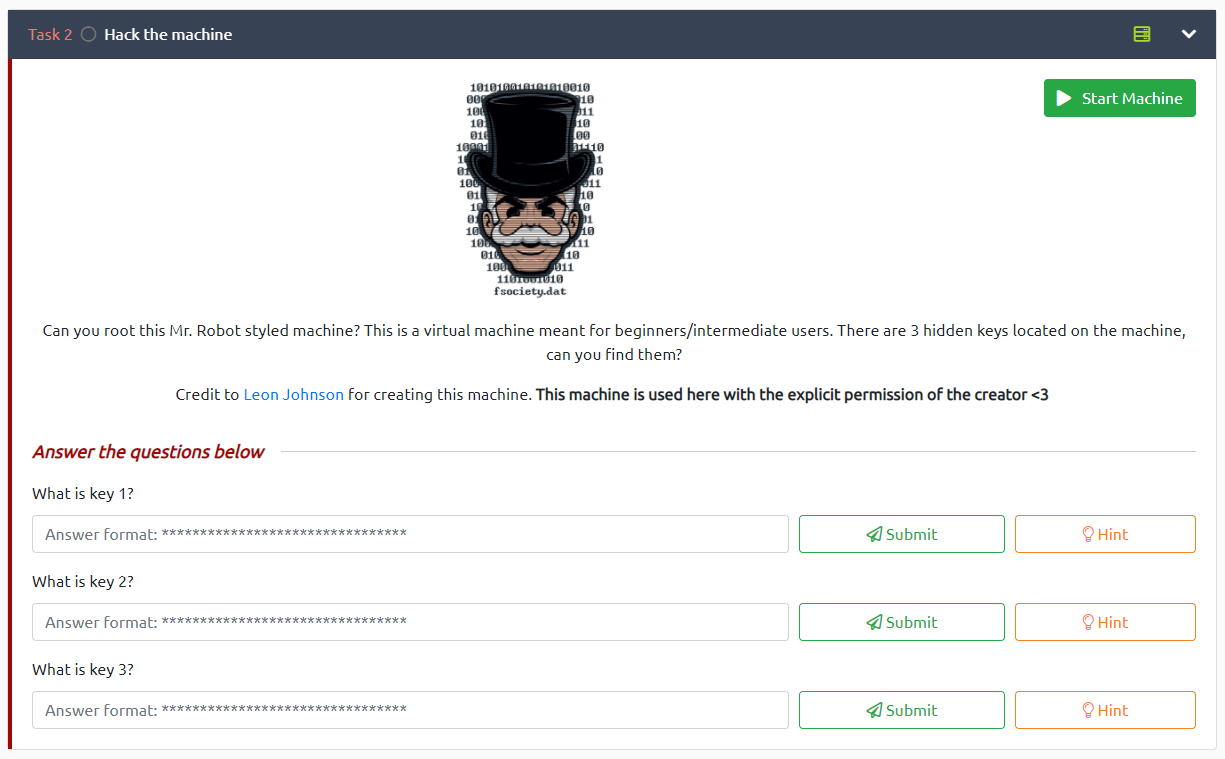
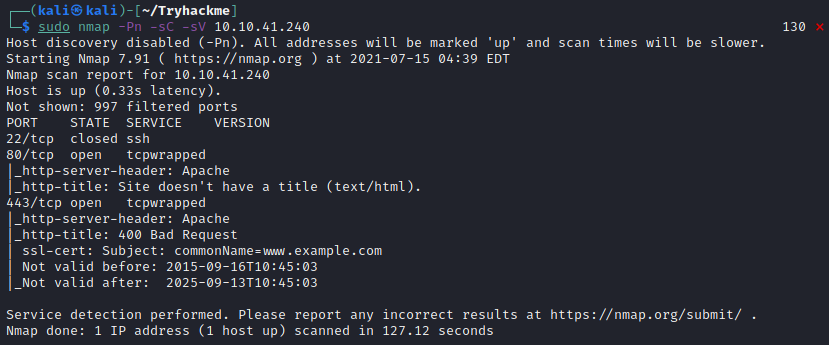
**Mr Robot CTF write-up**

This is write-up for Mr Robot CTF in TryHackMe which we have to exploit web server, find a way to access target machine and elevate our privilege to rock this box

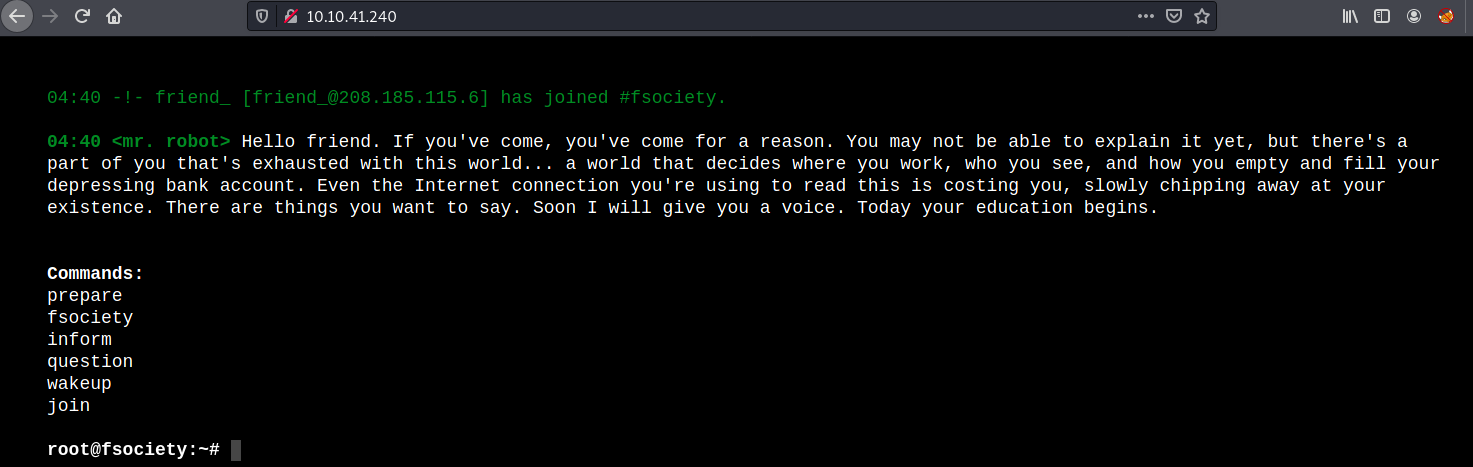
Site: <https://tryhackme.com/room/mrrobot>



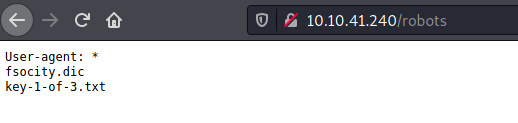
First always run nmap for port scanning and enumerate service which we see 2 ports are opened



Visit the Website and it look like a Terminal-like website that will execute specify command which related to Mr Robot Series and will be redirected to 6 web page that contain video and information about fsociety

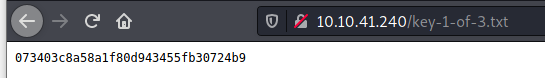


Now it’s time for gobuster to bruteforce directory after launch gobuster let’s check robots.txt and we found dictionary file and first flag



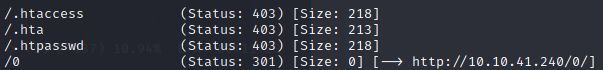
Download dictionary file and capture our first flag



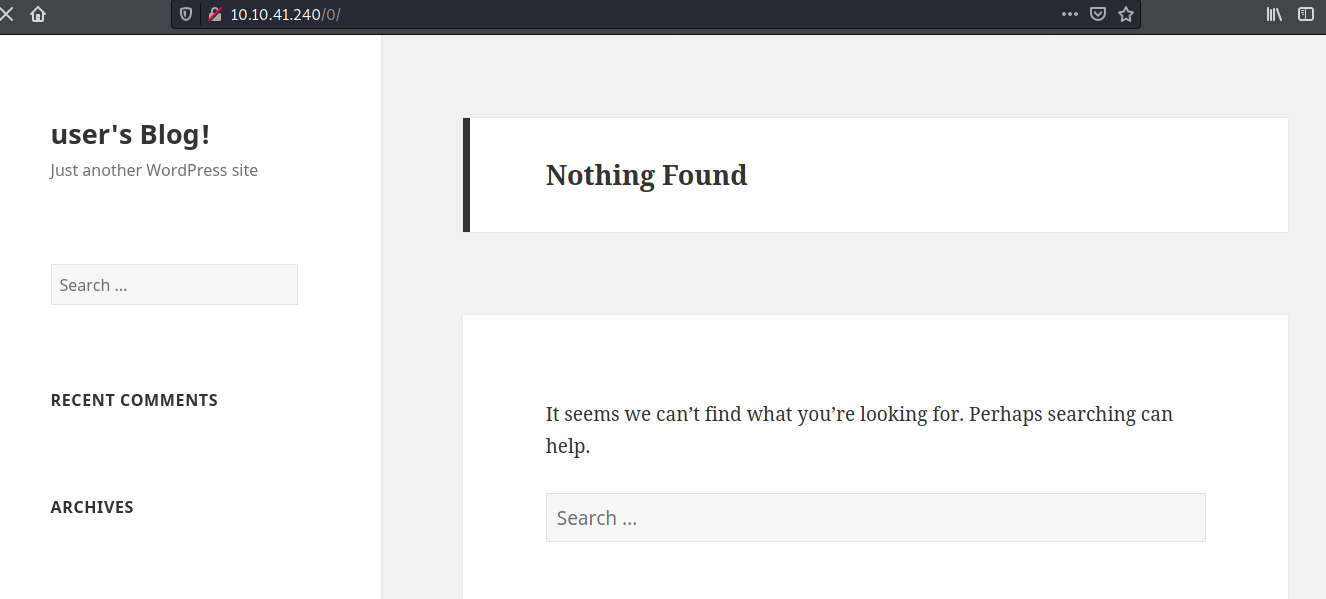




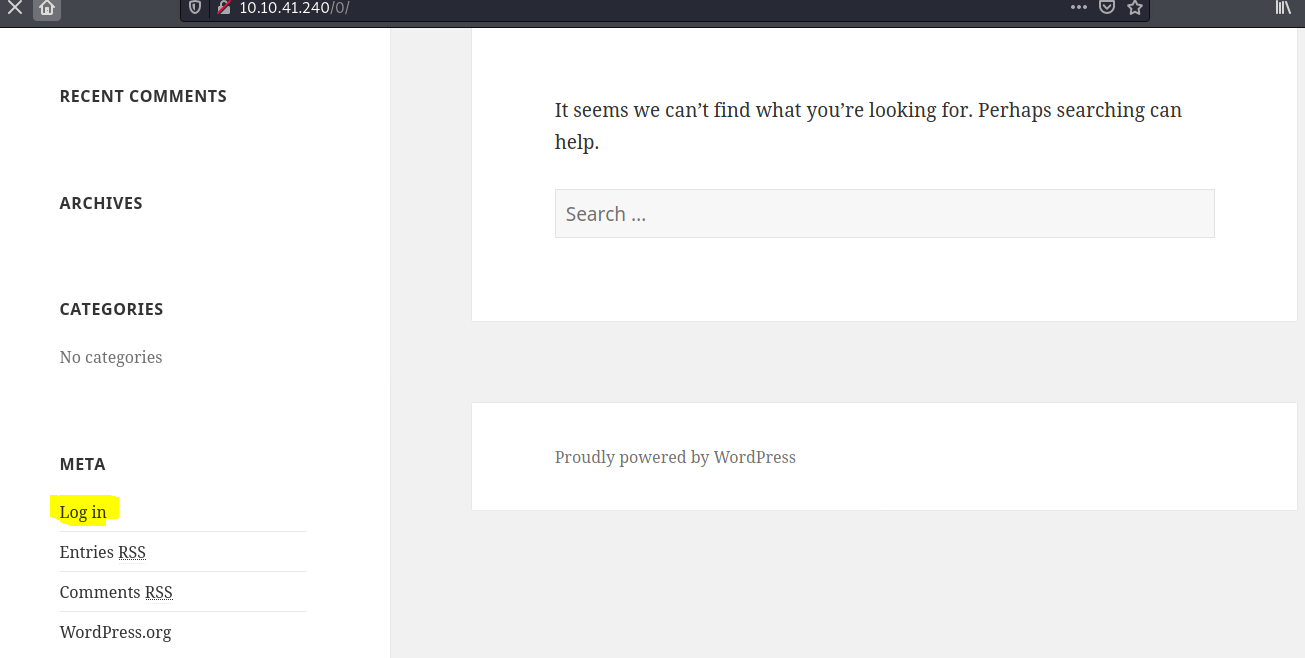
Back to gobuster, we found /0 directory



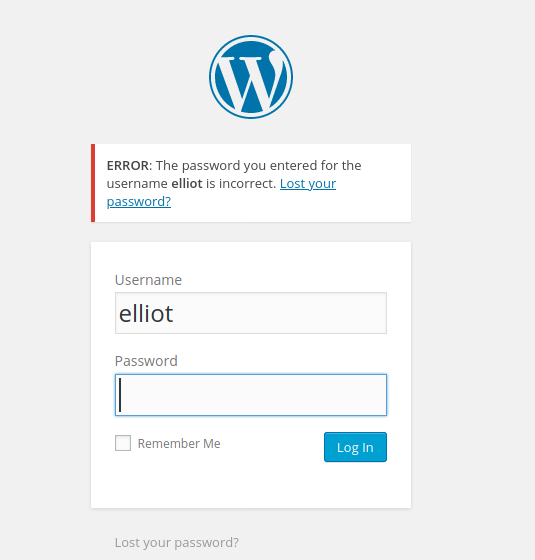
And it’s WordPress!



Scroll down and we can go to login page via this button or go to wp-login.php that could be a default login page for wordpress



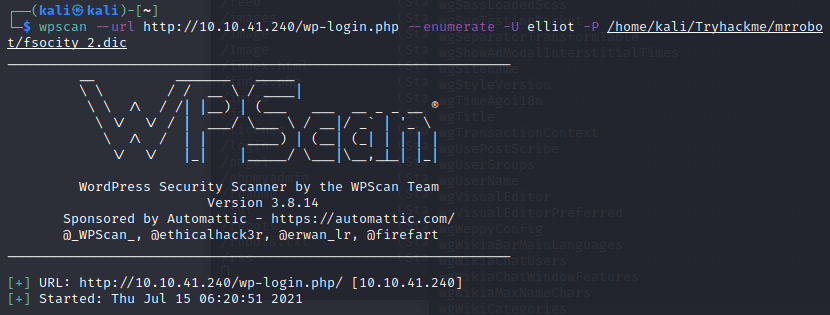
In login page we found that it has expose sensitive data after I typed Elliot as username



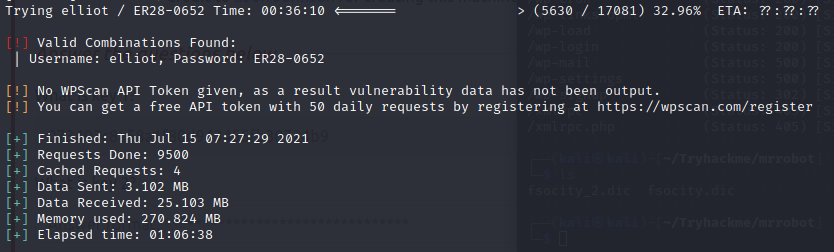
We have WPScan for WordPress scan and bruteforce password but first we need to sort and cut everything duplicate data first



Now let’s use wpscan with tag –url, --enumerate for password guessing, -U for username and –P for wordlists



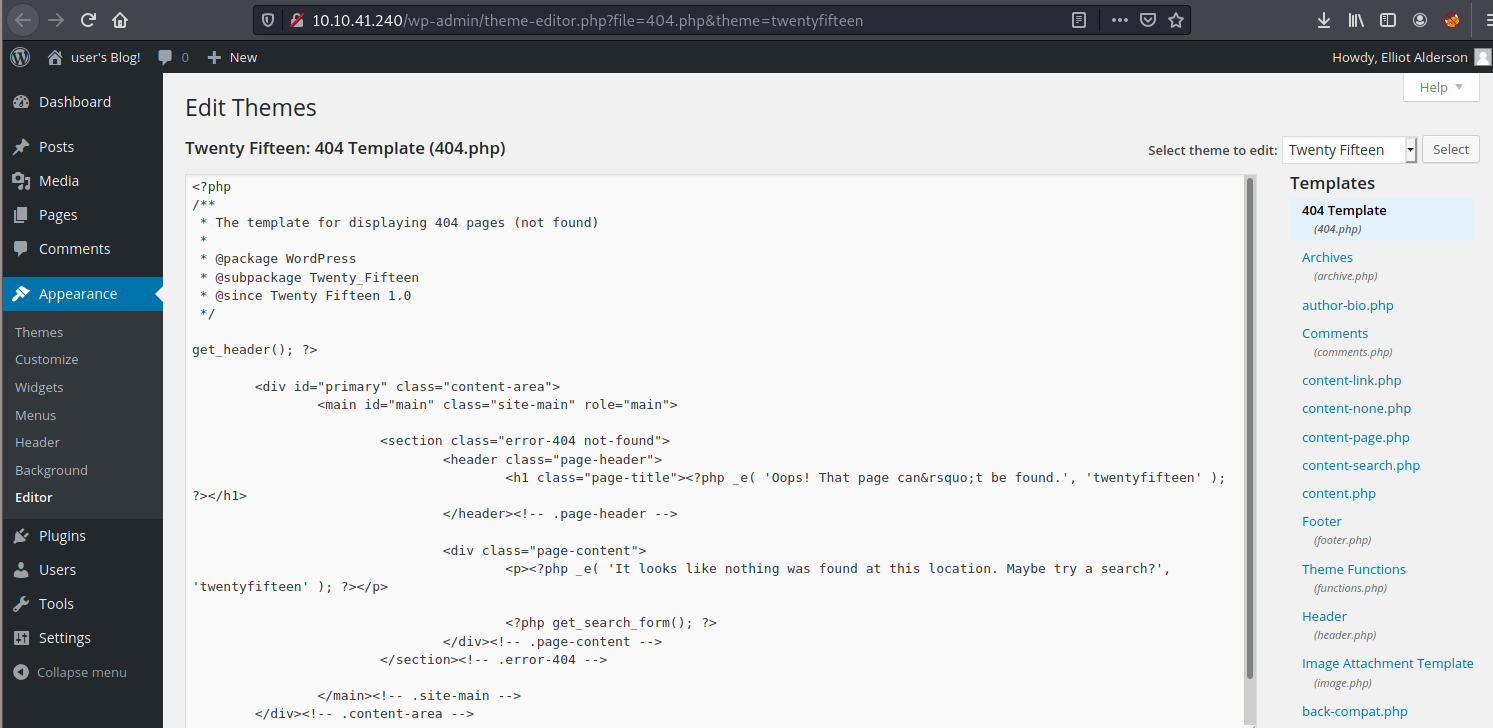
And finally we got a valid password for Elliot user



Now we can login as Elliot



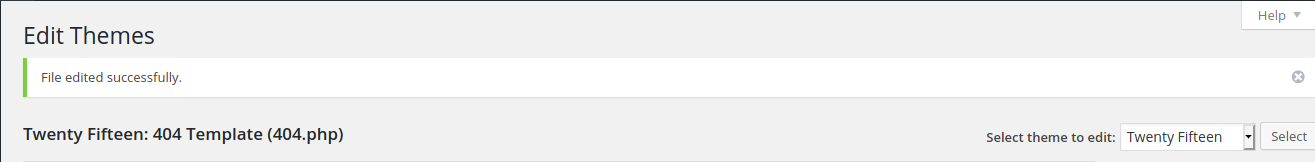
After explore a little bit, we found that Mr Alderson can edit these php themes



It’s time for PHP reverse shell to shine, paste php reverse shell code here and change ip and port that we will receive reverse shell

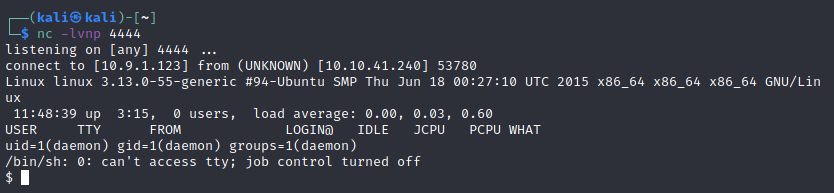


Update file

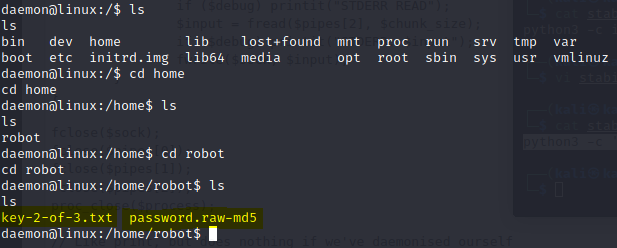


Set netcat listener and go the page that we edited for reverse shell





It’s time to explore file system and there is only 1 user in this box which have our second flag and password file in user directory

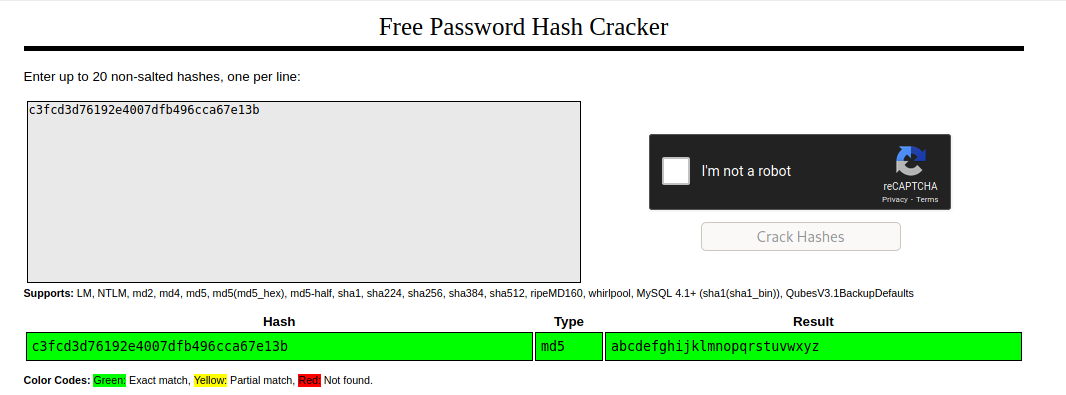


But we can’t capture this flag yet we need to be robot user first

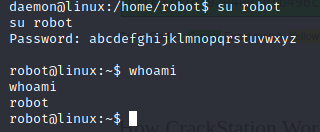


Get password.raw-md5 file and crack it





Now we can switch to user robot (we need to use stabilized shell to run command su

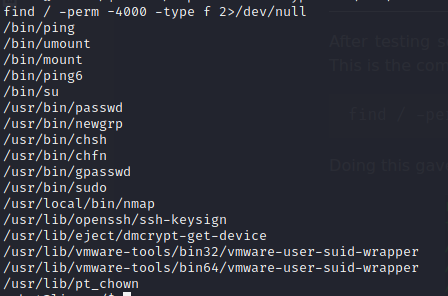


Capture our second flag

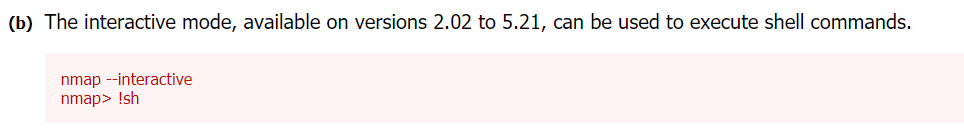




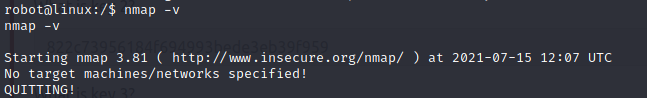
The last flag should be a root flag I tried sudo but it didn’t work so I will find executable that we can use to elevate our privilege and nmap can help us



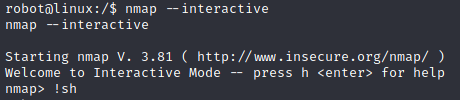
Search in GTFOBins will can see that nmap in many versions can use to spawn a shell



And this nmap is qualified

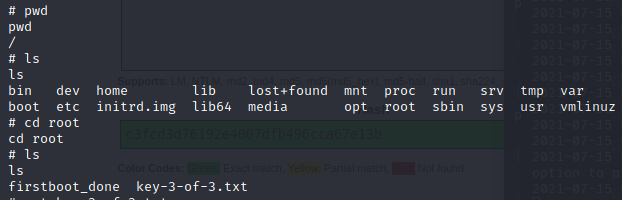


Now get our root shell





Go the root directory and capture last flag!







All keys have been captured!

