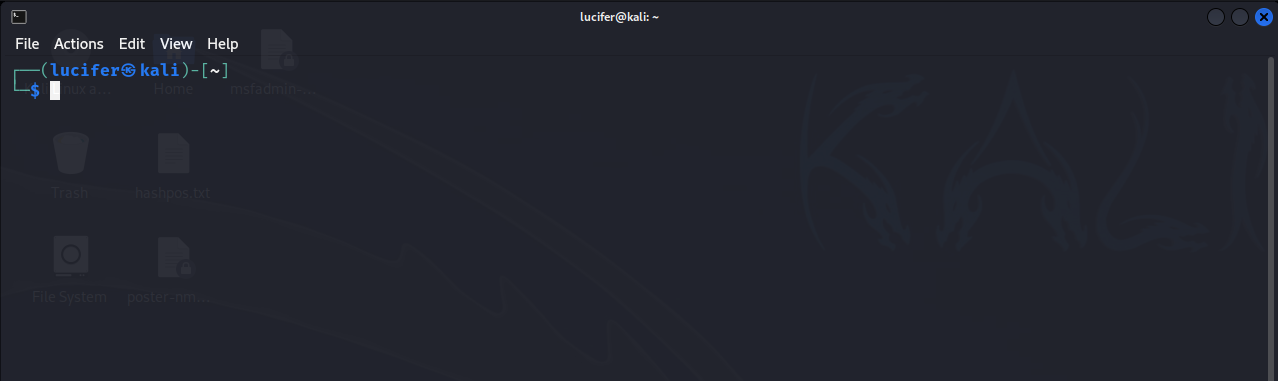
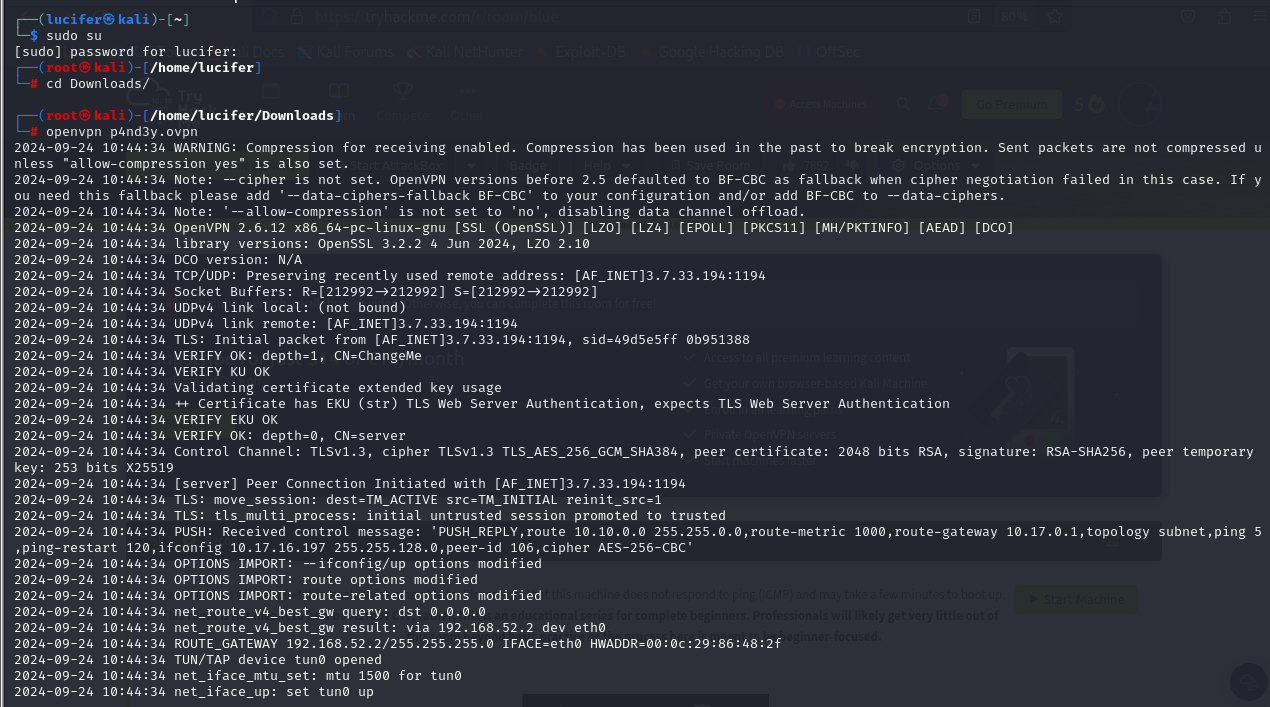
Bounty Hacker (cowboyhacker) is a box on tryhackme (<https://tryhackme.com/r/room/cowboyhacker> ) created by **sevuhl**.

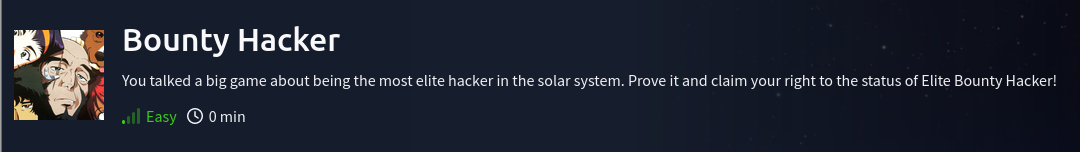
Here our **terminal**  is opened.

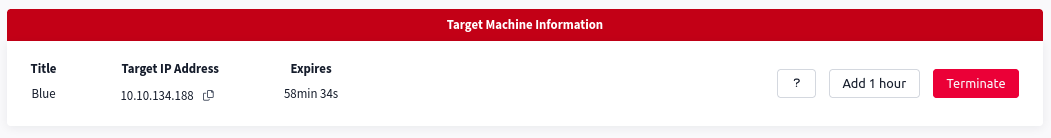


Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn’s file downloaded path after doing **sudo**.

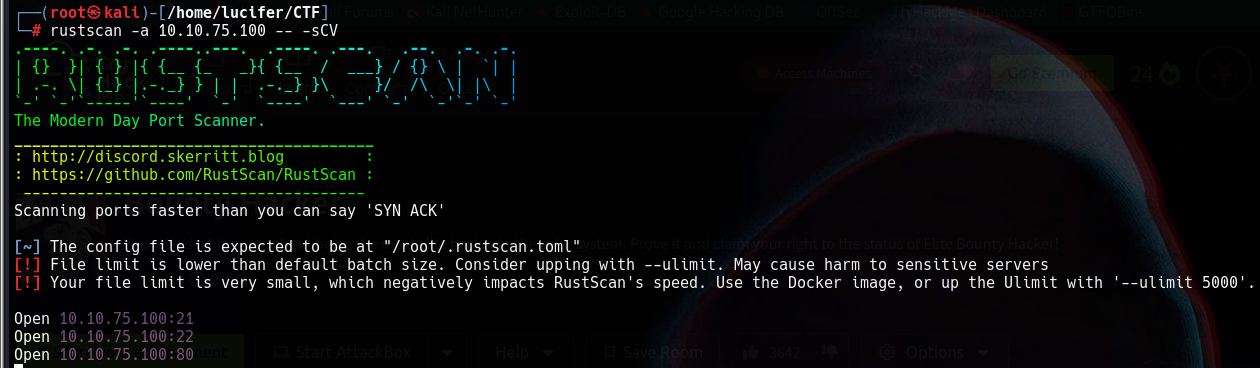


Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button.

After starting the machine it’ll get one minute to show the ip. 

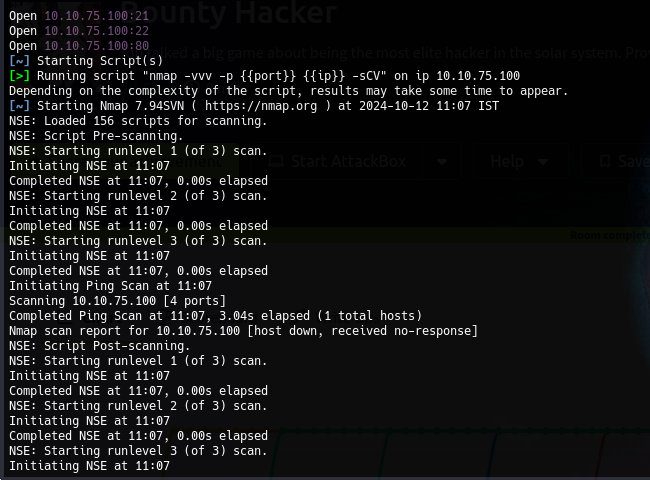


After getting the target ip first thing we’ll do is **rustscan** to see the open ports and more machine’s info.

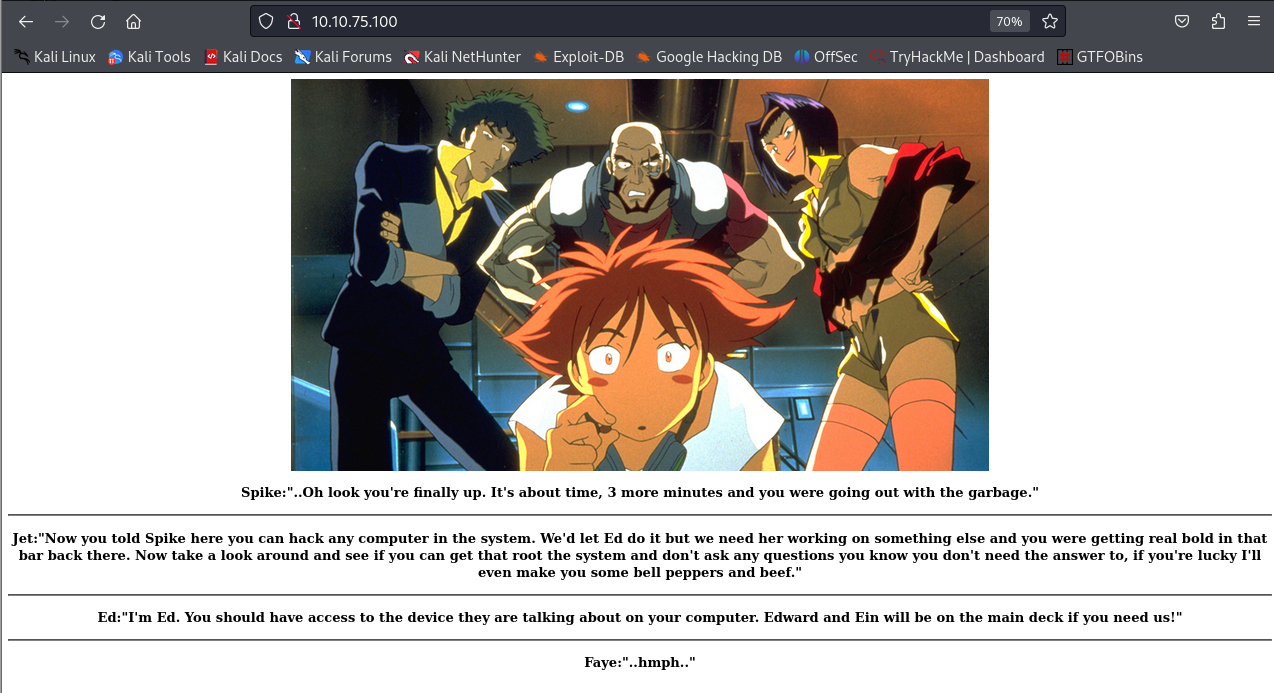


Here I am using **rustscan -a <IP> -- -sCV**  to see all the ports. You can use many more scripts like **-sCv -T4 <IP>**

Seems like our scan is completed. Looks like there are total 3 ports open.

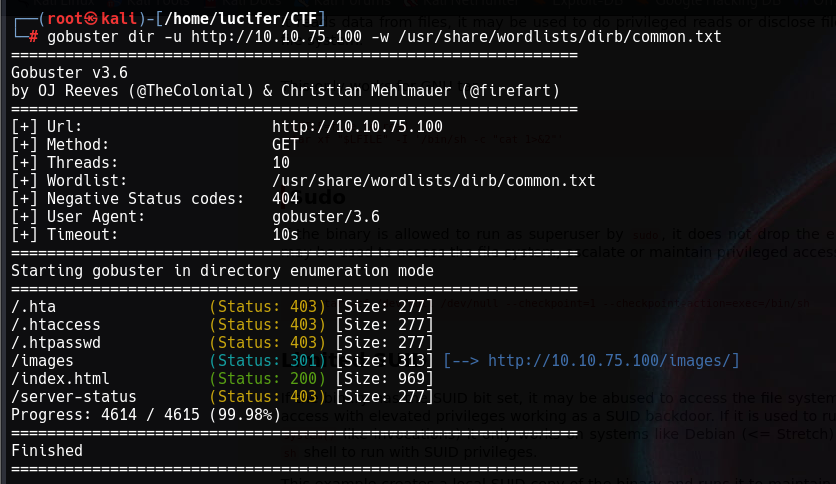


Now we know that we have a web server running we will explore the website first. The main page of website looks something like this.



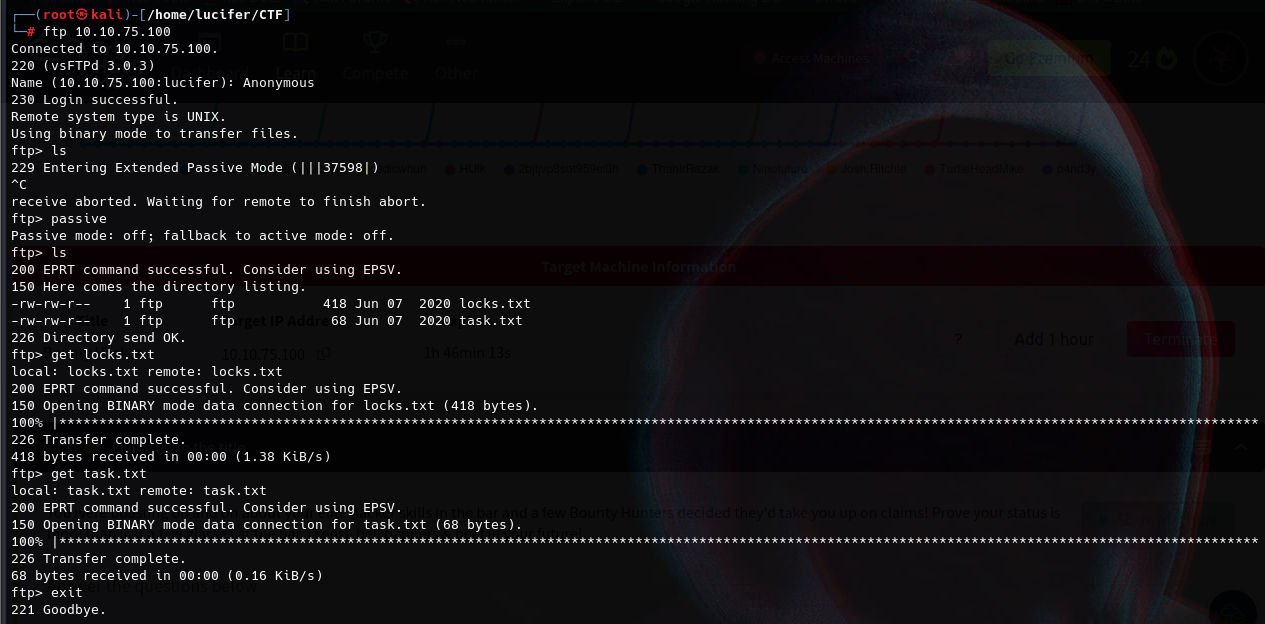
Here we can see number of users who can help us get ssh later. So we will note their names : **Spike, Jet, Edward, Ein, Faye**

We will now use gobuster to see all the directories.

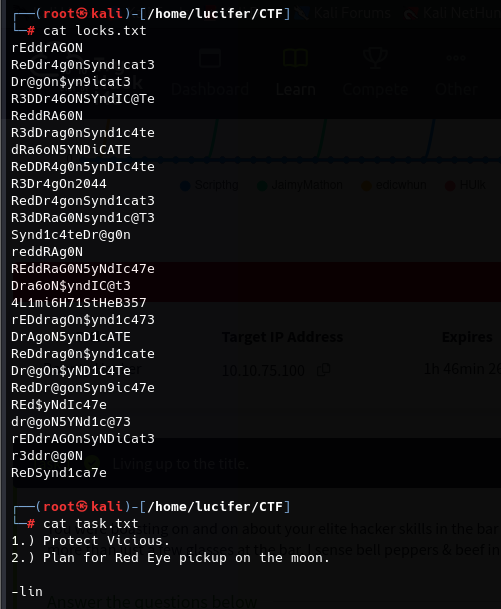


We won’t find anything suspicious later on the website.

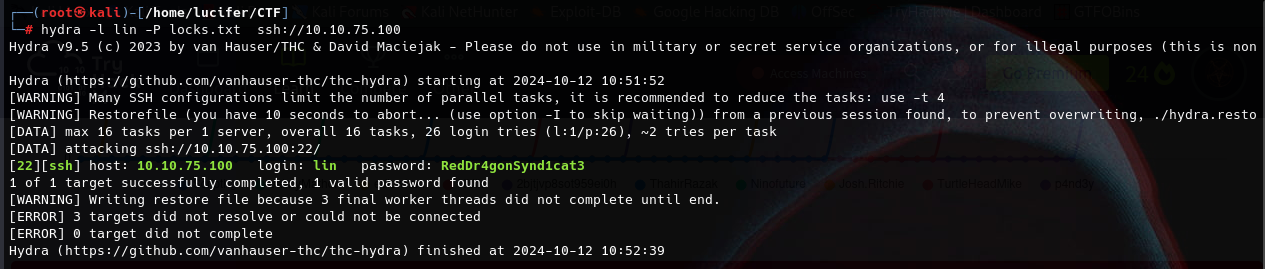
Now we have another port open as we know which is **ftp.** We will try to do **Anonymous** login and see what’s there.



We found two text files **tasks.txt** and **locks.txt**. The tasks file give us a information about a task which is given to us by another user **lin.** And the other text file gives us a list which could be a **password list.**

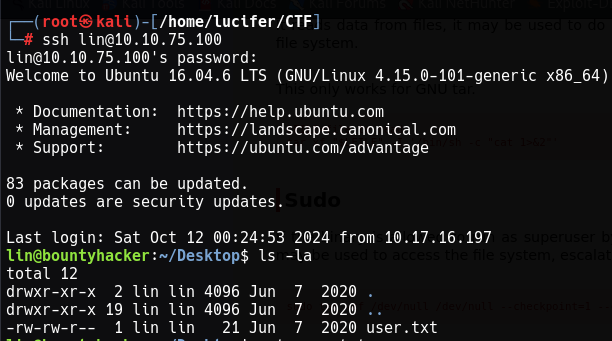


Now we can use the users and Passwords to brute-force ssh with the help of a tool called **hydra.**



We will get ssh login with user and pass : **lin:RedDr4gonSynd1cat3**

We will use the credentials for ssh login.

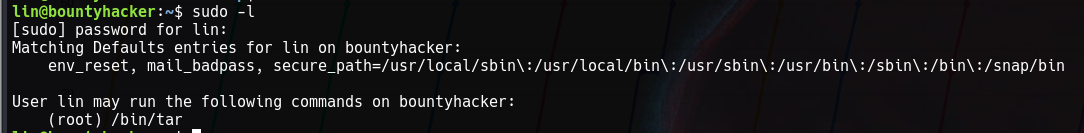


We get a successful ssh login and we got our first **user.txt** file.

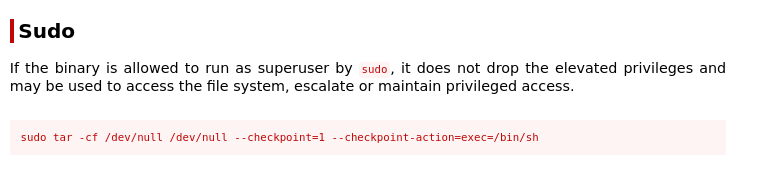
Now we need our second file which will be in **root**  folder .

But we need to escalate our privileges to get there. We can list what are the process ran by root and we can use them to get root access.

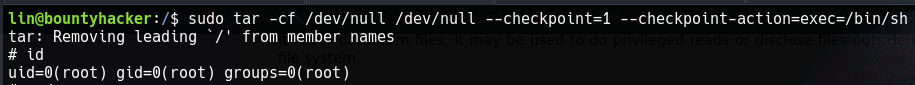
We will run **sudo -l** to see the processes.



There is a **/bin/tar** running as root. We can use **GTFOBins** to see the commands from the tar to get sudo access. The command will be like this:



Now we will run the following command to gain root.



And we can see we are root.

Now we can get our **root.txt** file from the root folder.

