Lab 3 Part 02 Report

Name: Brandon Cortez

ISU ID: 820561762

Date: 4/18/25

1. **Overview**

   Read through the entire lab document and give an overview of the objective of the lab and what you will be doing.

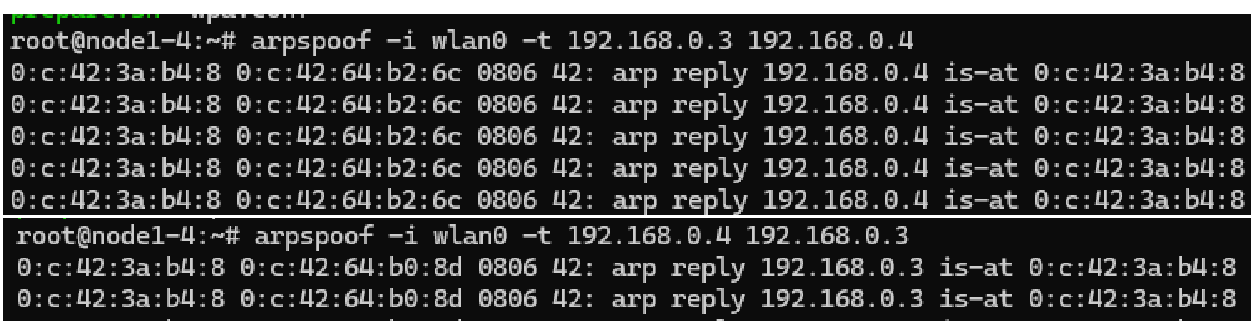
   The objective of this lab is to demonstrate how a Man-in-the-Middle (MITM) attack can be carried out on a Wi-Fi network using ARP spoofing. By impersonating the MAC addresses of both clients Alice and Bob, an attacker Mallory is able to intercept and sniff their traffic without detection.

2. **Lab steps and observations**

   Answer all questions in the lab document, and document all the steps you take and results that you get from this lab with screenshots and analysis.

   - You should see output on the terminal indicating that Mallory is sending gratuitous ARPs. Comment on what you see

   I can see in the results that the arp reply indicates that Bob's IP address is at Mallory's MAC address rather than his own, and the same for Alice.



- Try running arp -na on Alice or Bob. What do you see? Was the ARP poisoning successful?

I can see on both Alice and Bob that Mallory's MAC address is double registered for both Alice and Bob as well as Mallory. This indicates that the poisoning and impersonation was successful.

```
root@node1-2:~# arp -na
? (192.168.0.5) at 00:0c:42:3a:b4:08 [ether] on wlan0
? (192.168.0.4) at 00:0c:42:3a:b4:08 [ether] on wlan0
? (10.40.0.10) at 12:18:cf:c1:d0:d8 [ether] on eth1
? (10.40.0.1) at d8:9e:f3:cf:61:e2 [ether] on eth1
root@node1-2:~#
```

```
root@node1-3:~# arp -na
? (10.40.0.1) at d8:9e:f3:cf:61:e2 [ether] on eth1
? (192.168.0.5) at 00:0c:42:3a:b4:08 [ether] on wlan0
? (192.168.0.3) at 00:0c:42:3a:b4:08 [ether] on wlan0
? (10.40.0.10) at 12:18:cf:c1:d0:d8 [ether] on eth1
root@node1-3:~#
```

- Ettercap Plaintext Credentials
  - FTP

I can see Alice's credentials in plaintext in a singular sniffed packet. This shows the security issues with being able to see the plaintext credentials if you are sniffing ftp traffic.

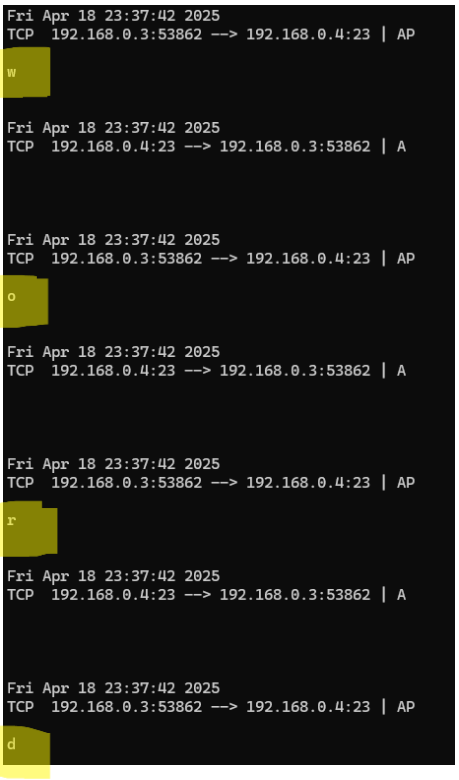
```
Fri Apr 18 23:18:00 2025
TCP  192.168.0.4:21 --> 192.168.0.3:41830 | AP

331 Please specify the password..



Fri Apr 18 23:18:01 2025
TCP  192.168.0.3:41830 --> 192.168.0.4:21 | A


FTP : 192.168.0.4:21 -> USER: alice  PASS: password
```

- SFTP

Using SFTP, Mallory can see that there is traffic occurring between Alice and Bob but they are unable to read the credentials in plaintext since the traffic is encrypted.

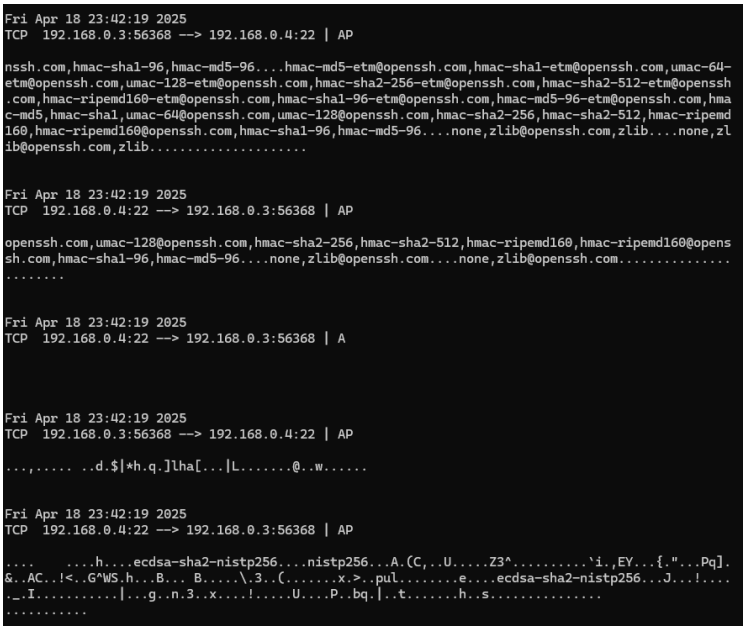
- telnet

When using telnet, Alice's credentials are readable in plaintext by Mallory, however it behaves differently in that each letter of the username and password is communicated in its own packet. Letters 'w', 'o', 'r', and 'd' of the password "password" pictured below.



- SSH

Similarly to SFTP, if Alice is using SSH, Mallory can see that there is traffic occurring between Alice and Bob but cannot read the credentials in plaintext from the encrypted traffic.



- For each of the four applications, use your experiment results to explain whether credentials sent using this application can be captured by a malicious user when using an insecure medium (like a public WiFi hotspot, or an unsecured WiFi network with no password).

In the experiment, **credentials were captured for FTP and Telnet**, since both transmit data in plaintext and are vulnerable on insecure networks. Contrarily, **SFTP and SSH encrypt the connection, preventing the attacker from seeing usernames or passwords.** This shows that only secure, encrypted applications can protect sensitive data on untrusted networks.

- Based on the results of this experiment: Which file transfer application - FTP or SFTP - is more secure? Which remote login application - telnet or SSH - is more secure? Explain why.
    - Which file transfer application is more secure, FTP or SFTP?

      SFTP is more secure than FTP. In the experiment, FTP credentials were clearly visible in Ettercap during the MITM attack, while SFTP encrypted the communication, making it unreadable to the attacker.

    - Which remote login application is more secure, Telnet or SSH?

      SSH is more secure than Telnet. Telnet transmitted Alice's username and password in plaintext, which were captured by Ettercap. SSH, on the other hand, encrypted the session, preventing Mallory from seeing any sensitive information.

3. **Summary and conclusions**

   Summarize your findings and conclusions for this lab.

   This lab demonstrated how a man-in-the-middle attack using ARP spoofing can compromise unencrypted communications on a WiFi hotspot. I was able to see first-hand as the attacker Mallory how intercepting traffic between Alice and Bob allowed me to capture login credentials when insecure protocols like FTP and Telnet were used. However, secure alternatives like SFTP and SSH effectively protected the data through encryption. The experiment highlights the critical importance of using secure, encrypted applications, especially when connected to untrusted networks.