

Insider Challenge

Scenario:

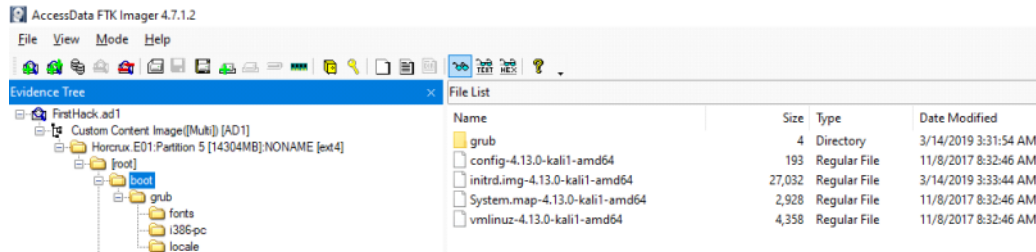
After Karen started working for 'TAAUSAI,' she began to do some illegal activities inside the company. 'TAAUSAI' hired you as a soc analyst to kick off an investigation on this case.

You acquired a disk image and found that Karen uses Linux OS on her machine. Analyze the disk image of Karen's computer and answer the provided questions.

Task 1:

What distribution of Linux is being used on this machine?

I opened the image file with FTK Imager and at the boot folder I saw the Kali version

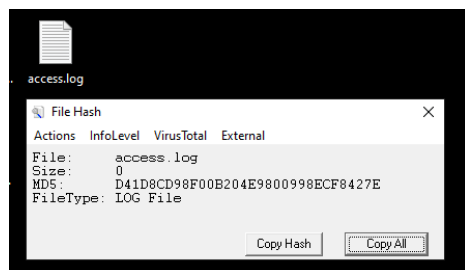
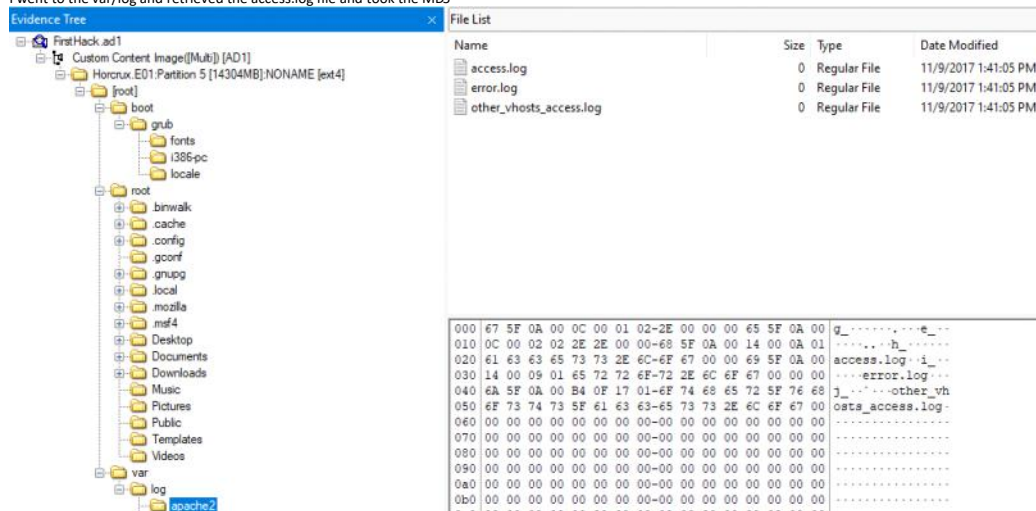


Answer: kali

Task 2:

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

I went to the var/log and retrieved the access.log file and took the MD5



Answer: d41d8cd98f00b204e9800998ecf8427e

Task 3:

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

I went to the Downloads folder

Evidence Tree

FirstHack.ad1

Custom Content Image(Multi) [AD1]

Horcrux.E01:Partition 5 [14304MB]:NONAME [ext4]

boot

grub

fonts

i386-pc

locale

root

binwalk

cache

config

gconf

gnupg

local

mozilla

msf4

Desktop

Documents

myfirsthack

Downloads

Music

Pictures

Public

Templates

Videos

var

log

apache2

apt

chkroutkit

couchdb

drac

exim4

gdm3

glusterfs

inetam

installer

macchanger.log.1.gz

mysql

nginx

ripstat

opensn

postgre

samba

speech-dispatcher

stunnel4

syslog.2.gz

sysstat

unattended-upgrades

File List

Name	Size	Type	Date Modified
Music	4	Directory	3/14/2019 3:36:07 AM
Pictures	4	Directory	3/22/2019 5:47:48 AM
Public	4	Directory	3/14/2019 3:36:07 AM
Templates	4	Directory	3/14/2019 3:36:07 AM
Videos	4	Directory	3/14/2019 3:36:07 AM
.bashrc	4	Regular File	11/9/2017 1:31:54 PM
.bash_history	2	Regular File	3/22/2019 5:48:44 AM
JCEaution	3	Regular File	3/22/2019 3:16:16 PM
.profile	1	Regular File	10/30/2017 12:46:42 PM
.rmd	1	Regular File	3/20/2019 9:26:21 PM
.viminfo	9	Regular File	3/22/2019 4:12:59 AM
k2LAchL.jpeg	128	Regular File	3/22/2019 5:39:18 AM
snky	0	Regular File	3/22/2019 2:48:15 AM

```

ls
vim firstscript
vim firstscript_fixed
./firstscript_fixed
flag{this is a flag}
ifconfig
od ..
od ..
od ..
od /var/log/
ls
od ..
od -
ls
pwd
pwd
top
wall -h
wall yolo
ls
pwd
od ..
ls
od home/
ls
od /root
ls
od ../root
od ../root/Documents/myfirsthack/../../Desktop/
sl
ls
od ../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-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
binwalk didyouthinkvedmakeiteasy.jpg
clear
history
exit
touch keye.txt
pwd

```

Custom Content Sources

Evidence:File System(Path)\File	Options

New

Edit

Remove

Remove All

Create Image

Answer: binwalk

Task 6:
What is the third goal from the checklist Karen created?

I found the Checklist file on the Desktop

FirstHack.ad1

Custom Content Image(Multi) [AD1]

Horcrux.E01:Partition 5 [14304MB]:NONAME [ext4]

boot

grub

fonts

i386-pc

locale

root

binwalk

cache

config

gconf

gnupg

local

mozilla

msf4

Desktop

Documents

myfirsthack

Downloads

Music

Pictures

Name	Size	Type	Date Modified
mimikatz	4	Directory	3/22/2019 3:04:57 AM
Checklist	1	Regular File	3/22/2019 4:18:50 AM

Check List:

- Gain Bob's Trust
- Learn how to hack
- Profit

Answer: profit

Task 7:
How many times was apache run?

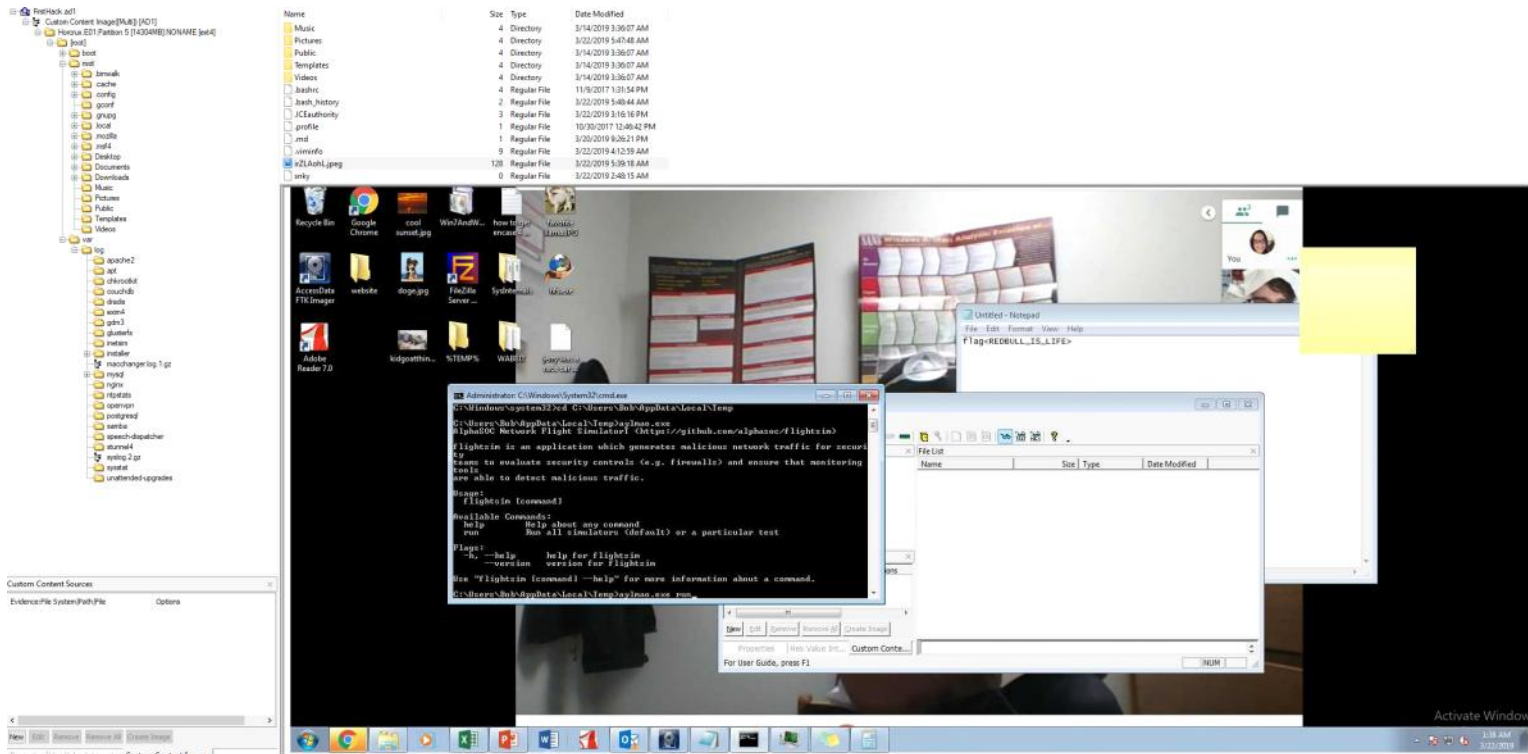
I checked the apache2 folder and all the logs was empty that means the Apache was never run

<div><div>FirstHack.ad1</div><div><div>Custom Content Image[Multi] [AD1]</div><div><div>Horoux.E01:Partition 5 [14304MB]:NONAME [ext4]</div><div><div>root</div><div><div>boot</div><div><div>root</div><div><div>binwalk</div><div><div>cache</div><div><div>config</div><div><div>gconf</div><div><div>gnupg</div><div><div>local</div><div><div>mozilla</div><div><div>msf4</div><div><div>Desktop</div><div><div>mimikatz</div><div><div>Documents</div><div><div>Downloads</div><div><div>Music</div><div><div>Pictures</div><div><div>Public</div><div><div>Templates</div><div><div>Videos</div><div><div>var</div><div><div>log</div><div><div>apache2</div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div>	<table><tr><th>Name</th><th>Size</th><th>Type</th><th>Date Modified</th></tr><tr><td>other_vhosts_access.log</td><td>0</td><td>Regular File</td><td>11/9/2017 1:41:05 PM</td></tr><tr><td>error.log</td><td>0</td><td>Regular File</td><td>11/9/2017 1:41:05 PM</td></tr><tr><td>access.log</td><td>0</td><td>Regular File</td><td>11/9/2017 1:41:05 PM</td></tr></table>	Name	Size	Type	Date Modified	other_vhosts_access.log	0	Regular File	11/9/2017 1:41:05 PM	error.log	0	Regular File	11/9/2017 1:41:05 PM	access.log	0	Regular File	11/9/2017 1:41:05 PM
Name	Size	Type	Date Modified														
other_vhosts_access.log	0	Regular File	11/9/2017 1:41:05 PM														
error.log	0	Regular File	11/9/2017 1:41:05 PM														
access.log	0	Regular File	11/9/2017 1:41:05 PM														

Answer: 0

Task 8:
It is believed this machine was used to attack another. What file proves this?

I saw an image inside the root folder and inside the image there was some picture from Windows machine with a cmd



Answer: irZLAohl.jpeg

Task 9:
Within the Documents file path, it is believed that Karen was taunting a fellow computer expert through a bash script. Who was Karen taunting?

I checked the firstscript_fixed inside the Documents\myfirsthack folder

Evidence Tree

FirstHack.ad1

Custom Content Image(Multi) [AD1]

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

[root]

boot

root

binwalk

cache

config

gconf

gnupg

local

mozilla

msf4

Desktop

Documents

myfirsthack

Downloads

Music

Pictures

Public

Templates

Videos

var

log

apache2

File List

Name	Size	Type	Date Modified
hellworld.sh	1	Regular File	3/22/2019 4:00:22 AM
firstscript_fixed	1	Regular File	3/22/2019 4:04:53 AM
firstscript	1	Regular File	3/22/2019 4:01:52 AM
didyouthinkwedmakeiteasy.jpg	2	Regular File	3/22/2019 4:14:58 AM
bob.txt	0	Regular File	3/22/2019 4:11:22 AM

```

echo "Showing you your current path"
pwd
echo "Show my default route"
ip route | grep --color default
echo "Show network connections w/ port 80"
netstat | grep --color 80
echo "Heck yeah! I can write bash too Young"

```

Answer: young

Task 10:

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

I checked the var/log/auth.log and opened it with Notepad++ and searched for 11:26

```

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

```

Answer: postgres

Task 11:

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

I checked the .bash_history and noticed the pwd command and then the path

Evidence Tree

FirstHack.ad1

Custom Content Image(Multi) [AD1]

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

[root]

boot

root

binwalk

cache

config

gconf

gnupg

local

mozilla

msf4

Desktop

Documents

myfirsthack

Downloads

Music

Pictures

Public

Templates

Videos

var

log

apache2

apt

chkrootkit

couchdb

dradis

exim4

gdm3

glusterfs

inetsim

installer

macchanger.log.1.gz

mysql

nginx

ntpstats

openvpn

postgrey

samba

speech-dispatcher

stunnel4

syslog.2.gz

sysstat

File List

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

```

ls
vim firstscript
vim firstscript_fixed
./firstscript_fixed
flag<this is a flag>
ifconfig
cd ..
cd ..
cd ..
cd /var/log/
ls
cd ..
cd ~
ls
pwd
pwd
top
wall -h
wall yolo
ls
pwd
cd ..
ls
cd home/
ls
cd /root
ls
cd ../root
cd ../root/Documents/myfirsthack/../../Desktop/

```

Answer: root/Documents/myfirsthack/