cs-sa07-24019
John_Mbithi_Mutave

L2 MAC Flooding & ARP Spoofing

Task 1: Getting Started

Objectives:

- Understand the basics of Layer 2 (Data Link Layer) networking.
- Set up the AttackBox environment for practical exercises.

Key Takeaways:

- **Layer 2 Basics**: Covered fundamental concepts such as MAC addresses, Ethernet frames, and switch operations.
- **AttackBox Setup**: Prepared the virtual environment to simulate network attacks safely.

Task 2: Initial Access

Objectives:

- Learn methods to gain initial access to a network.
- Understand basic reconnaissance techniques.

Key Takeaways:

- **Network Enumeration**: Used tools like nmap for discovering hosts and services on the network.

Task 3: Network Discovery

Objectives:

- Further explore the network to identify potential targets for attacks.
- Understand network topology and device interconnections.

Key Takeaways:

- **Topology Mapping**: Used tools like arp-scan to discover devices and their IP-MAC mappings.

Task 4: Passive Network Sniffing

Objectives:

- Learn how to passively sniff network traffic.
- Understand the risks associated with unencrypted network protocols.

Key Takeaways:

- **Packet Capture**: Used tools like tcpdump to capture and analyze network traffic.

Task 5: Sniffing while MAC Flooding

Objectives:

- Implement MAC flooding to disrupt network operations.
- Learn to capture traffic during a MAC flooding attack.

Key Takeaways:

- **MAC Flooding**: Executed attacks using tools like macof to flood the switch's MAC address table, causing it to behave like a hub and forwarding traffic to all ports.
- **Traffic Capture**: Used tcpdump to capture and analyze the flooded network traffic.

Task 6-8: Man-in-the-Middle: ARP Spoofing

Objectives:

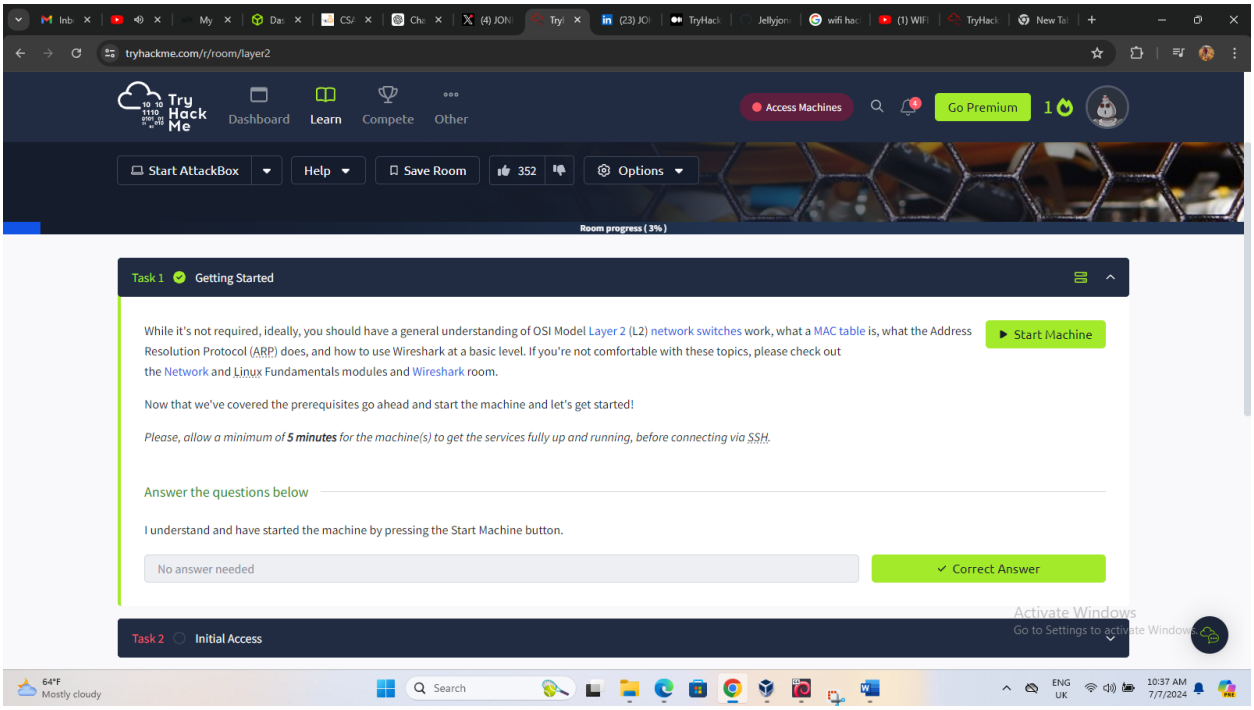
- Perform ARP cache poisoning to intercept and manipulate network traffic.
- Understand the principles and risks of man-in-the-middle (MITM) attacks.

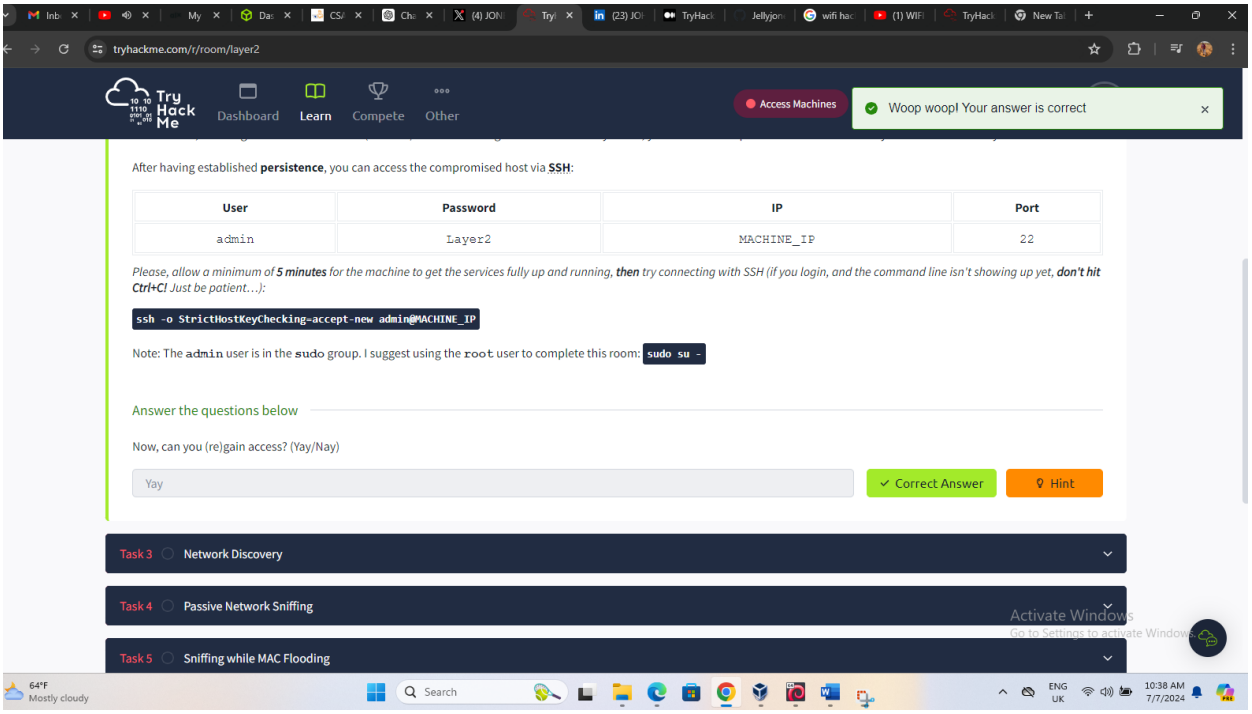
Key Takeaways:

- **ARP Spoofing**: Used tools like arpspoof to manipulate ARP tables, redirecting traffic through the attacker's machine.
- **MITM Techniques**: Intercepted and manipulated network packets to capture sensitive information or modify data in transit.

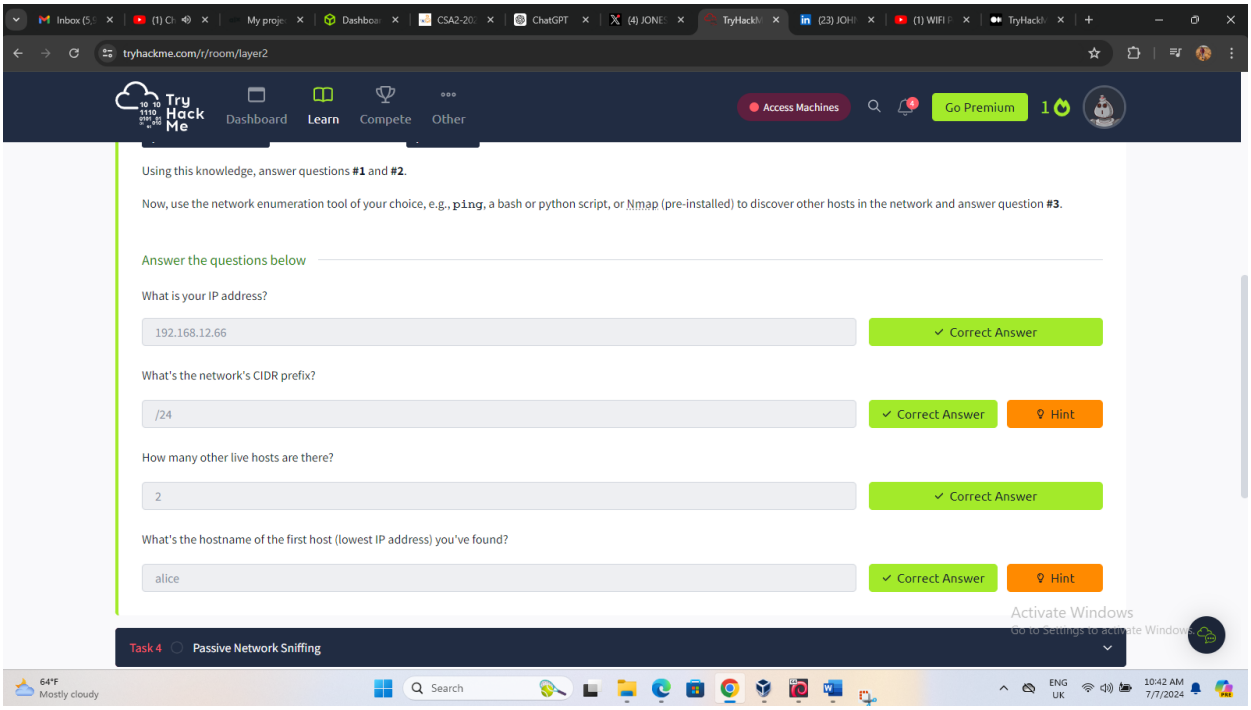
Screenshot Overview

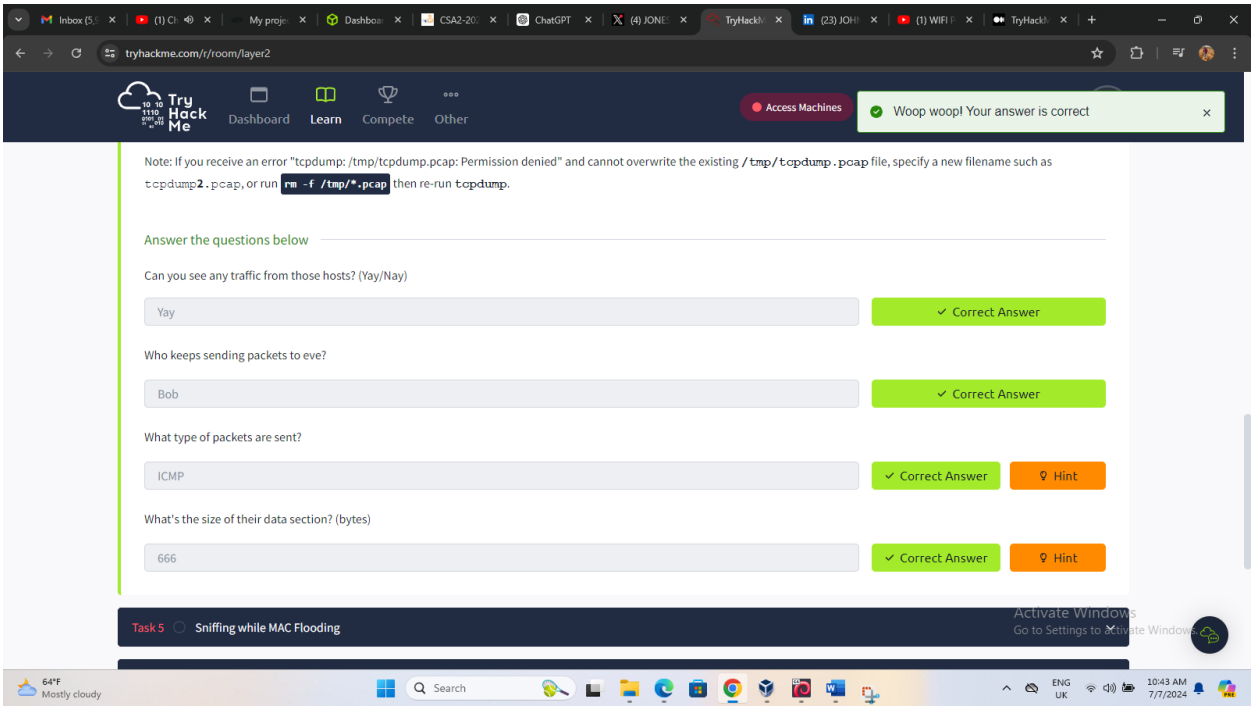
cs-sa07-24019
John_Mbithi_Mutave



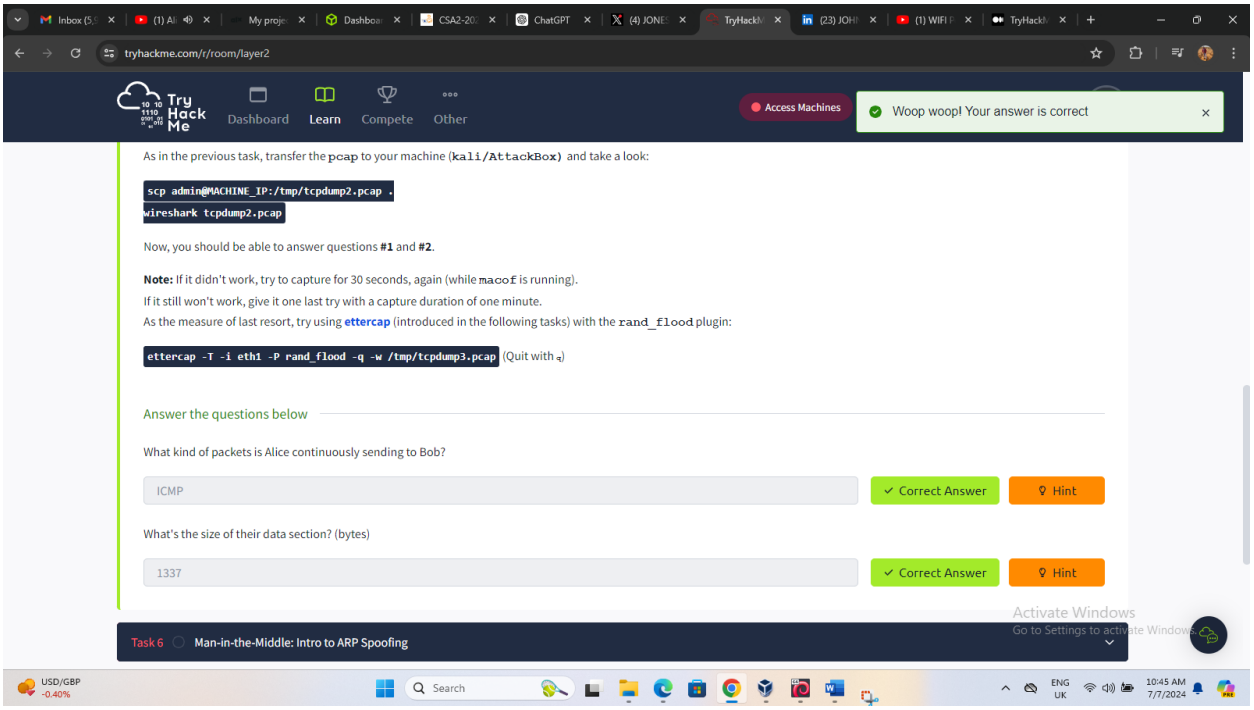


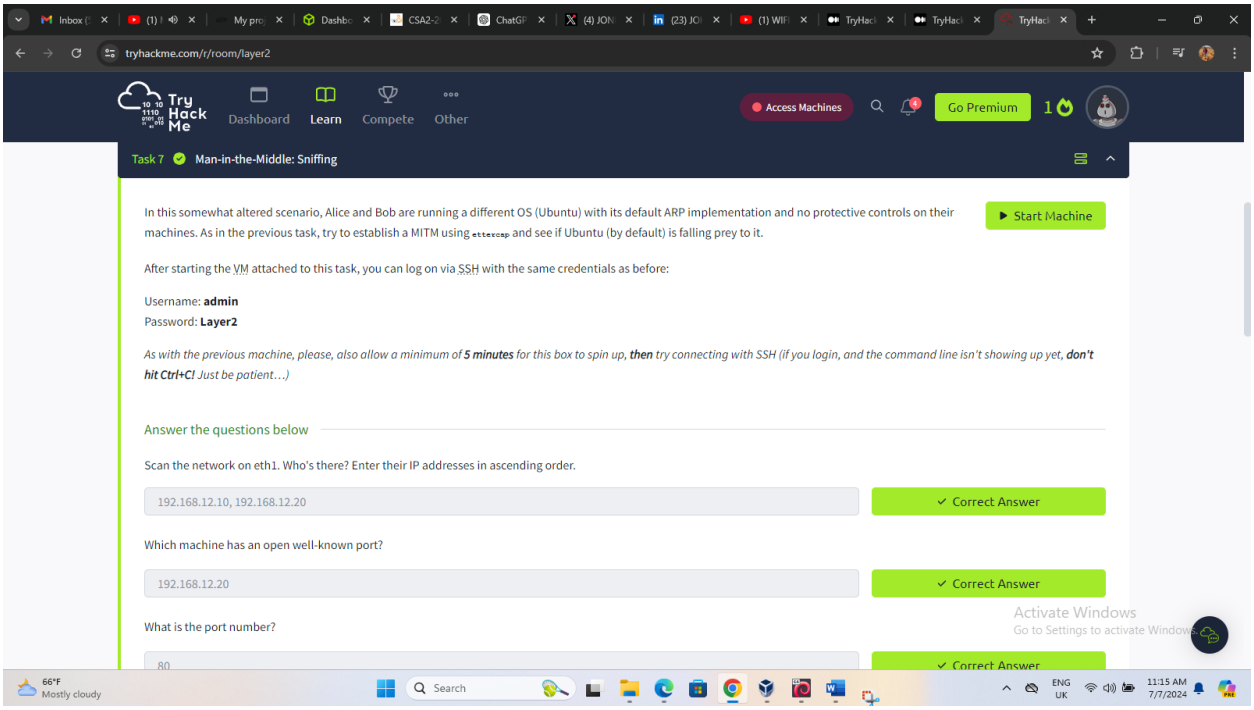
cs-sa07-24019
John_Mbithi_Mutave



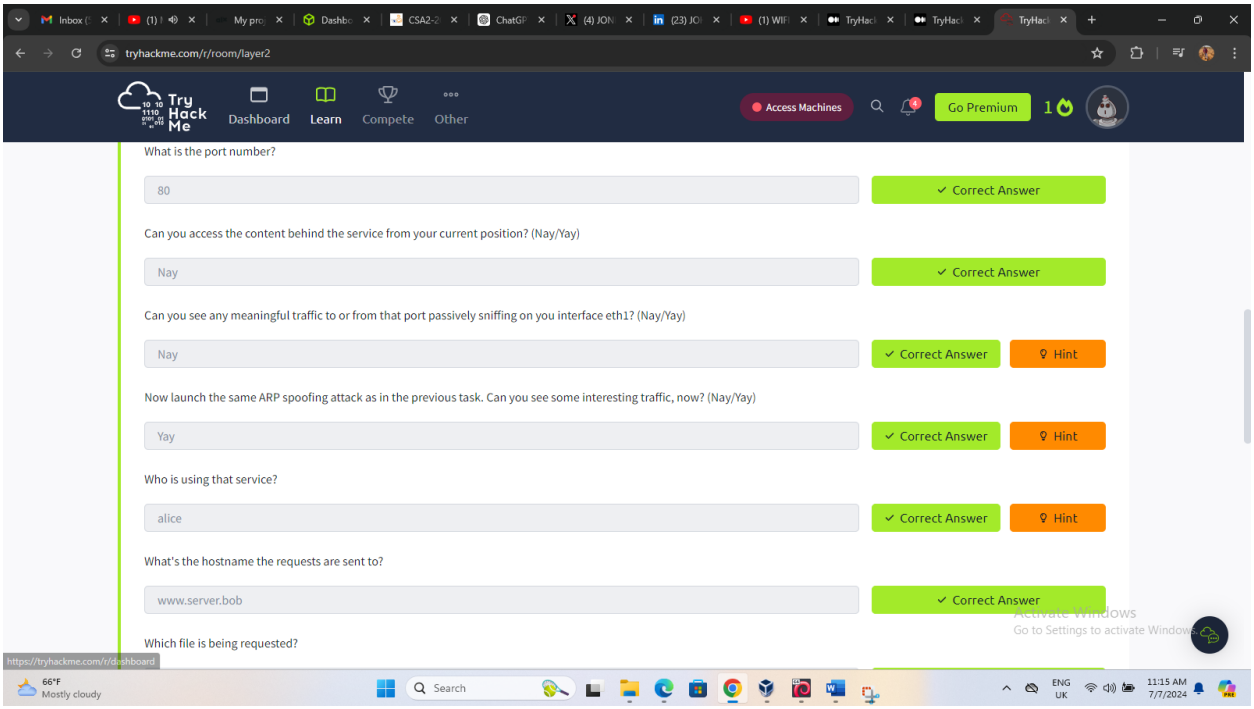


cs-sa07-24019
John_Mbithi_Mutave

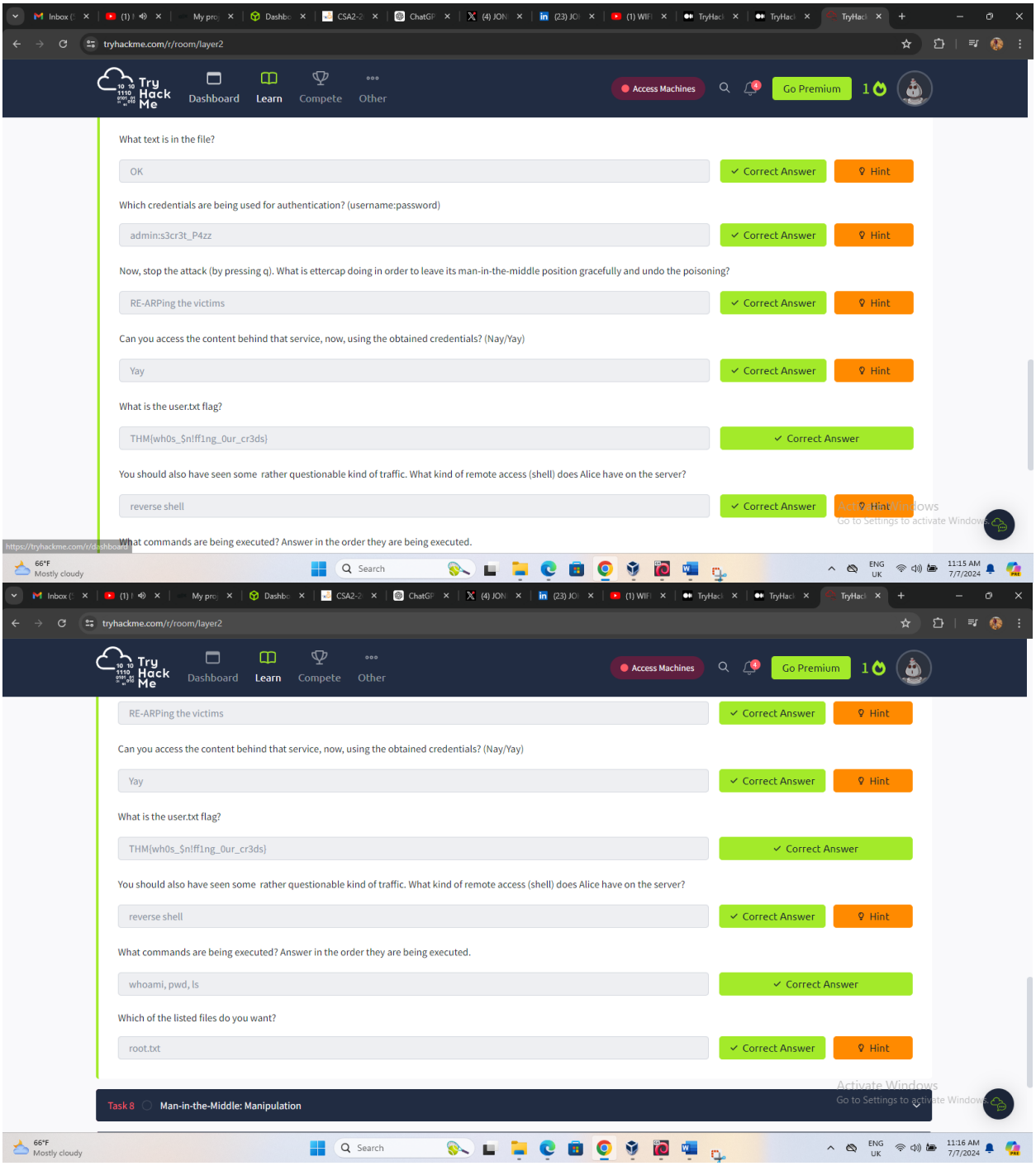




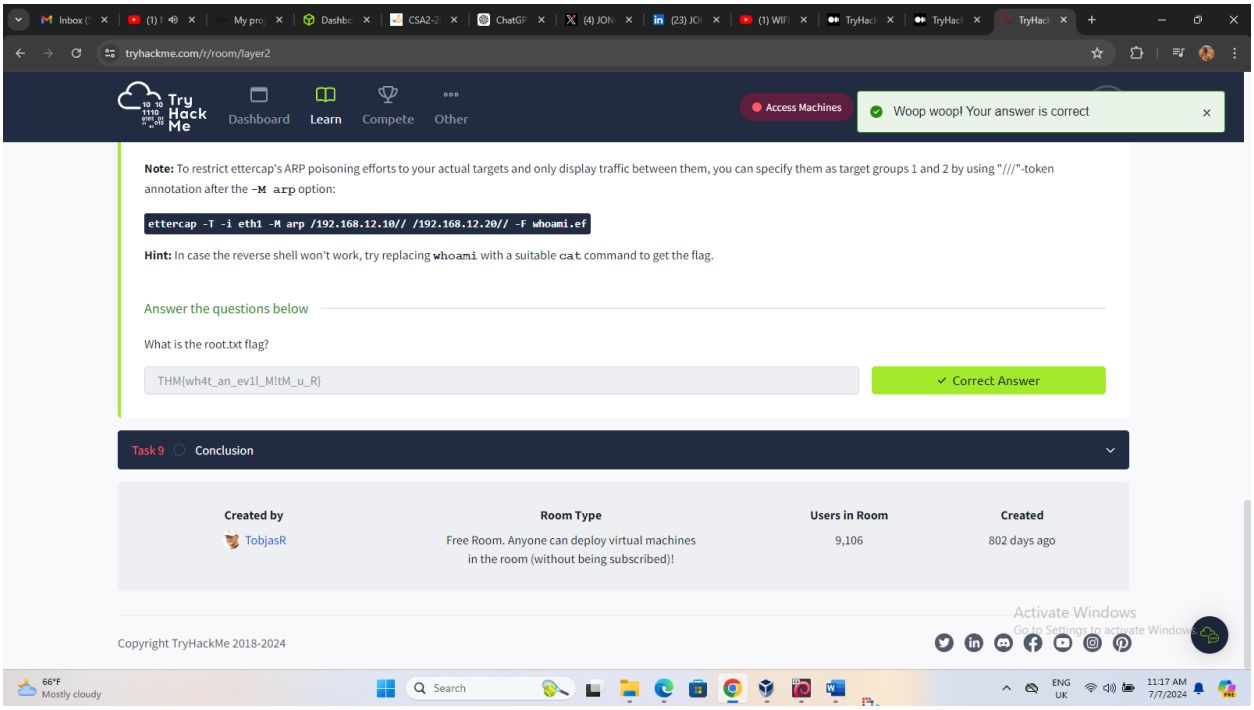
cs-sa07-24019
John_Mbithi_Mutave

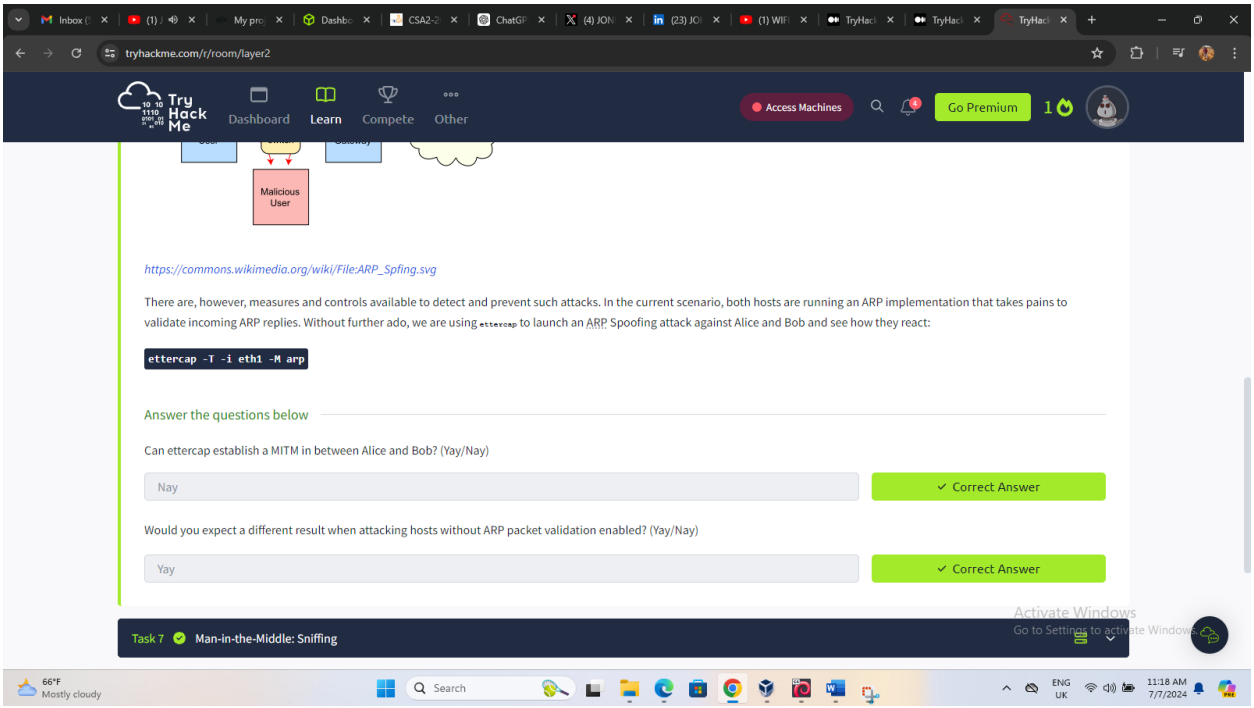


cs-sa07-24019
John_Mbithi_Mutave

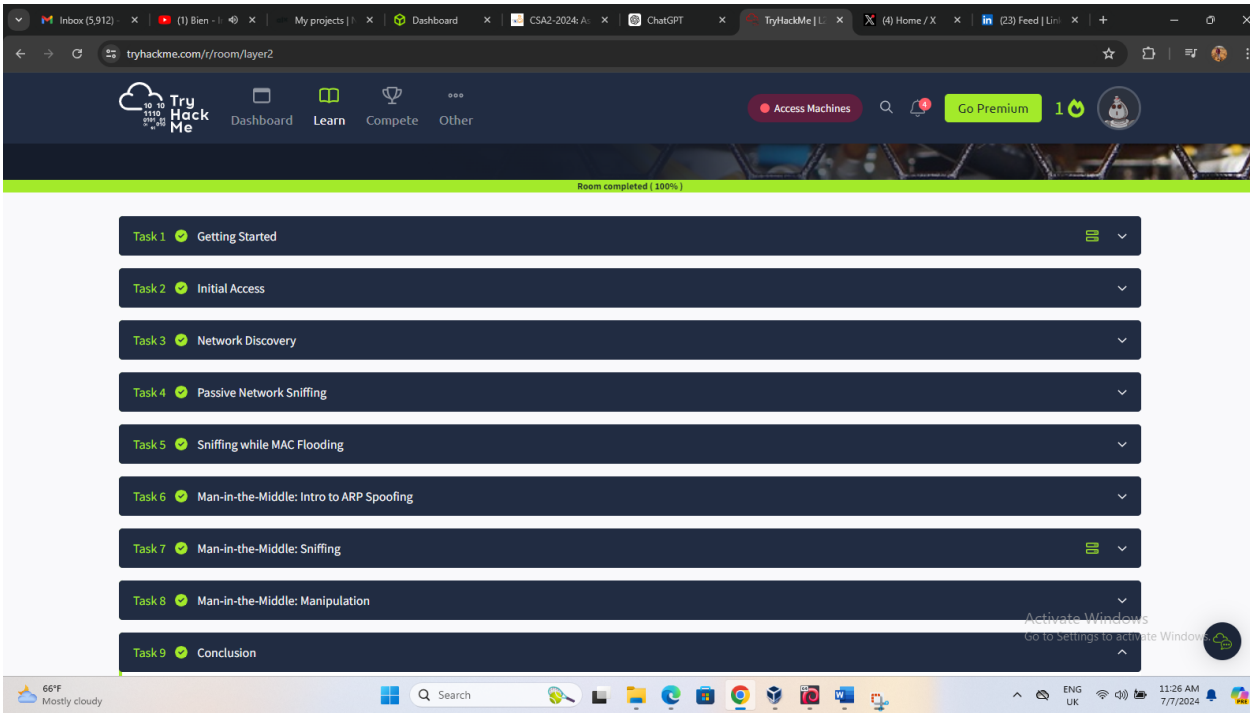


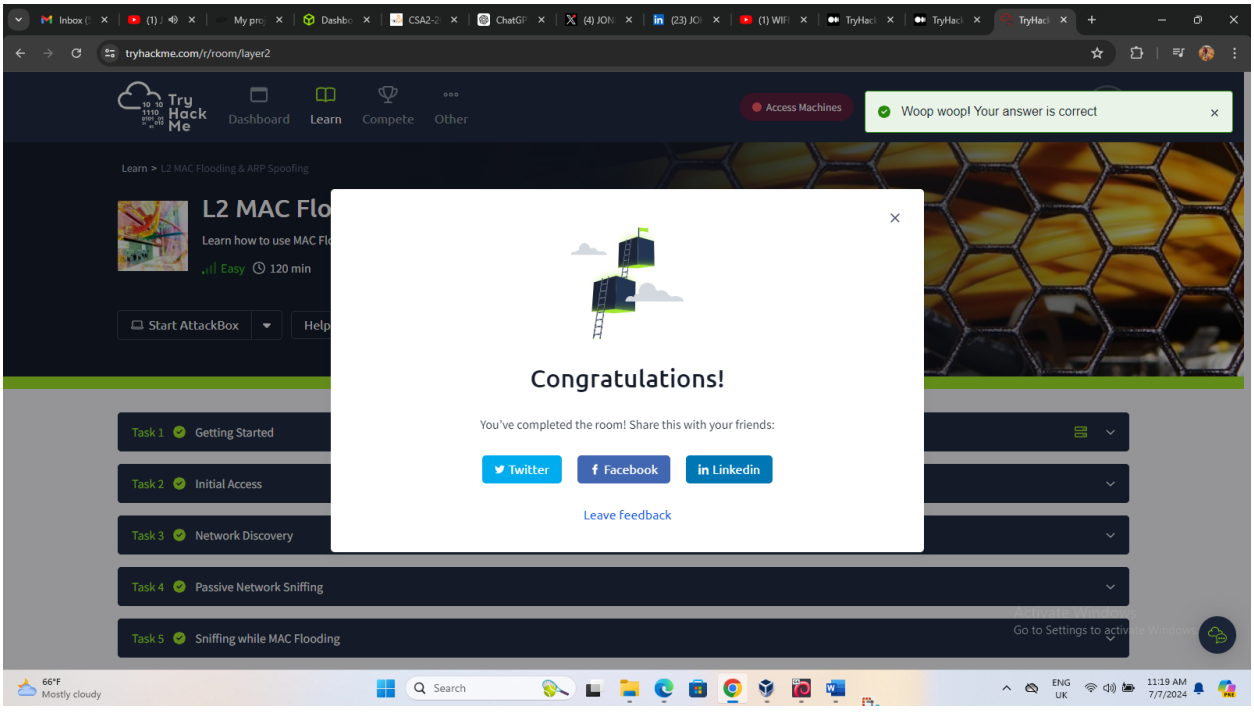
cs-sa07-24019
John_Mbithi_Mutave





cs-sa07-24019
John_Mbithi_Mutave





Shareable Link - https://tryhackme.com/r/room/layer2

Task 9: Conclusion

The L2 MAC Flooding & ARP Spoofing module provided practical insights into network manipulation techniques. By mastering these methods, I gain crucial skills in understanding and defending against such attacks.