Course: CEH

Date Assigned: 12-10-2025

Due Date: 13-10-2025

Student Name: **Praveen Kumar**

Batch/Section: **Super30 Batch**

Instructor: **Nitish kumar**

Summary

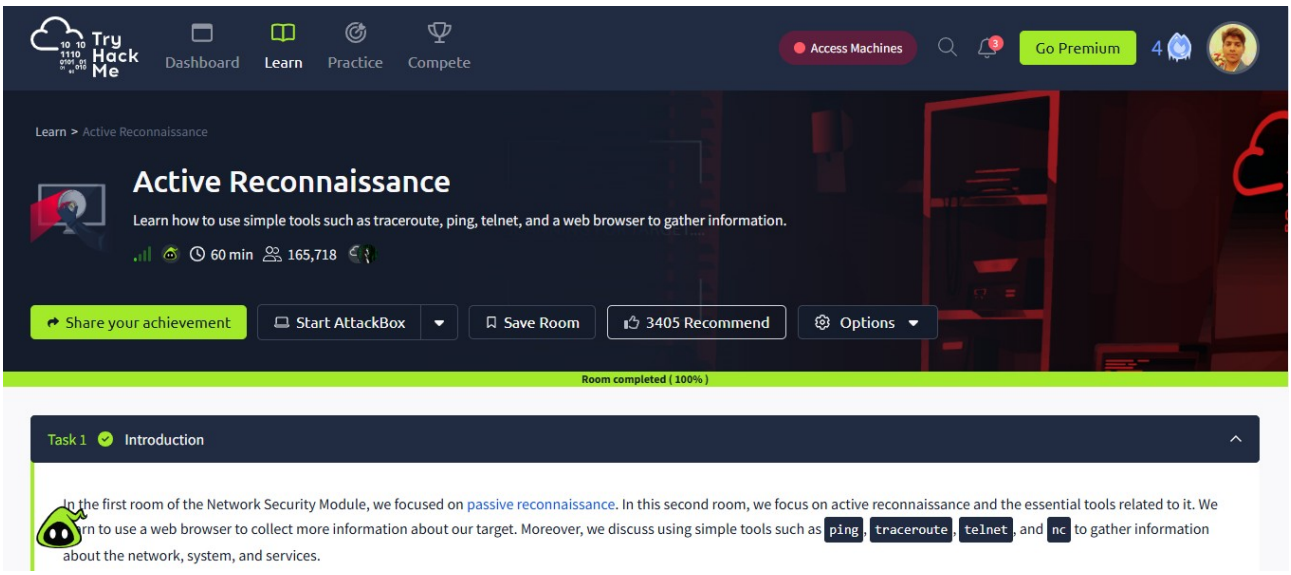
The PDF is a concise practical guide to *active reconnaissance* as taught in the TryHackMe lab. It explains what active recon is, how it differs from passive recon, and walks through a hands-on workflow for discovering and enumerating targets using commonly available tools. The document is aimed at learners who want a structured approach to finding live hosts, open services, and useful attack surface details.

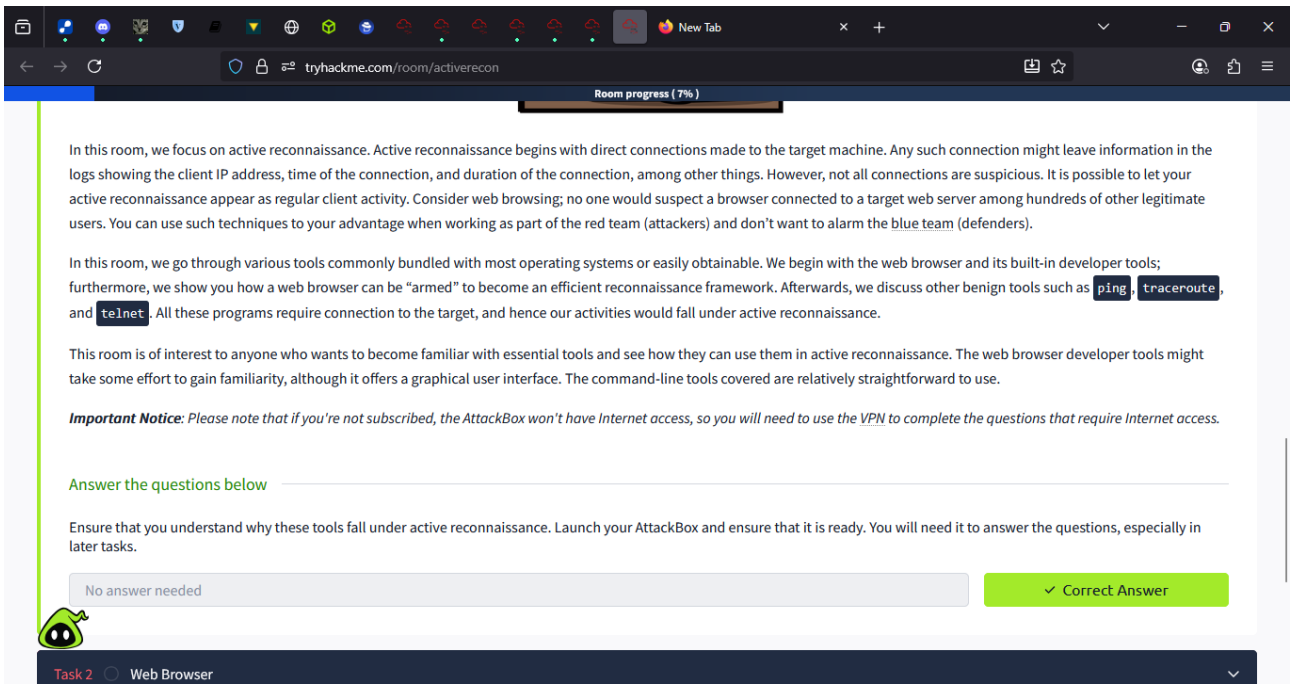
Active_Reconnaissance_lab

Active Reconnaissance involves direct interacting with the target to gather information. With this type of attack, it can be sure that you will be detected once you Recon the target directly since it involves sending requests to the target discovering vulnerabilities.

Active Reconnaissance requires using tools such as:

1. **Port-Scanning** to scan opened ports and version that can be used as an advantage
2. **Network Mapping** uses traceroute to scan the map out of network's target infrastructure since the packet you sent can be received by Routers, even Switches.
3. **Ping Sweeps** sends ICMP (Internet Control Message Protocol) echo requests. But multiple IP address are being received an ICMP to discover hosts that are active on the network.
4. **Social Engineering** now this type could also have Active Reconnaissance. One of the examples is engaging conversation to the certain target. You want them to give what they own (usually, accounts like emails or any social accounts. Knowing what company are they associated to or likely network infrastructure or any information that you think it can be used as advantage to your target)





Task 2. Web browsers

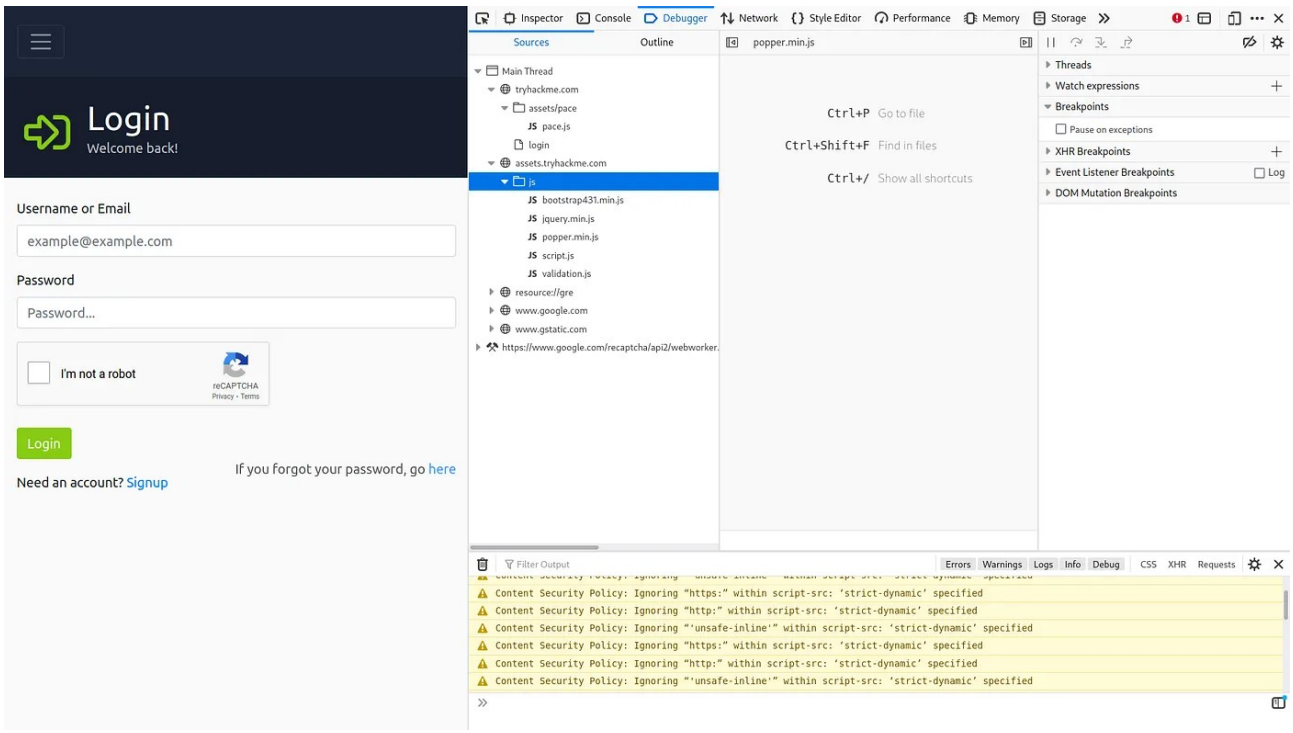
In the TryHackMe, the lecture focuses on Active Reconnaissance one of the first activity is about Web Browsers.

Web browser can be use to gather information about a target.

Browsers can access websites by connecting to **HTTP** or **HTTPS**. It is a type of Application that establishes connection to a server hosting website. Users connects to a:

TCP 80 by defalt when the website is accessed over **HTTP**.
TCP 443 by default when the website is accessed over **HTTPS.**

While browsing a web page, you can press **Ctrl +Shift + I** on a PC to open the Developer Tools on Web Browsers.



-

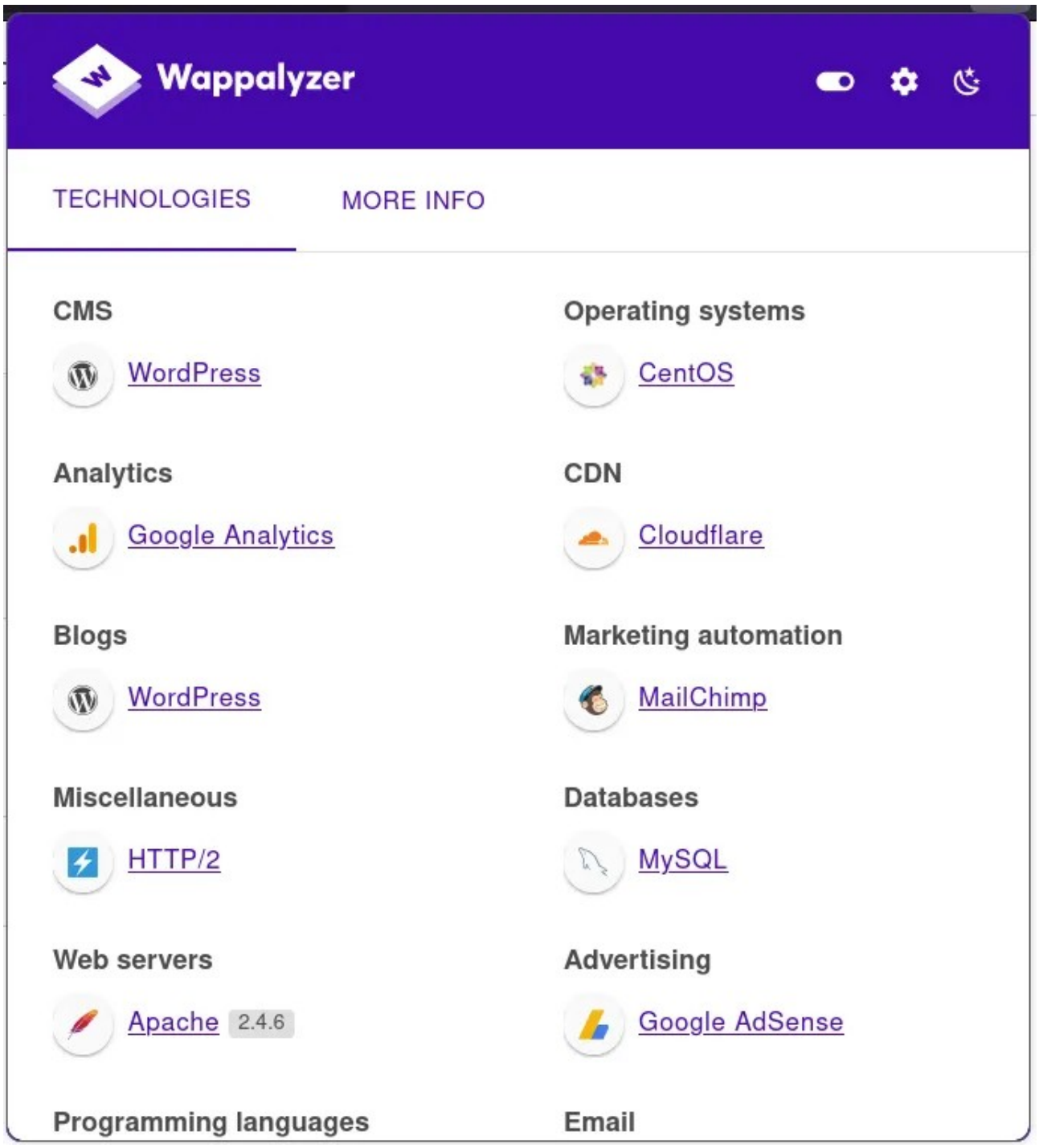
Developer Tools lets you inspect many things that your browser has received and exchanged with the remote server. For instance, you can view and even modify JavaScript (JS) files, inspect cookies set on your system and discover folder structure of the site content.

Plenty add-ons for Firefox and Chrome that can help in penetration testing. Here are a few examples:

FoxyProxy lets you quickly change the proxy server you are using to access the target website. convenient when using Burpsuite or if you need to switch proxy servers regularly.

User-Agent Switcher and Manager gives you the ability to pretend to be accessing the webpage from a different operating system or different web browser.

Wappalyzer provides insights about the technologies used on the visited websites.



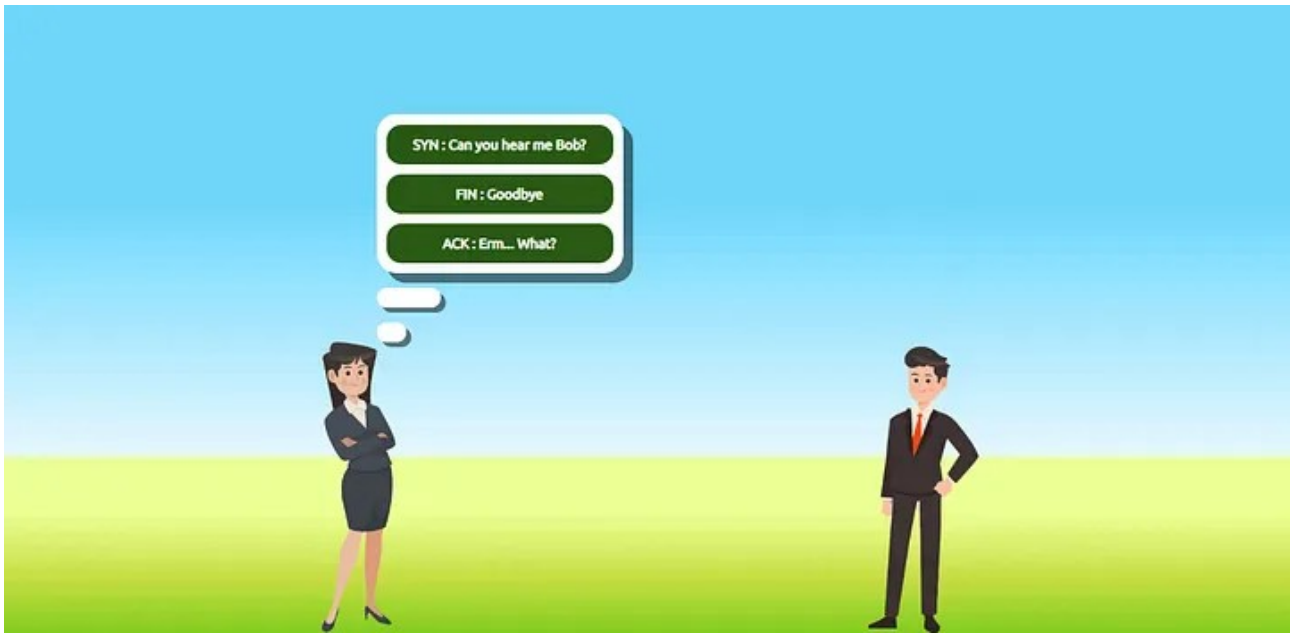
After reading the Lectures there is a questions that needed to answer.

The question is:

Browse to the following website and ensure that you have opened your Developer Tools on AttackBox Firefox, or the browser on your computer. Using the Developer Tools, figure out the total number of questions.

The **following website** from the question is clickable

It lead me to another website



Since the question requires me to use Developer Tools to figure out the total number of questions on the script.js

Our goal is to figure out the total number of questions.

Here are the steps:

1.First click the hyperlinked on following website and directs you to another page

2.The website involves Javascript so I pressed CTRL + SHIFT + I then the Developer Tools appears on the right side

3.Go to Sources and you'll see a hierarchy files you can easily locate the script.js (this tells on the hint)

4.The script.js has some following function codes.

```
let step = 1;
let questions = {
    1   :   {
        'speaking'  :  'alice',
        'answer_1'  :  'SYN : Can you hear me Bob?',
        'answer_2'  :  'FIN : Goodbye',
        'answer_3'  :  'ACK : Erm... What?',
        'answer'    :   1
    },
    2   :   {
        'speaking'  :  'bob',
        'answer_1'  :  'RST : Cya Later',
        'answer_2'  :  'PING : 77',
        'answer_3'  :  'SYN/ACK : Yes, I can hear you!',
        'answer'    :   3
    },
    3   :   {
        'speaking'  :  'alice',
        'answer_1'  :  'FAIL : SEGMENTATION FAULT',
        'answer_2'  :  'ACK : Okay Great',
        'answer_3'  :  'SYN : x = 3?',
        'answer'    :   2
    },
    4   :   {
        'speaking'  :  'alice',
        'answer_1'  :  'ICMP : 99',
        'answer_2'  :  'SYN : Yes, I can hear you!',
        'answer_3'  :  'DATA : Cheesecake is on sale!',
        'answer'    :   3
    },
    5   :   {
        'speaking'  :  'bob',
        'answer_1'  :  'ACK : I Hear ya!',
```

By counting the number of questions you'll just count the number of sequence questions. The number of questions is total of 8.

Task 3. Ping

One of the most common tools in troubleshooting in Networking is the ping. The ping simply just sends a packet message to the host machine sending ICMP echo request to know if the host is online, if the host receives an echo request it should also send a reply to that request telling you

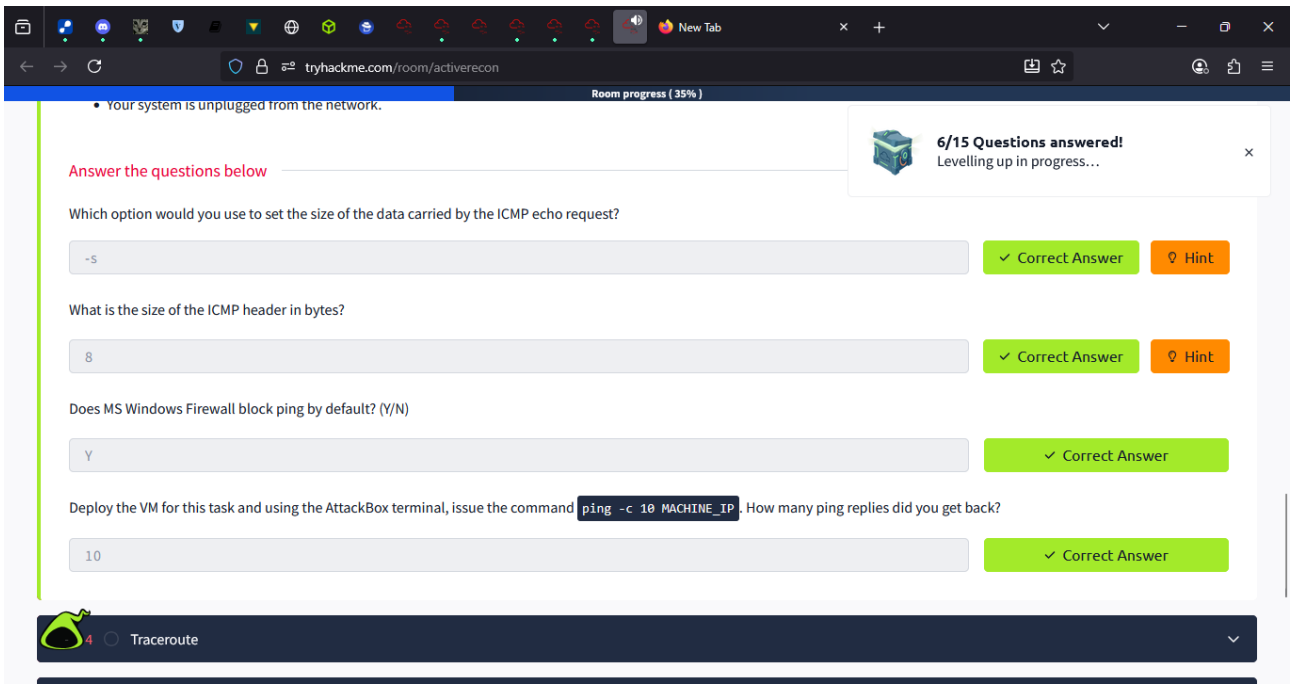
that the host is online. If the host doesn't receive your ping, it will display on your command prompt "**Requested Time out"** as it means that the host is unavailable.

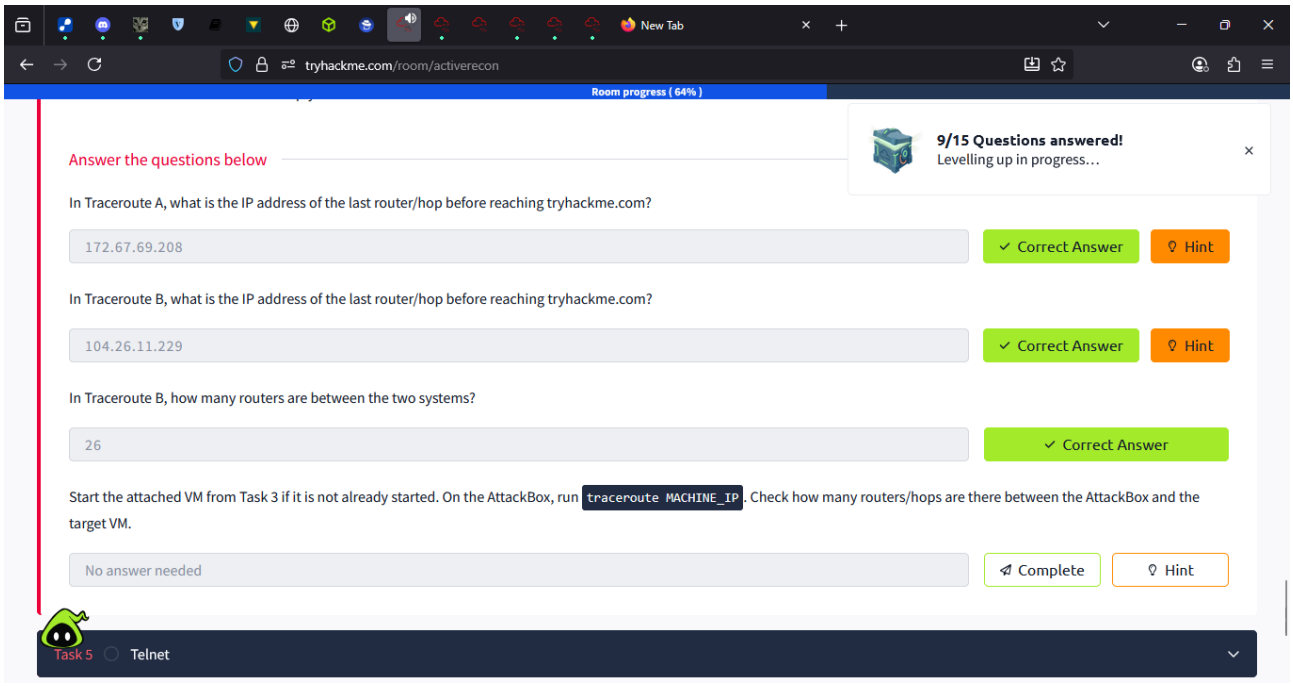
In this activity Tryhackme has some box that I can test with the ping. It requires me to connect to OpenVPN so I downloaded the config file and import it to my application.

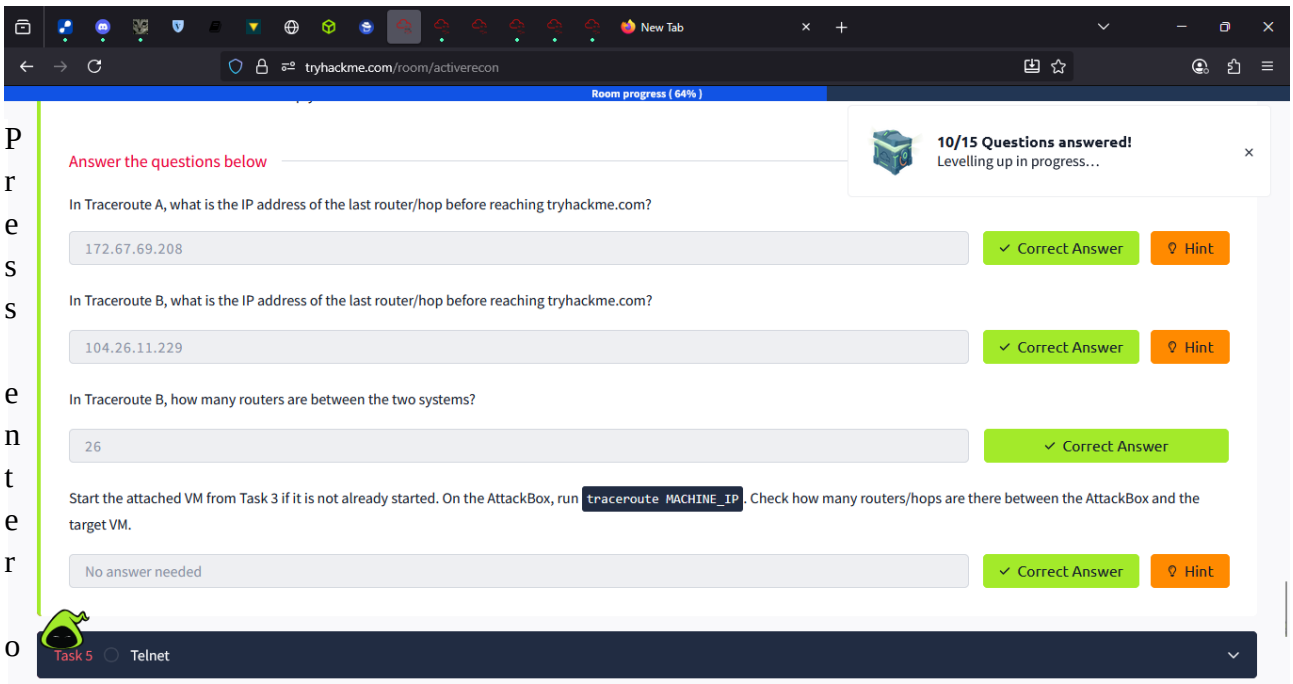
The IP Address of the machine shows up on the above the content.

What I need to try is to ping the IP address using ping and using some parameter -n (on Windows) and specify how many counts of ping.

```
Microsoft Windows [Version 10.0.22621.4037]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Anthony>ping 10.10.7.125

Pinging 10.10.7.125 with 32 bytes of data:
Reply from 10.10.7.125: bytes=32 time=358ms TTL=63
Reply from 10.10.7.125: bytes=32 time=351ms TTL=63
Reply from 10.10.7.125: bytes=32 time=352ms TTL=63
Reply from 10.10.7.125: bytes=32 time=350ms TTL=63

Ping statistics for 10.10.7.125:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 350ms, Maximum = 358ms, Average = 352ms

C:\Users\Anthony>ping -n 10 10.10.7.125

Pinging 10.10.7.125 with 32 bytes of data:
Reply from 10.10.7.125: bytes=32 time=254ms TTL=63
Reply from 10.10.7.125: bytes=32 time=343ms TTL=63
Reply from 10.10.7.125: bytes=32 time=342ms TTL=63
Reply from 10.10.7.125: bytes=32 time=341ms TTL=63
Reply from 10.10.7.125: bytes=32 time=253ms TTL=63
Reply from 10.10.7.125: bytes=32 time=338ms TTL=63
Reply from 10.10.7.125: bytes=32 time=262ms TTL=63
Reply from 10.10.7.125: bytes=32 time=301ms TTL=63
Reply from 10.10.7.125: bytes=32 time=446ms TTL=63
Reply from 10.10.7.125: bytes=32 time=373ms TTL=63
```


New Tab
tryhackme.com/room/activerecon
Room progress (35%)
• Your system is unplugged from the network.
6/15 Questions answered!
Levelling up in progress...
Answer the questions below
Which option would you use to set the size of the data carried by the ICMP echo request?
-s
✓ Correct Answer
Hint
What is the size of the ICMP header in bytes?
8
✓ Correct Answer
Hint
Does MS Windows Firewall block ping by default? (Y/N)
Y
✓ Correct Answer
Deploy the VM for this task and using the AttackBox terminal, issue the command ping -c 10 MACHINE_IP. How many ping replies did you get back?
10
✓ Correct Answer
4 Traceroute


New Tab
tryhackme.com/room/activerecon
Room progress (64%)
9/15 Questions answered!
Levelling up in progress...
Answer the questions below
In Traceroute A, what is the IP address of the last router/hop before reaching tryhackme.com?
172.67.69.208
✓ Correct Answer
Hint
In Traceroute B, what is the IP address of the last router/hop before reaching tryhackme.com?
104.26.11.229
✓ Correct Answer
Hint
In Traceroute B, how many routers are between the two systems?
26
✓ Correct Answer
Start the attached VM from Task 3 if it is not already started. On the AttackBox, run traceroute MACHINE_IP. Check how many routers/hops are there between the AttackBox and the target VM.
No answer needed
Complete
Hint
Task 5 Telnet



Please enter or click on the network icon to view Answer questions below

Task 4. Traceroute

As the name suggests, the traceroute command *traces the route* taken by the packets from your system to another host. The purpose of a traceroute is to find the IP addresses of the routers or hops that a packet traverses as it goes from your system to a target host.

Linux vs Windows command of Traceroute

Linux and macOS uses **traceroute <ip address>**

Windows uses **tracert <ip address>**

Answer questions below

In Traceroute A, what is the IP address of the last router/hop before reaching tryhackme.com?

```
12  120.28.9.254 (120.28.9.254)  7.724 ms  10.557 ms  9.159 ms
13  172.67.69.208 (172.67.69.208)  6.225 ms  5.657 ms  7.868 ms
```

Answer is 172.67.69.208

In Traceroute B, what is the IP address of the last router/hop before reaching tryhackme.com?

```
14  103.22.201.38 (103.22.201.38)  168.981 ms 103.22.201.27 (103.22.201.27)  226.802 ms 103
15  104.26.11.229 (104.26.11.229)  225.827 ms  225.272 ms  224.779 ms
```

Answer is 104.26.11.229

In Traceroute B, how many routers are between the two systems?

Answer is 26 hops to every routers

Task 5. Telnet

This protocol is used to connect to a remote host via command line interface (CLI). The port that it used is 23, though the client with its simplicity can be used for other purposes. Knowing that telnet client relies on the TCP protocol, you can use Telnet to connect to any service like Port 80.

The command to use is `telnet <ip address> <port number>`

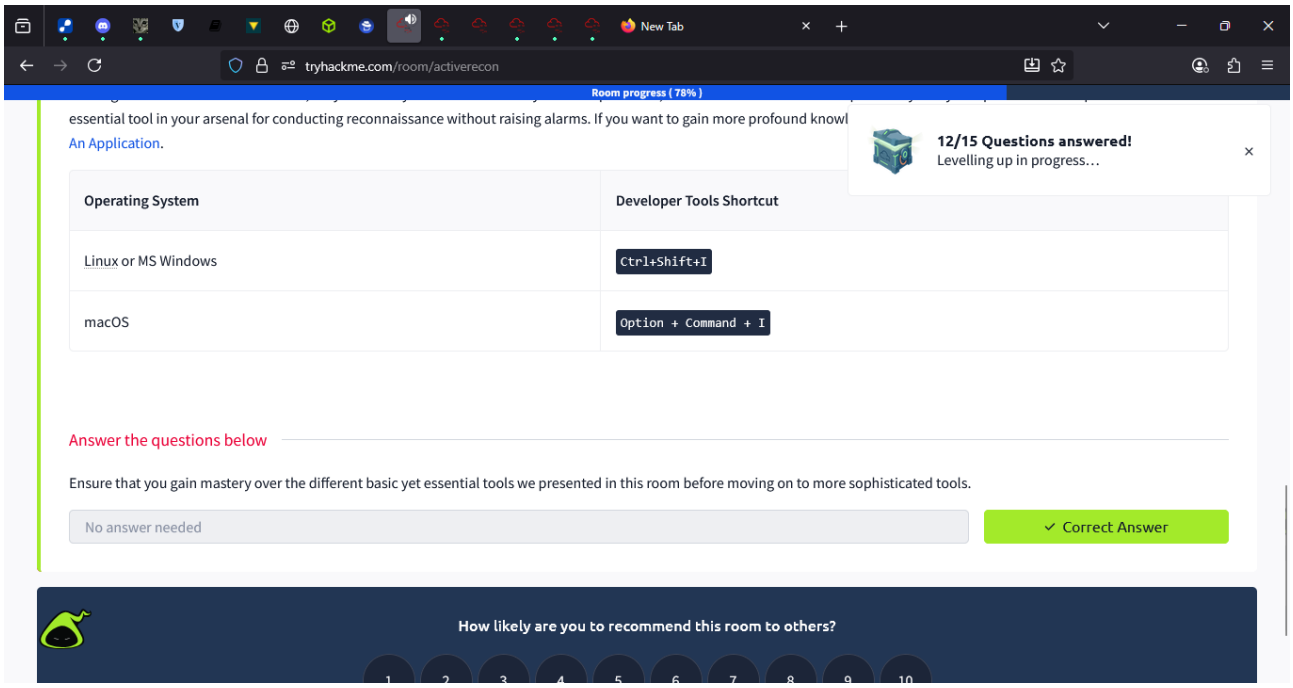
Answer questions below

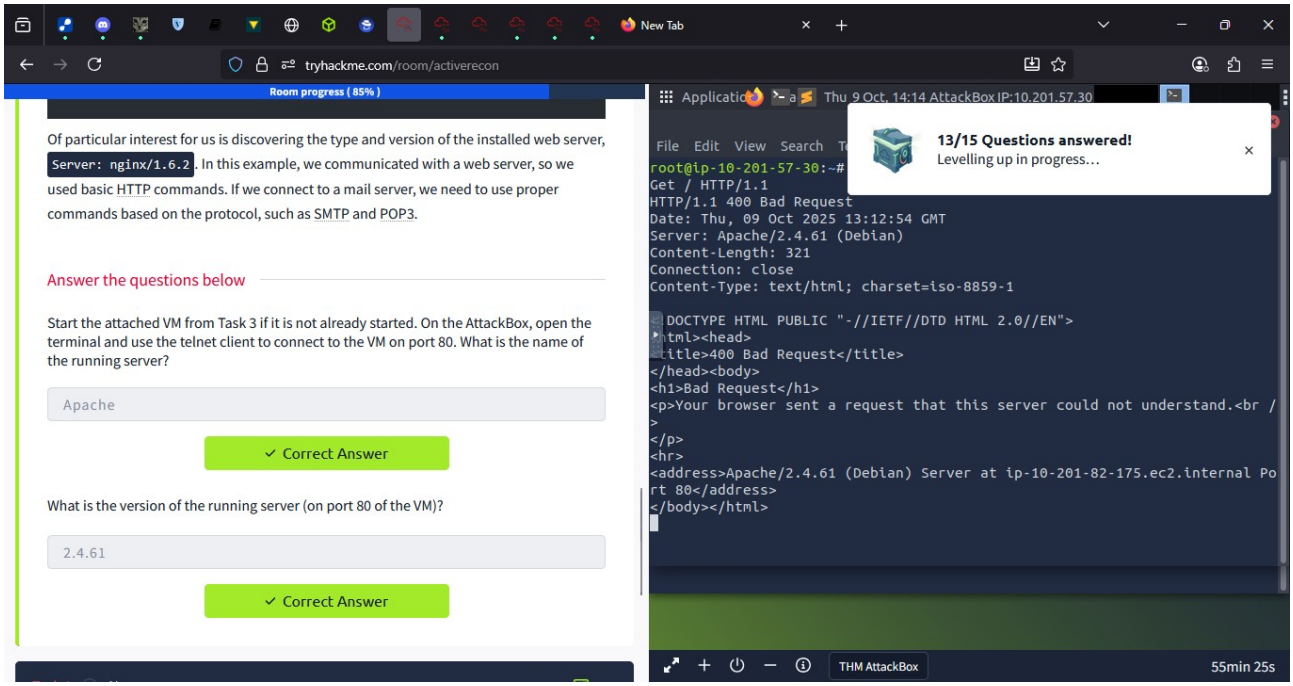
Start the attached VM from Task 3 if it is not already started. On the AttackBox, open the terminal and use the telnet client to connect to the VM on port 80. What is the name of the running server?

Answer is **Apache**

What is the version of the running server (on port 80 of the VM)?

Answer is **2.4.61**





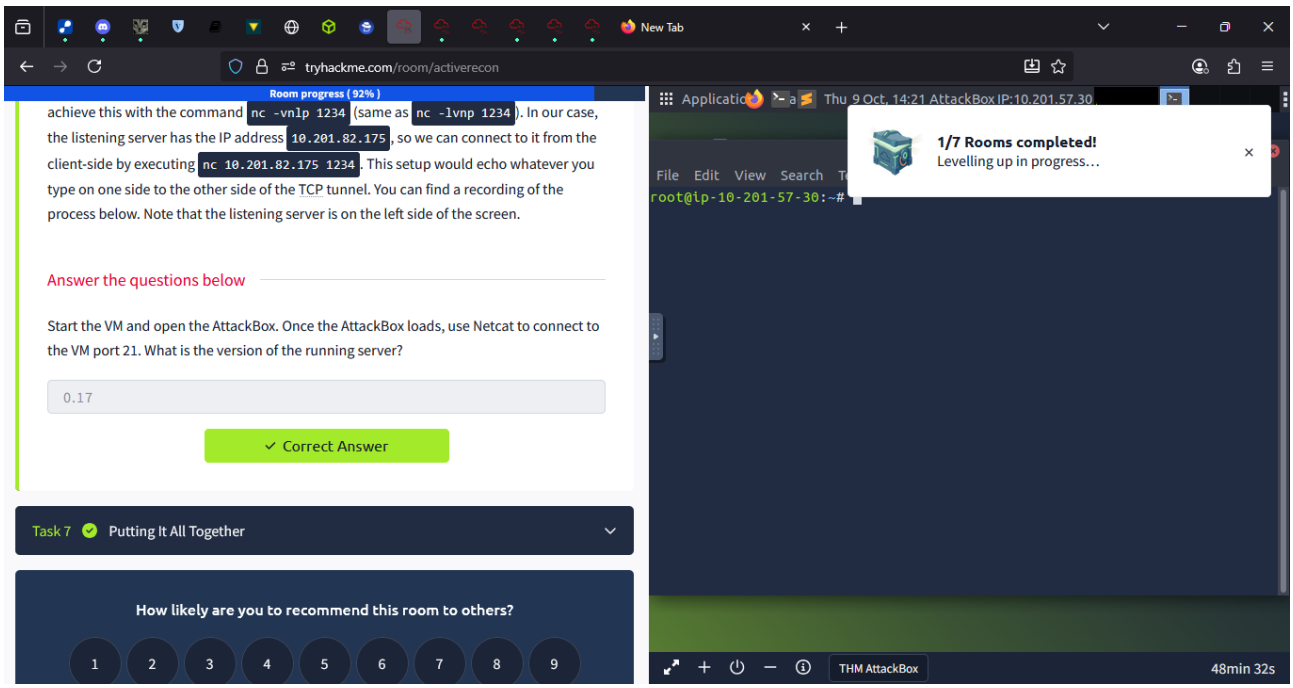
Task 6. Netcat

A different applications that can be of great value to a pentester. It supports TCP and UDP protocols. It can function as a client that connects to a listening port but also can act as server that listens on a port of your choice.

Answer the questions below

Start the VM and open the AttackBox. Once the AttackBox loads, use Netcat to connect to the VM port 21. What is the version of the running server?

The command is `nc <ip address> <port-number>`



Task 7 Putting it all together

This task is all about application of all the commands that I have learned from all the topics from Task 1–6. These are the tools that can be used to interact with the host machine:

Command	Example
ping	`ping -c 10 10.10.234.174` on Linux or macOS
ping	`ping -n 10 10.10.234.174` on MS Windows
traceroute	`traceroute 10.10.234.174` on Linux or macOS
tracert	`tracert 10.10.234.174` on MS Windows
telnet	`telnet 10.10.234.174 PORT_NUMBER`
netcat as client	`nc 10.10.234.174 PORT_NUMBER`
netcat as server	`nc -lvnp PORT_NUMBER`

Lessons Learned

This room highlighted the power of passive reconnaissance in gathering comprehensive target intelligence without triggering alarms. Public databases and search engines can expose a wealth of actionable information. The key is thorough documentation and cross-verification of data to build a solid target profile for subsequent phases.

Declaration

I declare that this work is my own and completed without unauthorized assistance.

Signature: Praveen Kumar

Date: 12-10-2025