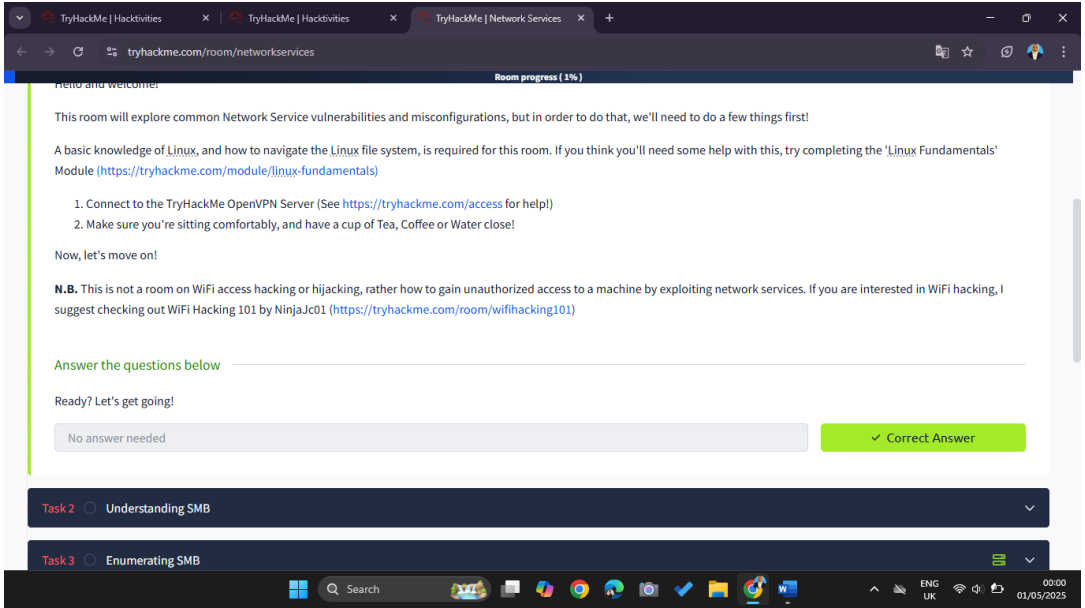
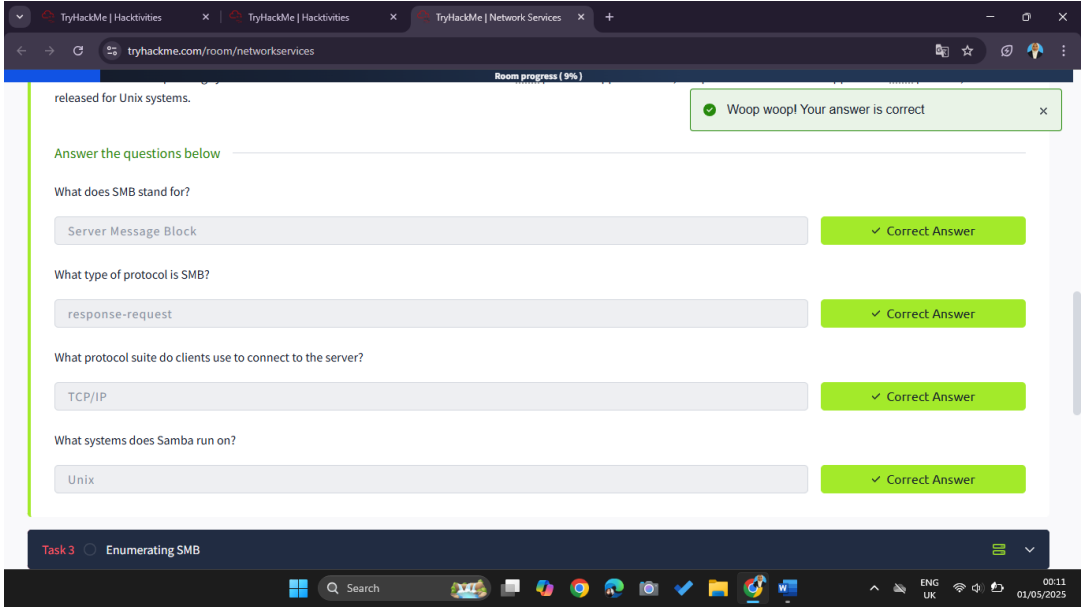


Nama : Aprintan Dwi Cahyani

NIM : 2231740021

Roadmap : Network Service

N O	Screenshoot Progres
1.	<div><h3>Task 1</h3></div>
2.	<div><h3>Task 2</h3></div>
3.	Task 3



	<div> <div>Room completed ( 100% )</div> <p>Great! Have a look around for any interesting documents that could contain valuable information. Who can we assume this profile folder belongs to?</p> <div> <input type="text" value="John Cactus"/> <div>✓ Correct Answer</div> </div> <p>What service has been configured to allow him to work from home?</p> <div> <input type="text" value="ssh"/> <div>✓ Correct Answer</div> </div> <p>Okay! Now we know this, what directory on the share should we look in?</p> <div> <input type="text" value=".ssh"/> <div>✓ Correct Answer</div> </div> <p>This directory contains authentication keys that allow a user to authenticate themselves on, and then access, a server. Which of these keys is most useful to us?</p> <div> <input type="text" value="id_rsa"/> <div>✓ Correct Answer</div> </div> <p>Download this file to your local machine, and change the permissions to "600" using "chmod 600 [file]".</p> <p>Now, use the information you have already gathered to work out the username of the account. Then, use the service and key to log-in to the server.</p> <p>What is the smb.txt flag?</p> <div> <input type="text" value="THM{smb_is_fun_eh?}"/> <div>✓ Correct Answer</div> </div> </div>
5.	<div> <div>Task 5</div> <p>Telnet commands in the Telnet prompt. You can connect to a telnet server with the following syntax: "telnet [ip] [port]"</p> <p>Answer the questions below</p> <p>What is Telnet?</p> <div> <input type="text" value="application protocol"/> <div>✓ Correct Answer</div> </div> <p>What has slowly replaced Telnet?</p> <div> <input type="text" value="ssh"/> <div>✓ Correct Answer</div> </div> <p>How would you connect to a Telnet server with the IP 10.10.10.3 on port 23?</p> <div> <input type="text" value="telnet 10.10.10.3 23"/> <div>✓ Correct Answer</div> </div> <p>The lack of what, means that all Telnet communication is in plaintext?</p> <div> <input type="text" value="encryption"/> <div>✓ Correct Answer</div> <div>Hint</div> </div> <div> <div>Task 6</div> <div>Enumerating Telnet</div> </div> </div>
6.	<div> <div>Task 6</div> </div>

tryhackme.com/room/networkservices

Room completed ( 100% )

What **port** is this?

8012

✓ Correct Answer

This port is unassigned, but still lists the **protocol** it's using, what protocol is this?

tcp

✓ Correct Answer

Now re-run the **nmap** scan, without the **-p-** tag, how many ports show up as open?

0

✓ Correct Answer

Here, we see that by assigning telnet to a **non-standard port**, it is not part of the common ports list, or top 1000 ports, that nmap scans. It's important to try every angle when enumerating, as the information you gather here will inform your exploitation stage.

No answer needed

✓ Correct Answer

Based on the title returned to us, what do we think this port could be **used for**?

a backdoor

✓ Correct Answer

Who could it belong to? Gathering possible **usernames** is an important step in enumeration.

Skidy

✓ Correct Answer

## 7. Task 7

tryhackme.com/room/networkservices

Room completed ( 100% )

Attacker IP: 192.168.1.25  
Listener Port: 4444  
Victim IP: 192.168.1.25

The attacking machine has a listening port, on which it receives the connection, resulting in code or command execution being achieved.

Answer the questions below

Okay, let's try and connect to this telnet port! If you get stuck, have a look at the syntax for connecting outlined above.

No answer needed

✓ Correct Answer

Great! It's an open telnet connection! What welcome message do we receive?

SKIDY'S BACKDOOR.

✓ Correct Answer

Let's try executing some commands, do we get a return on any input we enter into the telnet session? (Y/N)

N

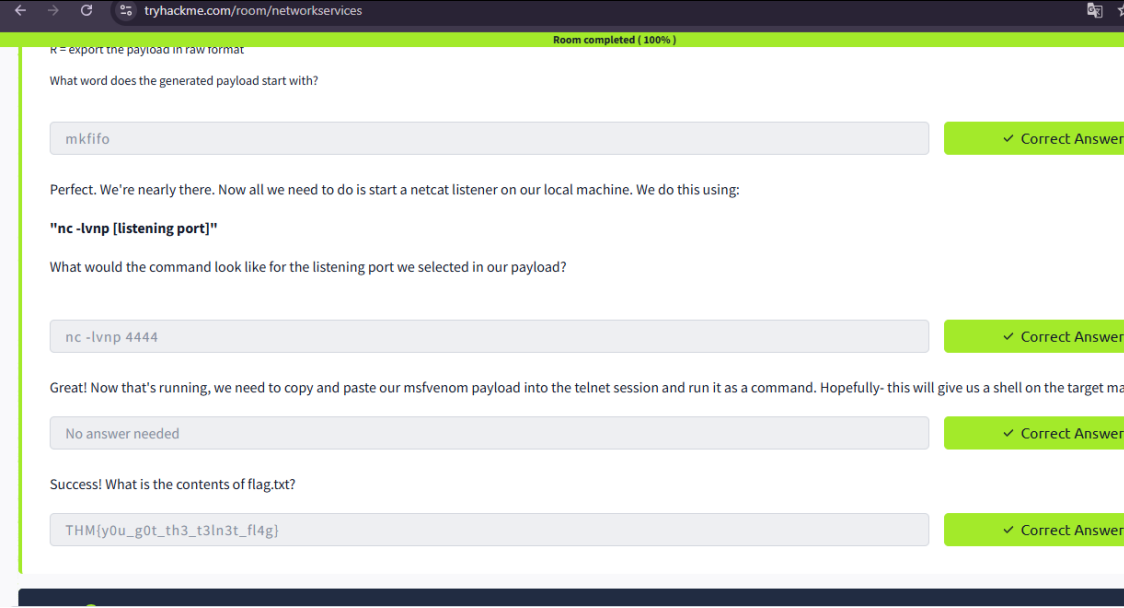
✓ Correct Answer

Hmm... that's strange. Let's check to see if what we're typing is being executed as a system command.

No answer needed

✓ Correct Answer

Start a tcpdump listener on your local machine.

	
8.	<h2>Task 8</h2> <p><b>More Details:</b></p> <p>You can find more details on the technical function, and implementation of <u>FTP</u> on the Internet Engineering Task Force website: <a href="https://www.ietf.org">https://www.ietf.org</a> number of standards agencies, who define and regulate internet standards.</p> <p>Answer the questions below</p> <p>What communications model does FTP use?</p> <p>client-server</p> <p>What's the standard FTP port?</p> <p>21</p> <p>How many modes of FTP connection are there?</p> <p>2</p>
9.	<h2>Task 9</h2>

	<div data-bbox="268 192 1402 795"> <p>Room progress ( 90% )</p> <p>Answer the questions below</p> <p>Run an <b>nmap</b> scan of your choice.</p> <p>How many <b>ports</b> are open on the target machine?</p> <p>1</p> <p>What <b>port</b> is ftp running on?</p> <p>21</p> <p>What <b>variant</b> of FTP is running on it?</p> <p>vsftpd</p> <p>Great, now we know what type of FTP server we're dealing with we can check to see if we are able to login anonymously to the FTP server. We can do this using by t console, and entering "anonymous", and no password when prompted.</p> <p>What is the name of the file in the anonymous FTP directory?</p> <p>PUBLIC_NOTICE.txt</p> </div> <div data-bbox="268 824 1402 1400"> <p>Room progress ( 96% )</p> <p>What <b>variant</b> of FTP is running on it?</p> <p>vsftpd</p> <p>Great, now we know what type of FTP server we're dealing with we can check to see if we are able to login anonymously to the FTP server. We can do this using by typing "ftp / console, and entering "anonymous", and no password when prompted.</p> <p>What is the name of the file in the anonymous FTP directory?</p> <p>PUBLIC_NOTICE.txt</p> <p>What do we think a possible username could be?</p> <p>mike</p> <p>Great! Now we've got details about the FTP server and, crucially, a possible username. Let's see what we can do with that...</p> <p>No answer needed</p> </div> <div data-bbox="268 1400 1402 1433"> <p>Task 10 Exploiting FTP</p> </div>
10	Task 10

tryhackme.com/room/networkservices

Room completed ( 100% )

[machine IP]    The IP address of the target machine

ftp / protocol    Sets the protocol

Let's crack some passwords!

Answer the questions below

What is the password for the user "mike"?

password

✓ Correct Answer

Bingo! Now, let's connect to the FTP server as this user using "ftp [IP]" and entering the credentials when prompted

No answer needed

✓ Correct Answer

What is ftp.txt?


THM{y0u\_g0t\_th3\_ftp\_fl4g}

✓ Correct Answer

Task 11 ✓ Expanding Your Knowledge

tryhackme.com/room/networkservices

Woop woop!



Congratulations on completing Network Services!!! 🎉

Points earned  
🔥 344

Completed tasks  
📋 11

Room type  
👤 Walkthrough

Difficulty  
📶 Easy

Streak  
🔥 3

📝 Leave Feedback

Next