**MR.ROBOT**

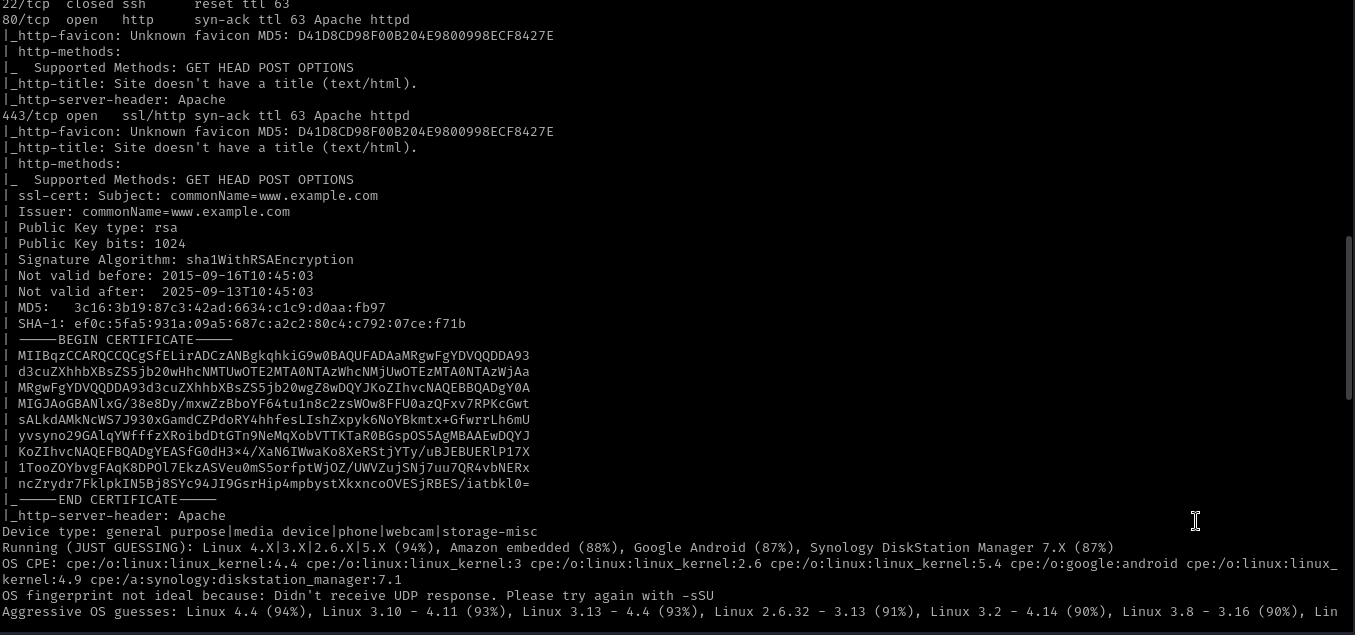
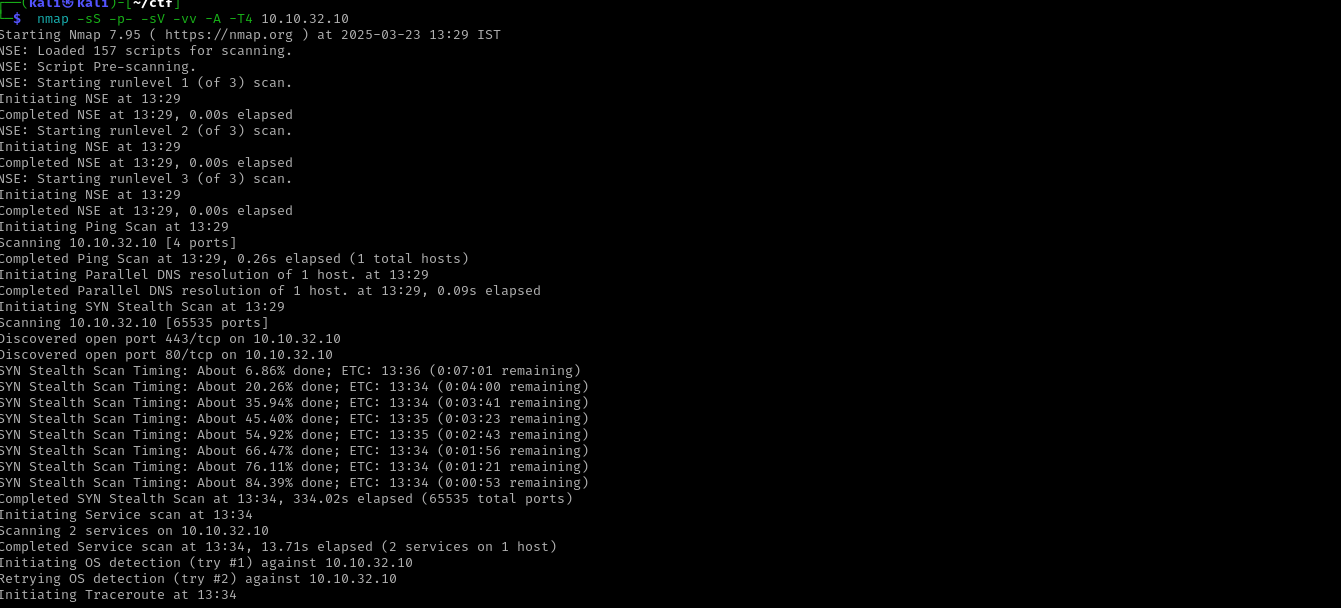
****

After having studied most of THM’s learning paths, I decided to focus on putting what I have been learning to practice and try my hand on its CTF challenges.

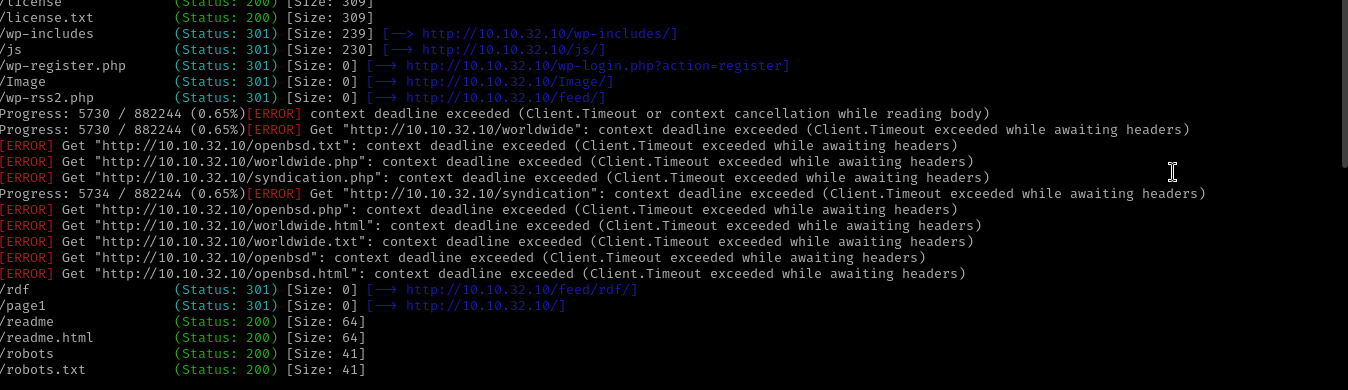
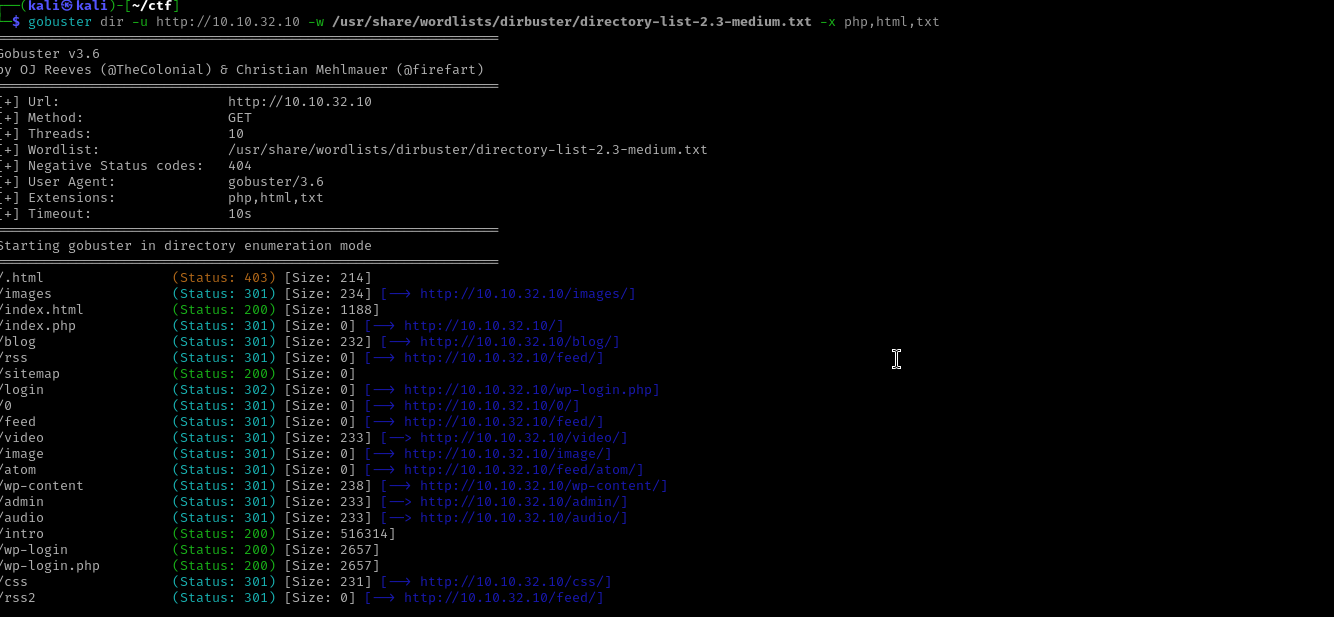
Having said that, take what I write with a grain (or many grains) of salt, as I am completely new to all these concepts and tools, and I will be writing walkthroughs mostly to learn and solidify what I know by repetition

The goal of [Mr. Robot’s room](https://tryhackme.com/room/mrrobot) is to **find 3 hidden keys.** Let’s crack on!

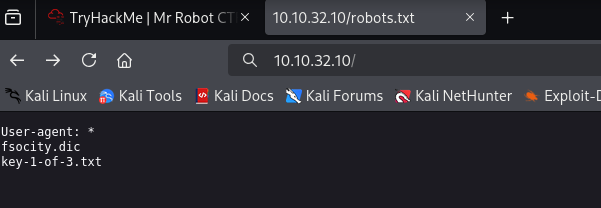
**first I am doing active recon with nmap but nothing find suspicious and second done with directory bruteforce with gobuster and find many directories and this directory have so many interesting thing.**

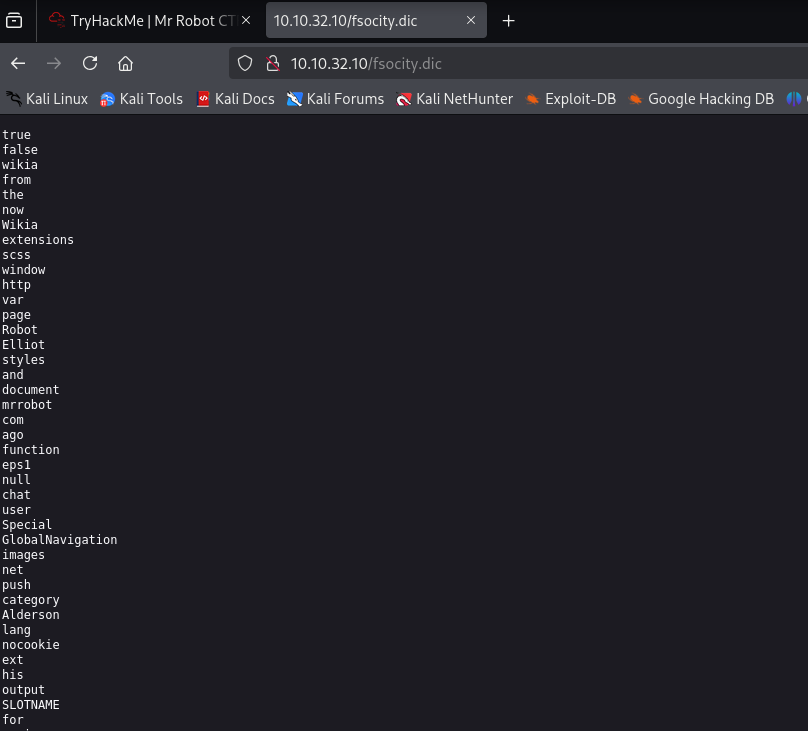


**Here gobuster result with interesting directory**

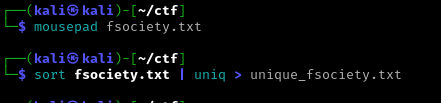


**And then go to the robots.txt directory u got your first key**

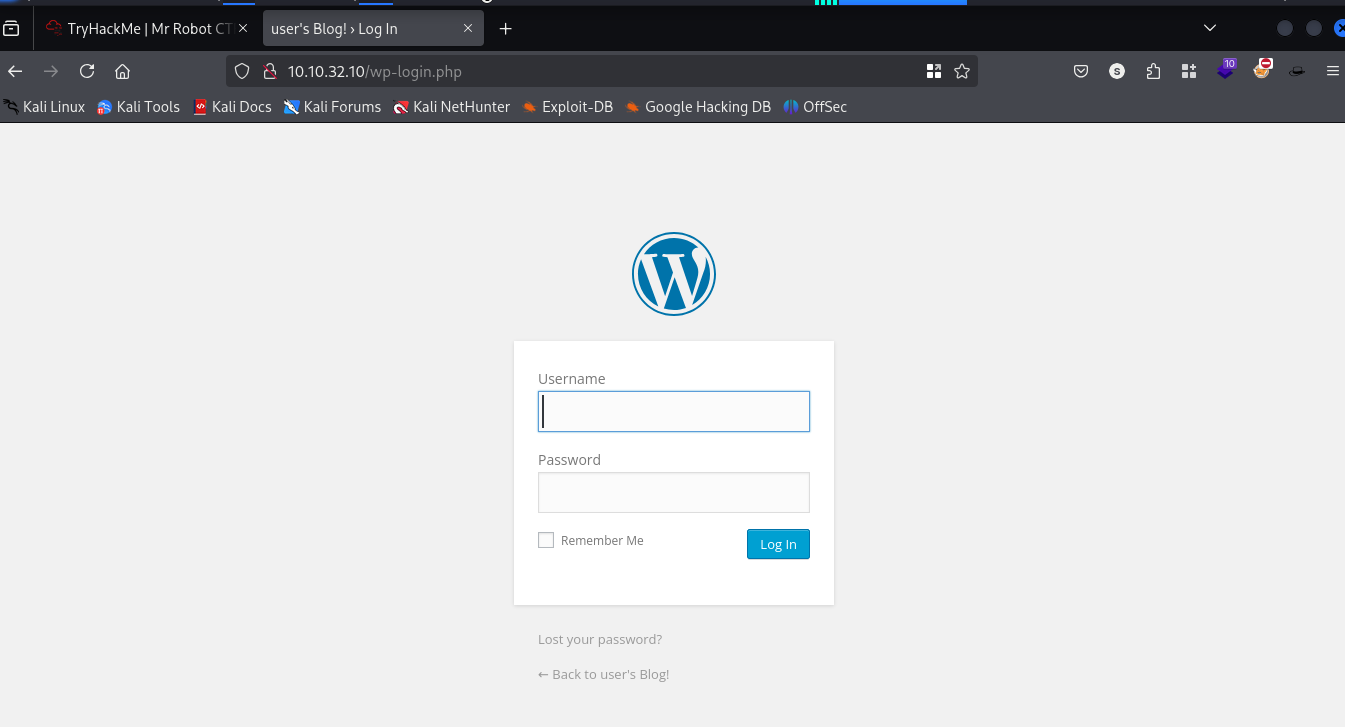


**Then go to the fsociety.dic u got a password wordlist** 

**Then save this wordlist in fsociety.txt and this wordlist is big and one word repeat many times so I use sort command to short this wordlist**

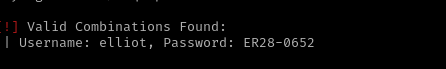


**Then u go to the wp-login directory u found a wordpress website**



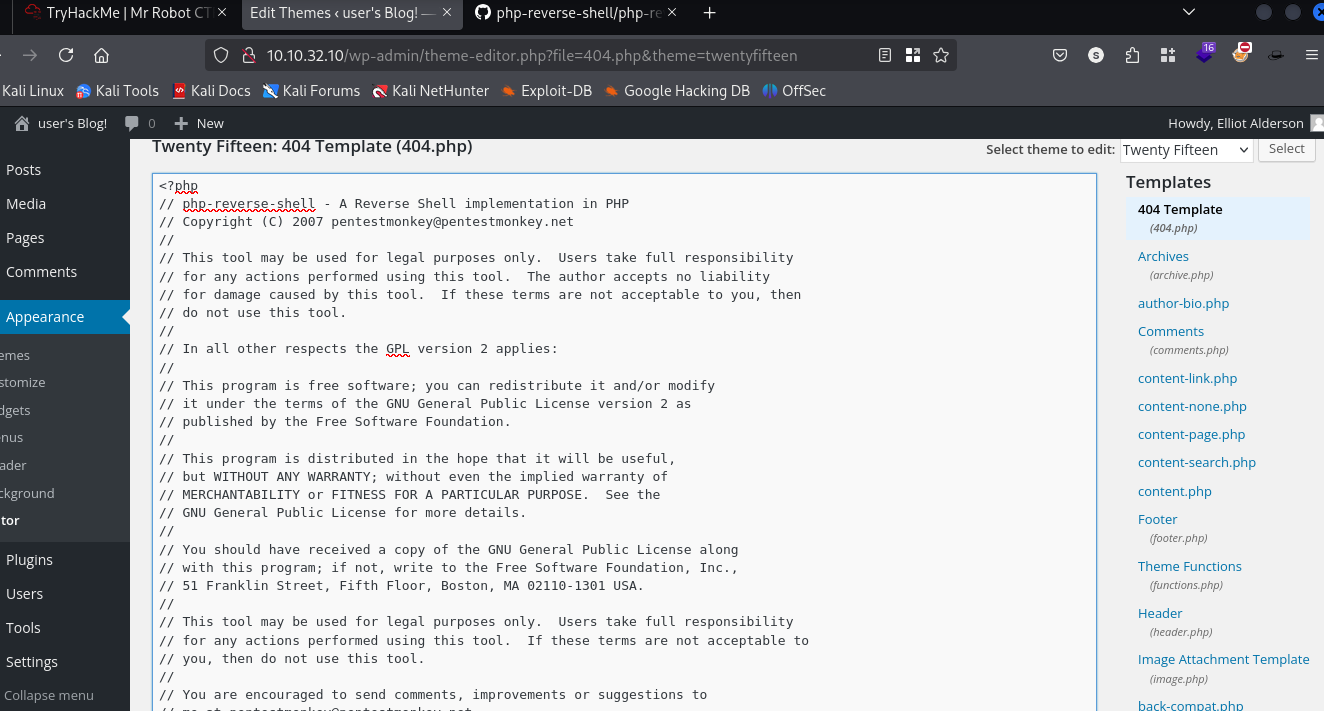
**I am already know this website of userame is Elliot when u boot your machine then this username was given and u saw a webseries of mr.robot the u know about Elliot who was Elliot. Then I am running wp scan (use for wordpress website) for password bruteforce fo this website I have already password wordlist. Run wp scan**



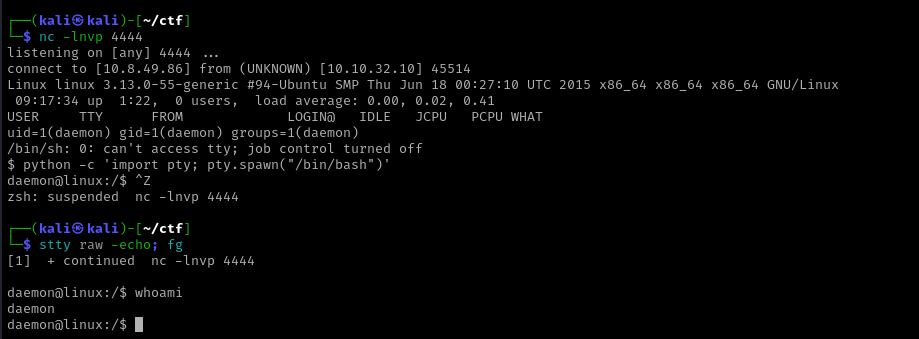


**Then I am loging in website with credential and go to the Appreance < editor and update 404.php with revshell here I my ip is look like change because my machine not worked good for some time the terminate my machine and restart and update page rev shell link**

[**https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php**](https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php)



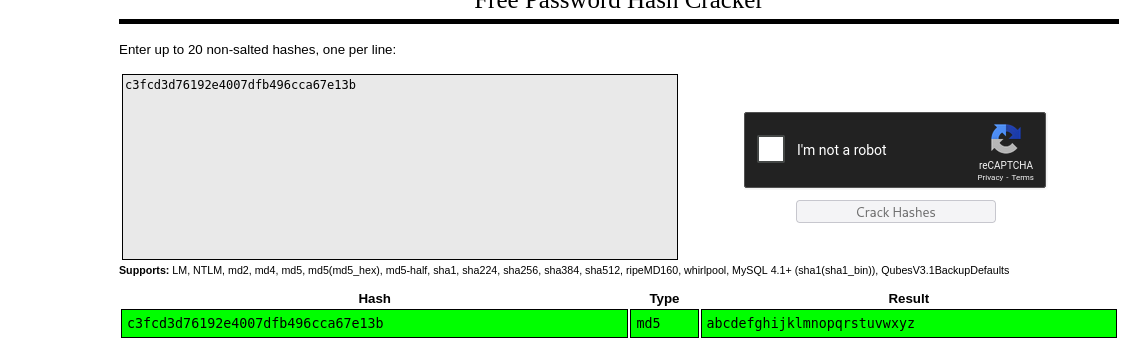
**Start nc and go to the http:/ip/wpincludes/themes/TwentyFifteen/404.php**



Then u go to **cd /home**

**cd /robot**

# u got a hash of password and crack this use of cracstation

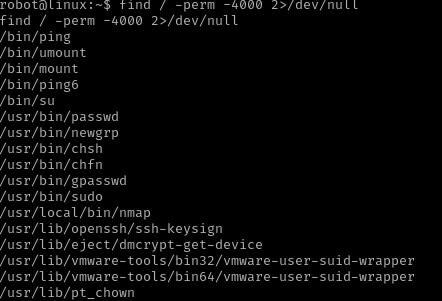


The use **su robot**

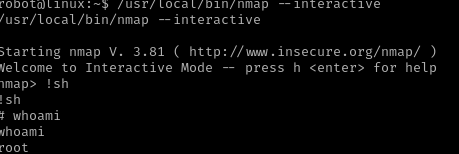
# And use the password and u got second key



**Then check for privilege escalation I am using linpeas.sh but not work then I go for suid binary(set owner user id)**



**The I found interesting /usr/local/bin/nmap here suid binary set on this then here I am going gftobins** [**https://gtfobins.github.io/**](https://gtfobins.github.io/) **and help of chatgpt I got root shell I am success fully escalate and became root user**

Then I found final key in root directory