LAB 2 REPORT

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ARP Cache Poisoning

Spring 2025

|  | **Name** | **ID** |
| --- | --- | --- |
| **Student 1** | Rania Kanaan | 769007321 |
| **Student 2** | Fatima Mansur Rabiu | 776006447 |
| **Student 3** | Suhaila Alfalasi | 764005288 |
| **Student 4** | Syed Shayan Ali | 393003651 |

Rubrics:

1. Report is organized properly with suitable objectives and structure. The organization of the report should be as follows: (/10%).
   1. Cover page which contains Lab general information, Group information, and Rubrics.
   2. Objectives and goals of this lab
   3. Steps of carrying out the attack with detailed discussion, and observation.
   4. Problems you have faced in this lab.
   5. All mitigation techniques with explanations of their pros and cons.
   6. Conclusion, and references. Full citation of each statement that does not describe your own work is very important.
2. The report provides all the figures and screenshots that demonstrate the steps of the attack according to the objectives and goals of this lab explained above. (/40%)
3. The report illustrates the solutions of the issues faced and the troubleshooting steps taken (/10%).
4. The report clearly specify the mitigation steps that have been carried out to prevent the attack. (/25%).
5. The report explains the tests that were carried to verify the attack is successful and after carrying out the mitigation it is prevented. (/15%)

# TABLE OF CONTENTS

**Fill in the page numbers**

1. Objectives …………………………………………………………………………………...……………5
2. Topology & Architecture …………………………………………………………………………….. 6
3. Software/Tools Used ………………………………………………………………………………… 7
4. Initial Configurations ……………………………………………………………………………….. 8
   1. Network Configurations
5. ARP Cache Poisoning Attack Description ……………………………………………………. 12
6. Steps of Attack …………………………………………………………………………………………. 13
   1. Basic Steps
   2. Attack Implementation
7. Problems/Issues Faced …………………………………………………………………………….. 24
8. Mitigation Techniques ……………………………………………………………………………... 25
   1. Dynamic ARP Inspection
   2. Rate Limit

1. Conclusion ………………………………………………………………………………………………. 35
2. References ………………………………………………………………………………………….…… 36

# 

# TABLE OF FIGURES & TABLES

# Fill in the figure and table with titles and page numbers

| **Figure #** | **Title** | **Page #** |
| --- | --- | --- |
| Figure 1 | Topology Diagram | Page 6 |
| Figure 2 | Assigning IP address on the interface Gig0/2 | Page 9 |
| Figure 3 | Assigning IP address on the interface Gig0/1 | Page 9 |
| Figure 4 | Attacker PC ipconfig | Page 10 |
| Figure 5 | Server PC ipconfig | Page 10 |
| Figure 6 | Client PC ipconfig | Page 11 |
| Figure 7 | Receiving the ICMP packets on WireShark | Page 13 |
| Figure 8 | Pinging Successfully | Page 14 |
| Figure 9 | Client PC pinging | Page 14 |
| Figure 10 | arp -a command on Client PC | Page 15 |
| Figure 11 | Starting the Attack on Kali machine | Page 16 |
| Figure 12 | Starting the Attack on Kali machine | Page 17 |
| Figure 13 | Ipconfig on the client machine | Page 18 |
| Figure 14 | Pinging on the client machine | Page 18 |
| Figure 15 | Receiving the FTP packets on WireShark | Page 19 |
| Figure 16 | Opening Ettercap | Page 20 |
| Figure 17 | Specifying Interface on Ettercap | Page 20 |
| Figure 18 | hosts added to the host lists | Page 21 |
| Figure 19 | TARGET 1 and TARGET 2 has been added | Page 21 |
| Figure 20 | FTP capture in wireshark | Page 22 |
| Figure 21 | FTP Wireshark anaylsis | Page 23 |
| Figure 22 | The MAC address changed to the attacker MAC address | Page 23 |
| Figure 23 | Switch 1 ACL | Page 26 |
| Figure 24 | Switch 2 ACL | Page 27 |
| Figure 25 | Show access lists in Switch 2 | Page 27 |
| Figure 26 | Show access lists in Switch 1 | Page 27 |
| Figure 27 | show ip arp inspection vlan 1 switch 1 | Page 28 |
| Figure 28 | show ip arp inspection vlan 1 switch 2 | Page 29 |
| Figure 29 | ip arp inspection trust switch 1 | Page 30 |
| Figure 30 | ip arp inspection trust switch 2 | Page 30 |
| Figure 31 | show ip arp inspection interfaces | Page 31 |
| Figure 32 | Attack verification | Page 32 |
| Figure 33 | ip arp inspection log-buffer entries 1 | Page 33 |
| Figure 34 | show ip arp inspection log | Page 33 |

| **Table #** | **Title** | **Page** |
| --- | --- | --- |
| Table 1 | IP address & MAC address of Network Devices | Page 8 |

# 

# OBJECTIVES

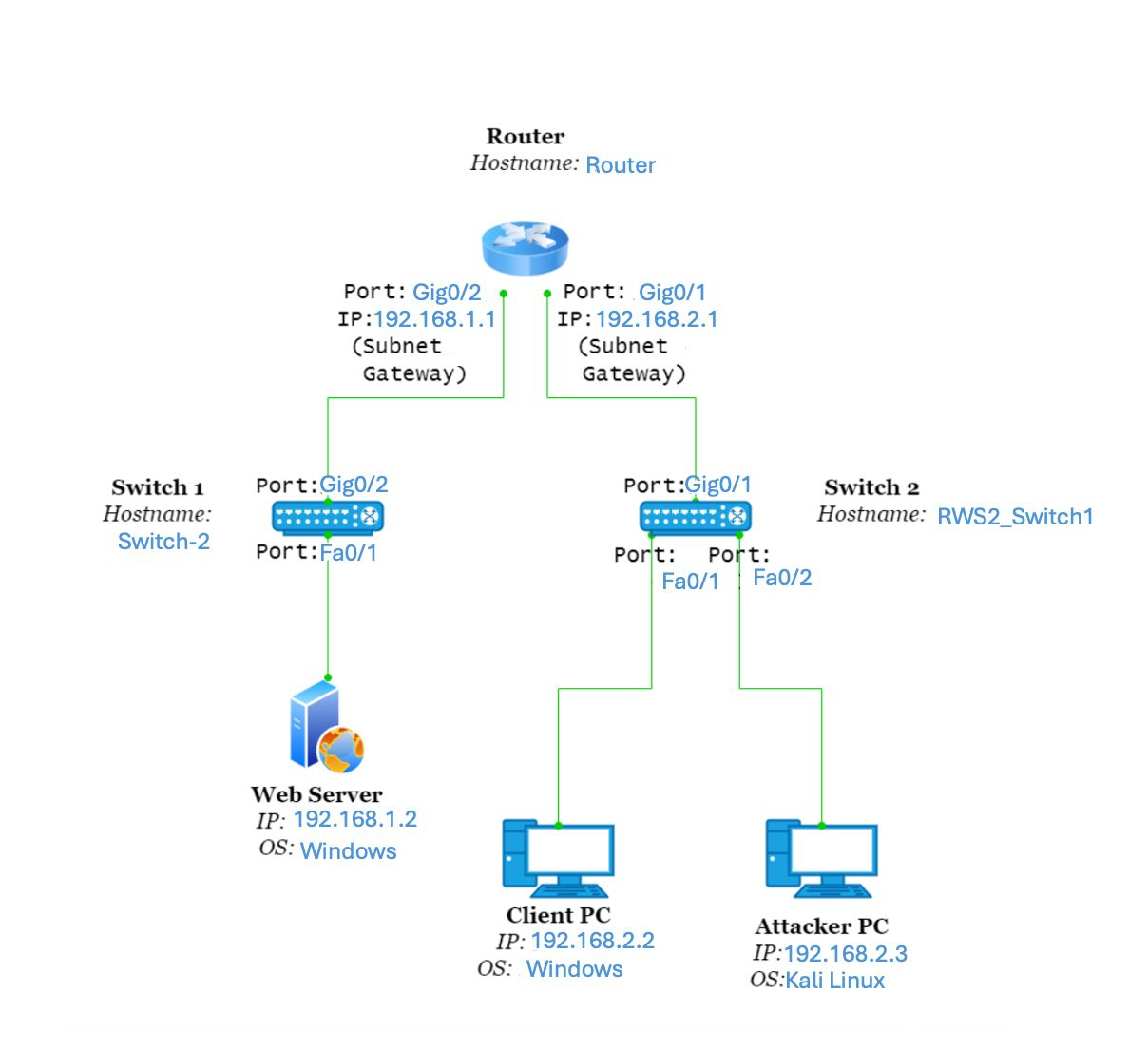
For this lab assignment, the group conducted an ARP cache poisoning attack, allowing an attacker to act as Man in the Middle (MITM) between a FTP client in one subnetwork and a FTP server in another subnetwork. The attacker is then able to sniff the data exchanged between the client and its default gateway. The following are the objectives the group aimed to fulfill with the implementation of this lab:

1. Configure a network with one Router, two switches, an attacker machine, and two PCs as the client and the FTP server.
2. Perform ARP poisoning attacks using Ettercap and Arpspoof.
3. Sniff FTP packets between the client, residing on one subnetwork, and the FTP server in another subnet.
4. Perform various mitigation steps to prevent ARP poisoning attack.

# 

# TOPOLOGY & ARCHITECTURE

Draw similar diagram to show the topology of the LAN configured for the execution and testing of this Lab 5 and write a description of the topology:



**Figure 1: Topology Diagram**

# SOFTWARE/TOOLS USED

In one statement describe why you have used the following tools.

1. PuTTY- Used to access and configure network devices, such as the router and switches, to set up VLANs, ARP inspection, and troubleshoot network connectivity.
2. Ettercap- Used to perform ARP poisoning and intercept FTP traffic, allowing us to act as a Man-in-the-Middle (MITM) and capture sensitive data between the client and FTP server.
3. Arpspoof in Dsniff- Used to execute ARP cache poisoning by sending spoofed ARP replies to trick the client and router into forwarding traffic through the attacker machine.
4. FTP client and Server (FileZilla) – As Discussed in Lab 1 - Used to simulate real-world file transfers, providing a communication stream between the client and server that we targeted during the ARP poisoning attack.
5. Wireshark- Once the attack started we pinged the ftp server from client so that we could capture the ping packet through the wireshark

# INITIAL CONFIGURATIONS

## Network Configurations

Configure the network devices in the LAN to the networks 10.1.2.0/24 and 10.2.2.0/24 with the IP address configurations and fill in the following table:

| NIC | IP | MAC Address |
| --- | --- | --- |
| Server | 1.2 | 4С:B0:4A:B9:E5:B9 |
| Client | 2.2 | 4C:D7:17:97:FB:68 |
| attacker | 2.3 | 4C:D7:17:97:FA:85 |
| Router | 2.1 | 18:8b:9d:45:25:b9 |
| Router | 1.1 | 18:8b: 9d:45:25:ba |

**Table 1: IP address & MAC address of Network Devices**

Provide screenshots for all PCs and FTP server configuration (Note: you need to use “ipconfig” command in CMD for windows machines and “ifconfig” command in Terminal for Linux machines).

Note: type “reload” in switch configuration to remove previous student work, if any, and provide a screenshot and display the current running configuration by typing “show run” command.

Configure the router’s interfaces with the IPs as mentioned in Table 1 and verify these configurations with the command “show interfaces” (provide screenshots).

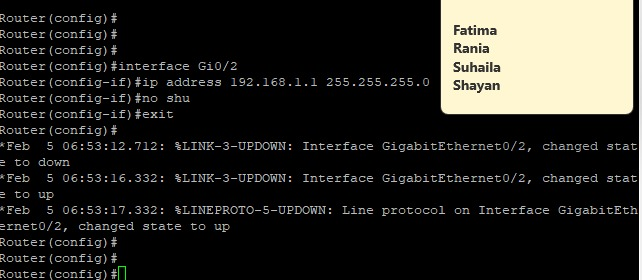


Figure 2. Assigning IP address on the interface Gig0/2

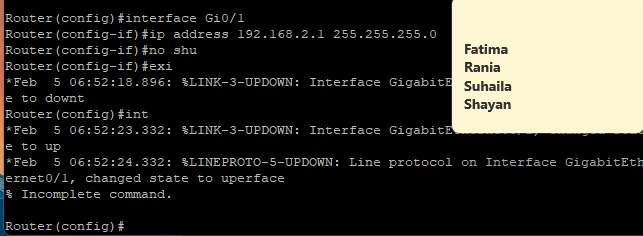


Figure 3. Assigning IP address on the interface Gig0/1

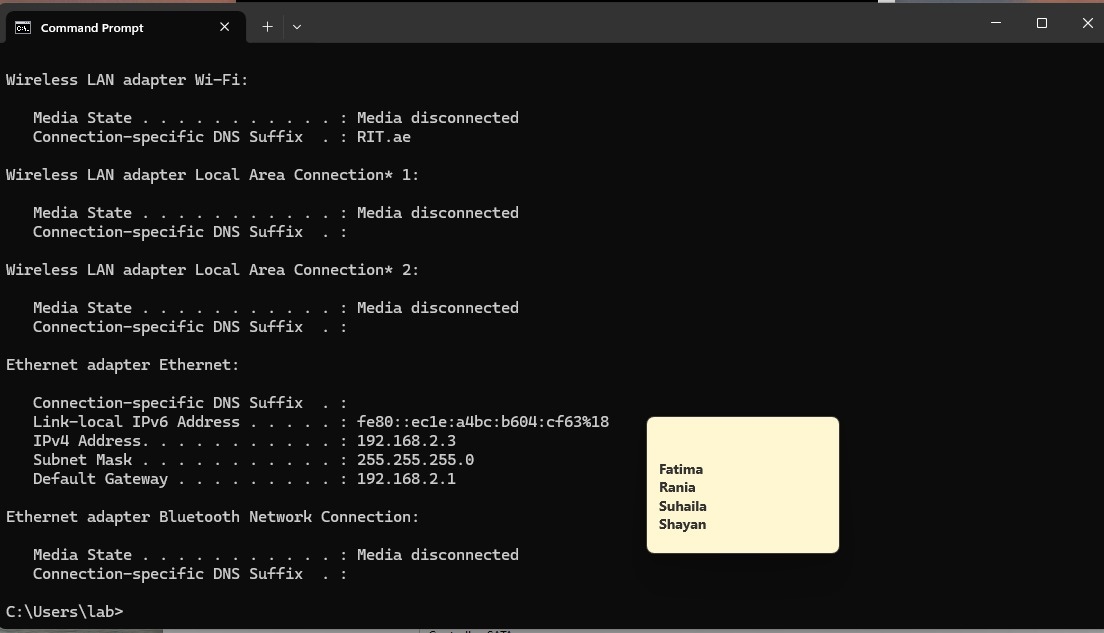


Figure 4. Attacker PC ipconfig

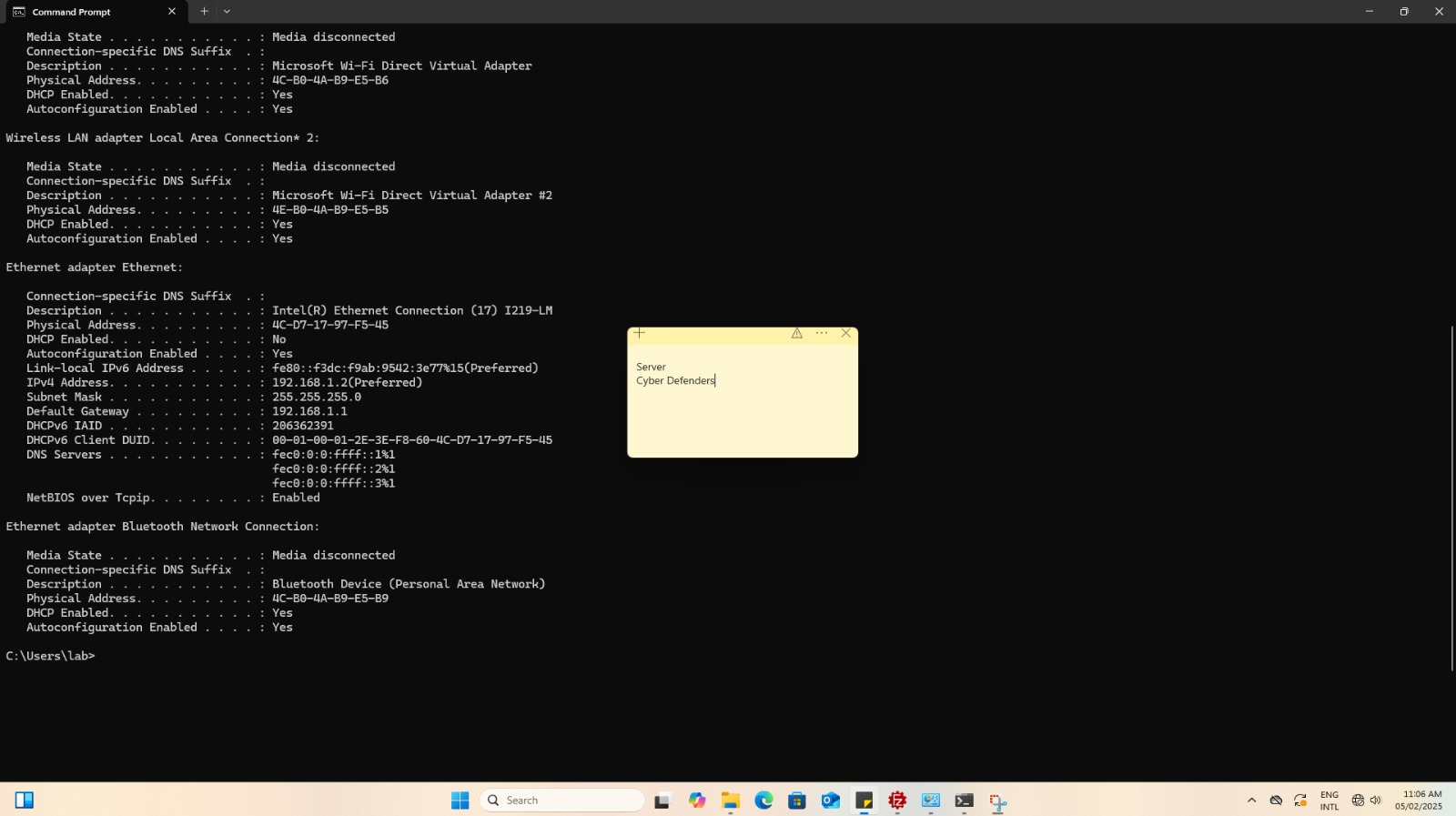


Figure 5. Server PC ipconfig

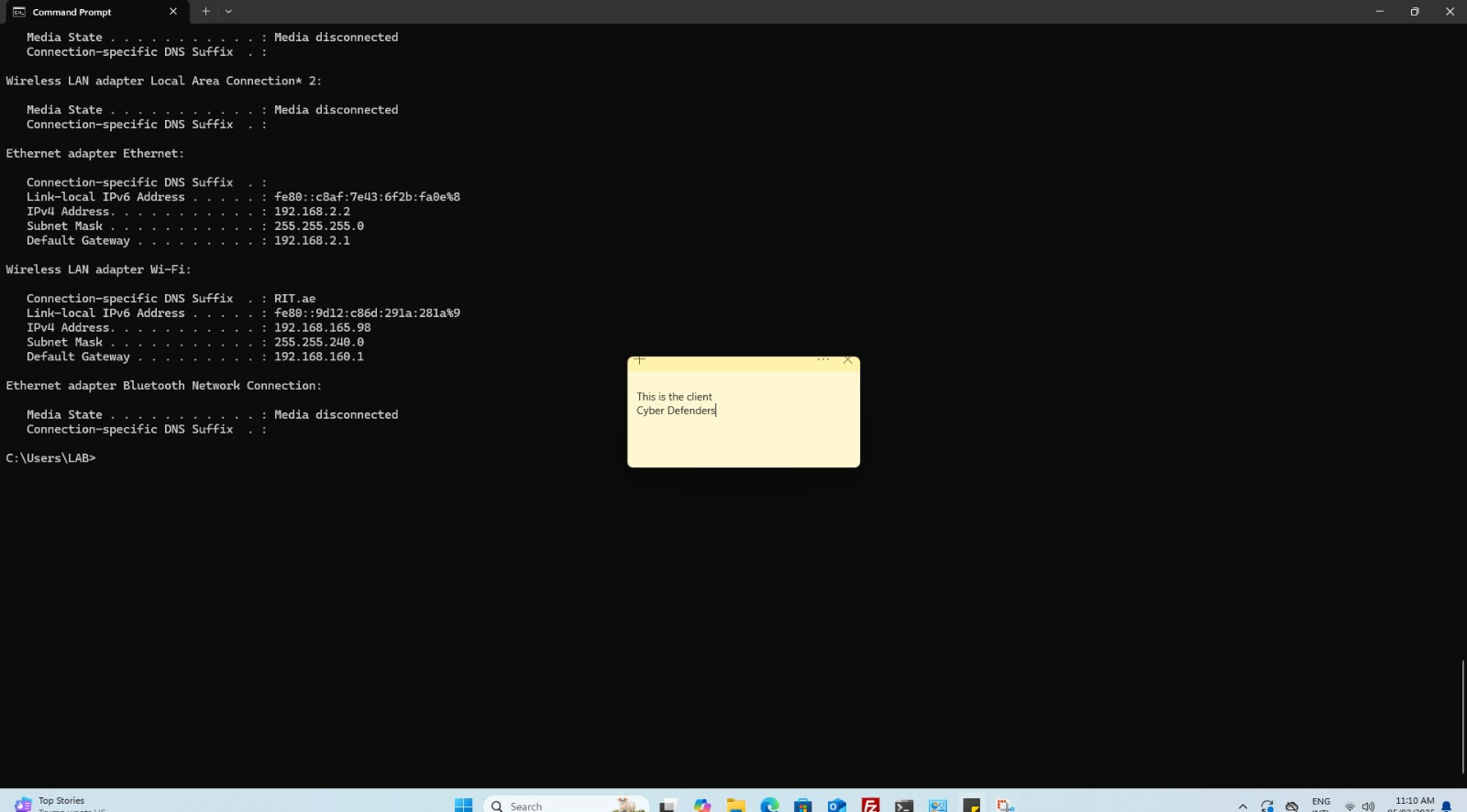


Figure 6. Client PC ipconfig

# ARP POISONING ATTACK DESCRIPTION

# In your own words describe ARP Poisoning attack.

It is a type of an attack where the bad actor tries to manipulate the ARP tables of devices on the network. This lets the attacker impersonate himself as another device by using its network gateway. The bad actor can then intercept, modify or even direct the traffic. So you can conduct this attack by sending forged ARP replies to the network. Then those replies will be used to trick the devices into thinking that the attacker's MAC address is legitimate as it will be associated with a legitimate IP. When a victim device sends data meant for the router or another machine, it directs it to the attacker first. The attacker can capture, read, change or drop packets before sending them to their destination (*Learning Center*, n.d.).

# STEPS OF ATTACK

## Attack Implementation

Give a detailed explanation of the implementation of the ARP Poisoning attack conducted by your group (Note: provide a screenshots of your steps).

1. Turn on All PCs and connect them as per the topology diagram in Figure 1 were made between the 3 PCs - *FTP Server, Client PC,* and *Attacker PC* - as well as the 2 switches. Boot the *Client PC* to Windows 10, and boot the *FTP Server*, and boot the *Attacker PC* to Kali Linux operating system.

Note: Make sure that there is no any issue in connections by using ping ICMP packets from the hosts to the others (provide screenshots).

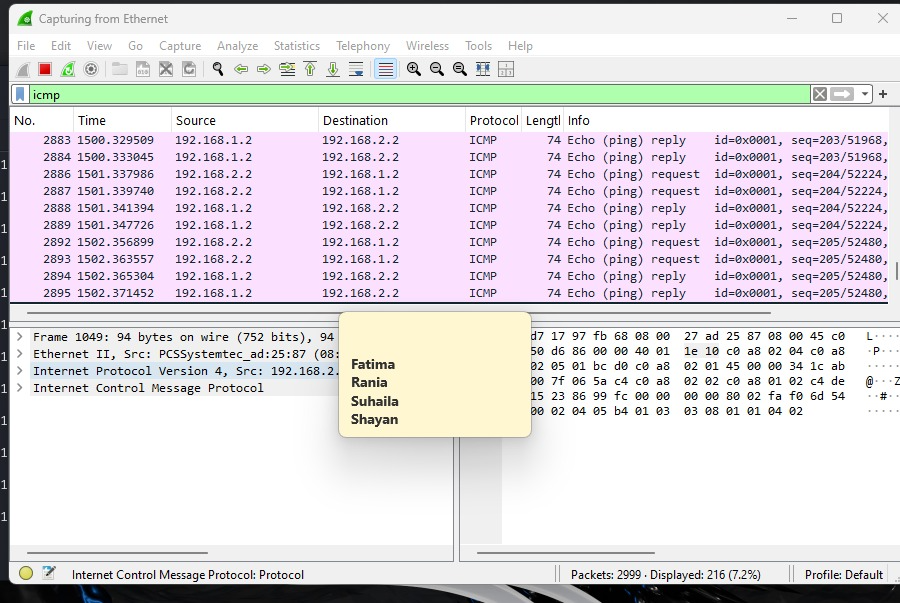


Figure 7. Receiving the ICMP packets on WireShark

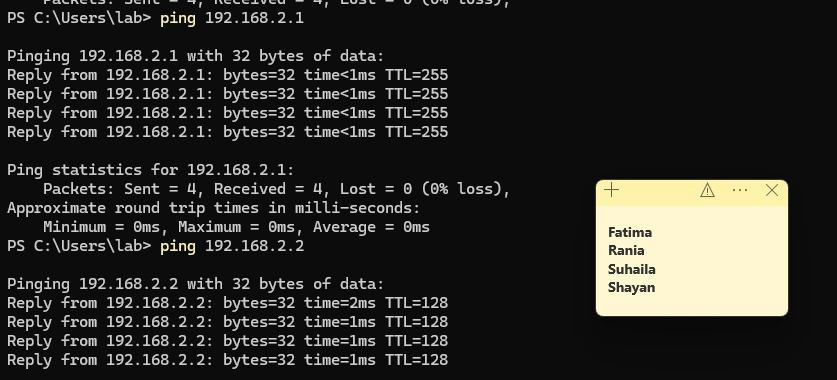


Figure 8. Pinging Successfully

1. Next, check the ARP cache on the client machine using the command “***arp -a”*** and clear it by using the command “***arp -a -ad***” or ***“arp -d”*** (provide screenshots).

Note: you can carry out these commands using the Windows command line on the client machine.

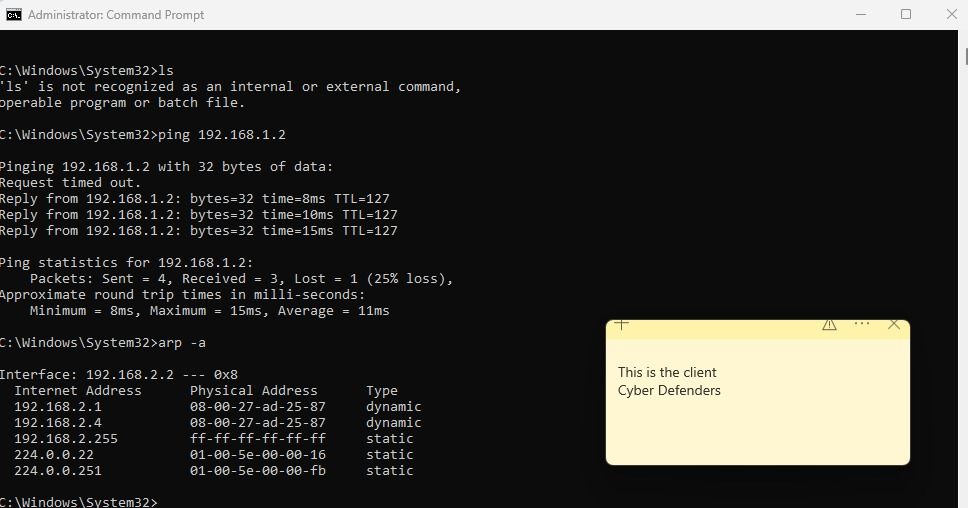


Figure 9. Client PC pinging

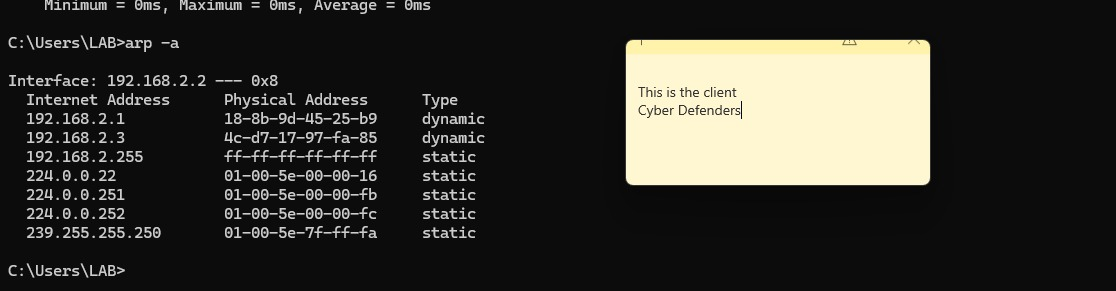


Figure 10. arp -a command on Client PC

1. Launch Wireshark on the *Attacker PC* using the command “***sudo wireshark”***. And choose the “eth0” interface option, The Wireshark then will begin capturing packets from the LAN traffic.

Note: Wireshark is prepared to sniff traffic in the LAN and analyze communication streams between PCs on the network.

1. Implement the attack by using the Arpspoof tool found in Dsniff. In new Kali versions, Arpspoof comes as a pre-built standalone tool.

Run the ARP spoofing attack through the Attacker machine’s terminal using the command “ sudo arpspoof -i eth0 -t [Client PC IP] [Router Interface IP]”. Since we want to poison both directions you should also attack the other direction: “ sudo arpspoof -i eth0 -t [Router Interface IP]” [Client PC IP].

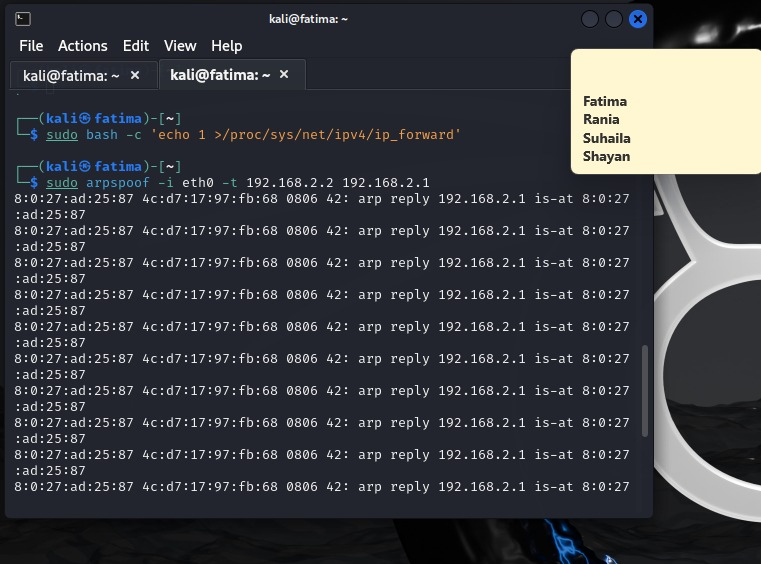


Figure 11. Starting the Attack on Kali machine

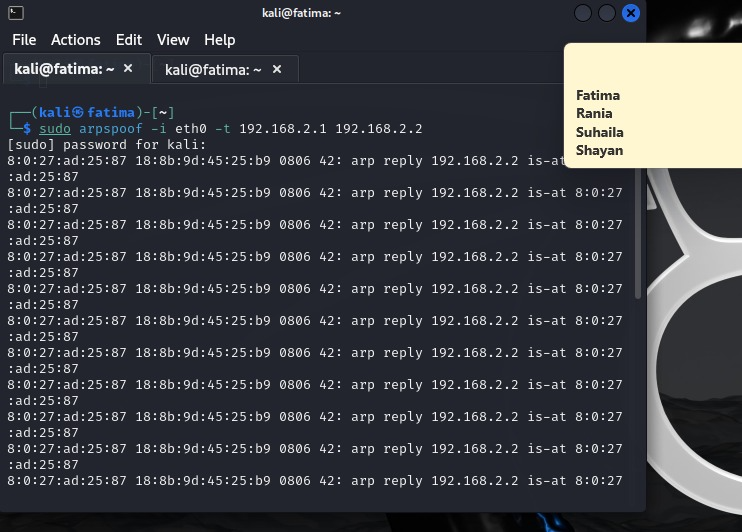


Figure 12. Starting the Attack on Kali machine

Once the attack is running using Dsniff’s arpspoof and the MAC address is spoofed, ping the FTP server from the client (provide screenshot).

IN ADDITION TO SPOOFING, DO NOT FORGET TO ENABLE IP FORWARDING IN THE ATTACKER!

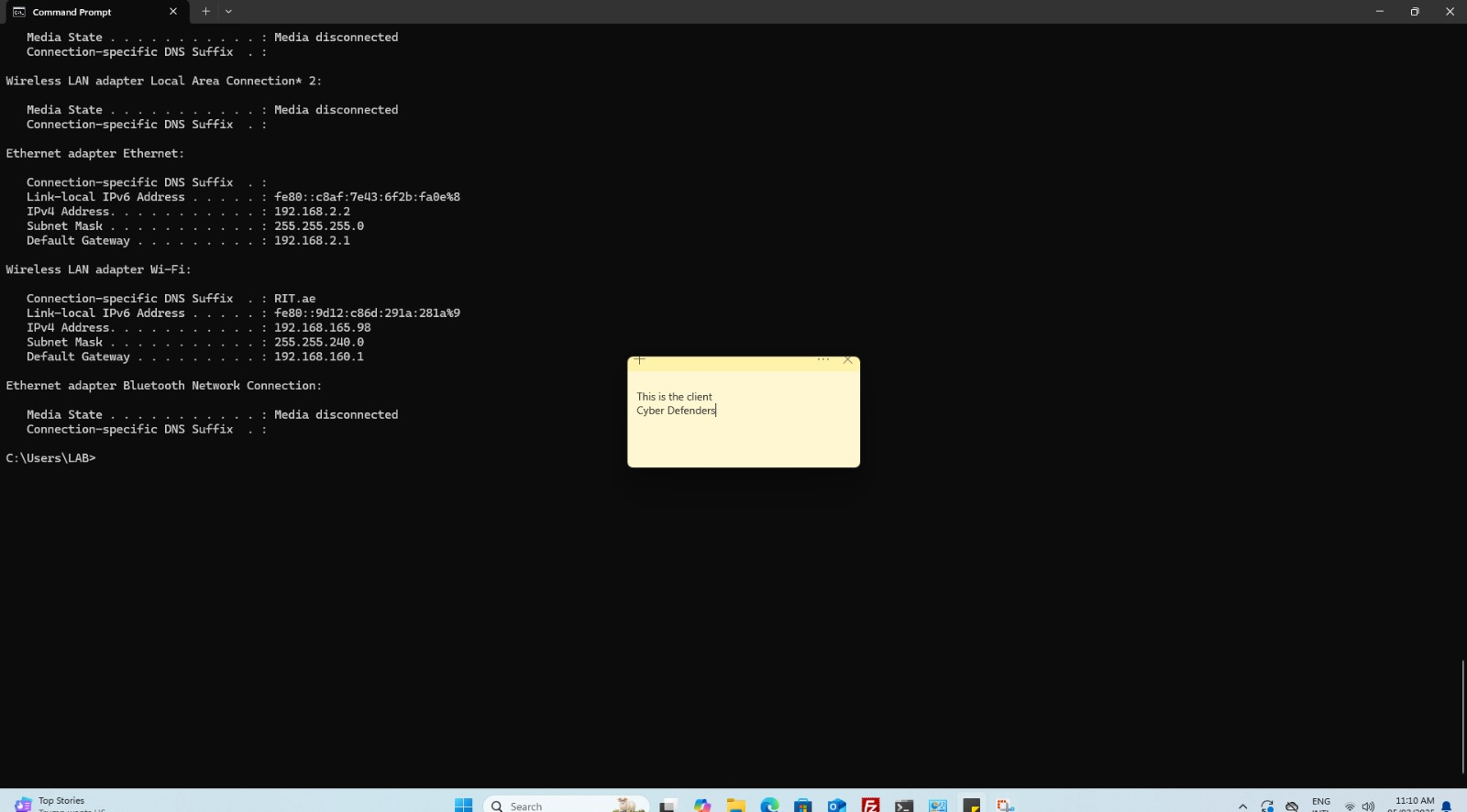
****

Figure 13. Ipconfig on the client machine

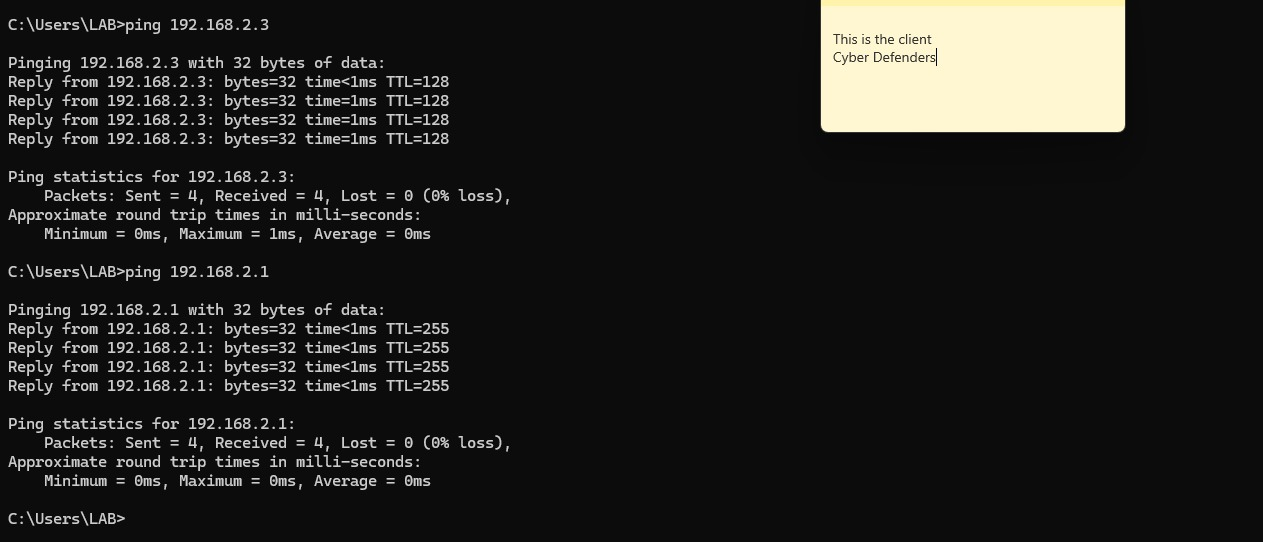
****

Figure 14. Pinging on the client machine

Once the ping packet is sent, you can capture it using Wireshark (provide screenshot).

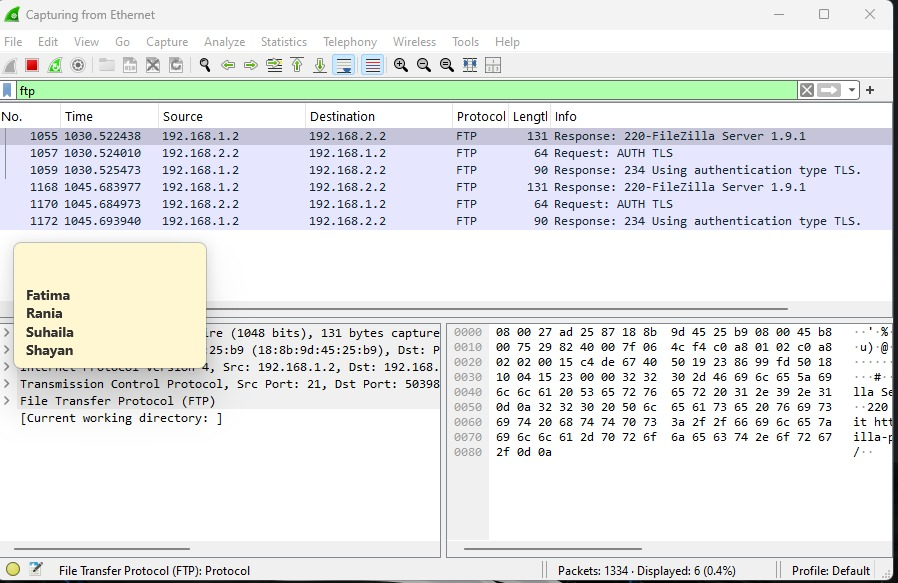
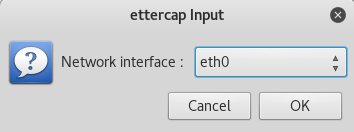
****

Figure 15. Receiving the FTP packets on WireShark

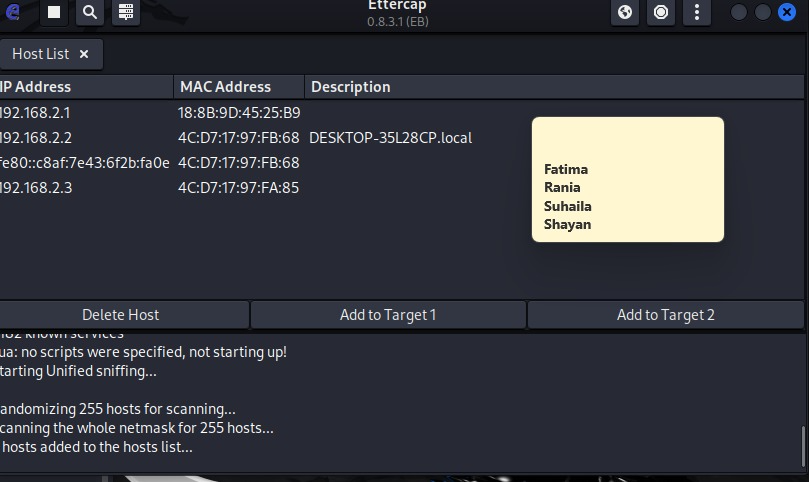
1. Carry out the ARP cache poisoning attack by using Ettercap tool, also it is pre-installed on the Kali machine, and follow similar steps to spoof the MAC address of the client machine with the Attacker machine’s MAC address. The following Figures show the steps taken:

  
**Figure 16: Opening Ettercap**

Next, specify the interface on which the attack must be carried out (provide screenshot).

**  
Figure 17. Specifying Interface on Ettercap**

Set the targets for the ARP Poisoning attacks, as shown in the below three Figures (provide screenshots), with Target 1 being the Client’s IP (X) and Target 2 being the gateway of the Client (X).

****Figure 18: hosts added to the host lists

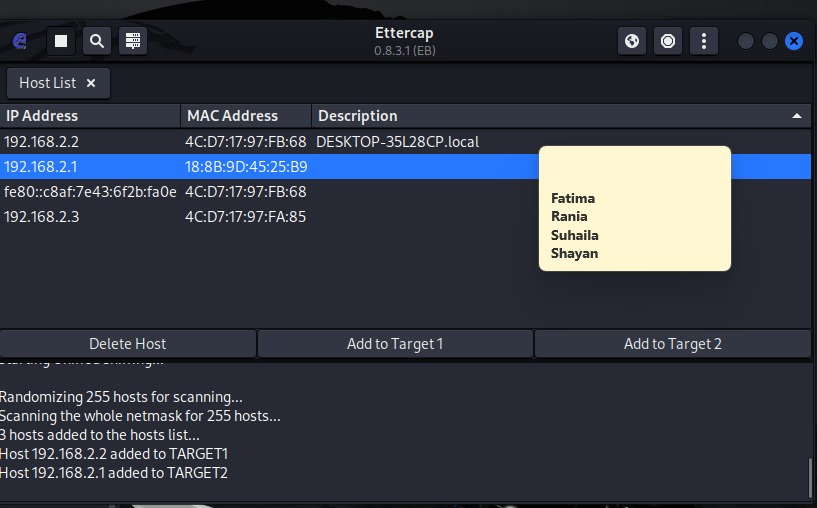
****

Figure 19. TARGET 1 and TARGET 2 has been added

Start the ARP spoofing attack through the Ettercap GUI by clicking on the play button in the toolbar.

Once the attack has started, ping the FTP server from the client to capture the ping packet through Wireshark and analyze the contents of the packet (provide screenshot).

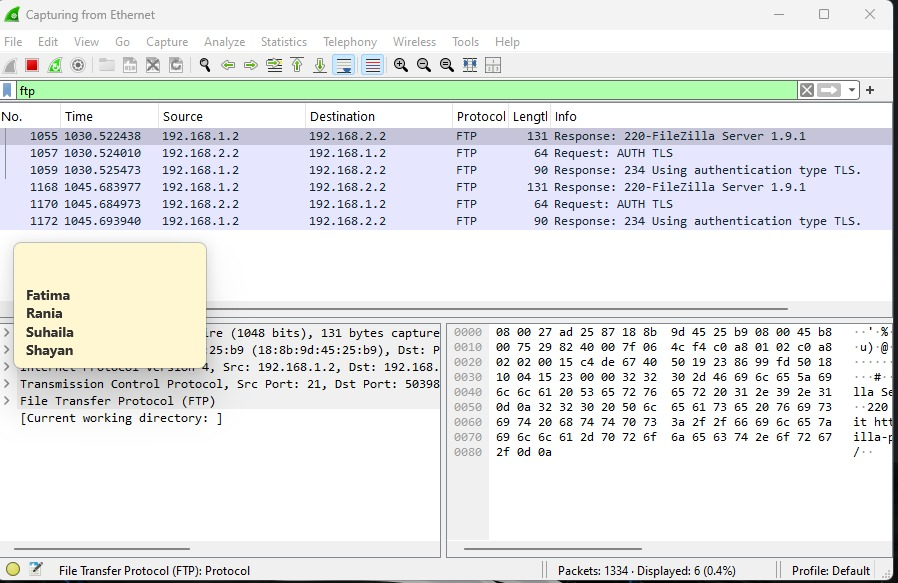
****

Figure 20. FTP capture in wireshark

You should notice that the MAC address of the source has been changed from the gateway’s MAC address to the Attacker’s MAC address. This proves the success of the attack. This is also can be shown by the entry in the ARP Cache (provide a screenshot).

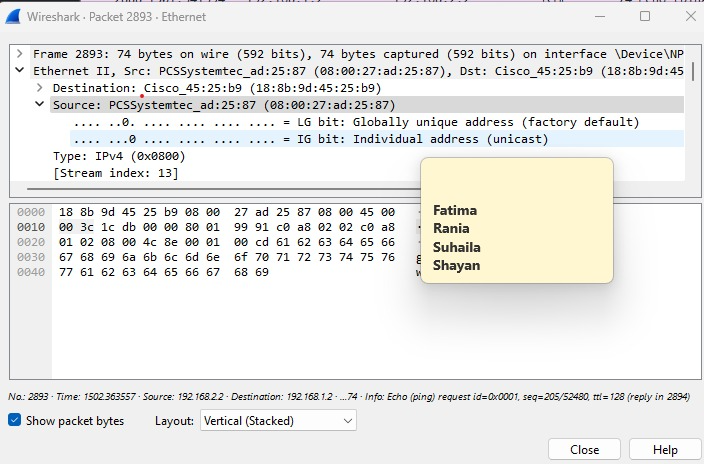


Figure 21. FTP Wireshark anaylsis

The gateway mac address is : 18:8B:9D:45:25:B9

The attacker mac address: 08:00:27:ad: 25:87

Is it shown below:

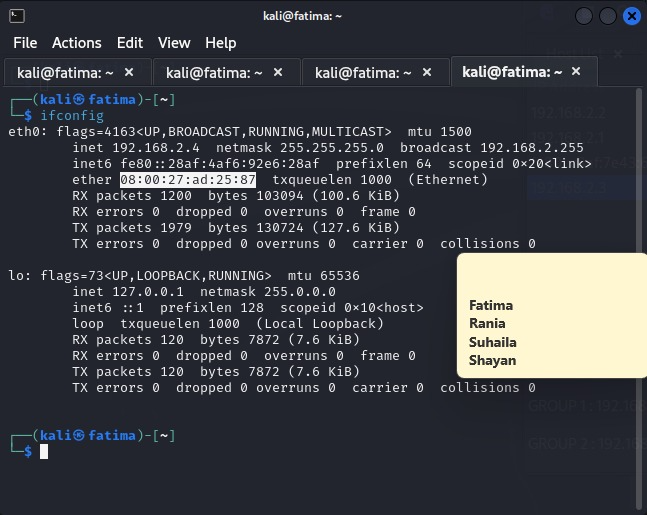


Figure 22. The MAC address changed to the attacker MAC address

So the MAC address at the end changed from the Gateway MAC address to the attacker MAC address

# PROBLEMS/ISSUES FACED

Write down any problems or issues you faced during your work.

We did not face any major or even minor hiccups while doing this lab . The one problem that we faced was that our switch was not reloading because of the mitigation techniques we implemented from Lab1. To solve this problem, we simply used another switch.

# 

# MITIGATION TECHNIQUES

Use Dynamic ARP Inspection technique in order to mitigate ARP cache poisoning attack for each step provide screenshots that demonstrate your works with brief description of the rationale behind that step.

## Dynamic ARP Inspection

Implementation:

Follow the below steps to prevent the network from being vulnerable to ARP cache poisoning attacks.

First, create access control lists (ACLs) on both switches and add certain IP & MAC permissions to the ACLs by using following commands:

1. For switch 1:
   * config t
   * arp access-list (NAME OF ACL)
   * permit ip host [GATEWAY IP] mac host [GATEWAY MAC ADDRESS]
   * permit ip host [FTP SERVER IP] mac host [FTP SERVER MAC ADDRESS]

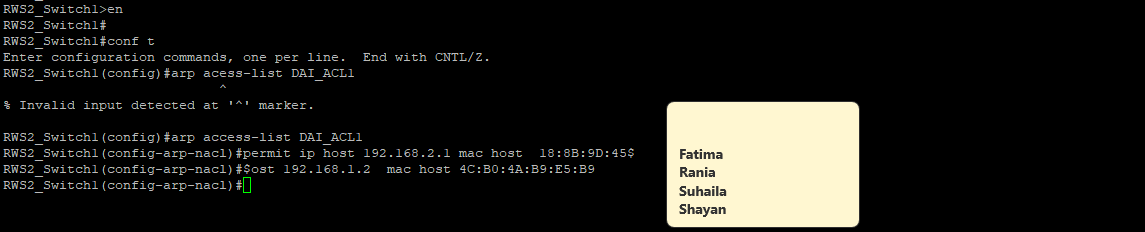


Figure 23. Switch 1 ACL

1. For switch 2:
   * config t
   * arp access-list (NAME OF ACL)
   * permit ip host [CLIENT IP] mac host [CLIENT MAC ADDRESS]
   * permit ip host [GATEWAY IP] mac host [GATEWAY MAC ADDRESS]

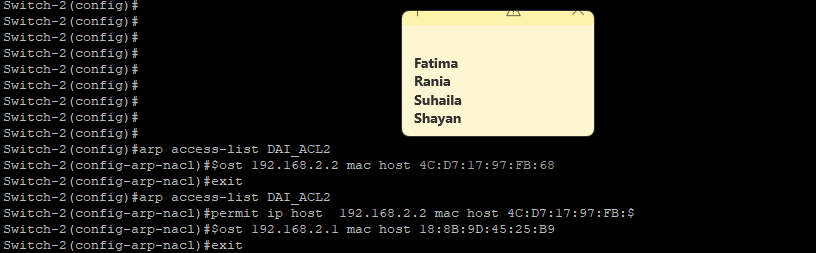


Figure 24. Switch 2 ACL

Verify these configurations with the “**show access-lists”** command in both switches.

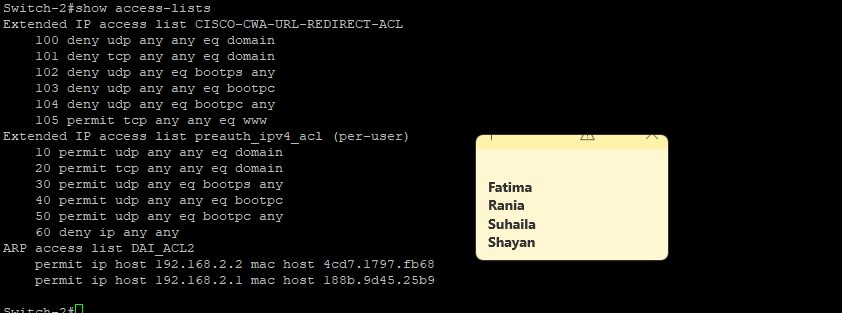


Figure 25. Show access lists in Switch 2

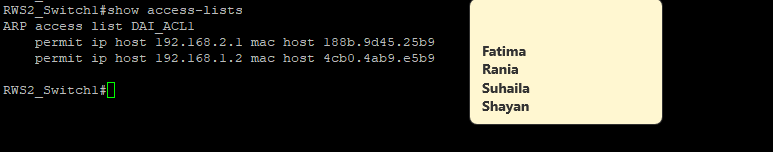


Figure 26. Show access lists in Switch 1

Next, Enable the ARP inspection by using this command in both switches

* ip arp inspection filter [ARP ACCESS LIST NAME] vlan 1
* ip arp inspection vlan 1

Lastly, you can check the inspection by ***“show ip arp inspection vlan 1”***

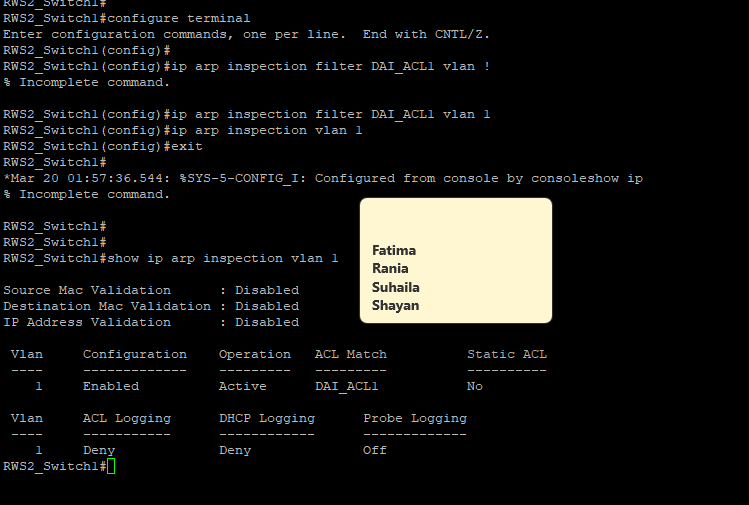
******

Figure 27. show ip arp inspection vlan 1 switch 1

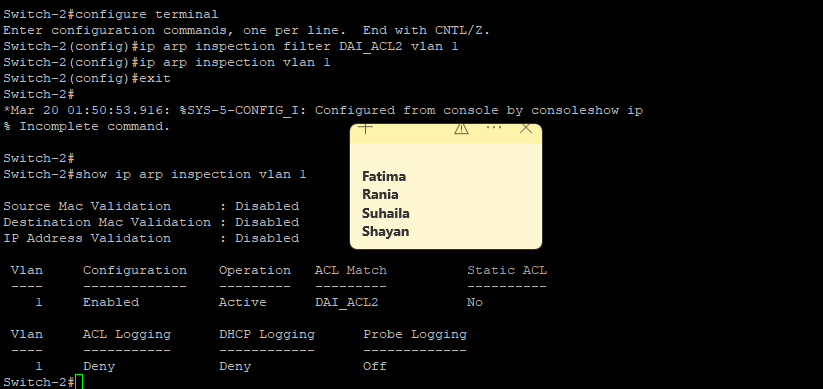
******

Figure 28. show ip arp inspection vlan 1 switch 2

After those configurations, the ports on the switches should be assigned as trusted or untrusted depending on whether they’re connected to a router. The ports used for connections with the router are trusted ports and the switches will not inspect traffic coming inbound or outbound from these ports against the ACL. All other ports were untrusted by default and traffic on those ports are checked against the ACL. Provide screenshots to demonstrate the configurations of ports as trusted and untrusted your work.

To do this go to the interface configuration mode (you need to enter each interface except the one attacker pc is connected) in both switches and use command **“ip arp inspection trust”**

****

Figure 29. ip arp inspection trust switch 1

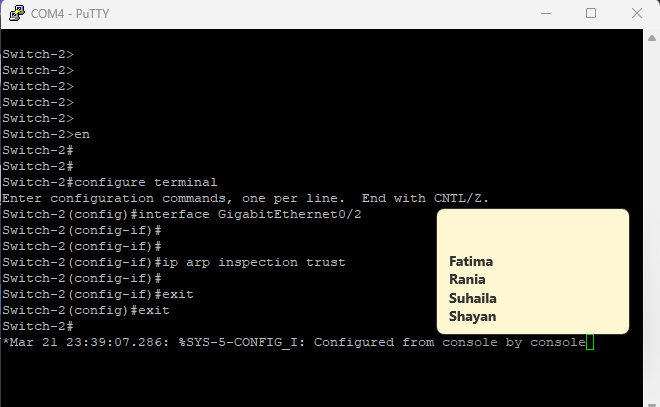
****

Figure 30. ip arp inspection trust switch 2

Use the following command to show ARP inspection interfaces **“show ip arp inspection interfaces”**



Figure 31. show ip arp inspection interfaces

**Repeat the attack and verify that it was not successful (provide screenshots).**

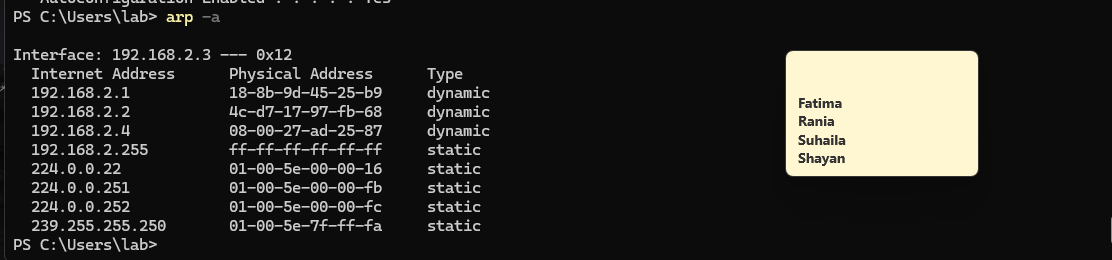
****

Figure 32. Attack verification

**Write the Pros and Cons for Dynamic ARP Inspection.**

There are several pros and cons for dynamic ARP inspection. Here are some of the important ones:

Pros:

Prevents ARP Spoofing Attacks – Prevents rogue ARP replies, preventing ARP cache poisoning and man in the middle attacks.

Verifies ARP Packets – Only permits valid ARP responses by cross-checking IP-to-MAC mappings with a trusted database.

Enhances network security – Adds an extra layer of security to switches, protecting critical network infrastructure.

Real time attack mitigation – Automatically detects and blocks suspicious ARP traffic without the intervention of a human operator.

Works without end-user configuration – DAI works to secure the network automatically without requiring each device to be configured separately, in contrast to static ARP entries.

Cons:

Must set up correctly – Wrong ACLs block valid traffic or let harmful ARP packets pass.

Can slow large networks – Real-time check and block ARP packets cause latency.

Works only with managed switches – Requires DAI support and enterprise equipment.

Does not defend against outside attacks – DAI covers only local networks; it does not block DNS or IP spoofs or attacks from outside.

May wrongly block correct ARP packets – Incorrect setup stops normal network work.

## Rate Limit

Implementation:

The rate limit allows you to set a particular size for the ARP cache buffer which helps in detecting any suspicious activities such as a DoS attack. This can also be used to prevent a Man In The Middle attack such as ARP Spoofing as it will disable the channel in case the switch exceeds the rate limit set. As shown below, we set the rate limit to be 1 pps.

Rate limit mitigation on Switch 2 by using this command “ip arp inspection log-buffer entries 1”. (provide screenshot)

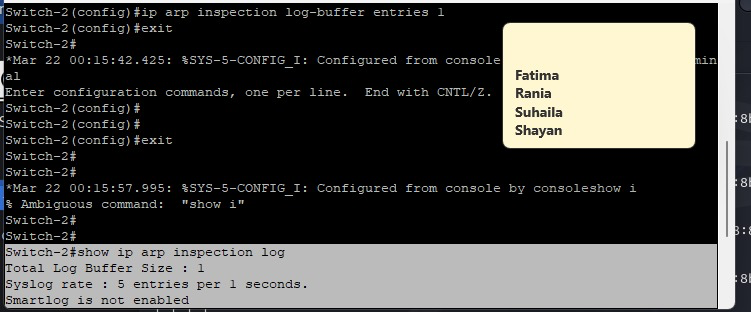


Figure 33. ip arp inspection log-buffer entries 1

To verify rate limit mitigation on Switch 2 use this command “show ip arp inspection log”. (provide screenshot)



Figure 34. show ip arp inspection log

Pros and cons for Rate Limit:

There are several pros and cons for rate limits. Here are some of the important ones:

Pros:

1. Stops ARP flooding attacks – Limits DoS attacks that overwhelm the network with many ARP requests.
2. Cuts harmful ARP activity – Lowers ARP packets per second to reduce MITM attack risks caused by ARP spoofing.
3. Boosts network performance – Limits ARP traffic to avoid overloading the switch’s ARP cache and keep the network flow smooth.
4. Auto protection – Runs without manual input and blocks ARP requests that exceed the set limit.
5. Cooperates with other security measures – Pairs with Dynamic ARP Inspection (DAI) or port security to add another defense layer (Radware, n.d.).

Cons:

1. May Block Legitimate ARP Requests – If the rate limit is very strict, it could block valid ARP requests from new devices connecting to the network.
2. Not a Complete ARP Spoofing Solution – Rate llimiting only controls ARP request frequency but does not verify the legitimacy of ARP replies like Dynamic ARP Inspection (DAI) does.
3. Not effective against slow attacks – Attackers can bypass rate limits by sending ARP packets at a slow, steady rate rather than flooding the network all at once.
4. Only protects against excessive traffic – It does not validate ARP responses, meaning that a well-timed ARP spoofing attack may still succeed if it stays within the defined limit.

# 

# 

# 

# 

# CONCLUSION

Write down a conclusion of the work you have done and discuss security implication.

For this lab, we were able to successfully conduct an ARP cache poisoning attack and demonstrate how a malicious user can hijack and manipulate network traffic by taking control of ARP tables. With the help of tools such as Arpspoof and Ettercap, we were able to impersonate the gateway, routing FTP traffic between the client and server through our attacker machine. We then used wireshark to analyze the attack by sniffing packets, after which we could confirm that the client's ARP cache was poisoned and prove that traffic was being intercepted. To mitigate the attack, we implemented Dynamic ARP Inspection (DAI) and Rate Limiting on our network switches. DAI verified ARP packets against a trusted database, denying spurious ARP responses and neutralizing the attack. Rate limiting helped in restricting the number of ARP requests per second, reducing the threat of excessive ARP-related traffic that would be used as a Denial of Service (DoS) attack. Now let’s discuss some security implications regarding the lab. First we have the Man-in-the-Middle Attack, where ARP poisoning shows a major weakness. It lets attackers take sensitive data such as login details sent over unencrypted FTP. Then there is the Network integrity risks where Attackers can change or drop packets. This disrupts network talk and lowers system trust. With the Lack of ARP Authentication, ARP gives no built in check. Networks stay open unless they add security steps like DAI, fixed ARP lists or VPNs.This lab shows why FTP must switch to methods like SFTP or FTPS to stop easy capture of login details.

# REFERENCES

*Learning center*. (n.d.). Learning Center. <https://www.imperva.com/learn/application-security/arp-spoofing/>

Radware. (n.d.). *What is rate limiting?* Radware. <https://www.radware.com/cyberpedia/bot-management/rate-limiting/>