Net Sec Challenge

So all that is mentioned in this challenge is: Use this challenge to test your mastery of the skills you have acquires in the network security module. In this challenge, the questions can be solved using only nmap, telnet and hydra.

So the first question is

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

So I had to remind myself, we need to enable our scan to capture more than 100, which is what we are used to. So in this case I did the command:

nmap -sS -p1-10000 10.10.238.228

What this does is a Stealth scan, and goes from port 1 to 10000 on the IP address provided.

```
root@ip-10-10-200-203:~# nmap -sS -p1-10000 10.10.238.228
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-27 17:53 BST
Nmap scan report for ip-10-10-238-228.eu-west-1.compute.internal (10.10.238.228)
Host is up (0.0065s latency).
Not shown: 9995 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
MAC Address: 02:3B:6F:13:F4:7F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
root@ip-10-10-200-203:~#
```

There is an open port outside the common 1000 pots, it is above 10000, what is it?

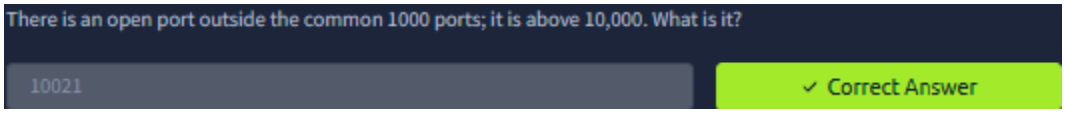
So building on our current knowledge from the last scan, let's extend it further.

nmap -sS -p10000- 10.10.238.228

```
root@ip-10-10-200-203:~# nmap -sS -p10000- 10.10.238.228
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-27 17:55 BST
Nmap scan report for ip-10-10-238-228.eu-west-1.compute.internal (10.10.238.228)
Host is up (0.0045s latency).
Not shown: 55535 closed ports
PORT      STATE SERVICE
10021/tcp open  unknown
MAC Address: 02:3B:6F:13:F4:7F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.51 seconds
root@ip-10-10-200-203:~#
```

So our code is still the same, but it changes it so it starts from port 10,000 and goes through all the ports available starting from port 10000. So here it shows 10021/TCP



How many TCP ports are open?

Well this is an easy one we just count the open TCP ports from our first and second scan. In this case there was a grand total of 6 total TCP connections open.

What flag is hidden in the HTTP server header?

So for this I think I remember using telnet so I am going to fabricate some code prior to doing it.
telnet 10.10.238.228 23 Telnet is not working
telnet 10.10.238.228 80 Connected okay! We can use this to our advantage. I made a small error before where I had the wrong IP, easily done so now I can see what I can find.
Let's pre fabricate code to send in to get the flag in the HTTP header.

1. telnet 10.10.238.228 80
2. GET / HTTP/1.1
3. host: 10.10.238.228

```
Server: lighttpd THM{web_server_25352}
```

There is it!

What is the flag hidden in the SSH server header?

```
root@ip-10-10-200-203:~# telnet 10.10.238.228 22
Trying 10.10.238.228...
Connected to 10.10.238.228.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
```

This was achieved by sending a telnet request on port 22, SSH port.

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

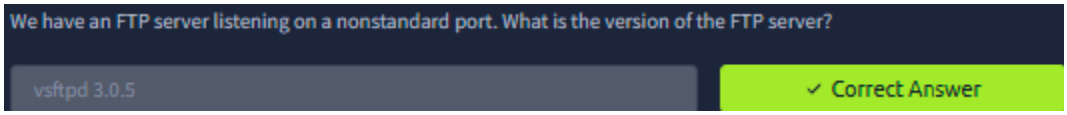
```
root@ip-10-10-200-203:~# nmap -sV -p 21 10.10.238.228
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-27 18:41 BST
Nmap scan report for ip-10-10-238-228.eu-west-1.compute.internal (10.10.238.228)
Host is up (0.00060s latency).

PORT   STATE  SERVICE VERSION
21/tcp closed ftp
MAC Address: 02:3B:6F:13:F4:7F (Unknown)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
root@ip-10-10-200-203:~#
```

Using command **nmap -sV -p 21 10.10.238.228** - 21/TCP closed

Using command **nmap -sV -p- 10.10.238.228 - We scan all ports** ftp open on port 10021 version is **vsftpd 3.0.5**



We learned usernames using social engineering: eddie and quinn. What is the flag hidden in one of these 2 account files accessible using ftp?

So firstly what I am going to do is use hydra to crack the passwords of both accounts, or try to at least.
hydra: Tool used for performing brute force attack
-1 eddie: Specifies username to test eddie
-P: Tells hydra to use this **password list**
/usr/share/wordlists/rockyou.txt: Is the file location specified on the VM
ftp: specifies file transfer protocol we are attacking

```
[STATUS] 319.00 tries/min, 319 tries in 00:01h, 14344112 to do in 749:26h, 16 active
```

As much as I love TryHackme, I am not sure I want to wait 740 Hours…. So I am going to tweak my code using some research on how to do so.
-64 increases tasks
-f means when 1 successful attempt is found it will terminate
hydra -l eddie -P /usr/share/wordlists/rockyou.txt -t 64 -f 10.10.238.228 ftp
hydra -l eddie -P /usr/share/wordlists/rockyou-75.txt -t 64 -f 10.10.238.228 ftp

hydra -l eddie -P /usr/share/wordlists/rockyou.txt ftp://10.10.238.228:10021
hydra -l quinn -P /usr/share/wordlists/rockyou.txt ftp://10.10.238.228:10021

Username: **eddie**
password: **jordan**

Username: **quinn**
Password: **andrea**

```
root@ip-10-10-200-203:~# ftp 10.10.238.228 10021
Connected to 10.10.238.228.
220 (vsFTPd 3.0.5)
Name (10.10.238.228:root): eddie
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

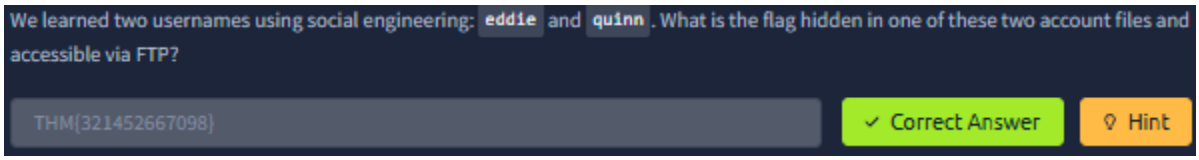
ftp 10.10.238.228 10021

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> bye
```

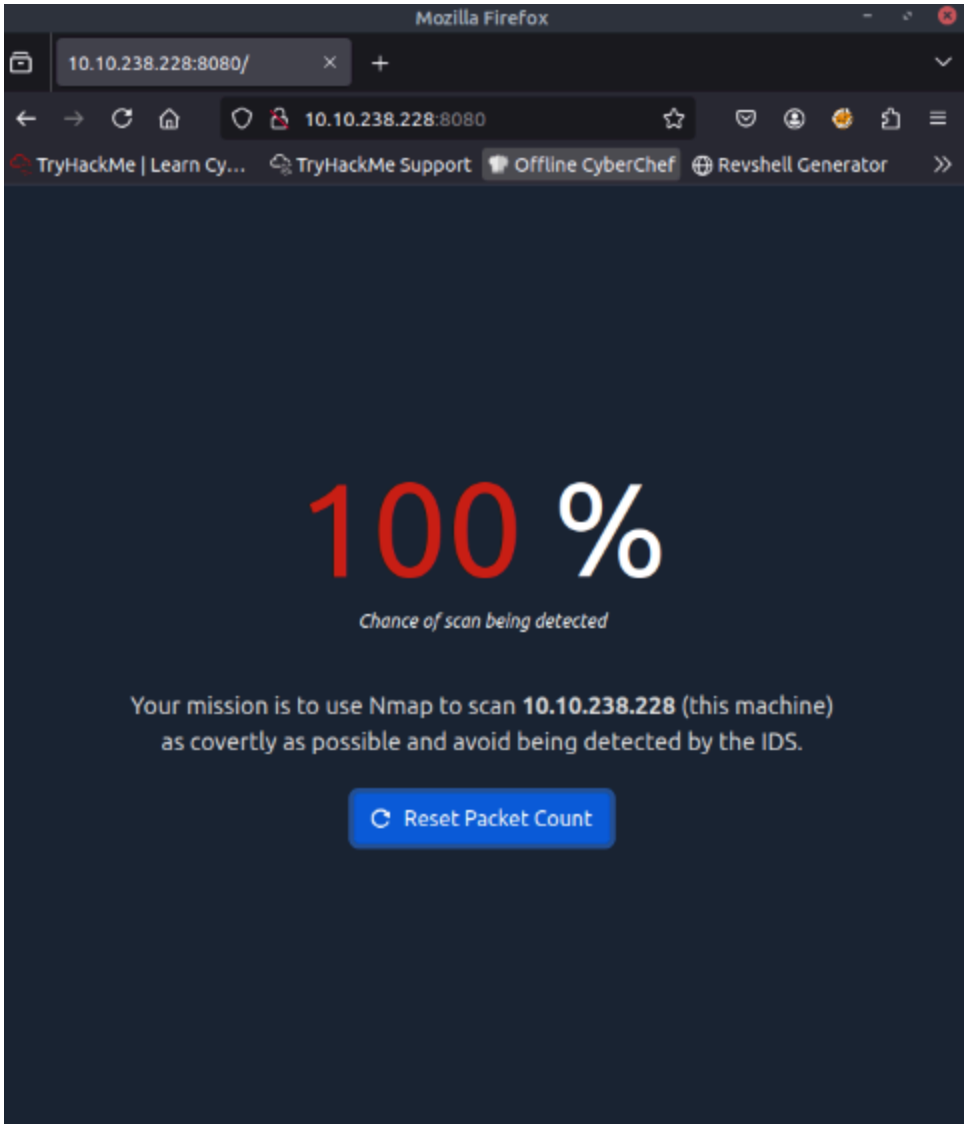
```
Name (10.10.238.228:root): quinn
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 1002     1002           18 Sep 20  2021 ftp_flag.txt
226 Directory send OK.
ftp>
```

```
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).
WARNING! 1 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
18 bytes received in 0.00 secs (28.4436 kB/s)
ftp>
```

```
root@ip-10-10-200-203:~# cat ftp_flag.txt
THM{321452667098}
root@ip-10-10-200-203:~#
```



So our final challenge wants us to browse to http://10.10.238.228:8080
Stealth without being detected. I have some tricks up my sleeve.



I searched the web address in the browser and It got flagged immediately of course. So we will do it sneaky.

```
root@ip-10-10-200-203:~# nmap -sS 10.10.238.228.8080
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-27 19:36 BST
Failed to resolve "10.10.238.228.8080".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
root@ip-10-10-200-203:~#
```

-sS won't work..
nmap -sS -Pn -T2 -f --data-length 50 --max-retries 2 --randomize-hosts 10.10.238.228 8080
-sS Stealth Scan (SYN)
-Pn Skip Ping - Avoid ICMP detection
-T2 Slow scan
-f Fragment packets (smaller chunks)
--data-length 50 Pads packets to throw off fingerprint

--max-retries 2 reduces number of retires
--randomize-hosts avoids predictable scanning patterns

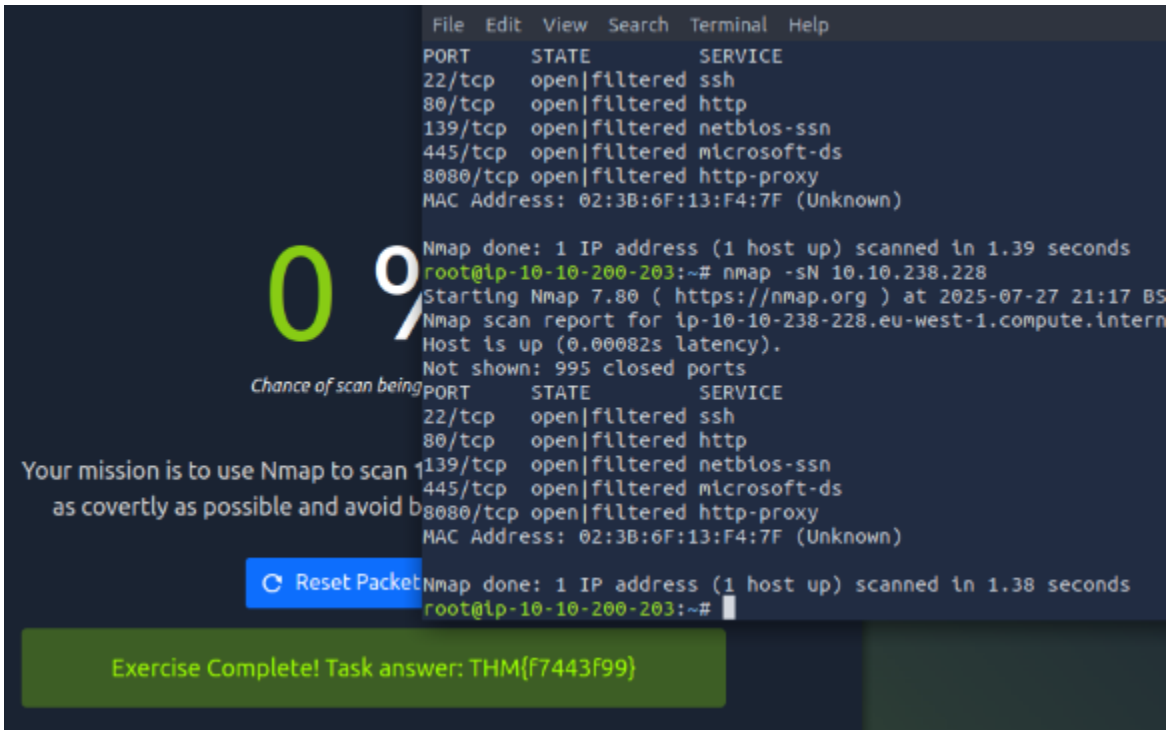
```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-27 19:38 BST
Nmap scan report for ip-10-10-238-228.eu-west-1.compute.internal (10.10.238.228)
Host is up (0.000072s latency).
All 1000 scanned ports on ip-10-10-238-228.eu-west-1.compute.internal (10.10.238.228) are
filtered
MAC Address: 02:3B:6F:13:F4:7F (Unknown)
```

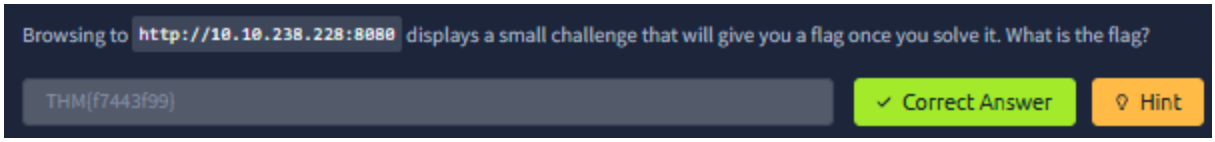
Unfortunately after waiting some time, the scan came back without any clear responses.

So we will fabricate a new scan

nmap -sS -T0 -f -p 1-100 10.10.238.228
-sS - SYN Scan (**Half-open, quiet and hard to detect)**
-T0 - Paranoid timing, MAX delay
-f - Packet fragment, sneaks past deep packet inspection
-p 1-100 Narrowed scan, reduces noise
10.10.238.228 Target system

So I did get slightly tired of waiting and just used a simple -sN scan but I also wanted to go beyond that and go full stealth, unfortunately because of time constraints I had to look for alternatives but it was very enjoyable seeing the different strategies I could have used.




Browsing to http://10.10.238.228:8080 displays a small challenge that will give you a flag once you solve it. What is the flag?
THM{f7443f99}
Correct Answer
Hint