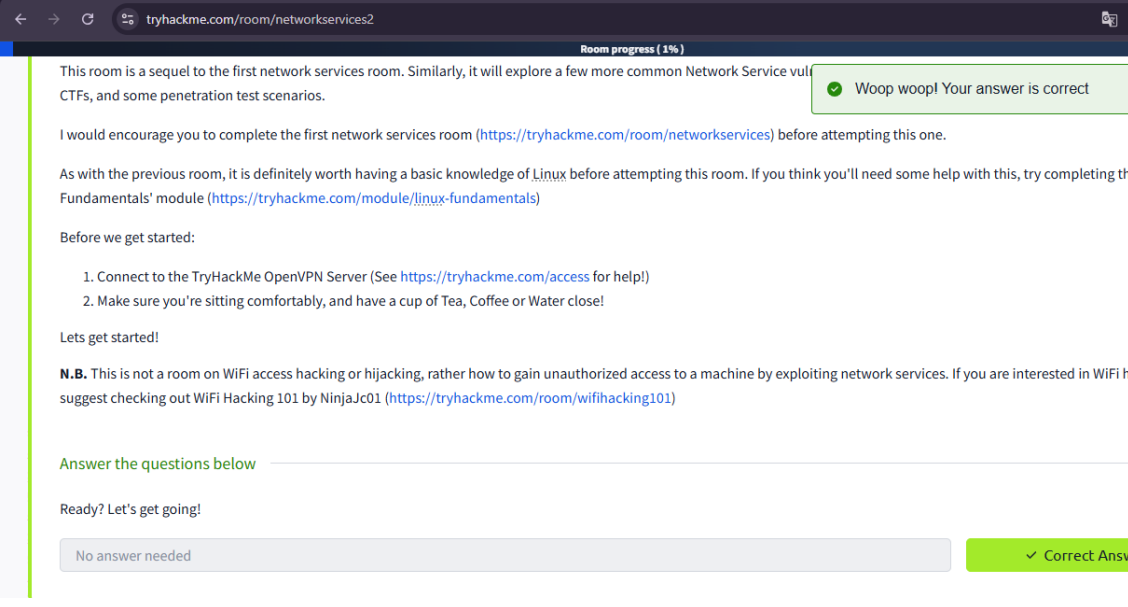
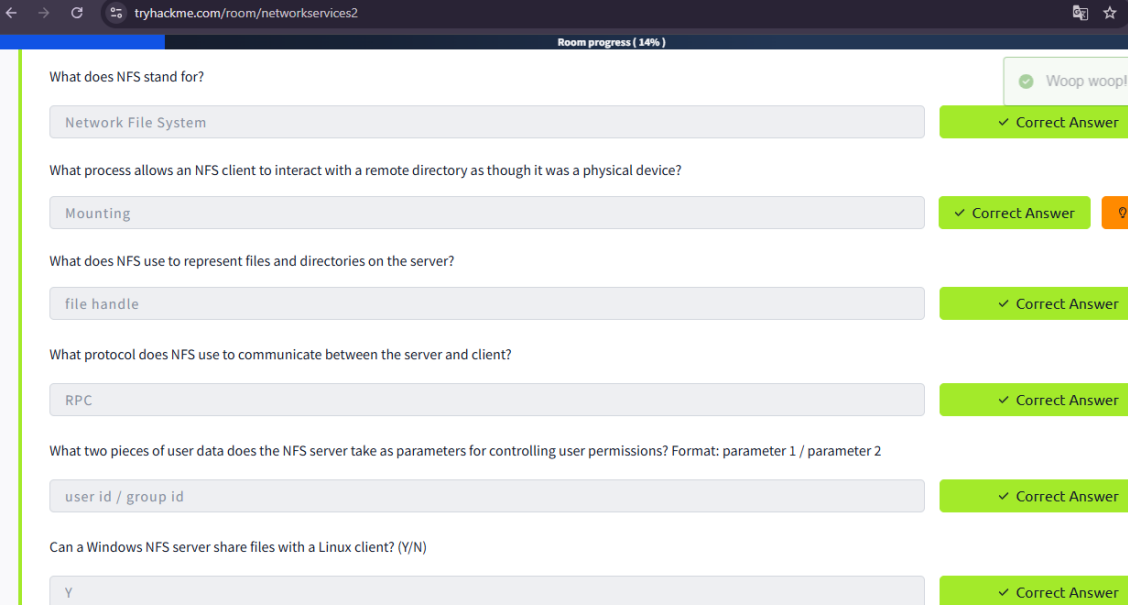


Nama : Aprintan Dwi Cahyani

NIM : 2231740021

Roadmap : Network Service 2

NO	Screenshoot Progres
1.	<div><div>Task 1</div><div><p>tryhackme.com/room/networkservices2</p><p>Room progress ( 1% )</p><p>This room is a sequel to the first network services room. Similarly, it will explore a few more common Network Service vulnerabilities, CTFs, and some penetration test scenarios.</p><p>I would encourage you to complete the first network services room (<a href="https://tryhackme.com/room/networkservices">https://tryhackme.com/room/networkservices</a>) before attempting this one.</p><p>As with the previous room, it is definitely worth having a basic knowledge of Linux before attempting this room. If you think you'll need some help with this, try completing the 'Fundamentals' module (<a href="https://tryhackme.com/module/linux-fundamentals">https://tryhackme.com/module/linux-fundamentals</a>)</p><p>Before we get started:</p><ol style="list-style-type: none"><li>1. Connect to the TryHackMe OpenVPN Server (See <a href="https://tryhackme.com/access">https://tryhackme.com/access</a> for help!)</li><li>2. Make sure you're sitting comfortably, and have a cup of Tea, Coffee or Water close!</li></ol><p>Lets get started!</p><p><b>N.B.</b> This is not a room on WiFi access hacking or hijacking, rather how to gain unauthorized access to a machine by exploiting network services. If you are interested in WiFi Hacking suggest checking out WiFi Hacking 101 by NinjaJc01 (<a href="https://tryhackme.com/room/wifihacking101">https://tryhackme.com/room/wifihacking101</a>)</p><p>Answer the questions below</p><p>Ready? Let's get going!</p><p>No answer needed</p><p>✓ Correct Answer</p></div></div>
2.	<div><div>Task 2</div><div><p>tryhackme.com/room/networkservices2</p><p>Room progress ( 14% )</p><p>What does NFS stand for?</p><p>Network File System</p><p>✓ Correct Answer</p><p>What process allows an NFS client to interact with a remote directory as though it was a physical device?</p><p>Mounting</p><p>✓ Correct Answer</p><p>What does NFS use to represent files and directories on the server?</p><p>file handle</p><p>✓ Correct Answer</p><p>What protocol does NFS use to communicate between the server and client?</p><p>RPC</p><p>✓ Correct Answer</p><p>What two pieces of user data does the NFS server take as parameters for controlling user permissions? Format: parameter 1 / parameter 2</p><p>user id / group id</p><p>✓ Correct Answer</p><p>Can a Windows NFS server share files with a Linux client? (Y/N)</p><p>Y</p><p>✓ Correct Answer</p></div></div>

	<p>Can a Windows NFS server share files with a Linux client? (Y/N)</p> <p>Y</p> <p>✓ Correct Answer</p> <p>Can a Linux NFS server share files with a MacOS client? (Y/N)</p> <p>Y</p> <p>✓ Correct Answer</p> <p>What is the latest version of NFS? [released in 2016, but is still up to date as of 2020] This will require external research.</p> <p>4.2</p> <p>✓ Correct Answer</p>
3.	<h3>Task 3</h3> <p>Room progress ( 18% )</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>7</p> <p>✓ Cor</p> <p>Which port contains the service we're looking to enumerate?</p> <p>2049</p> <p>Now, use <code>/usr/sbin/showmount -e [IP]</code> to list the NFS shares, what is the name of the visible share?</p> <p>/home</p> <p>Time to mount the share to our local machine!</p> <p>First, use "<code>mkdir /tmp/mount</code>" to create a directory on your machine to mount the share to. This is in the <code>/tmp</code> directory- so be aware that it will be removed</p> <p>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- wh</p> <p>Room progress ( 25% )</p> <p>Then, use the mount command we broke down earlier to mount the NFS share to your local machine. Change directory to inside?</p> <p>cappucino</p> <p>✓ Correct An</p> <p>Have a look inside this directory, look at the files. Looks like we're inside a user's home directory...</p> <p>No answer needed</p> <p>✓ Correct An</p> <p>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?</p> <p>.ssh</p> <p>✓ Correct An</p> <p>Which of these keys is most useful to us?</p> <p>id_rsa</p> <p>✓ Correct Answer</p> <p>Copy this file to a different location your local machine, and change the permissions to "600" using "<code>chmod 600 [file]</code>".</p> <p>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.</p> <p>Can we log into the machine using <code>ssh -i &lt;key-file&gt; &lt;username&gt;@&lt;ip&gt;</code> ? (Y/N)</p> <p>Y</p> <p>✓ Correct An</p>
4.	<h3>Task 4</h3>

Room progress ( 35% )

Download the bash executable to your Downloads directory. Then use "cp ~/Downloads/bash ." to copy the bash executable to the current directory. Now, as the root user, you can set this using "sudo chown root bash".

No answer needed

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 permissions using chmod?

s

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

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

No answer needed

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

THM{nfs\_got\_pwned}

✓ Woop woop! Your answer is correct

✓ Woop woop! Your answer is correct

✓ Correct

✓ Correct

✓ Correct

✓ Correct

## 5. Task 5

tryhackme.com/room/networkservices2

Room progress ( 43% )

<https://www.afternerd.com/blog/sntp/>

Answer the questions below

What does SMTP stand for?

Simple Mail Transfer Protocol

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

emails

What is the first step in the SMTP process?

SMTP handshake

What is the default SMTP port?

25

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

smtp queue

✓ Woop woop! Your answer is correct

✓ Correct Answer

✓ Correct Answer

✓ Correct Answer

✓ Correct Answer

✓ Correct Answer

Room progress ( 46% )

25

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

smtp queue

On what server does the Email ultimately end up on?

POP/IMAP

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

Y

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

y

✓ Woop woop! Your answer is correct

✓ Woop woop! Your answer is correct

✓ Correct Answer

✓ Correct Answer

✓ Correct Answer

Task 6 Enumerating SMTP Locked

## 6. Task 6

Room progress ( 54% )

Now we've covered the theory. Let's get going!

Woop woop! Your answer is correct

Answer the questions below

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

tryhackme.com/room/networkservices2

Room progress ( 60% )

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](#).

	<div><div>Room progress ( 67% )</div><div>auxiliary/scanner/smtp/smtp_enum</div><div>Woop woopl! Your answer is correct</div><p>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 wordlists from <a href="#">here</a>.</p><p>What option do we need to set to the wordlist's path?</p><div>USER_FILE</div><div>✓ Correct</div><p>Once we've set this option, what is the other essential parameter we need to set?</p><div>RHOSTS</div><div>✓ Correct</div><p>Now, run the exploit, this may take a few minutes, so grab a cup of tea, coffee, water. Keep yourself hydrated!</p><div>No answer needed</div><div>✓ Correct</div><p>Okay! Now that's finished, what username is returned?</p><div>administrator</div><div>✓ Correct</div></div>
7.	<div><div>Task 7</div><div><div>ssh / protocol</div><div>Sets the protocol</div></div><p>Looks like we're ready to rock n roll!</p><p>Answer the questions below</p><p>What is the password of the user we found during our enumeration stage?</p><div>alejandro</div><p>Great! Now, let's SSH into the server as the user, what is contents of smtp.txt</p><div>THM{who_knew_email_servers_were_c00l?}</div><div>Task 8 Understanding MySQL</div></div>
8.	<div><div>Task 8</div></div>

	<div> <div> <div>Room progress ( 100% )</div> <div> <div>Answer the questions below</div> <div> <div> <div>What type of software is MySQL?</div> <div>relational database management system</div> <div>✓ Correct Answer</div> </div> <div> <div>What language is MySQL based on?</div> <div>SQL</div> <div>✓ Correct Answer</div> </div> <div> <div>What communication model does MySQL use?</div> <div>client-server</div> <div>✓ Correct Answer</div> </div> <div> <div>What is a common application of MySQL?</div> <div>back end database</div> <div>✓ Correct Answer</div> </div> <div> <div>What major social network uses MySQL as their back-end database? This will require further research.</div> <div>Facebook</div> <div>✓ Correct Answer</div> </div> </div> <div> <div>Woop woopl! Your answer is correct</div> </div> </div> <div> <div>tryhackme.com/room/networkservices/</div> <div>Room progress ( 87% )</div> <div> <div>3306</div> <div>✓ Correct Answer</div> </div> <div> <div>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 [user]".</div> <div>No answer needed</div> <div>✓ Correct Answer</div> </div> <div> <div>Okay, we know that our login credentials work. Lets quit out of this session with "exit" and launch up Metasploit.</div> <div>No answer needed</div> <div>✓ Correct Answer</div> </div> <div> <div>We're going to be using the "mysql_sql" module.</div> <div>Search for, select and list the options it needs. What three options do we need to set? (in descending order).</div> <div>PASSWORD/RHOSTS/USERNAME</div> <div>✓ Correct Answer</div> </div> <div> <div>Run the exploit. By default it will test with the "select version()" command, what result does this give you?</div> <div>5.7.29-0ubuntu0.18.04.1</div> <div>✓ Correct Answer</div> </div> <div> <div>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?</div> <div>4</div> <div>✓ Correct Answer</div> </div> </div> </div></div>
9.	<div>Task 9</div>
10.	<div>Task 10</div>

Room progress ( 98% )

Answer the questions below

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

auxiliary/scanner/mysql/mysql\_schemadump

✓ Correct

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?

x\$waits\_global\_by\_latency

✓ Correct

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's full name?

auxiliary/scanner/mysql/mysql\_hashdump

✓ Correct

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

carl

✓ Correct

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?

carl:\*EA031893AA21444B170FC2162A56978B8CEECE18

✓ 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?

carl

✓ 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?

carl:\*EA031893AA21444B170FC2162A56978B8CEECE18

✓ Correct Answer

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?

doggie

✓ 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

THM{congratulations\_you\_got\_the\_mySQL\_flag}

✓ Correct Answer

tryhackme.com/room/networkservices2

Woop woop! Your answer is correct



Congratulations on completing Network Services 2!!! 🎉

Leave Feedback

Next