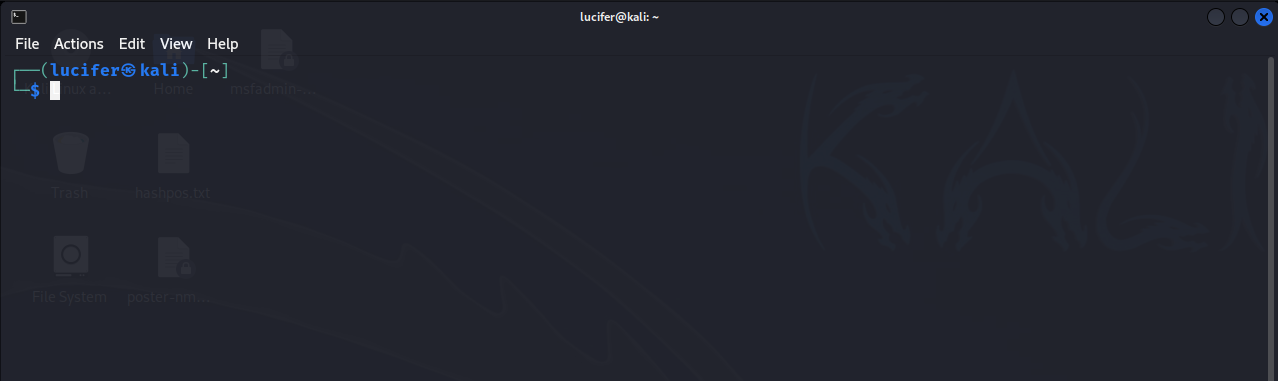
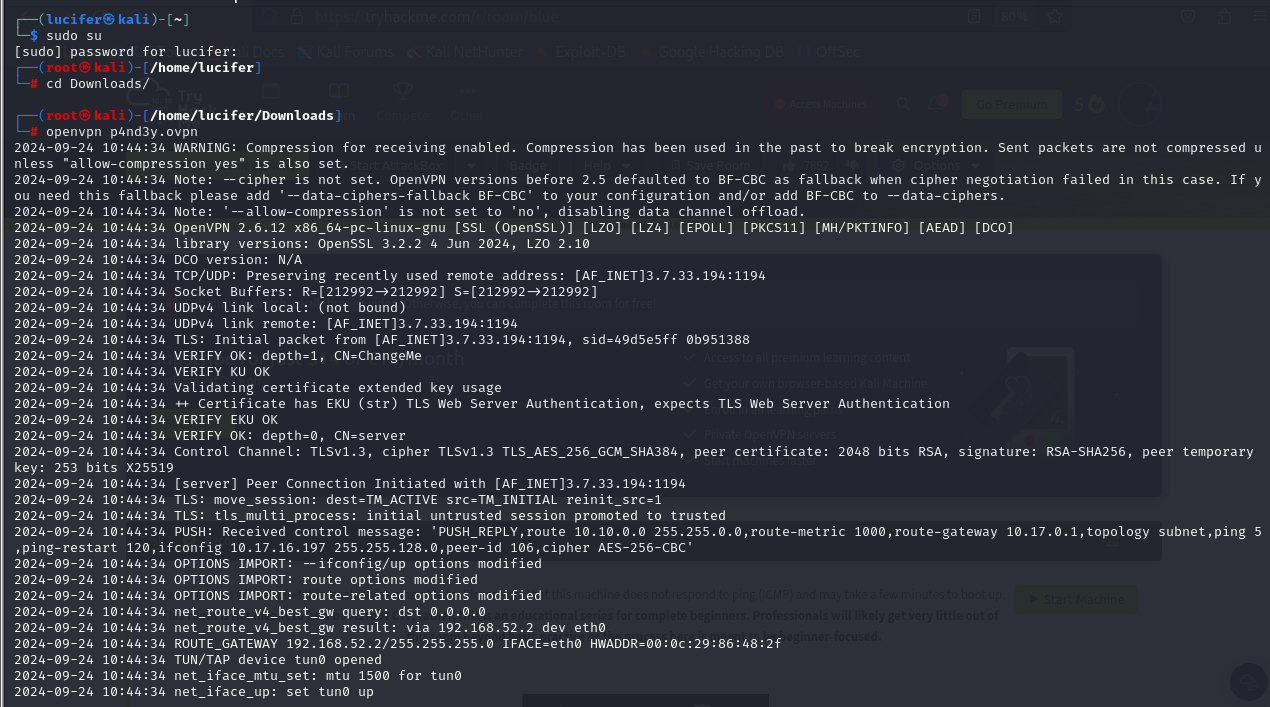
Pickle Rick is a box on tryhackme (<https://tryhackme.com/r/room/picklerick> ) created by **ar33zy and tryhackme**.

Here our **terminal**  is opened.

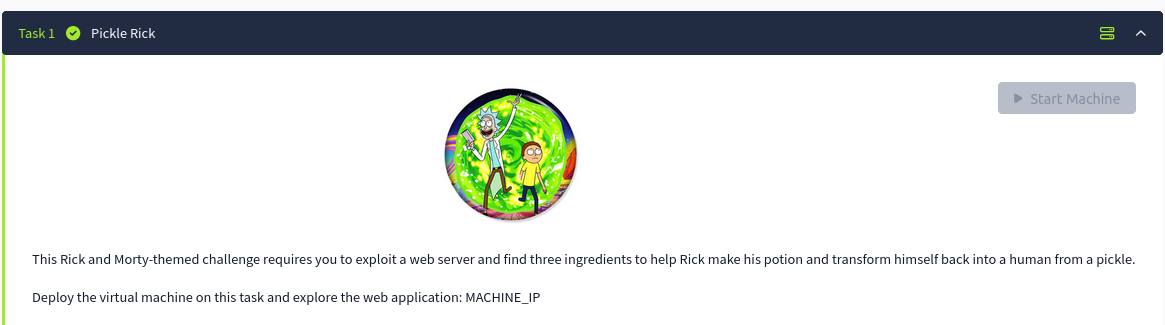


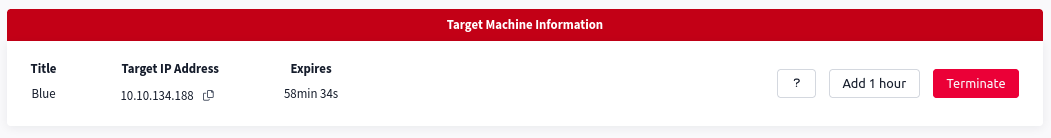
Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn’s file downloaded path after doing **sudo**.



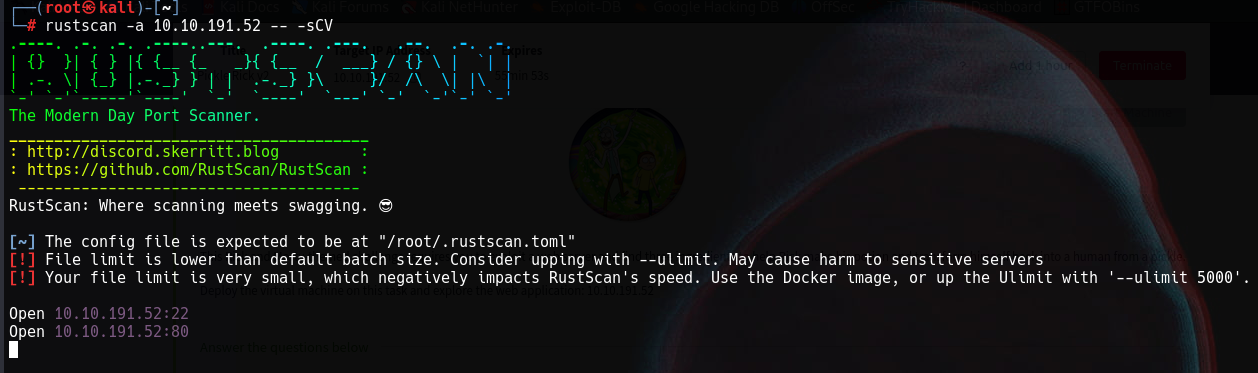
Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button.

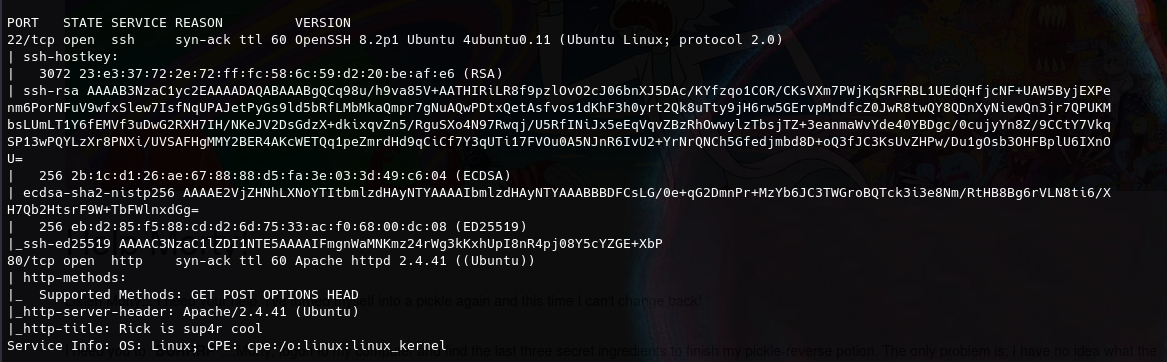
After starting the machine it’ll get one minute to show the ip.





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

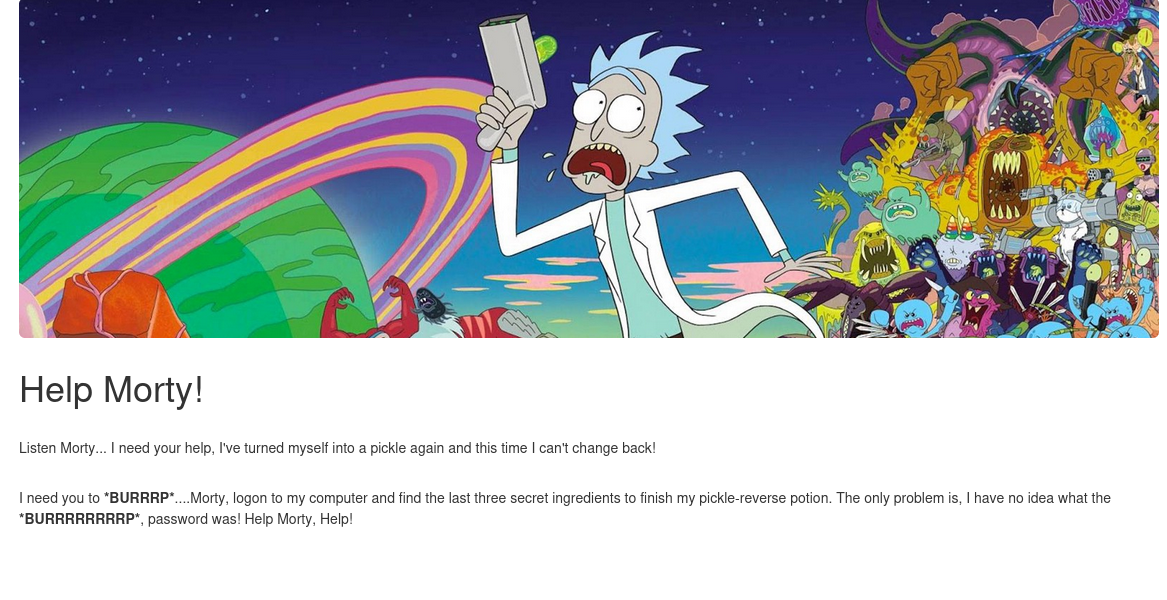
Here I am using **rustscan -a <IP> -- -sCV**  to see all the ports. You can use many more scripts like **-sCv -T4 <IP>**



Here we can see there are only two ports open which are **ssh** and **http.**

Now we will explore the web page as we know http server is running on this ip and look for any exploit or vulnerability present.

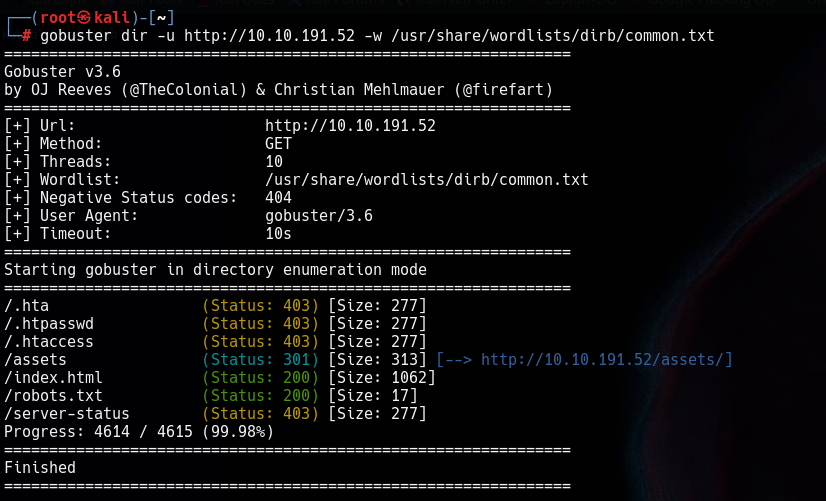
Website’s main page looks something like this.



After further exploring the main page we got a username is main page’s page source.

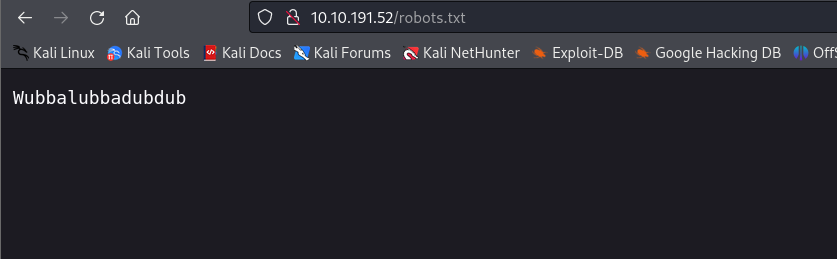


We will note the username in case. We will also start directory busting using gobuster and look for different directories which are present.

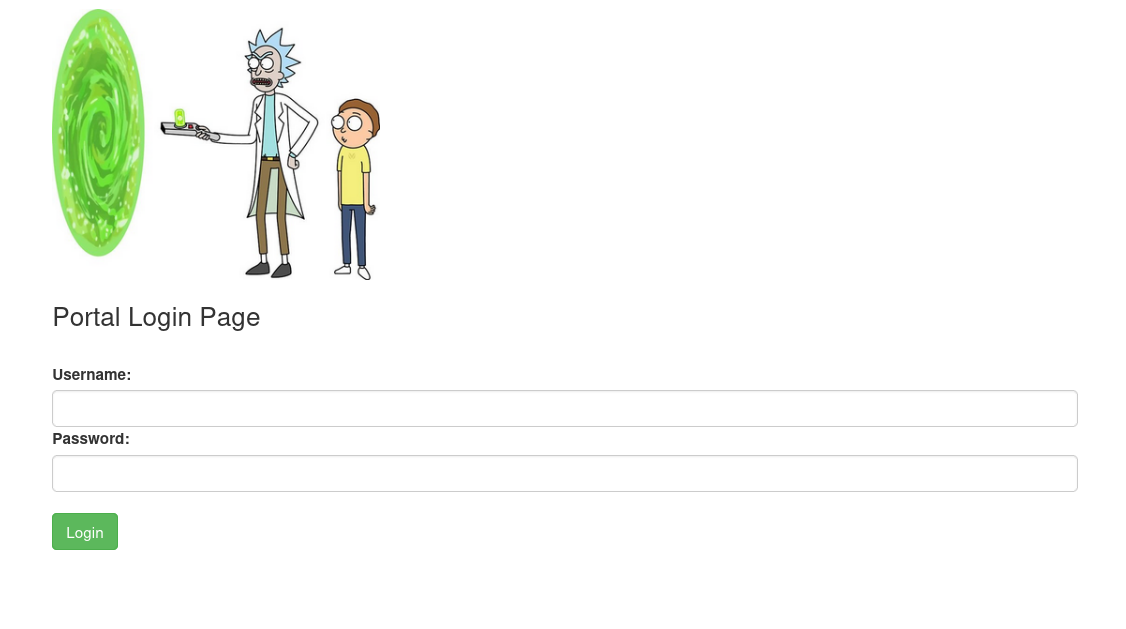


We will check every directory one-by-one and look for anything important.

We found a text in **robots.txt** file which can be a password somewhere. We will not that also.



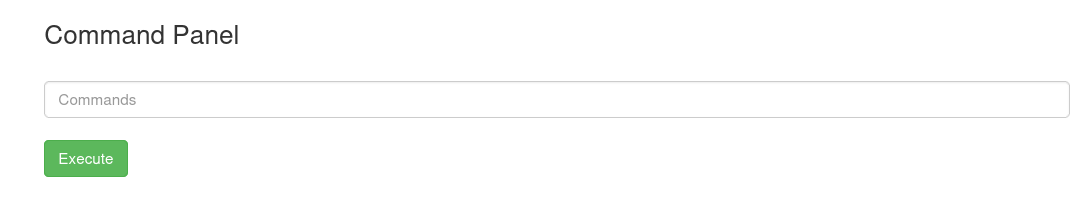
We will try for **login.php** in the website and we will get one after further enum. We can see there is a username and password filed in that directory.



We will try with the username and the text we found previously which was

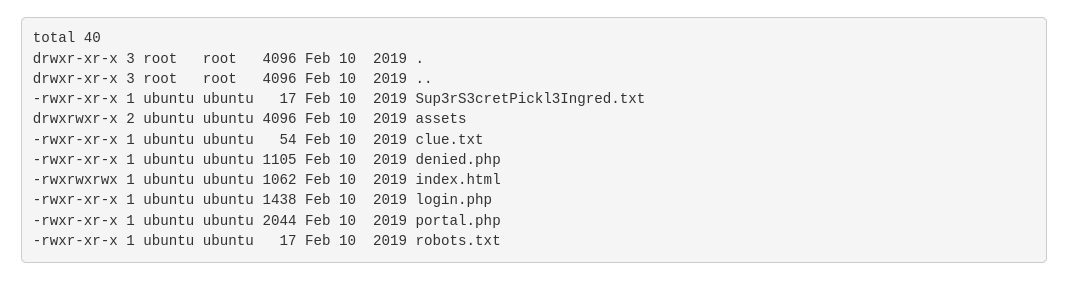
**R1ckRul3s:** **Wubbalubbadubdub**

And we got a command prompt.



Now we can try different commands we know like **ls -la, pwd, sudo, sudo -l, etc.**

After ls -la we get the following list with the first ingredient and the clue for other.



We can’t use commands like **cat, vim,** etc. But we can use **less** to read our files.

After typing **less Sup3rS3retPickl3Ingred.txt** we get our 1st ingredient.



Now we check for the other two but before that we should check what sudo privileges we have got by command **sudo -l**

****

It says that we can do all sudo commands to check and read any file without password.

After further exploring we found our 2nd ingredient in the home directory .

It contains user rick who have the 2nd ingredient.

We will use command **sudo less ‘/home/rick/second ingredients’** to read the file.



We get our 2nd ingredient.

Now we all know our third and final ingredient will be in root folder.

As we know we have sudo access we will use same command for the 3rd ingredient.

It is **‘sudo less /root/3rd.txt’** and we will get our third ingredient.

