Ex. No. 10 **L2 MAC Flooding & ARP Spoofing**

Date: 13-10-2025

Aim:

To perform and analyze L2 MAC Flooding and ARP Spoofing attacks in the TryHackMe platform to understand their impact on network security.

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.*

Task 2 **Initial Access**

For the sake of this room, let's assume the following:

While conducting a pentest, you have gained initial access to a network and escalated privileges to root on a Linux machine. During your routine OS enumeration, you realize it's a dual-homed host, meaning it is connected to two (or more) networks. Being the curious hacker you are, you decided to explore this network to see if you can move laterally.

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 -

Task 3 **Network Discovery**

As mentioned previously, the host is connected to one or more additional networks. You are currently connected to the machine via SSH on Ethernet adapter **eth0**. The network of interest is connected with Ethernet adapter **eth1**.

First, have a look at the adapter:

ip address show eth1 or the shorthand version: ip a s eth1

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?

192.168.12.66

What's the network's CIDR prefix?

/24

How many other live hosts are there?

2

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

alice

Task 4 **Passive Network Sniffing**

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

Yay

Who keeps sending packets to eve?

Bob

What type of packets are sent?

ICMP

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

666

Task 5 Sniffing while MAC Flooding

What kind of packets is Alice continuously sending to Bob?

ICMP

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

1337

Task 6 Man-in-the-Middle: Intro to ARP Spoofing

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

Nay

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

Yay

Task 7 Man-in-the-Middle: Sniffing

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

192.168.12.10, 192.168.12.20

Which machine has an open well-known port?

192.168.12.20

What is the port number?

80

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

Nay

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

Nay

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

Yay

Who is using that service?

alice

What's the hostname the requests are sent to?

www.server.bob

Which file is being requested?

test.txt

What text is in the file?

OK

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

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?

RE-ARPing the victims

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

Yay

What is the user.txt flag?

THM{wh0s_$n!ff1ng_0ur_cr3ds}

Task 8 **Man-in-the-Middle: Manipulation**

What is the root.txt flag?

THM{wh4t_an_ev1l_M!tM_u_R}

Task 9 **Conclusion**

I hope this room offered a new perspective for network pentesting and gave you a new *layer* of attacks for your toolbelt, and hopefully, you've had some fun along the way, too!

It was also meant as an inspiration for the community to create more L2 content and learning resources, so feel free to take a look at Eve's L2 virtualization "backend" (GNS3): http://MACHINE_IP:3080

Please, don't hesitate to provide me any feedback or questions on implementing GNS3 boxes, and stay tuned for some more L2 action!

Result:

Successfully executed MAC Flooding and ARP Spoofing attacks and observed network traffic interception and disruption.