**Amanuel Reda**

**Lab 2**

**Question 1)** How does the Internet protocol suite documented in RFC 1122 map to the OSI Model?

Internet Protocol Model

A picture containing application

Description automatically generated

Network Access

Internet

Transport

Application

**Question 2)** What layers of the OSI Model does the ARP protocol bridge?

ANS: Network Layer and Data Link (MAC) Layer

**Question 3)** What tool did he leverage on the Windows device to perform the MitM attack?

ANS: Cain & Abel v4.9.40

Command Prompt

**Step 1:**

Screen Shot 1) Take a snip of the screen to show you found the password used to FTP using tcpdump.

A picture containing text, electronics, black, display

Description automatically generated

**Step 2:**

Screen Shot 2) Take a snip of the screen to show you found the password for the FTP session using Ettercap.

A computer screen capture

Description automatically generated with low confidence

Screen Shot 3) Take a snip of the screen to show you found the password used to FTP using Wireshark.

A picture containing text, electronics, black, display

Description automatically generated

**Question 4)** Why was the telnet password harder to obtain in the Wireshark data as compared to FTP?

Because it’s harder to see the password in a clear mode like FTP. Its surrounded by many letters and dots.

**Question 5)** Can you perform a MitM Attack using the APR Cache Poisoning approach if the devices are on separate networks (separated by a router)?

To perform MitM Attack using the APR Cache Poisoning approach the devices must be on the same network.

**Question 6)** This lab was performed using version 4 of the IP protocol. Can you poison the ARP cache using IPv6? Why or Why Not?

ARP doesn’t exist in the IPv6 protocol list; therefore, we cannot poison the ARP cache using IPv6. Instead, we can use NDP (Neighbor Discovery Protocol).

**Question 7)** List two ways to prevent the MitM Attack using ARP Cache Poisoning? Hint: Not asking for ways to prevent seeing sensitive data on the network using encryption; instead, I am looking for ways to initially prevent the poisoning of the ARP Cache.

* Having a static ARP
* Packet filtering