

LAPORAN TUGAS
PEMBELAJARAN TRYHACKME
“Network Services 2”



Olgeh :

Fannisa Az Zahra (2231740037)

Dosen Pengajar :

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

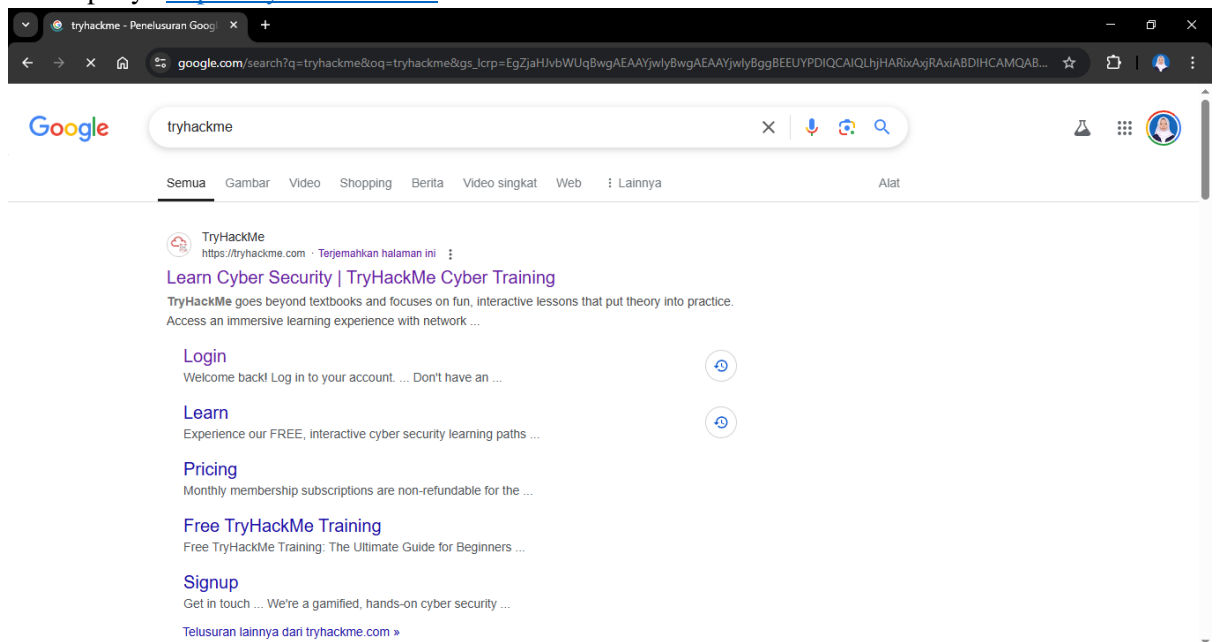
POLITEKNIK NEGERI MALANG PSDKU LUMAJANG

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

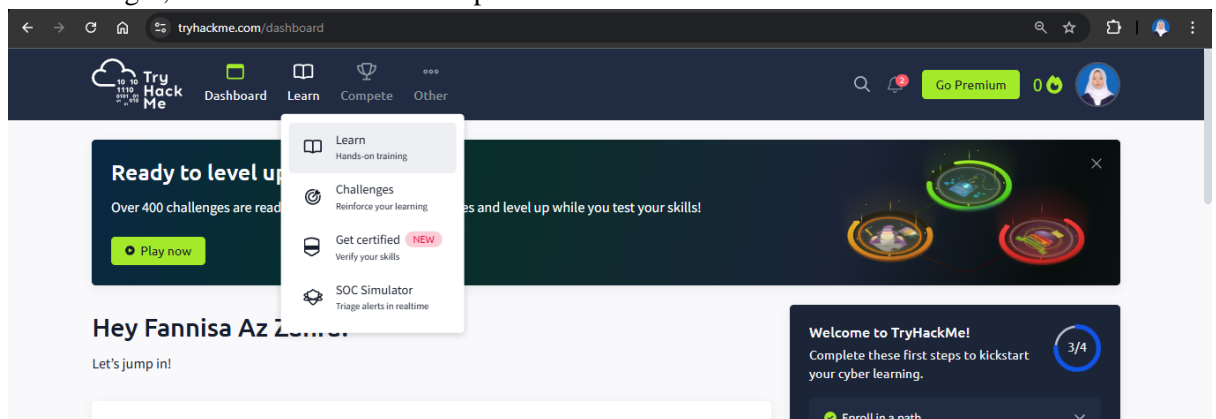
Jawa Timur 67314

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.



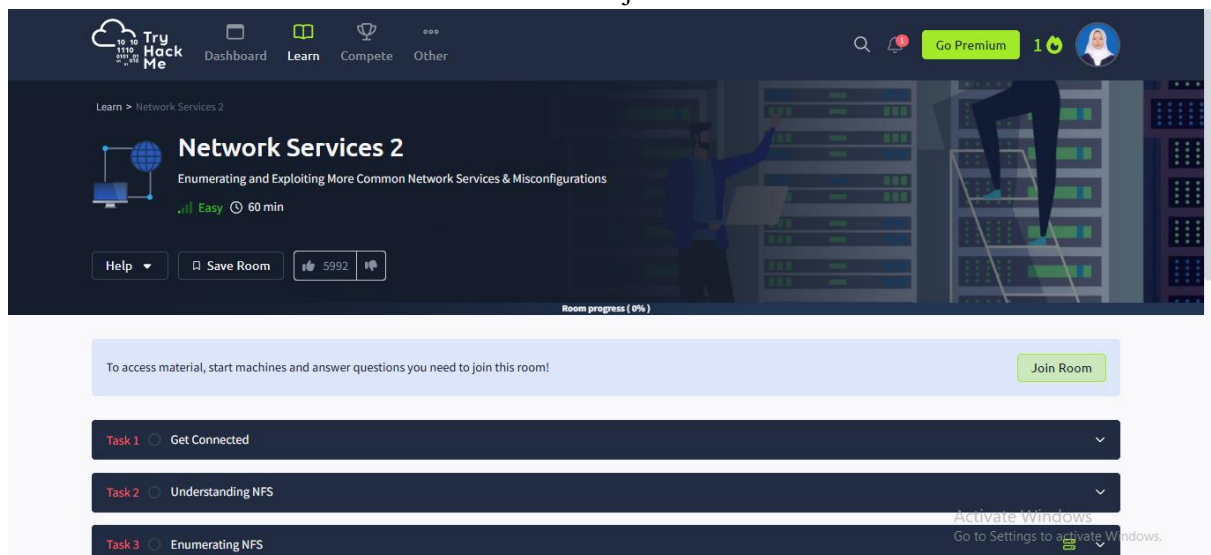
3. Setelah itu scroll kebawah dan pilih Free Roadmap



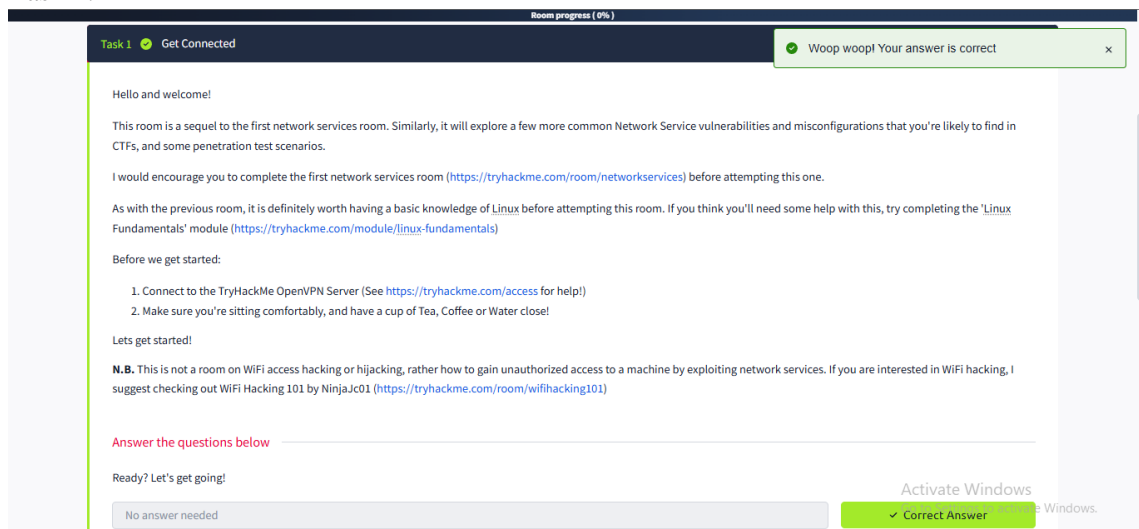
4. Lalu scroll kebawah dan pilih “room Network Services 2”



5. Setelah masuk room “Network Services 2” lalu klik join



6. Task 1.



7. Task 2.

Room progress (14%)

What does NFS stand for?

Network File System

✓ Correct Answer

What process allows an NFS client to interact with a remote directory as though it was a physical device?

Mounting

✓ Correct Answer

What does NFS use to represent files and directories on the server?

file handle

✓ Correct Answer

What protocol does NFS use to communicate between the server and client?

RPC

✓ Correct Answer

What two pieces of user data does the NFS server take as parameters for controlling user permissions? Format: parameter 1 / parameter 2

user id / group id

✓ Correct Answer

Can a Windows NFS server share files with a Linux client? (Y/N)

Y

✓ Correct Answer

Can a Linux NFS server share files with a MacOS client? (Y/N)

Y

✓ Correct Answer

What is the latest version of NFS? [released in 2016, but is still up to date as of 2020] This will require external research.

4.2

✓ Correct Answer

Woop woopl! Your answer is correct

Activate Windows

8. Task 3.

Room progress (20%)

Answer the questions below

Run an **nmap** scan of your choice.

How many **ports** are open on the target machine?

7

✓ Correct Answer

Which port contains the service we're looking to enumerate?

2049

✓ Correct Answer

Now, use `/usr/bin/showmount -e [IP]` to list the NFS shares, what is the name of the visible share?

/home

✓ Correct Answer

Time to mount the share to our local machine!

First, use `"mkdir /tmp/mount"` to create a directory on your machine to mount the share to. This is in the `/tmp` directory- so be aware that it will be removed on restart.

Then, use the mount command we broke down earlier to mount the NFS share to your local machine. Change directory to where you mounted the share- what is the name of the folder inside?

cappuccino

✓ Correct Answer

Have a look inside this directory, look at the files. Looks like we're inside a user's home directory...

No answer needed

✓ Correct Answer

Interesting! Let's do a bit of research now, have a look through the folders. Which of these folders could contain keys that would give us remote access to the server?

.ssh

✓ Correct Answer

Which of these keys is most useful to us?

id_rsa

✓ Correct Answer

Copy this file to a different location your local machine, and change the permissions to "600" using `"chmod 600 [file]"`.

Assuming we were right about what type of directory this is, we can pretty easily work out the name of the user this key corresponds to.

Can we log into the machine using `ssh -i <key-file> <username>@<ip>`? (Y/N)

Y

✓ Correct Answer

Woop woopl! Your answer is correct

Activate Windows

9. Task 4.

Room progress (34%)

Lets do this!

Woop woopl! Your answer is correct

Answer the questions below

First, change directory to the mount point on your machine, where the NFS share should still be mounted, and then into the user's home directory.

No answer needed

✓ Correct Answer

Download the bash executable to your Downloads directory. Then use `"cp ~/Downloads/bash "` to copy the bash executable to the NFS share. The copied bash shell must be owned by a root user, you can set this using `"sudo chown root bash"`

No answer needed

✓ Correct Answer

Now, we're going to add the SUID bit permission to the bash executable we just copied to the share using `"sudo chmod -[permission] bash"`. What letter do we use to set the SUID bit set using `chmod`?

s

✓ Correct Answer

Let's do a sanity check, let's check the permissions of the "bash" executable using `"ls -la bash"`. What does the permission set look like? Make sure that it ends with `-sr-x`.

-rwsr-sr-x

✓ Correct Answer

Now, SSH into the machine as the user. List the directory to make sure the bash executable is there. Now, the moment of truth. Lets run it with `"./bash -p"`. The `-p` persists the permissions, so that it can run as root with SUID- as otherwise bash will sometimes drop the permissions.

No answer needed

✓ Correct Answer

Great! If all's gone well you should have a shell as root! What's the root flag?

THM[nfs_got_pwned]

✓ Correct Answer

Activate Windows

10. Task 5.

Room progress (43%)

What does SMTP stand for?

Simple Mail Transfer Protocol

✔ Correct Answer

Woop woop! Your answer is correct

What does SMTP handle the sending of? (answer in plural)

emails

✔ Correct Answer

What is the first step in the SMTP process?

SMTP handshake

✔ Correct Answer

What is the default SMTP port?

25

✔ Correct Answer

Where does the SMTP server send the email if the recipient's server is not available?

smtp queue

✔ Correct Answer

On what server does the Email ultimately end up on?

POP/IMAP

✔ Correct Answer

Can a Linux machine run an SMTP server? (Y/N)

Y

✔ Correct Answer

Can a Windows machine run an SMTP server? (Y/N)

Y

✔ Correct Answer

Activate Windows
Go to Settings to activate Windows.

11. Task 6.

Room progress (69%)

Answer the questions below

Woop woop! Your answer is correct

First, lets run a port scan against the target machine, same as last time. What port is SMTP running on?

25

✔ Correct Answer

Okay, now we know what port we should be targeting, let's start up Metasploit. What command do we use to do this?

If you would like some more help or practice using Metasploit, TryHackMe has a module on Metasploit that you can check out here:

<https://tryhackme.com/module/metasploit>

msfconsole

✔ Correct Answer

Let's search for the module "smtp_version", what's it's full module name?

auxiliary/scanner/smtp/smtp_version

✔ Correct Answer

Great, now- select the module and list the options. How do we do this?

options

✔ Correct Answer

Have a look through the options, does everything seem correct? What is the option we need to set?

RHOSTS

✔ Correct Answer

Set that to the correct value for your target machine. Then run the exploit. What's the system mail name?

polosmtp.home

✔ Correct Answer

What Mail Transfer Agent (MTA) is running the SMTP server? This will require some external research.

Postfix

✔ Correct Answer

Good! We've now got a good amount of information on the target system to move onto the next stage. Let's search for the module "smtp_enum", what's it's full module name?

auxiliary/scanner/smtp/smtp_enum

✔ Correct Answer

We're going to be using the "top-usernames-shortlist.txt" wordlist from the Usernames subsection of seclists (/usr/share/wordlists/SecLists/Usernames if you have it installed).

SecLists is an amazing collection of wordlists. If you're running Kali or Parrot you can install seclists with: "sudo apt install seclists" Alternatively, you can download the repository from [here](#).

What option do we need to set to the wordlist's path?

USER_FILE

✔ Correct Answer

Once we've set this option, what is the other essential paramater we need to set?

RHOSTS

✔ Correct Answer

Now, run the exploit, this may take a few minutes, so grab a cup of tea, coffee, water. Keep yourself hydrated!

No answer needed

✔ Correct Answer

Okay! Now that's finished, what username is returned?

administrator

✔ Correct Answer

Activate Windows
Go to Settings to activate Windows.

12. Task 7.

Room progress (70%)
Woop woop! Your answer is correct

SECTION	FUNCTION
hydra	Runs the hydra tool
-t 16	Number of parallel connections per target
-l [user]	Points to the user who's account you're trying to compromise
-P [path to dictionary]	Points to the file containing the list of possible passwords
-vV	Sets verbose mode to very verbose, shows the login+pass combination for each attempt
[machine IP]	The IP address of the target machine
ssh / protocol	Sets the protocol

Looks like we're ready to rock n roll!

Answer the questions below

What is the password of the user we found during our enumeration stage?

✓ Correct Answer

Great! Now, let's SSH into the server as the user, what is contents of smtp.txt

✓ Correct Answer

13. Task 8.

Room progress (78%)
Woop woop! Your answer is correct

MySQL can run on various platforms, whether it's Linux or windows. It is commonly used as a back end database for many prominent websites and forms an essential component of the LAMP stack, which includes: Linux, Apache, MySQL, and PHP.

More information:

Here are some resources that explain the technical implementation, and working of, MySQL in more detail than I have covered here:

https://dev.mysql.com/doc/dev/mysql-server/latest/PAGE_SQL_EXECUTION.html

https://www.w3schools.com/php/php_mysql_intro.asp

Answer the questions below

What type of software is MySQL?

✓ Correct Answer

What language is MySQL based on?

✓ Correct Answer

What communication model does MySQL use?

✓ Correct Answer

What is a common application of MySQL?

✓ Correct Answer

What major social network uses MySQL as their back-end database? This will require further research.

✓ Correct Answer

14. Task 9.

Room progress (87%)
Woop woop! Your answer is correct

Answer the questions below

As always, let's start out with a port scan, so we know what port the service we're trying to attack is running on. What port is MySQL using?

✓ Correct Answer

Good, now we think we have a set of credentials. Let's double check that by manually connecting to the MySQL server. We can do this using the command "mysql -h [IP] -u [username] -p"

✓ Correct Answer

Okay, we know that our login credentials work. Let's quit out of this session with "exit" and launch up Metasploit.

✓ Correct Answer

We're going to be using the "mysql_sql" module.

Search for, select and list the options it needs. What three options do we need to set? (in descending order).

✓ Correct Answer
Hint

Run the exploit. By default it will test with the "select version()" command, what result does this give you?

✓ Correct Answer

Great! We know that our exploit is landing as planned. Let's try to gain some more ambitious information. Change the "sql" option to "show databases", how many databases are returned?

✓ Correct Answer

15. Task 10.

First, let's search for and select the "mysql_schemadump" module. What's the module's full name?

✓ Correct Answer

Great! Now, you've done this a few times by now so I'll let you take it from here. Set the relevant options, run the exploit. What's the name of the last table that gets dumped?

✓ Correct Answer

Awesome, you have now dumped the tables, and column names of the whole database. But we can do one better... search for and select the "mysql_hashdump" module. What's the module's full name?

✓ Correct Answer

Again, I'll let you take it from here. Set the relevant options, run the exploit. What non-default user stands out to you?

✓ Correct Answer

Another user! And we have their password hash. This could be very interesting. Copy the hash string in full, like: bob:"HASH" to a text file on your local machine called "hash.txt". What is the user/hash combination string?

✓ Correct Answer 🔍 Hint

Now, we need to crack the password! Let's try John the Ripper against it using: "john hash.txt" what is the password of the user we found?

✓ Correct Answer

Awesome. Password reuse is not only extremely dangerous, but extremely common. What are the chances that this user has reused their password for a different service?

What's the contents of MySQL.txt

✓ Correct Answer

Activate Windows
Go to Settings to activate Windows.

16. Task 11.

Room completed (100%)

Task 11 🟢 Further Learning

Reading

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

- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/4/html/security_guide/ch-exploits
- <https://www.nextgov.com/cybersecurity/2019/10/nsa-warns-vulnerabilities-multiple-ypp-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

Congratulations! You did it!

✓ Correct Answer

17. Maka selesai sudah room "Network Services 2"

Woop woop! Your answer is correct

Congratulations on completing Network Services 2!!! 🎉

Points earned 🔥 440	Completed tasks 📋 11	Room type 🧭 Walkthrough	Difficulty 📊 Easy	Streak 🔥 2
------------------------	-------------------------	----------------------------	----------------------	---------------

[Leave Feedback](#) [Next](#)

Activate Windows
Go to Settings to activate Windows.