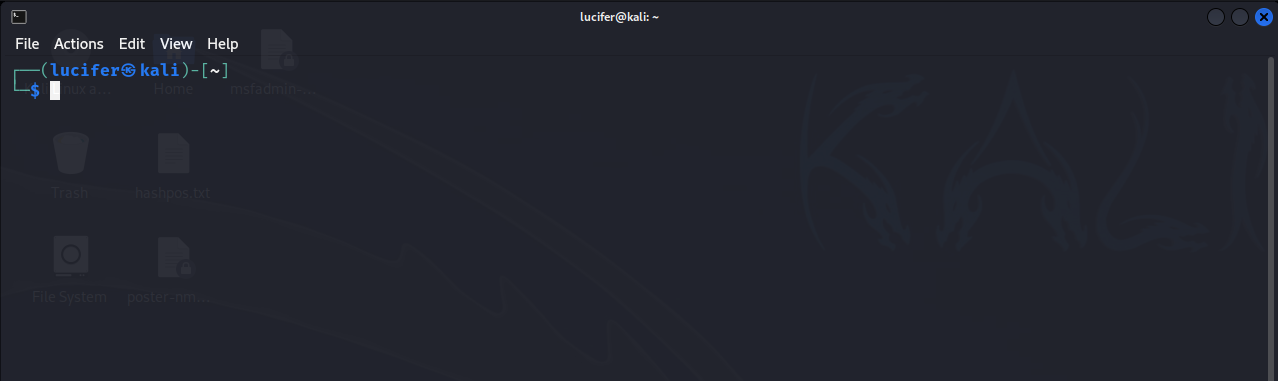
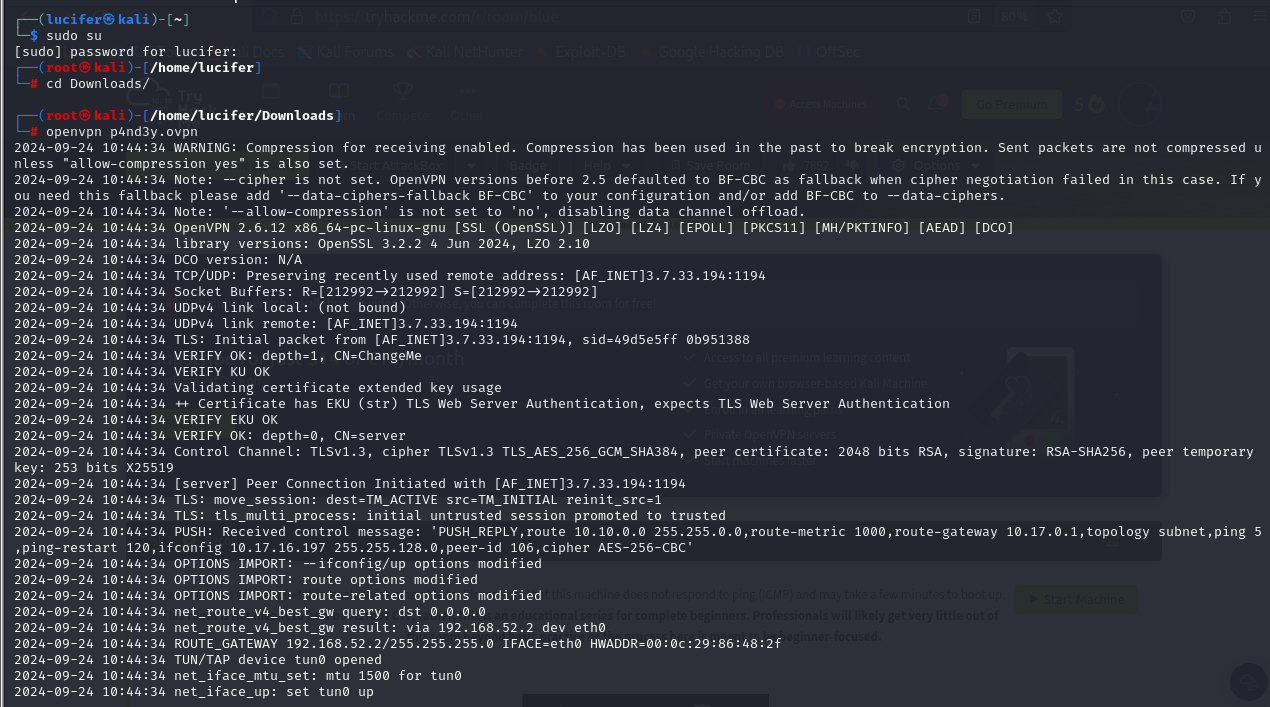
Mr Robot is a box on tryhackme ([https://tryhackme.com/r/room/mrrobot](https://tryhackme.com/r/room/poster)) created by **ben** and **tryhackme** itself.

Here our **terminal**  is opened.

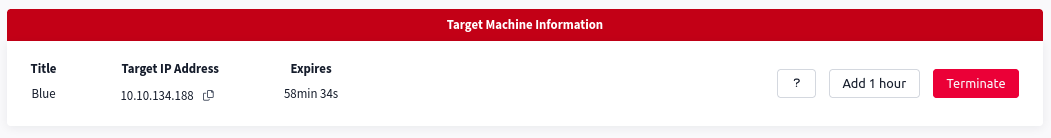


Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn’s file downloaded path after doing **sudo**.

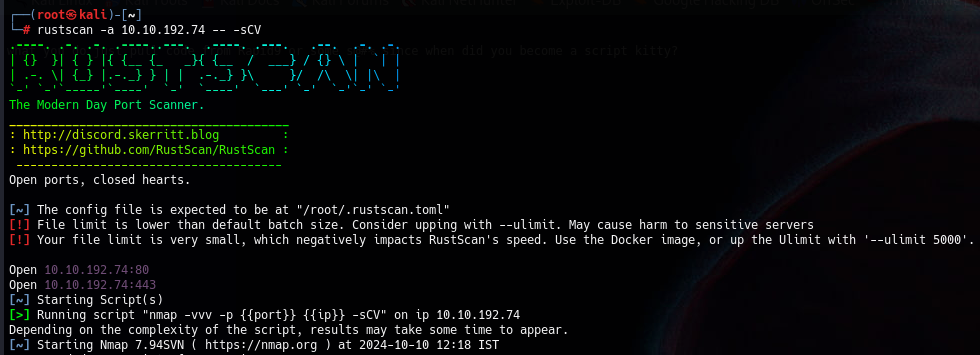


Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button. 

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

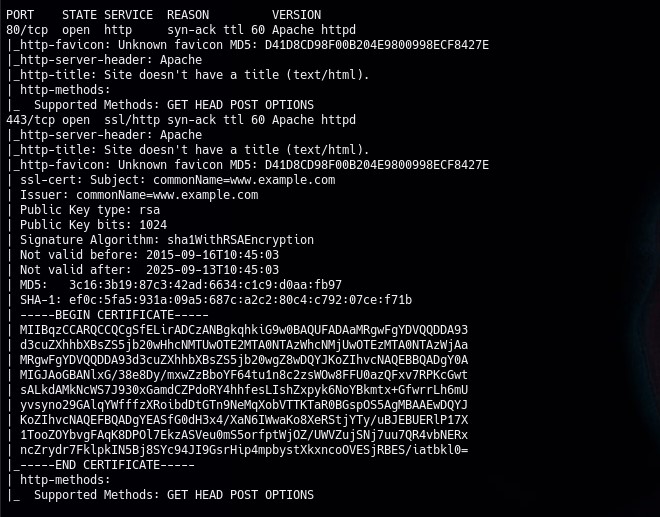


After getting the target ip first thing we’ll do is **rustscan** to see the open ports and more machine’s info.

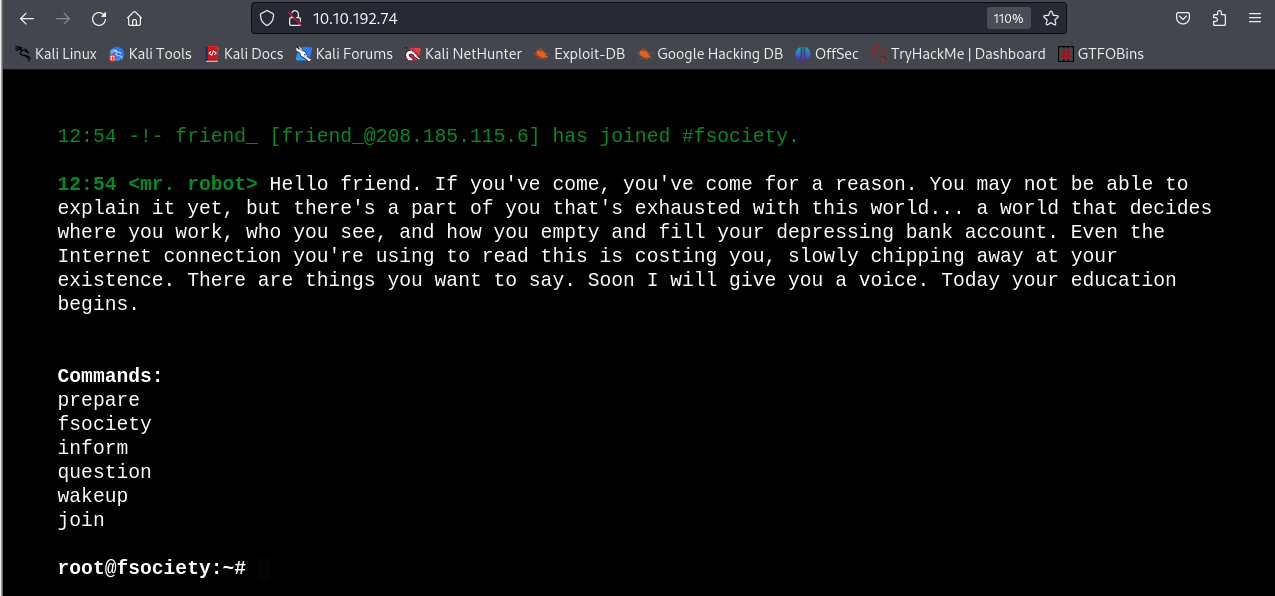


Here I am using **rustscan -a <IP> -- -sCV**  to see all the ports. You can use many more scripts like **-sCv -T4 <IP>** etc.

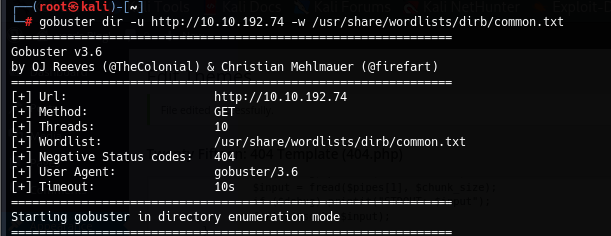
Seems like our scan is completed. Looks like there are total 2 ports open



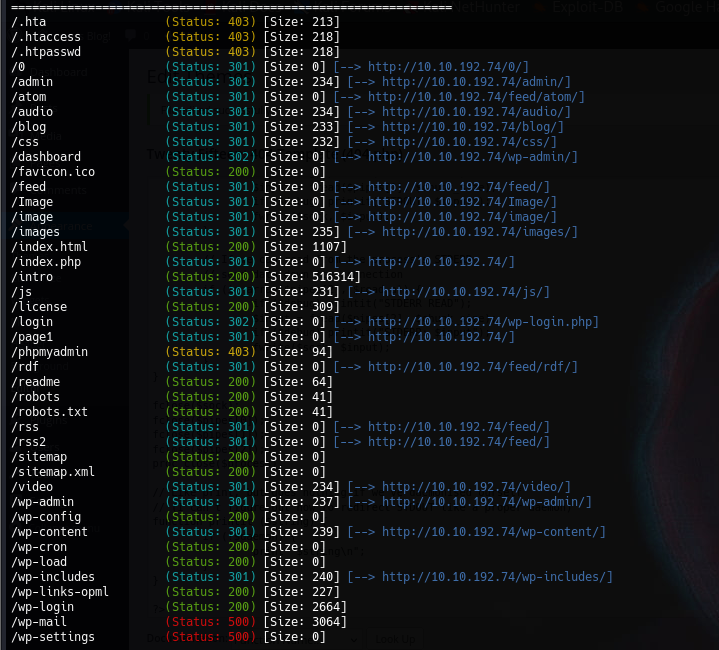
Now that we know the information from port 80 and port 443 which are both web servers. There are no other ports open. So may be the vulnerability lies in the website somewhere. We will now gather information from the website and do a deep recon. Our website main page looks like this.



Now we will do directory busting using **gobuster.**

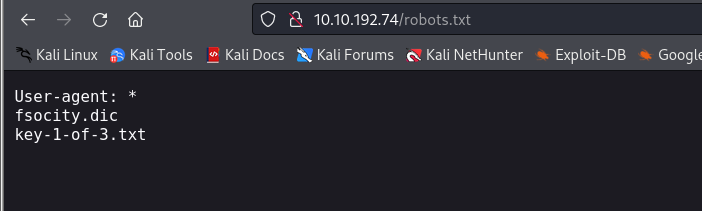


Our directory busting has been started let’s wait.



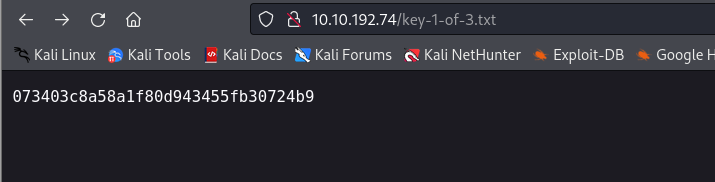
Here we can see several directories and some of them may be contain information about the keys we need.

We will open **robots.txt** file in the website.



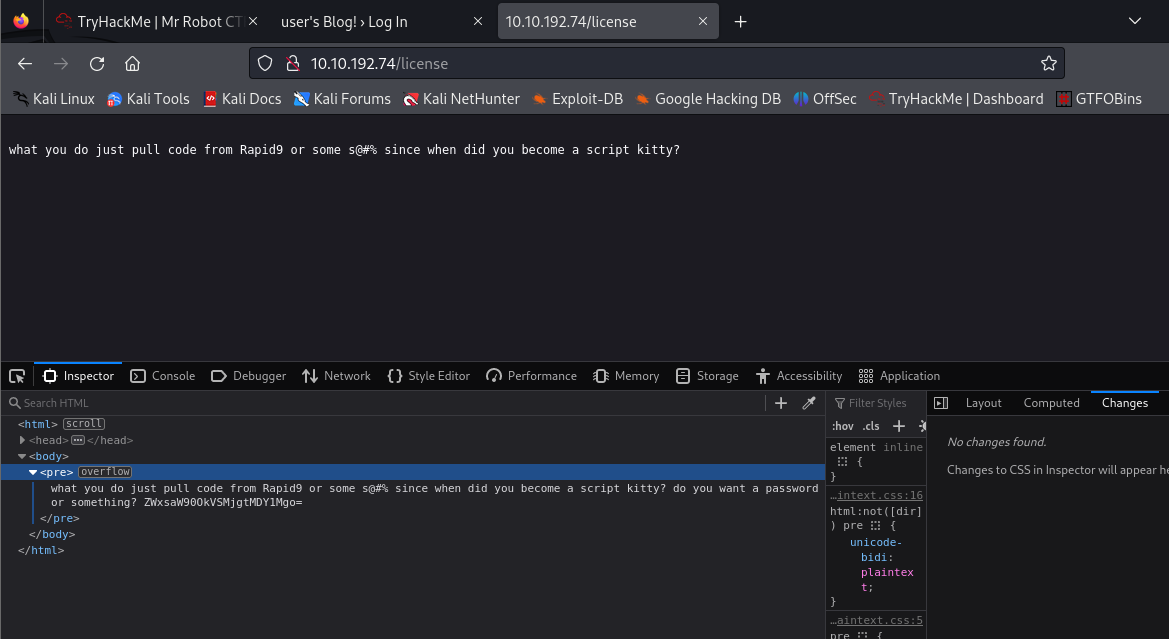
Voila!! It contains the first key.

We can get this key directly by typing **key-1-of-3.txt** in the directory list.



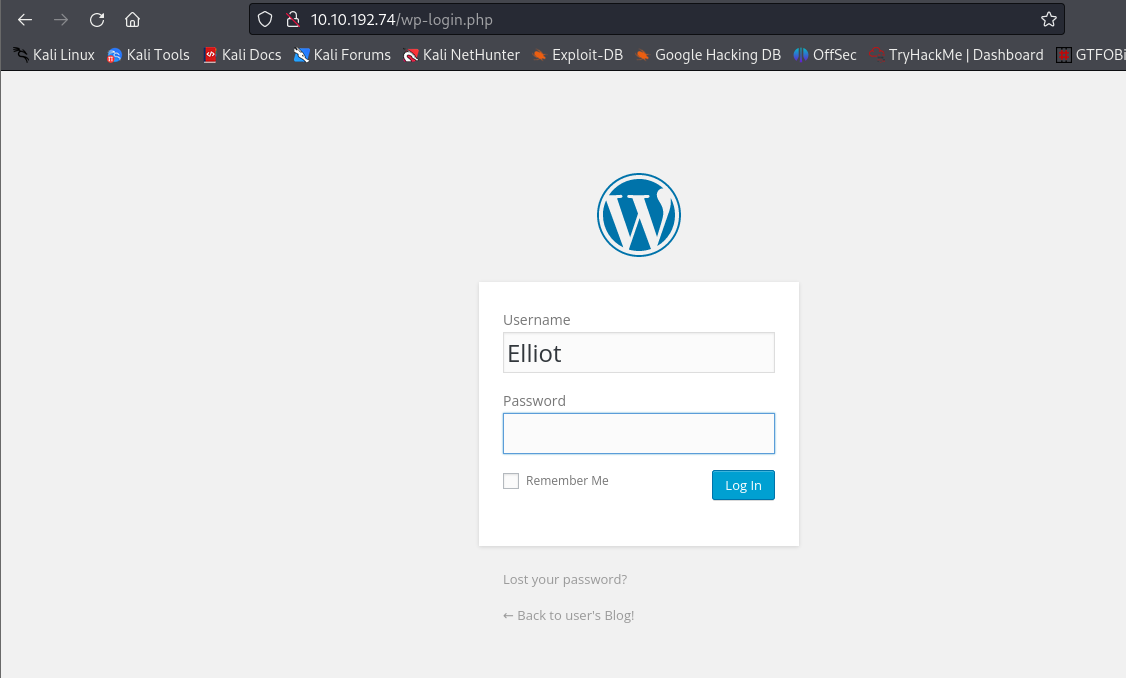
And thus we found our first key. Let’s enumerate further.

After further enumeration we found a base64 encoded string on **license**  page’s developer tools (inspection) that is **ZWxsaW90OkVSMjgtMDY1Mgo=** which gives **Elliot:** **ER28-0652** after decrypting. We will note it.

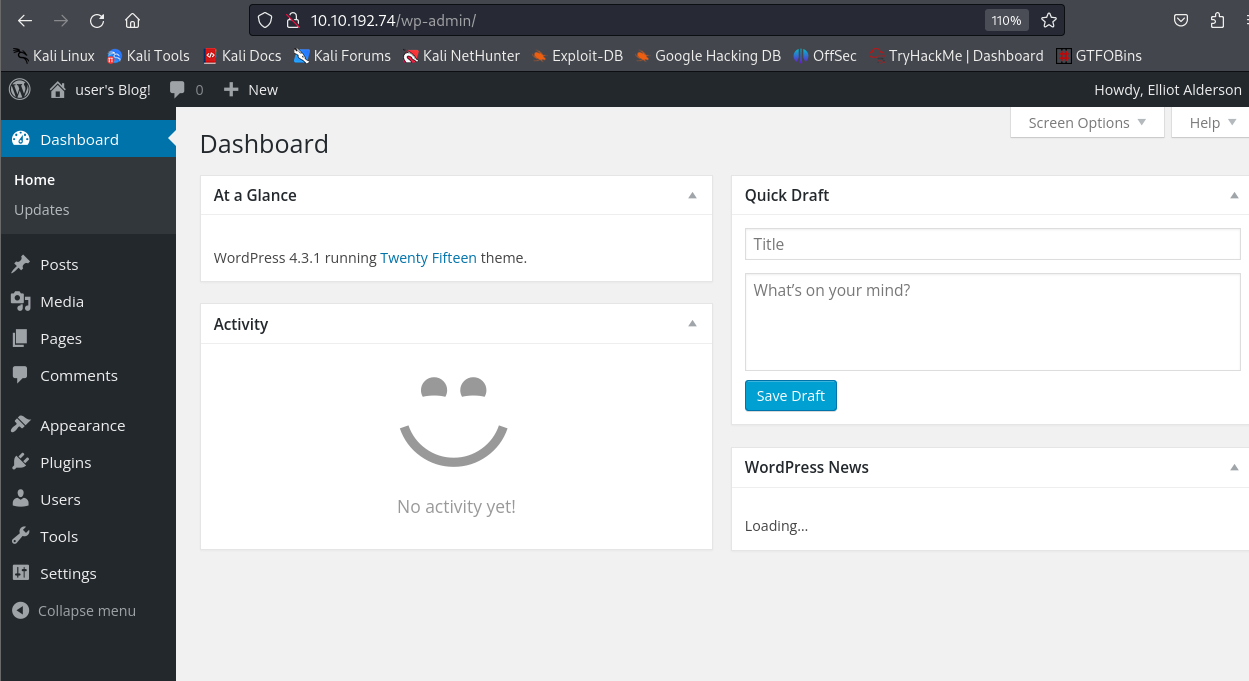




Next we found a login page of **wordpress** site on login directory.

We will try to login with the username and password we have found earlier. 

It leads us to the dashboard of the website’s main page.



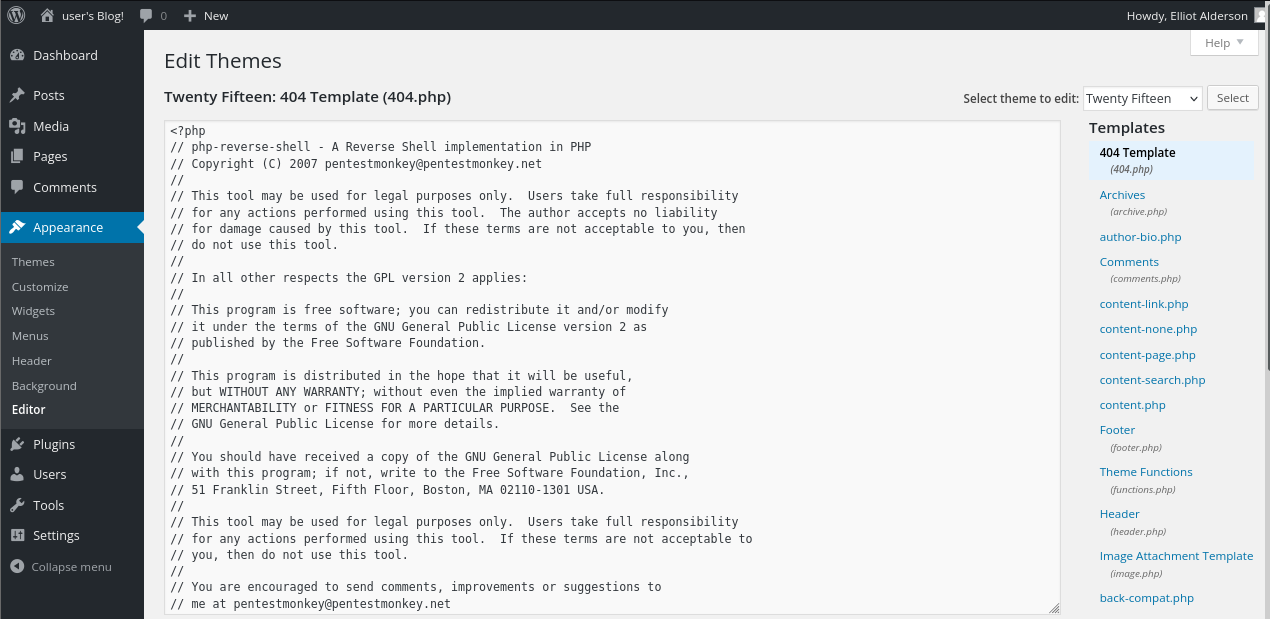
Now we will explore the website and look for any bugs or vulnerabilities.

After further enumeration we found that we can customize and upload php files in **appearance -> editor -> theme-editor.php**  option.

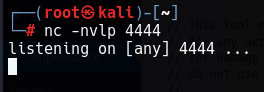
We will customize/edit one of the php files of themes and use it for **php reverse shell.**

We can use the code and copy it by **pentestmonkey**  available on **github.**

We will change the **LHOST and LPORT** (LHOST is your kali machine’s IP address and LPORT can be 4444). Here we have changed the **404.php**  file and used it for reverse shell.



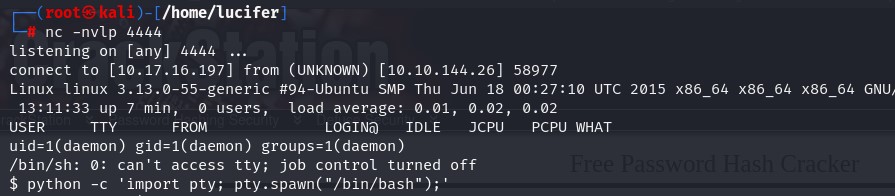
We will start a listener on our kali machine using **nc -nvlp 4444** and wait for the shell to appear.





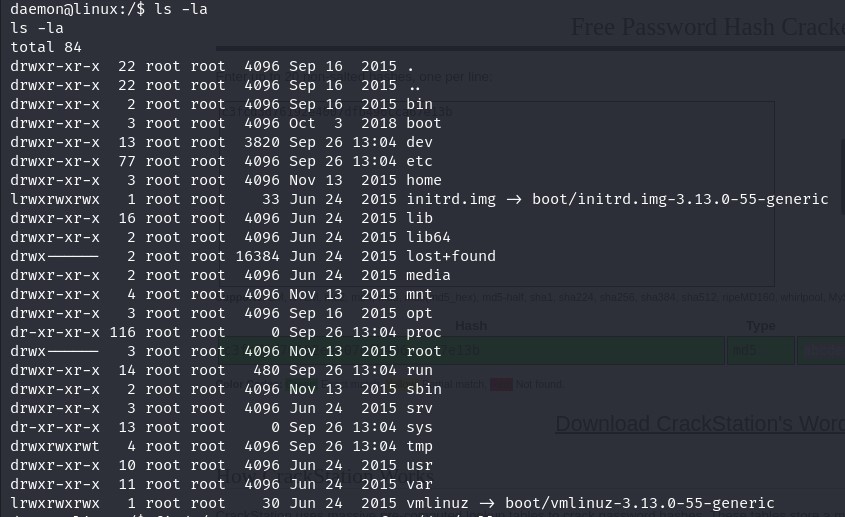
We will reload the site following the link of the edited file (<http://10.10.192.74/wp-admin/themes/twentyfifteen/404.php>)

When the link is reloaded we get our reverse shell on our machine.



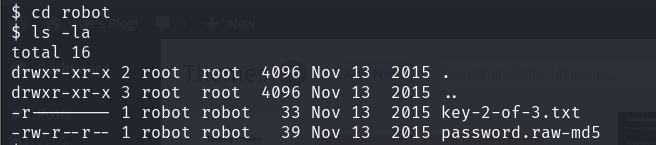


We will try to get a **python interactive shell**  and then explore the system.



After exploring we found a user **robot** on the home directory.

We will check if something is important there.



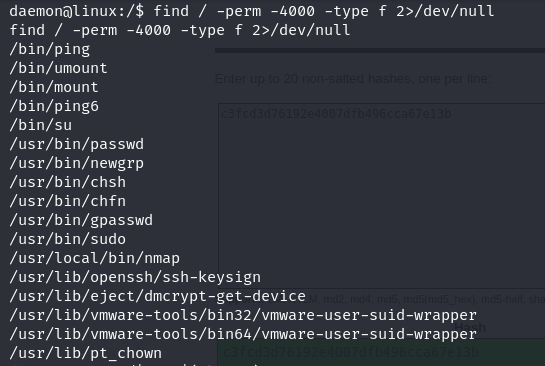
We found our second key **key-2-of-3.txt**  and we can easily read and see it.

Now only our third and final key is remaining which we all know that it will be in root folder. But we don’t have root privileges so we need privilege escalation here.

We will check for the permissions which have root access and look for the something odd to get root privileges.

We will use the following command :

**find / -perm -4000 -type f 2> /dev/null**



We can see **nmap** and we have got hint on tryhackme for the 3rd key which is also nmap**.** So may be we can gain root from here.We know that nmap has it’s own interactive shell. We will try to get that interactive shell from the **/usr/local/bin** folder.



After getting into nmap interactive shell we will type  **!sh**  for getting bash shell.

And yes we are root.

Now we can go to the root folder and copy our 3rd key which is **key-3-of-3.txt.**

