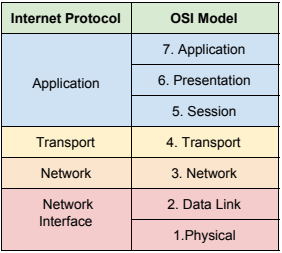
**Lab #2**

**CECS 378 – Spring 2021 Cappel**

**Due:** Wednesday, February 10th prior to lab (11:59 PM)

Question 1) How does the Internet protocol suite documented in [RFC 1122](https://tools.ietf.org/html/rfc1122) map to the OSI Model?



Question 2) At what layers of the OSI Model does the ARP protocol function?

ARP functions at both the Data Link layer (MAC Addresses) and Network layer (IP Addresses).

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

The Cane and Abel program was used on the Windows device to perform the MitM attack. I’ll accept Canary (Pre-Trojan) as well since it was listed at the top of the window running in the video.

Question 4) Why was the telnet password harder to obtain in the Wireshark data?

Because the telnet password shows up in multiple packets (frames) in the Wireshark capture data.

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)?

No, ARP cache poisoning only works on an individual network as ARP is broadcast based and broadcast traffic does not span a router.

Question 6) Can you poison the ARP cache using IPv6? Why?

No. ARP is replaced in IPv6 with Neighbor Discovery Protocol (NDP) and it will determine neighboring hosts.

Question 7) List two ways to prevent the MitM Attack using ARP Cache Poisoning?

Here are a few answers that are acceptable:

1. Enable DHCP Snooping and Dynamic ARP Inspection on the network switches.
2. Encrypt all traffic using technology like a VPN or IPSec tunnel.
3. Migrate to IPv6.