

## 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

tryhackme.com/r/room/layer2

TryHackMe Dashboard Learn Compete Other Access Machines Go Premium 1

Start AttackBox Help Save Room 352 Options

Room progress (3%)

**Task 1** Getting Started

While it's not required, ideally, you should have a general understanding of OSI Model **Layer 2 (L2)** **network switches** work, what a **MAC table** is, what the **Address Resolution Protocol (ARP)** does, and how to use **Wireshark** at a basic level. If you're not comfortable with these topics, please check out the **Network** and **Linux** Fundamentals modules and **Wireshark** room.

Now that we've covered the prerequisites go ahead and start the machine and let's get started!

Please, allow a minimum of **5 minutes** for the machine(s) to get the services fully up and running, before connecting via **SSH**.

Answer the questions below

I understand and have started the machine by pressing the Start Machine button.

No answer needed

**Task 2** Initial Access

64°F Mostly cloudy

tryhackme.com/r/room/layer2

TryHackMe Dashboard Learn Compete Other Access Machines Woop woopl! Your answer is correct

After having established **persistence**, you can access the compromised host via **SSH**:

User	Password	IP	Port
admin	Layer2	MACHINE_IP	22

Please, allow a minimum of **5 minutes** for the machine to get the services fully up and running, **then** try connecting with **SSH** (if you login, and the command line isn't showing up yet, **don't hit Ctrl+C!** Just be patient...):

```
ssh -o StrictHostKeyChecking=accept-new admin@MACHINE_IP
```

Note: The **admin** user is in the **sudo** group. I suggest using the **root** user to complete this room: `sudo su -`

Answer the questions below

Now, can you (re)gain access? (Yay/Nay)

Yay

**Task 3** Network Discovery

**Task 4** Passive Network Sniffing

**Task 5** Sniffing while MAC Flooding

64°F Mostly cloudy

10:37 AM 7/7/2024

The screenshot shows the TryHackMe interface for room 'layer2'. The navigation bar includes 'Dashboard', 'Learn', 'Compete', and 'Other'. A 'Go Premium' button is visible. The main content area contains instructions and four questions:

- Using this knowledge, answer questions #1 and #2.
- Now, use the network enumeration tool of your choice, e.g., `ping`, a bash or python script, or `Nmap` (pre-installed) to discover other hosts in the network and answer question #3.

Answer the questions below

What is your IP address?  
 ✓ Correct Answer

What's the network's CIDR prefix?  
 ✓ Correct Answer 🔍 Hint

How many other live hosts are there?  
 ✓ Correct Answer

What's the hostname of the first host (lowest IP address) you've found?  
 ✓ Correct Answer 🔍 Hint

Task 4 ☐ Passive Network Sniffing

64°F Mostly cloudy 10:42 AM 7/7/2024

The screenshot shows the TryHackMe interface for room 'layer2'. A notification banner at the top says 'Woop woop! Your answer is correct'. The main content area contains a note and four questions:

Note: If you receive an error "`tcpdump: /tmp/tcpdump.pcap: Permission denied`" and cannot overwrite the existing `/tmp/tcpdump.pcap` file, specify a new filename such as `tcpdump2.pcap`, or run `rm -f /tmp/*.pcap` then re-run `tcpdump`.

Answer the questions below

Can you see any traffic from those hosts? (Yay/Nay)  
 ✓ Correct Answer

Who keeps sending packets to eve?  
 ✓ Correct Answer

What type of packets are sent?  
 ✓ Correct Answer 🔍 Hint

What's the size of their data section? (bytes)  
 ✓ Correct Answer 🔍 Hint

Task 5 ☐ Sniffing while MAC Flooding

64°F Mostly cloudy 10:43 AM 7/7/2024

cs-sa07-24019  
John\_Mbithi\_Mutave

tryhackme.com/r/room/layer2

TryHackMe

DashboardLearnCompeteOther

Access Machines

Woop woop! Your answer is correct

As in the previous task, transfer the `pcap` to your machine (`kali/AttackBox`) and take a look:

```
scp admin@MACHINE_IP:/tmp/tcpdump2.pcap .
wireshark tcpdump2.pcap
```

Now, you should be able to answer questions #1 and #2.

**Note:** If it didn't work, try to capture for 30 seconds, again (while `macof` is running).  
If it still won't work, give it one last try with a capture duration of one minute.

As the measure of last resort, try using `ettercap` (introduced in the following tasks) with the `rand_flood` plugin:

```
ettercap -T -i eth1 -P rand_flood -q -w /tmp/tcpdump3.pcap (Quit with a)
```

Answer the questions below

What kind of packets is Alice continuously sending to Bob?

ICMP

✓ Correct Answer

Hint

What's the size of their data section? (bytes)

1337

✓ Correct Answer

Hint

Task 6

Man-in-the-Middle: Intro to ARP Spoofing

Activate Windows  
Go to Settings to activate Windows.

USD/GBP  
-0.40%

Search

ENG  
UK

10:45 AM  
7/7/2024

tryhackme.com/r/room/layer2

TryHackMe

DashboardLearnCompeteOther

Access Machines

Go Premium

1

**Task 7** Man-in-the-Middle: Sniffing

In this somewhat altered scenario, Alice and Bob are running a different OS (Ubuntu) with its default ARP implementation and no protective controls on their machines. As in the previous task, try to establish a MITM using `ettercap` and see if Ubuntu (by default) is falling prey to it.

After starting the VM attached to this task, you can log on via SSH with the same credentials as before:

Username: `admin`  
Password: `Layer2`

As with the previous machine, please, also allow a minimum of **5 minutes** for this box to spin up, then try connecting with SSH (if you login, and the command line isn't showing up yet, **don't hit Ctrl+C!** Just be patient...)

Answer the questions below

Scan the network on `eth1`. Who's there? Enter their IP addresses in ascending order.

192.168.12.10, 192.168.12.20

✓ Correct Answer

Which machine has an open well-known port?

192.168.12.20

✓ Correct Answer

What is the port number?

80

✓ Correct Answer

Task 7

Man-in-the-Middle: Sniffing

Start Machine

Activate Windows  
Go to Settings to activate Windows.

66°F  
Mostly cloudy

Search

ENG  
UK

11:15 AM  
7/7/2024

cs-sa07-24019  
John\_Mbithi\_Mutave

The screenshot shows a web browser window with the URL `tryhackme.com/r/room/layer2`. The browser's address bar and tabs are visible at the top. The TryHackMe interface has a dark blue header with navigation links: **Dashboard**, **Learn**, **Compete**, and **Other**. On the right side of the header, there are buttons for **Access Machines**, **Go Premium**, and a user profile icon.

The main content area displays a list of questions and answers:

- Question: "What is the port number?"  
Answer: `80`  
Status: **✓ Correct Answer**
- Question: "Can you access the content behind the service from your current position? (Nay/Yay)"  
Answer: `Nay`  
Status: **✓ Correct Answer**
- Question: "Can you see any meaningful traffic to or from that port passively sniffing on you interface eth1? (Nay/Yay)"  
Answer: `Nay`  
Status: **✓ Correct Answer** (with a **Hint** button)
- Question: "Now launch the same ARP spoofing attack as in the previous task. Can you see some interesting traffic, now? (Nay/Yay)"  
Answer: `Yay`  
Status: **✓ Correct Answer** (with a **Hint** button)
- Question: "Who is using that service?"  
Answer: `alice`  
Status: **✓ Correct Answer** (with a **Hint** button)
- Question: "What's the hostname the requests are sent to?"  
Answer: `www.server.bob`  
Status: **✓ Correct Answer**
- Question: "Which file is being requested?"  
Answer: (empty input field)

At the bottom of the browser window, the Windows taskbar is visible, showing the system clock as 11:15 AM on 7/7/2024, and the weather as 66°F Mostly cloudy. An "Activate Windows" watermark is also present in the bottom right corner of the screen.

The screenshot displays the TryHackMe web application interface. The top navigation bar includes links for Dashboard, Learn, Compete, and Other, along with buttons for Access Machines, Go Premium, and a user profile icon. The main content area shows a list of questions and answers for a room titled 'layer2'. The questions are as follows:

- What text is in the file?  
Answer: OK
- Which credentials are being used for authentication? (username:password)  
Answer: admin:s3cr3t\_P4zz
- Now, stop the attack (by pressing q). What is ettercap doing in order to leave its man-in-the-middle position gracefully and undo the poisoning?  
Answer: RE-ARPing the victims
- Can you access the content behind that service, now, using the obtained credentials? (Nay/Yay)  
Answer: Yay
- What is the user.txt flag?  
Answer: THM{wh0s\_\$n1ff1ng\_0ur\_cr3ds}
- You should also have seen some rather questionable kind of traffic. What kind of remote access (shell) does Alice have on the server?  
Answer: reverse shell
- What commands are being executed? Answer in the order they are being executed.  
Answer: RE-ARPing the victims
- Can you access the content behind that service, now, using the obtained credentials? (Nay/Yay)  
Answer: Yay
- What is the user.txt flag?  
Answer: THM{wh0s\_\$n1ff1ng\_0ur\_cr3ds}
- You should also have seen some rather questionable kind of traffic. What kind of remote access (shell) does Alice have on the server?  
Answer: reverse shell
- What commands are being executed? Answer in the order they are being executed.  
Answer: whoami, pwd, ls
- Which of the listed files do you want?  
Answer: root.txt

The bottom of the interface shows a task bar with the title 'Task 8 Man-in-the-Middle: Manipulation' and a Windows taskbar at the very bottom with the date 7/7/2024.

tryhackme.com/r/room/layer2

TryHackMe

DashboardLearnCompeteOther

Access Machines

Woop woop! Your answer is correct

**Note:** To restrict ettercap's ARP poisoning efforts to your actual targets and only display traffic between them, you can specify them as target groups 1 and 2 by using "////"-token annotation after the `-M arp` option:

```
ettercap -T -i eth1 -M arp //192.168.12.10// //192.168.12.20// -F whoami.ef
```

**Hint:** In case the reverse shell won't work, try replacing `whoami` with a suitable `cat` command to get the flag.

Answer the questions below

What is the root.txt flag?

THM{wh4t\_an\_ev1l\_M1tm\_u\_R}

✓ Correct Answer

Task 9

Conclusion

Created by	Room Type	Users in Room	Created
TobiasR	Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)	9,106	802 days ago

Copyright TryHackMe 2018-2024

Activate Windows  
Go to Settings to activate Windows.

66°F Mostly cloudy

Search

ENG UK 11:17 AM 7/7/2024

tryhackme.com/r/room/layer2

TryHackMe

DashboardLearnCompeteOther

Access Machines

Go Premium

1

[https://commons.wikimedia.org/wiki/File:ARP\\_Spfig.svg](https://commons.wikimedia.org/wiki/File:ARP_Spfig.svg)

There are, however, measures and controls available to detect and prevent such attacks. In the current scenario, both hosts are running an ARP implementation that takes pains to validate incoming ARP replies. Without further ado, we are using `ettercap` to launch an ARP Spoofing attack against Alice and Bob and see how they react:

```
ettercap -T -i eth1 -M arp
```

Answer the questions below

Can ettercap establish a MITM in between Alice and Bob? (Yay/Nay)

Nay

✓ Correct Answer

Would you expect a different result when attacking hosts without ARP packet validation enabled? (Yay/Nay)

Yay

✓ Correct Answer

Task 7

Man-in-the-Middle: Sniffing

66°F Mostly cloudy

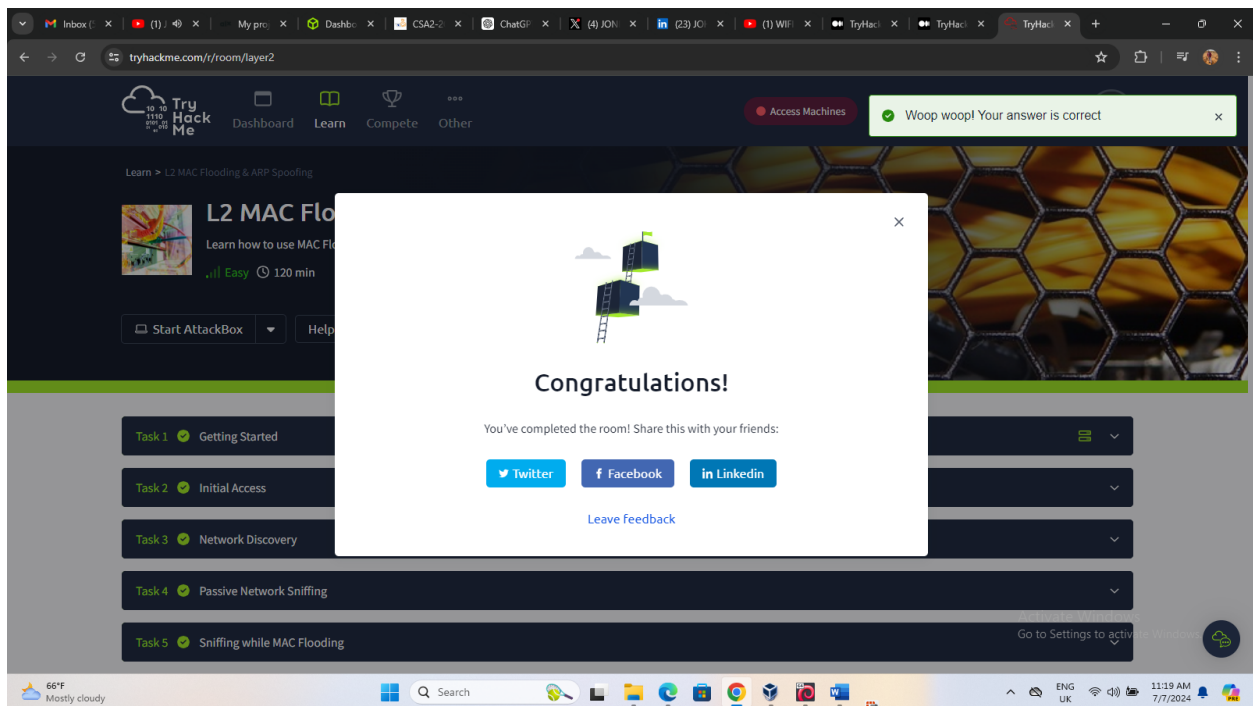
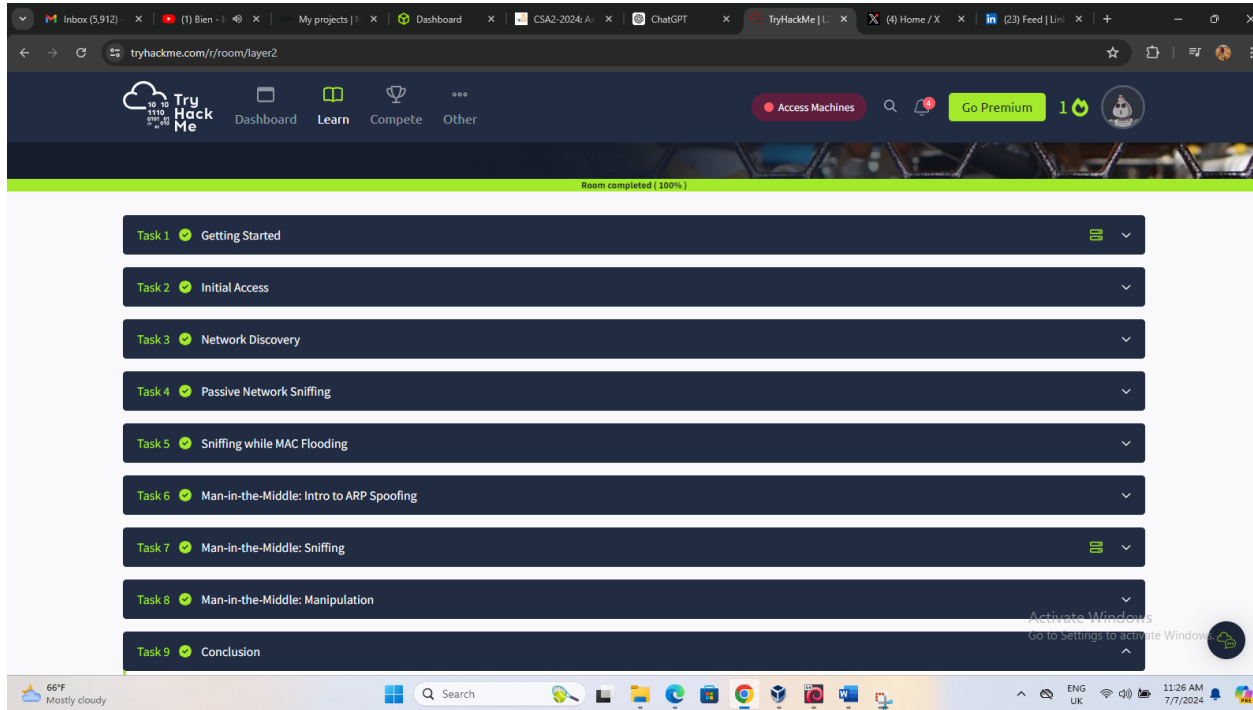
Search

ENG UK 11:18 AM 7/7/2024



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.