The File List on the right shows the following files:

Name	Size	Type	Date Modified
Win32	0	Directory	2018-12-09 11:...
x64	0	Directory	2018-12-09 11:...
kiwi_passwords.yar	3	Regular File	2018-08-19 10:...
mimicom.idl	3	Regular File	2018-08-19 10:...
README.md	5	Regular File	2018-08-19 10:...

There was a super-secret file created. What is the absolute path?

The screenshot shows the Evidence Tree on the left with the path: Forensic.ad1 > Custom Content Image(Multi) [AD1] > Horosx.E01:Partition 5 (14304MB) NONAME [ext4] > [root] > var > log. The File List on the right shows the following files:

Name	Size	Type	Date Modified
Downloads	4	Directory	2019-03-22 3:0...
Music	4	Directory	2019-03-14 3:3...
Pictures	4	Directory	2019-03-22 5:4...
Public	4	Directory	2019-03-14 3:3...
Templates	4	Directory	2019-03-14 3:3...
Videos	4	Directory	2019-03-14 3:3...
.bashrc	4	Regular File	2017-11-09 1:3...
.bash_history	2	Regular File	2019-03-22 5:4...
.ICAuthn	3	Regular File	2019-03-22 3:1...
profile	1	Regular File	2017-10-30 12:...
.rmd	1	Regular File	2019-03-20 9:2...
.viminfo	9	Regular File	2019-03-22 4:1...
izZLaohL.jpeg	128	Regular File	2019-03-22 5:3...
enky	0	Regular File	2019-03-22 2:4...

The Properties window on the left shows the file name: .bash_history. The File List on the right shows the following files:

Name	Size	Type	Date Modified
Downloads	4	Directory	2019-03-22 3:0...
Music	4	Directory	2019-03-14 3:3...
Pictures	4	Directory	2019-03-22 5:4...
Public	4	Directory	2019-03-14 3:3...
Templates	4	Directory	2019-03-14 3:3...
Videos	4	Directory	2019-03-14 3:3...
.bashrc	4	Regular File	2017-11-09 1:3...
.bash_history	2	Regular File	2019-03-22 5:4...
.ICAuthn	3	Regular File	2019-03-22 3:1...
profile	1	Regular File	2017-10-30 12:...
.rmd	1	Regular File	2019-03-20 9:2...
.viminfo	9	Regular File	2019-03-22 4:1...
izZLaohL.jpeg	128	Regular File	2019-03-22 5:3...
enky	0	Regular File	2019-03-22 2:4...

The Properties window on the left shows the file name: .bash_history. The File List on the right shows the following files:

Name	Size	Type	Date Modified
Downloads	4	Directory	2019-03-22 3:0...
Music	4	Directory	2019-03-14 3:3...
Pictures	4	Directory	2019-03-22 5:4...
Public	4	Directory	2019-03-14 3:3...
Templates	4	Directory	2019-03-14 3:3...
Videos	4	Directory	2019-03-14 3:3...
.bashrc	4	Regular File	2017-11-09 1:3...
.bash_history	2	Regular File	2019-03-22 5:4...
.ICAuthn	3	Regular File	2019-03-22 3:1...
profile	1	Regular File	2017-10-30 12:...
.rmd	1	Regular File	2019-03-20 9:2...
.viminfo	9	Regular File	2019-03-22 4:1...
izZLaohL.jpeg	128	Regular File	2019-03-22 5:3...
enky	0	Regular File	2019-03-22 2:4...

What program used didyouthinkwedmakeiteasy.jpg during execution?

Evidence Tree

FirstHack.ad1

Custom Content Image(Multi) [AD1]

Horoux.E01-Partition 5 [14304MB] [NONAME] [ext4]

[root]

boot

root

var

log

File List

Name	Size	Type	Date Modified
Downloads	4	Directory	2019-03-22 3:0...
Music	4	Directory	2019-03-14 3:3...
Pictures	4	Directory	2019-03-22 5:4...
Public	4	Directory	2019-03-14 3:3...
Templates	4	Directory	2019-03-14 3:3...
Videos	4	Directory	2019-03-14 3:3...
.bashrc	4	Regular File	2017-11-09 1:3...
.bash_history	2	Regular File	2019-03-22 5:4...
.clicauthority	3	Regular File	2019-03-22 3:1...
.profile	1	Regular File	2017-10-30 12:...
.rmd	1	Regular File	2019-03-20 9:2...
.viminfo	9	Regular File	2019-03-22 4:1...
inZLAohL.jpeg	128	Regular File	2019-03-22 5:3...
only	0	Regular File	2019-03-22 2:4...

```

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 vi sudo
ls
sudo ifng
ifconfig
apt-get moo
sudo apt-get moo
sudo apt-get moo
sudo apt-get 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
history > didyouthinkwedmakeiteasy.jpg
clear
history
exit
touch keys.txt
pwd

```

Properties

.bash_history

Regular File

1,435

4,096

3,047,437

2019-03-22 5:48:41 AM

2019-03-21 6:52:07 PM

2019-03-22 5:48:41 AM

True

UNIX Security Attributes

Unix Permissions

UID

What is the third goal from the checklist Karen created?

Evidence Tree

FirstHack.ad1

Custom Content Image(Multi) [AD1]

Horoux.E01-Partition 5 [14304MB] [NONAME] [ext4]

[root]

boot

root

binwalk

cache

config

group

local

mozilla

ms4

Desktop

Documents

Downloads

Music

Pictures

Public

Templates

Videos

var

File List

Name	Size	Type	Date Modified
minimalkatz	4	Directory	2019-03-22 3:0...
Checklist	1	Regular File	2019-03-22 4:1...

```

Check List:
- Gain Bob's Trust
- Learn how to hack
- Profit

```

Properties

Checklist

Regular File

60

4,096

3,058,198

2019-03-22 4:18:33 AM

2019-03-22 4:18:33 AM

2019-03-22 4:18:50 AM

True

How many times was apache run? Apache did not run

Evidence Tree

log

apache2

apt

chirookit

couchdb

drda

esim4

gdm3

glusterfs

inetam

installer

colleconf

macchanger.log.1.gz

mysql

error.log.1.gz

error.log.2.gz

nginx

ntpdate

openvpn

postgresql

samba

speech-dispatcher

stunm4

File List

Name	Size	Type	Date Modified
access.log	0	Regular File	2017-11-09 1:4...
error.log	0	Regular File	2017-11-09 1:4...
other_vhosts_access.log	0	Regular File	2017-11-09 1:4...

```

000 67 5F 0A 00 0C 00 01 02-2E 00 00 00 65 5F 0A 00 0A .....t...
010 0C 00 02 02 2E 00 00-69 5F 0A 00 14 00 0A 01 .....h.....
020 61 63 65 73 73 2E 0C-6F 67 00 00 69 5F 0A 00 access.log.1...
030 14 00 09 01 65 72 72 6F-72 2E 6C 6F 00 00 00 ...error.log...
040 6A 5F 0A 00 B4 0F 17 01-6F 74 69 65 72 5F 76 69 j...other_vh...
050 6F 73 74 73 5F 61 63 63-65 73 73 2E 6C 6F 67 00 osts_access.log...
060 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
070 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
080 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....

```

Properties

access.log

Regular File

0

0

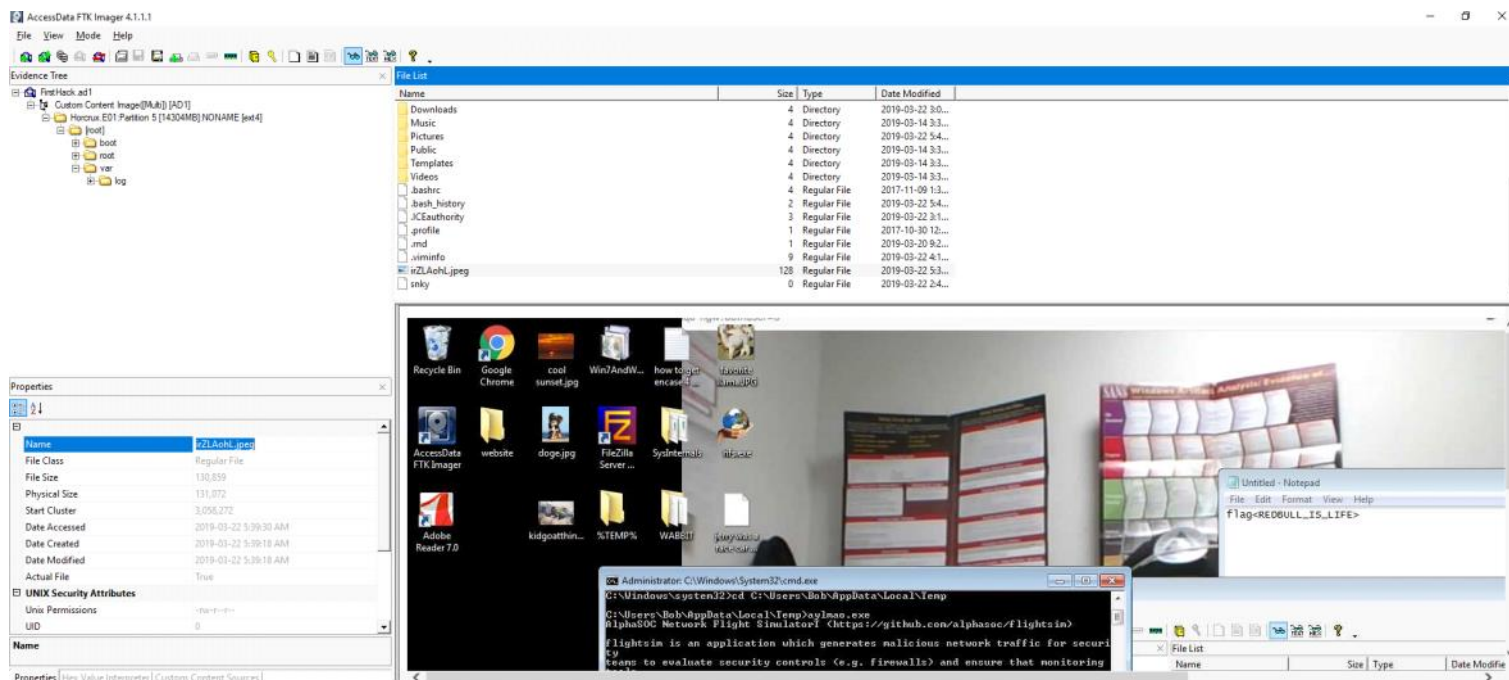
0

2017-11-09 1:4...

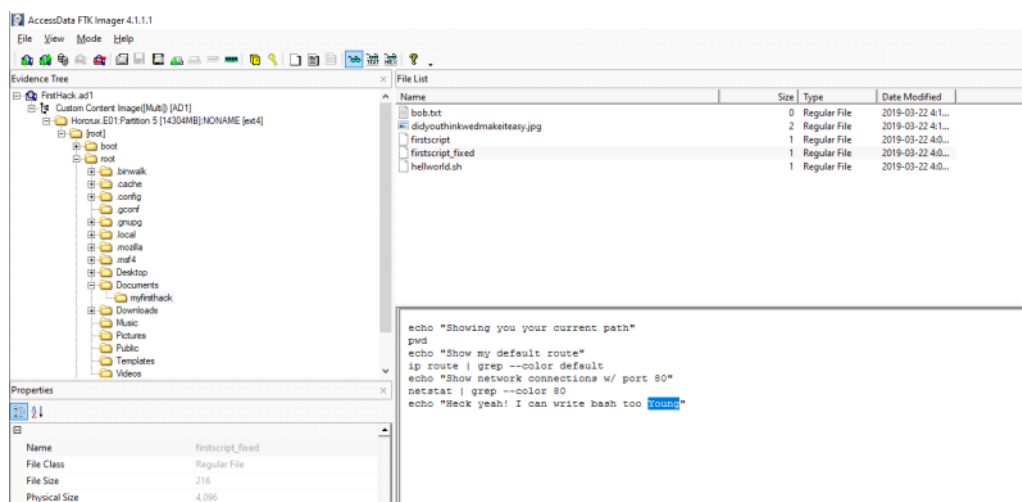
2017-11-09 1:4...

2017-11-09 1:4...

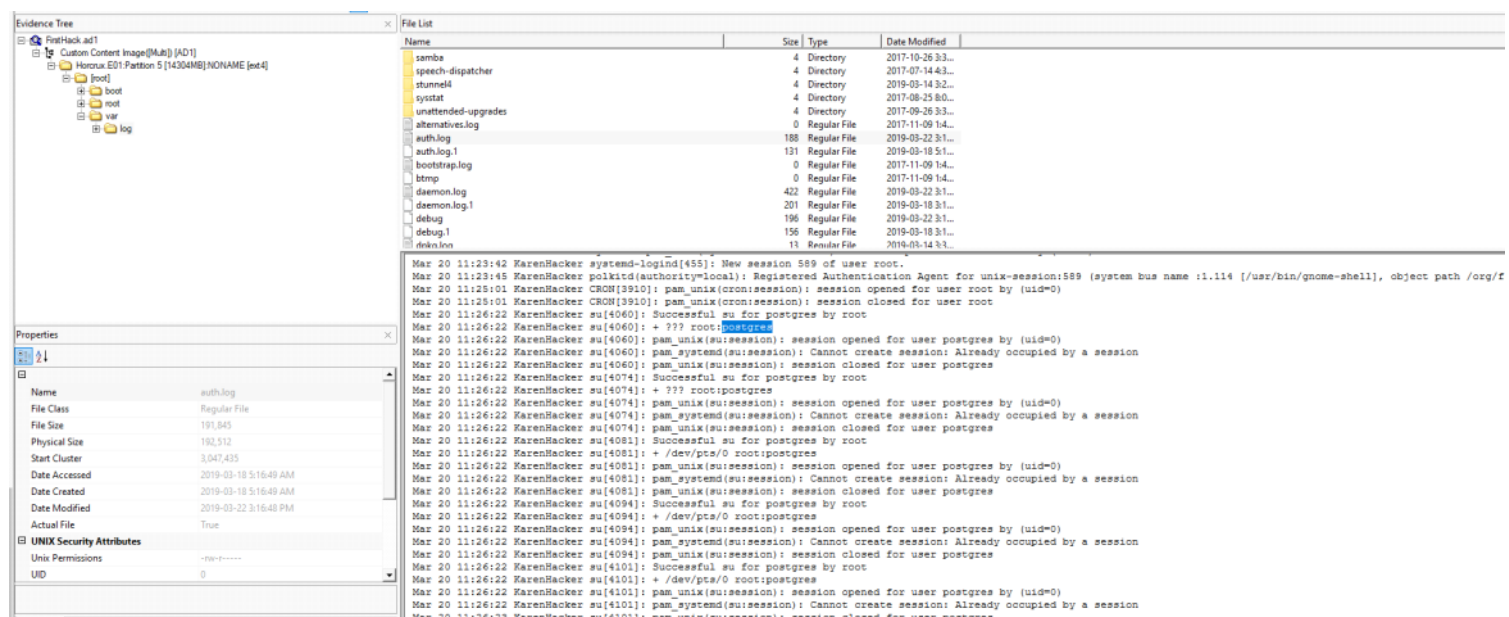
It is believed this machine was used to attack another. What file proves this?



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



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



Based on the bash history, what is the current working directory?

File View Mode Help

Evidence Tree

- firsthack.ad1
 - Custom Content Image(1)(Akh)(AD1)
 - Heroux.E01-Partition 5 [14304MB] NONAME [ext4]
 - [root]
 - boot
 - root
 - var
 - log

File List

Name	Size	Type	Date Modified
Downloads	4	Directory	2019-03-22 3:0...
Music	4	Directory	2019-03-14 3:3...
Pictures	4	Directory	2019-03-22 5:4...
Public	4	Directory	2019-03-14 3:3...
Templates	4	Directory	2019-03-14 3:3...
Videos	4	Directory	2019-03-14 3:3...
.bashrc	4	Regular File	2017-11-09 1:3...
.bash_history	2	Regular File	2019-03-22 5:4...
.ICEauthority	3	Regular File	2019-03-22 3:1...
.profile	1	Regular File	2017-10-30 12:...
.rmd	1	Regular File	2019-03-20 9:2...
.viminfo	9	Regular File	2019-03-22 4:1...
wZAohl.jpeg	128	Regular File	2019-03-22 5:3...
.snky	0	Regular File	2019-03-22 2:4...

Properties

Name: .bash_history

File Class: Regular File

File Size: 1,455

Physical Size: 4,096

Start Cluster: 3,047,457

Date Accessed: 2019-03-22 5:40:44 AM

Date Created: 2019-03-21 6:50:07 PM

Date Modified: 2019-03-22 5:40:44 AM

Actual File: True

UNIX Security Attributes

Unix Permissions: -rwxr-xr-x

UID: 0

```
ls
cd ../root
cd ../root/Documents/myfirsthack/../../Desktop/
#l
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
ifconfi
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 didyouthinkvedmakeiteasy.jpg
clear
history
exit
touch keys.txt
pwd
```