

CyberDefenders: Insider Lab

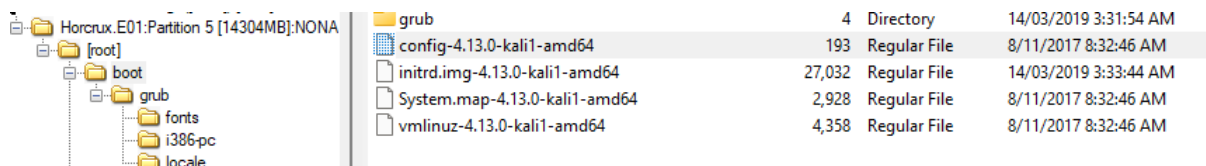
The following writeup is for [Insider Lab](#) on CyberDefenders, it involves analysing a disk image from a Linux OS using FTK Imager. Those new to disk forensics should find this room helpful and enjoyable.

Scenario: After Karen started working for 'TAAUSAI,' she began doing 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.

Which Linux distribution is being used on this machine?

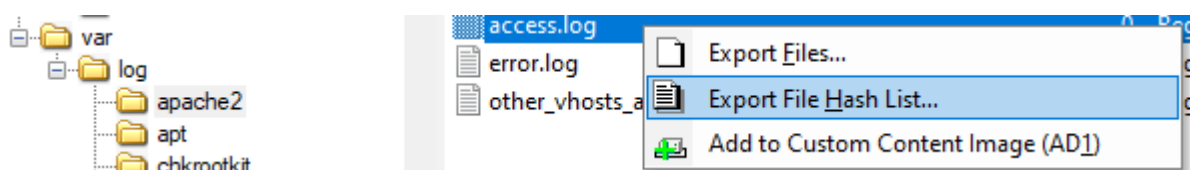
Start by loading the disk image into FTK Imager. Once loaded, we can navigate to the boot directory and see references to kali:



Answer: Kali

What is the MD5 hash of the Apache access.log file?

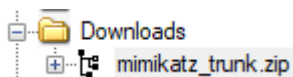
Apache's access.log file can be found in var/log/apache2. We can then right click to export the MD5 hash of the selected file:



Answer: d41d8cd98f00b204e9800998ecf8427e

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

The best place to look for downloaded files is the Downloads folder:



Mimikatz is a notorious credential dumping tool

Answer: mimikatz_trunk.zip

A super-secret file was created. What is the absolute path to this file?

Whenever someone enters a command on Linux, it gets stored in the .bash_history file. Viewing this can possibly indicate what file was created:



```
touch snky snky > /root/Desktop/SuperSecretFile.txt
cat snky snky > /root/Desktop/SuperSecretFile.txt
```

In the above image, we can see a file called “SuperSecretFile.txt” being created.

Answer: /root/Desktop/SuperSecretFile.txt

What program used the file didyouthinkwedmakeiteasy.jpg during its execution?

If you continue looking through the bash history file, we can see the binwalk is being used to analyse didyouthinkwedmakeiteasy:

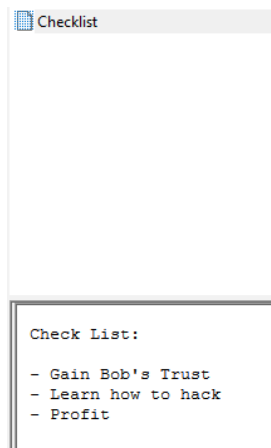
```
binwalk didyouthinkwedmakeiteasy.jpg
```

Binwalk is a tool that can identify and extract files and data that is embedded inside other files.

Answer: binwalk

What is the third goal from the checklist Karen created?

In the desktop directory, we can find the Checklist file:



Answer: Profit

How many times was Apache run?

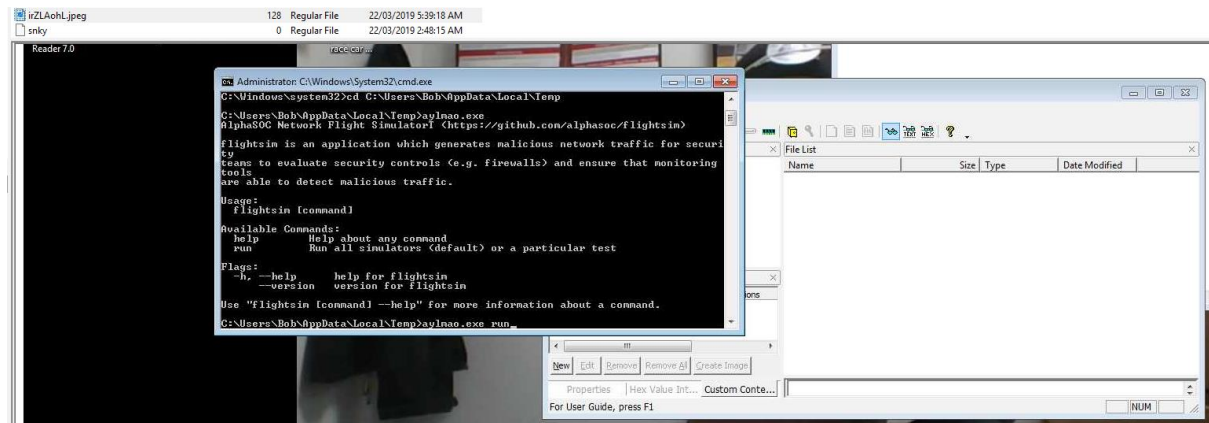
Logs can be found in the var/log directory, and in this case, we can see that all 3 apache related logs are empty, which indicate that Apache was likely not run.

Name	Size
access.log	0
error.log	0
other_vhosts_access.log	0

Answer: 0

This machine was used to launch an attack on another. Which file contains the evidence for this?

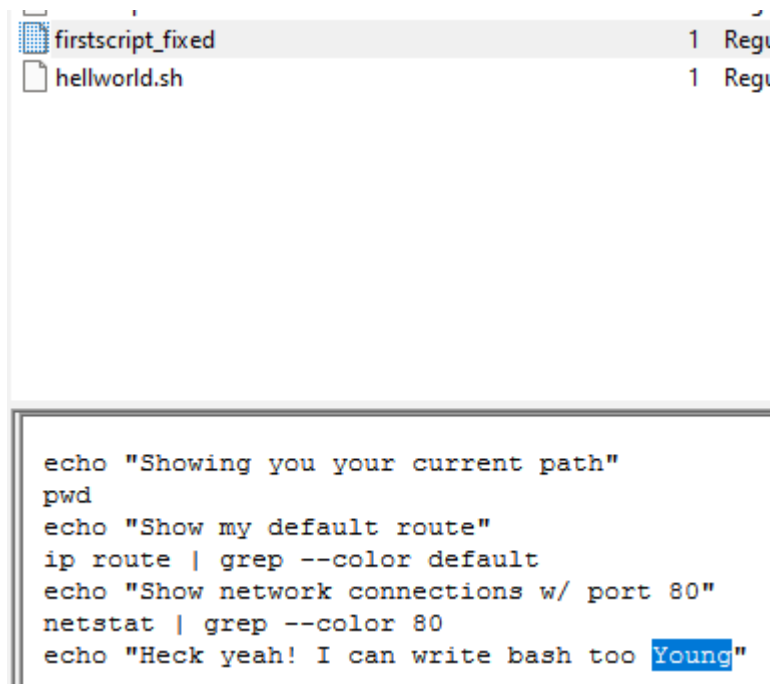
In the Root directory you can find one image file:



It appears as if this is a screenshot from a potentially compromised machine.

Answer: irZLAohL.jpeg

It is believed that Karen was taunting a fellow computer expert through a bash script within the Documents directory. Who was the expert that Karen was taunting?



```
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

A user executed the su command to gain root access multiple times at 11:26. Who was the user?

We can find logs relate to authentication in the auth.log file found in /var/log. Here we can see that the user postgres executed the su command to gain root access:

```
11:26:22 KarenHacker su[4060]: Successful su for postgres by root
11:26:22 KarenHacker su[4060]: + ??? root:postgres
11:26:22 KarenHacker su[4060]: pam_unix(su:session): session opened for user postgres by (uid=0)
11:26:22 KarenHacker su[4060]: pam_systemd(su:session): Cannot create session: Already occupied by a session
11:26:22 KarenHacker su[4060]: pam_unix(su:session): session closed for user postgres
11:26:22 KarenHacker su[4074]: Successful su for postgres by root
11:26:22 KarenHacker su[4074]: + ??? root:postgres
11:26:22 KarenHacker su[4074]: pam_unix(su:session): session opened for user postgres by (uid=0)
11:26:22 KarenHacker su[4074]: pam_systemd(su:session): Cannot create session: Already occupied by a session
11:26:22 KarenHacker su[4074]: pam_unix(su:session): session closed for user postgres
11:26:22 KarenHacker su[4081]: Successful su for postgres by root
11:26:22 KarenHacker su[4081]: + /dev/pts/0 root:postgres
11:26:22 KarenHacker su[4081]: pam_unix(su:session): session opened for user postgres by (uid=0)
11:26:22 KarenHacker su[4081]: pam_systemd(su:session): Cannot create session: Already occupied by a session
11:26:22 KarenHacker su[4081]: pam_unix(su:session): session closed for user postgres
11:26:22 KarenHacker su[4094]: Successful su for postgres by root
```

Answer: Postgres

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

```
cd ../root/Documents/myfirsthack/
```

Answer: /root/Documents/myfirsthack/