CYBERSPLOIT1

> Welcome to my writeup where I am gonna be pwning the **CyberSploit1** machine from **offsec proving grounds**. This challenge has two flags, and our goal is to capture both. Let's get started!

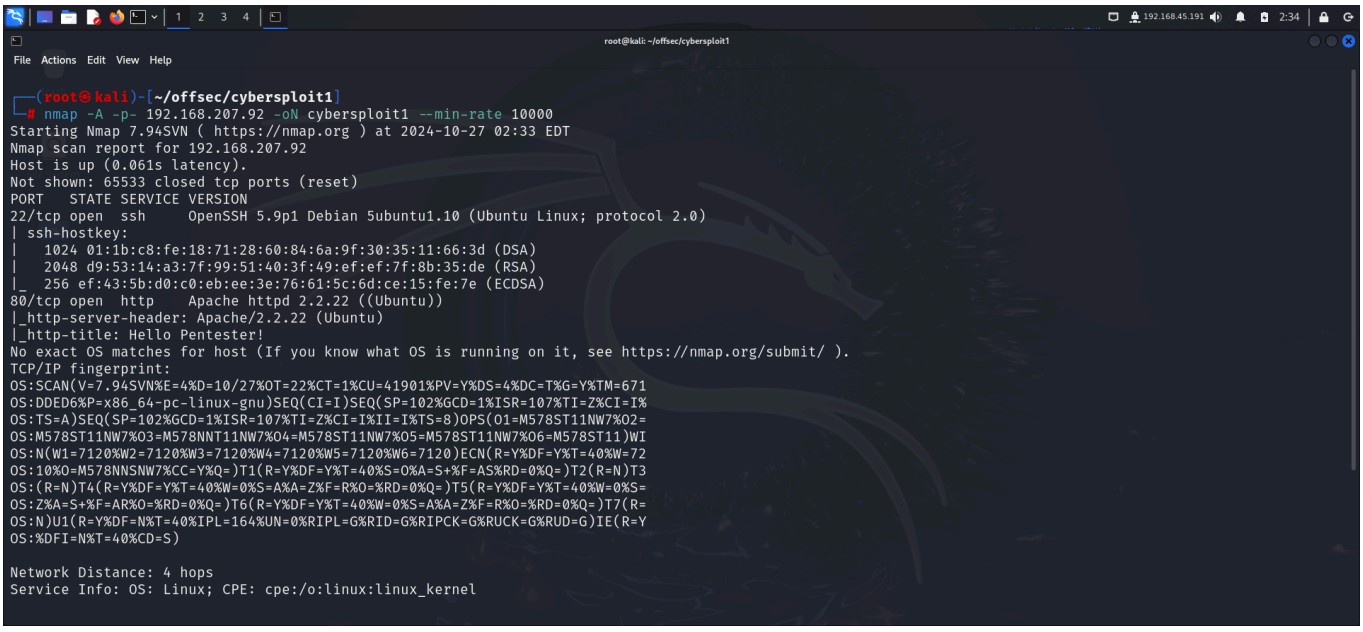
GETTING STARTED

This machine can be accessed in [proving grounds play] and is ranked as **easy**.

> **Note**
>
> This writeup documents the steps that successfully led to pwnage of the machine. It does not include the dead-end steps encountered during the process (which were numerous). This is just my take on pwning the machine and you are welcome to choose a different path.

SCANNING

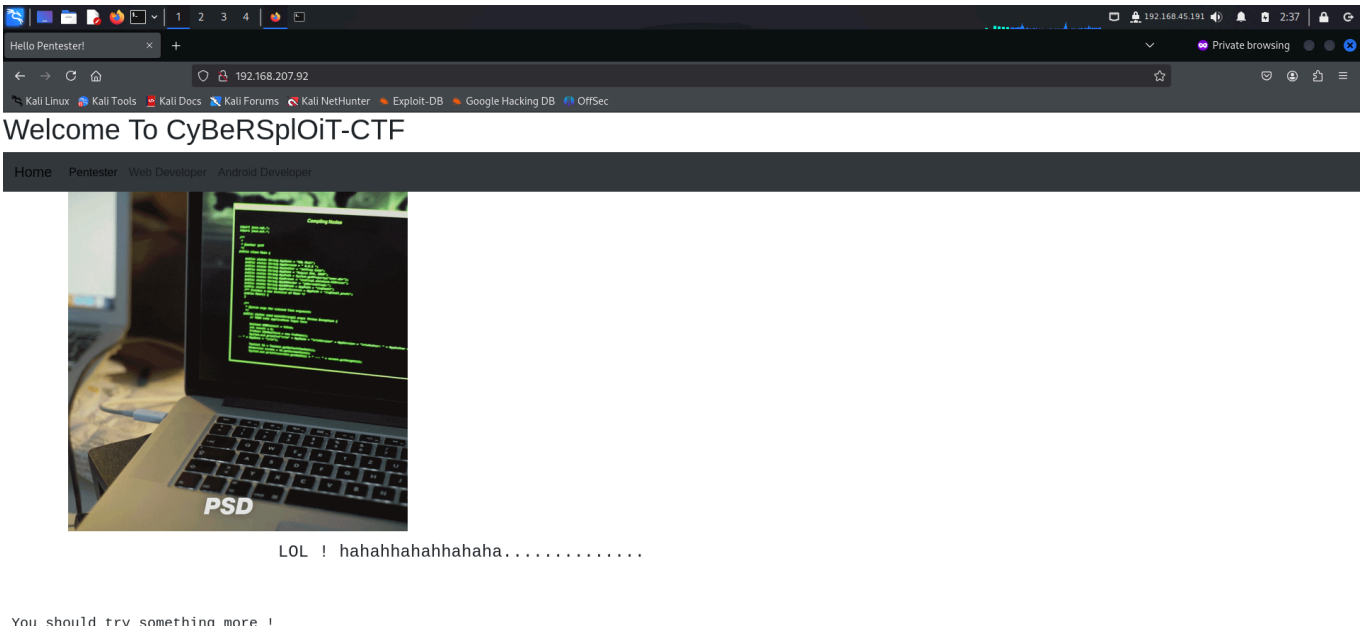
I performed an **nmap** aggressive scan to find running ports, services and os related information.



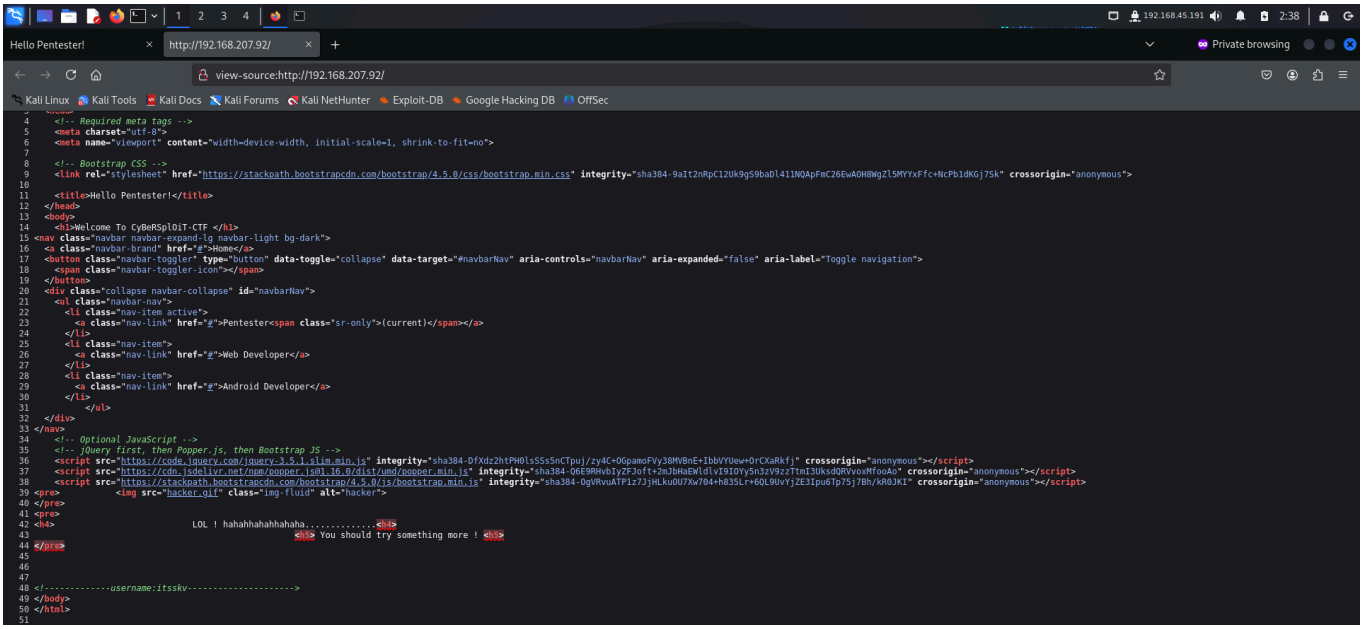
The scan revealed 2 active ports, **ssh** and **http**.

FOOTHOLD

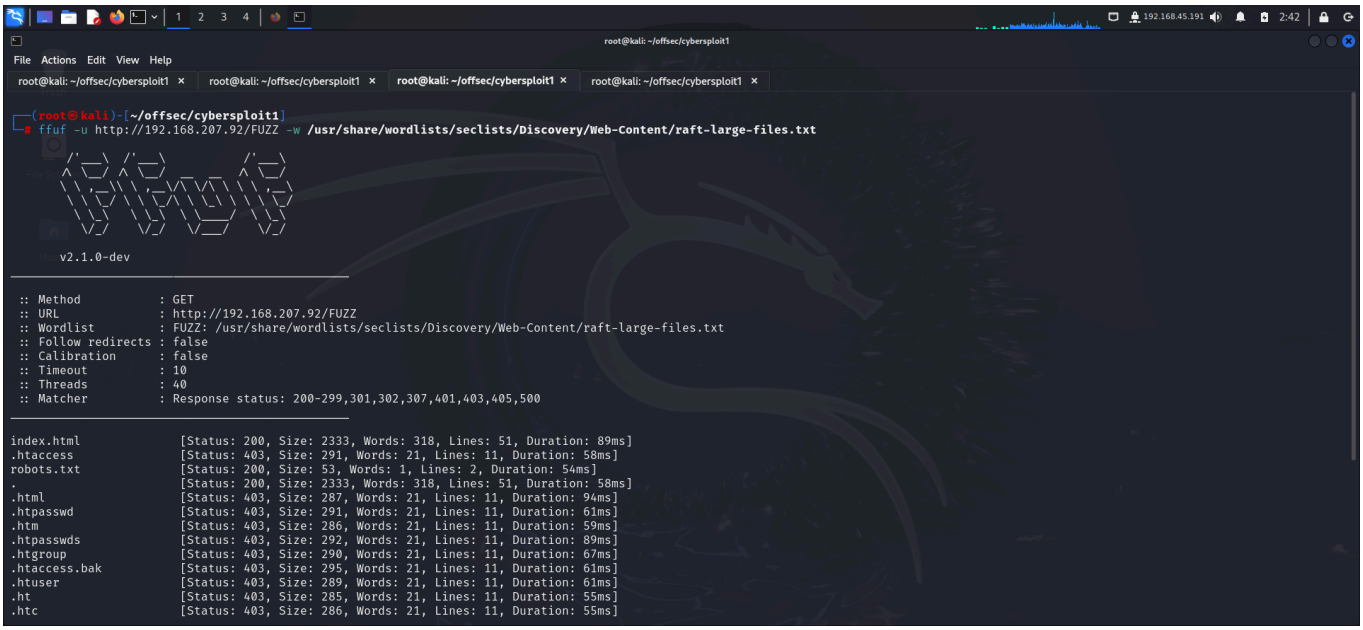
I visited the target on a browser to access the **http** service and found a static webpage.



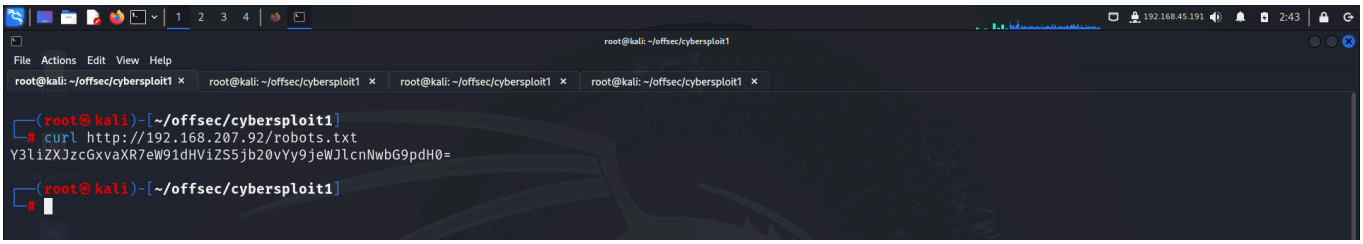
The page did not reveal anything useful initially so I viewed the page source and found a username commented out towards the end of the **html** document.



Next I performed web fuzzing using **ffuf** and discovered the **robots.txt** file.

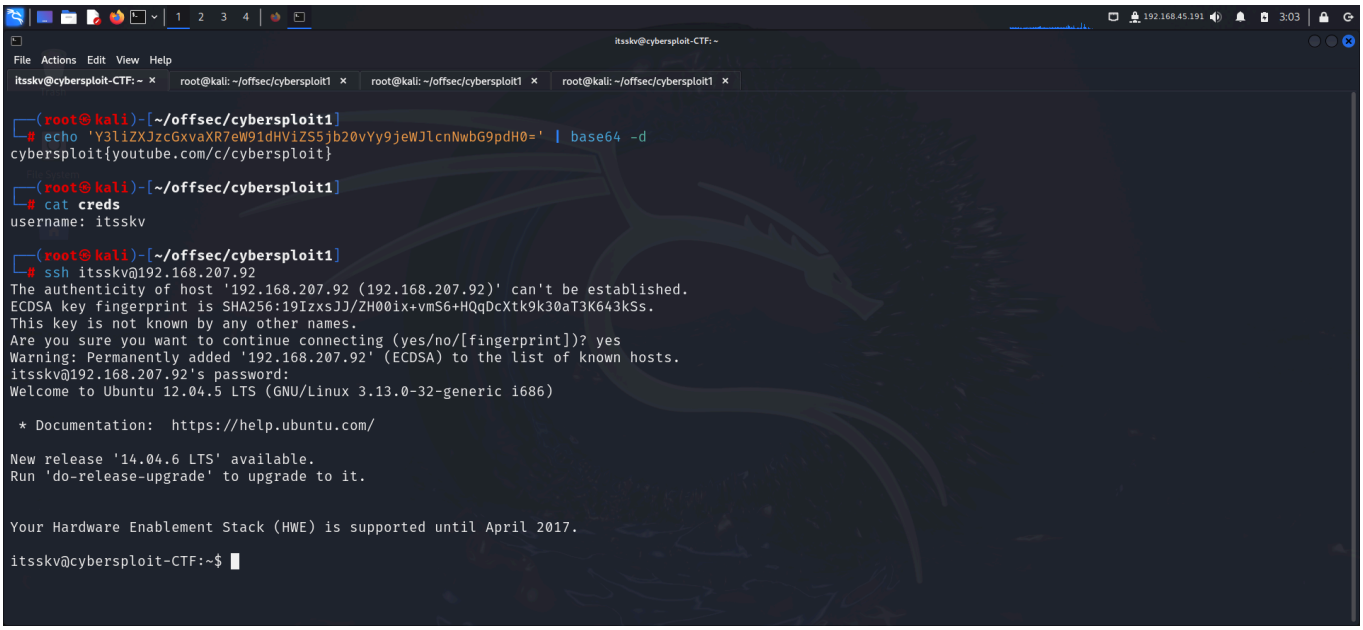


accessing `/robots.txt` revealed a base64 encoded string. So I decoded it using the **base64** command line utility.

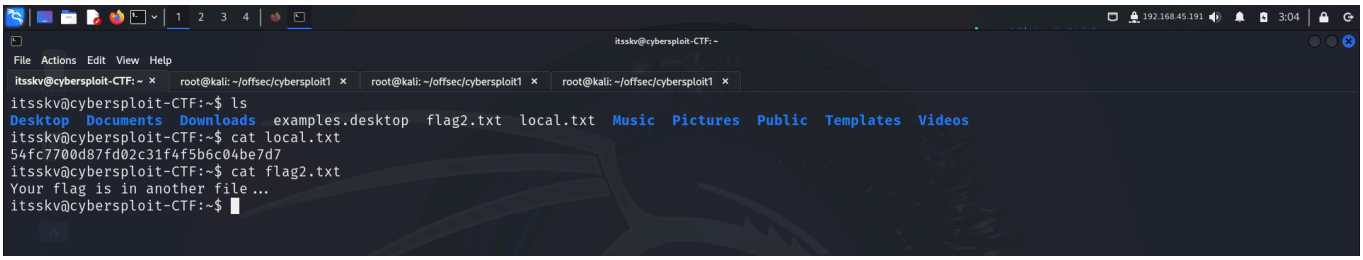


This seemed interesting but initially I had no idea what this meant. I did some more reconnaissance on the website and found nothing useful.

Since the target was running **ssh**, and I had discovered a username; I tried using this as a password to log into the system.



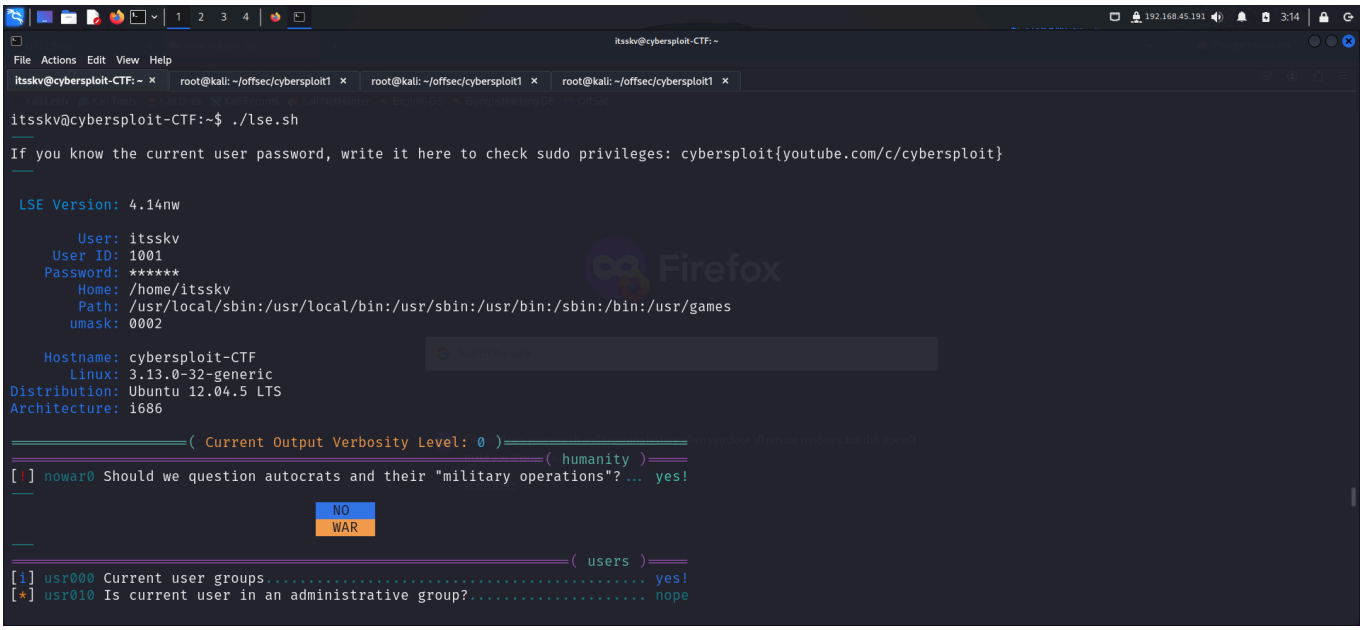
After getting initial access, I listed out the contents of my current directory and found the first flag in **local.txt**.

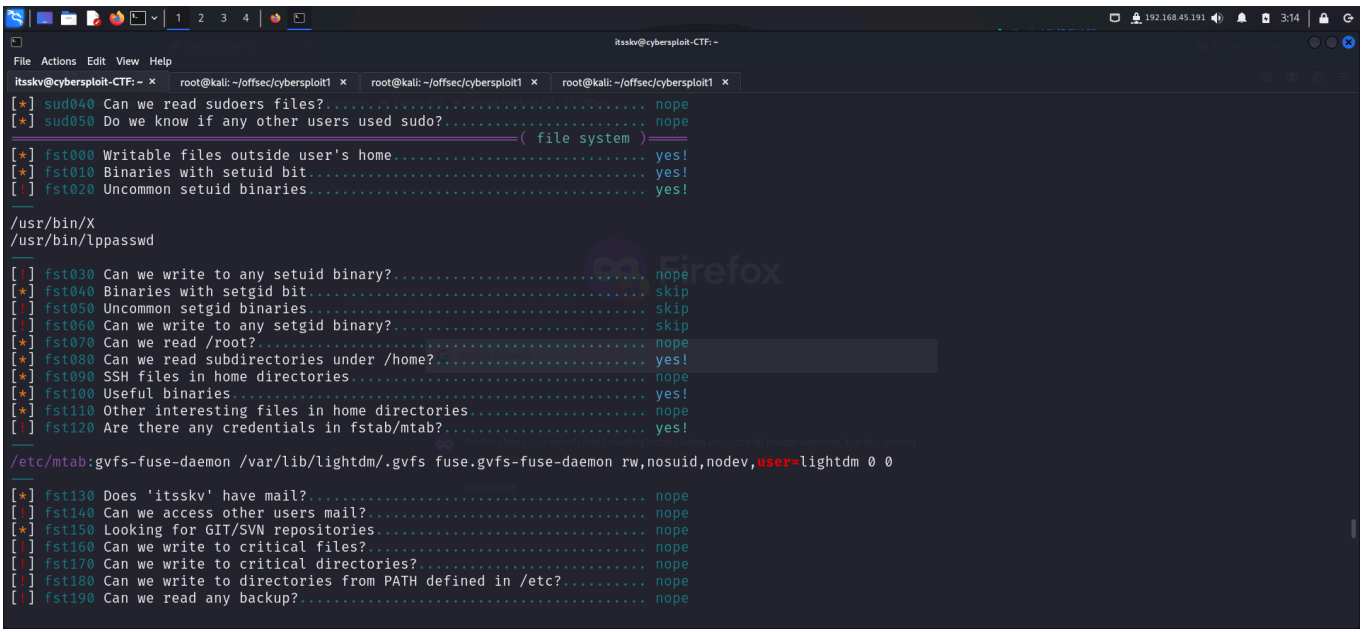


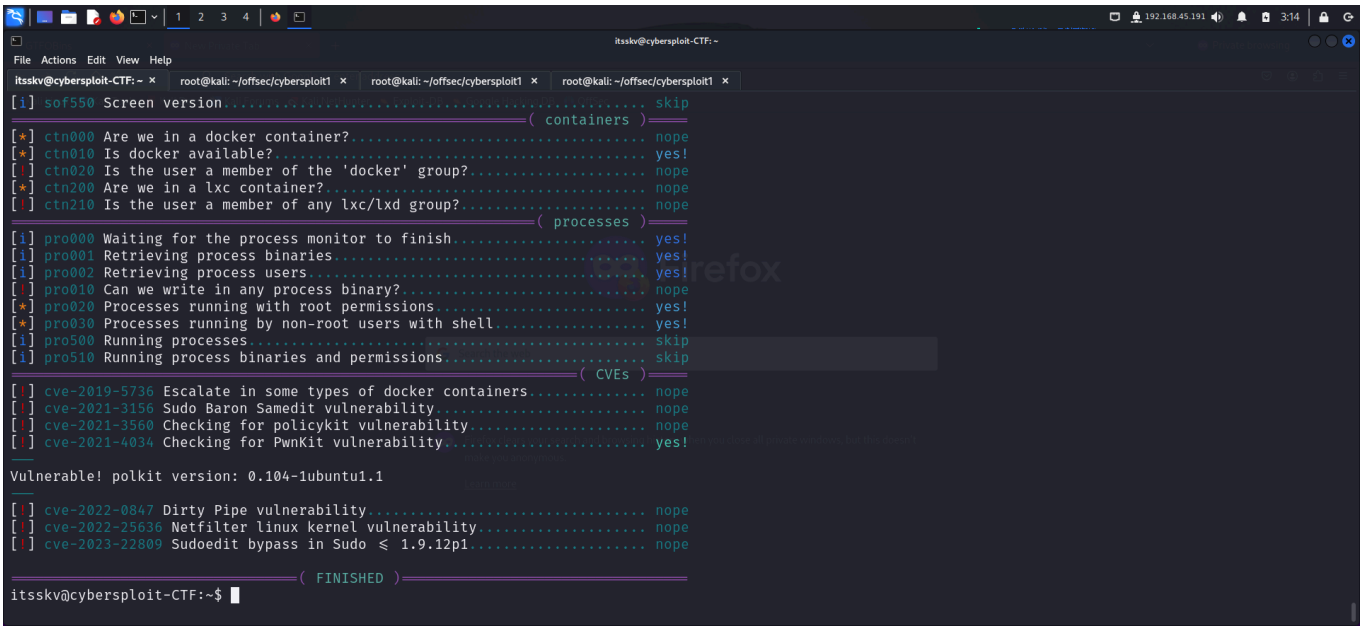
PRIVILEGE ESCALATION

For privilege escalation, I downloaded **linux smart enumeration** script from github on my local system and transferred it to the target.

I executed the script and found some interesting results.


itsskv@cybersploit-CTF: ~
File Actions Edit View Help
itsskv@cybersploit-CTF: ~
root@kali: ~/offsec/cybersploit1
root@kali: ~/offsec/cybersploit1
root@kali: ~/offsec/cybersploit1
itsskv@cybersploit-CTF:~$ ./lse.sh
If you know the current user password, write it here to check sudo privileges: cybersploit{youtube.com/c/cybersploit}
LSE Version: 4.14nw
User: itsskv
User ID: 1001
Password: ******
Home: /home/itsskv
Path: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
umask: 0002
Hostname: cybersploit-CTF
Linux: 3.13.0-32-generic
Distribution: Ubuntu 12.04.5 LTS
Architecture: i686
(Current Output Verbosity Level: 0)
(humanity)
[!] nowar0 Should we question autocrats and their "military operations"?... yes!
NO
WAR
(users)
[i] usr000 Current user groups..... yes!
[*] usr010 Is current user in an administrative group?..... nope

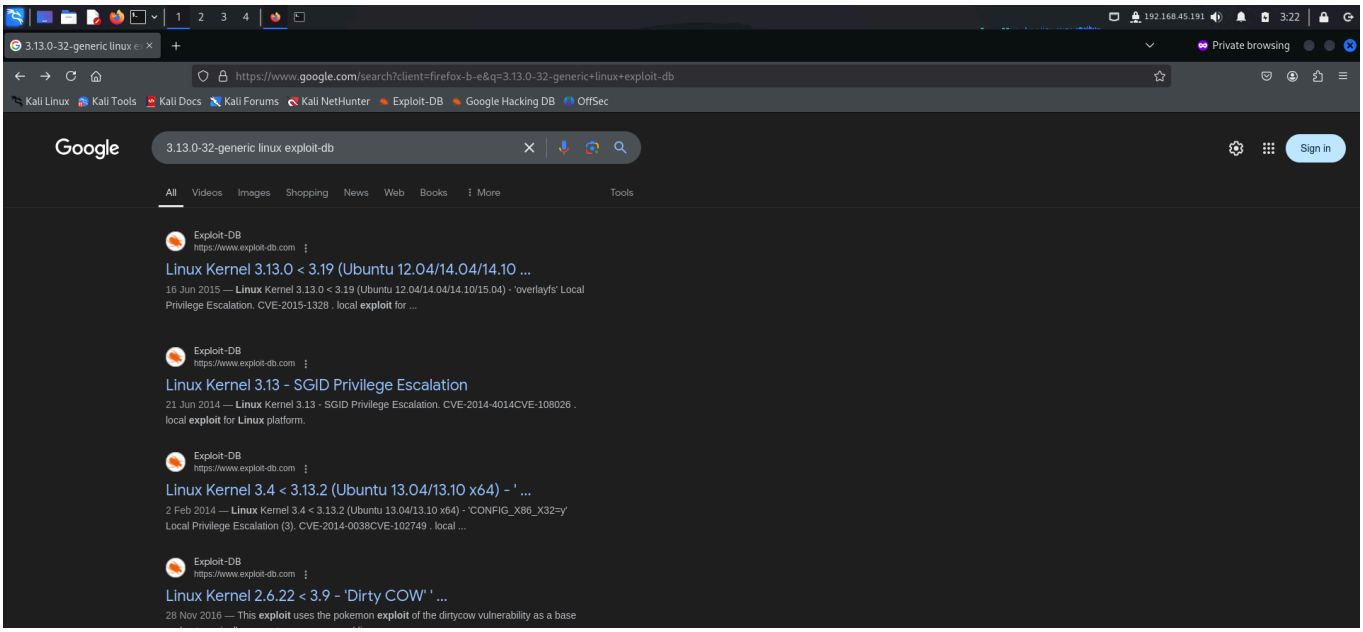

itsskv@cybersploit-CTF: ~
File Actions Edit View Help
[*] sud040 Can we read sudoers files?..... nope
[*] sud050 Do we know if any other users used sudo?..... nope
(file system)
[*] fst000 Writable files outside user's home..... yes!
[*] fst010 Binaries with setuid bit..... yes!
[!] fst020 Uncommon setuid binaries..... yes!
/usr/bin/X
/usr/bin/lppasswd
[!] fst030 Can we write to any setuid binary?..... nope
[*] fst040 Binaries with setgid bit..... skip
[!] fst050 Uncommon setgid binaries..... skip
[!] fst060 Can we write to any setgid binary?..... skip
[*] fst070 Can we read /root?..... nope
[*] fst080 Can we read subdirectories under /home?..... yes!
[*] fst090 SSH files in home directories..... nope
[*] fst100 Useful binaries..... yes!
[*] fst110 Other interesting files in home directories..... nope
[!] fst120 Are there any credentials in fstab/mtab?..... yes!
/etc/mtab:gvfs-fuse-daemon /var/lib/lightdm/.gvfs fuse.gvfs-fuse-daemon rw,nosuid,nodev,user=lightdm 0 0
[*] fst130 Does 'itsskv' have mail?..... nope
[!] fst140 Can we access other users mail?..... nope
[*] fst150 Looking for GIT/SVN repositories..... nope
[!] fst160 Can we write to critical files?..... nope
[!] fst170 Can we write to critical directories?..... nope
[!] fst180 Can we write to directories from PATH defined in /etc?..... nope
[!] fst190 Can we read any backup?..... nope

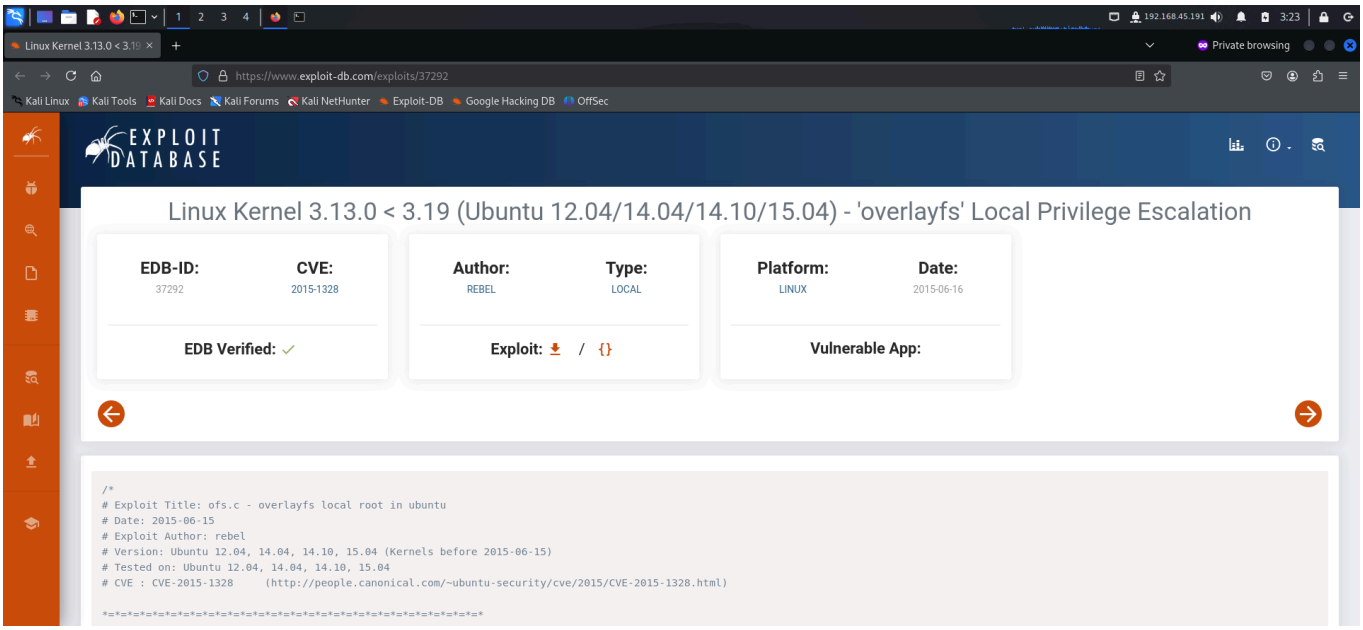


The script identified a couple of misconfigurations which I looked into but found nothing interesting. I then tried looking for kernel exploits. I viewed my kernel version using the following command:

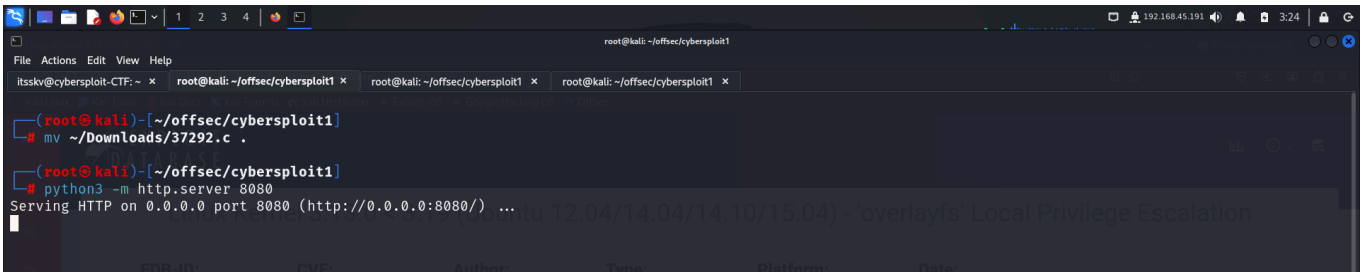
```
itsskv@cybersploit-CTF:~$ uname -r
3.13.0-32-generic
```

I googled available exploits for this version and found some on **exploit db**.



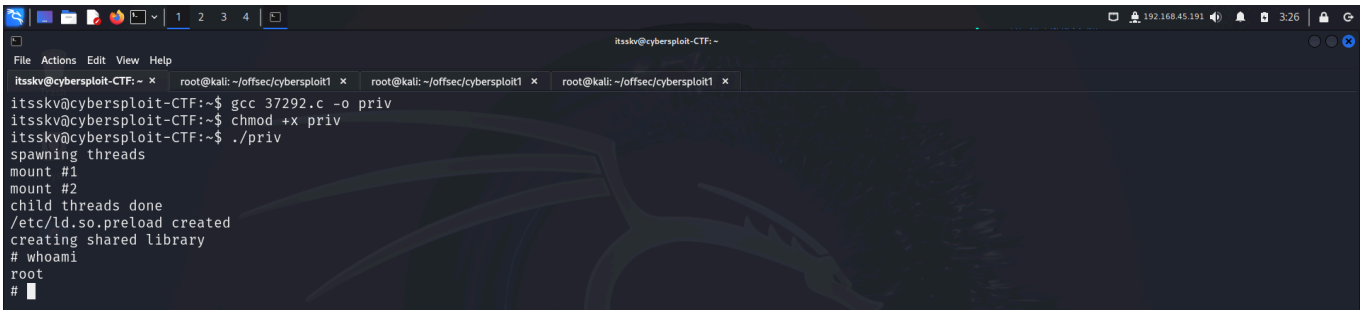


I downloaded the exploit on my system and started a python http server to transfer it on the target.



I downloaded the exploit from my local machine and compiled it using **gcc**

Finally I ran the exploit and got root shell.



I spawned a pty shell and then navigated to the `/root` directory to capture the final flag.

CONCLUSION

Here's a summary of how I pwned the machine:

- I found the username to be hardcoded in the html page.
- I performed web fuzzing and found `/robot.txt`
- I found the password in base64 encoded format in `/robots.txt`.
- I used the username and password to get initial access.
- I found the first flag in my home directory.
- I exploited the kernel to escalate my privilege.
- I captured the final flag from the `root` directory.


YOU HARD
CODE. I CODE HARD.
WE ARE
NOT THE SAME

Happy Hacking! 🎉