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

Layer 5, 6 and 7 are equivalent to the 4th layer – the application layer in TCP/IP model.
Layer 4 is the same as the 3rd layer – the transport layer.
Layer 3 is equivalent to the 2nd layer- internet.
Layer 1 and 2 are equivalent to the 1st layer – network access.
And in both models, data is divided into packets and each packet may take the individual route from the source to destination.

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

ARP protocol functions at layer 2 and layer 3 since layer 2 contains the MAC address and the IP address exists on layer 3.

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

cain and abel

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

Unlike the other protocols like ftp which sent the password in one packet, telnet send every letter in the password in a separate packet.

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 it is not possible if the devices are on separate networks.

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

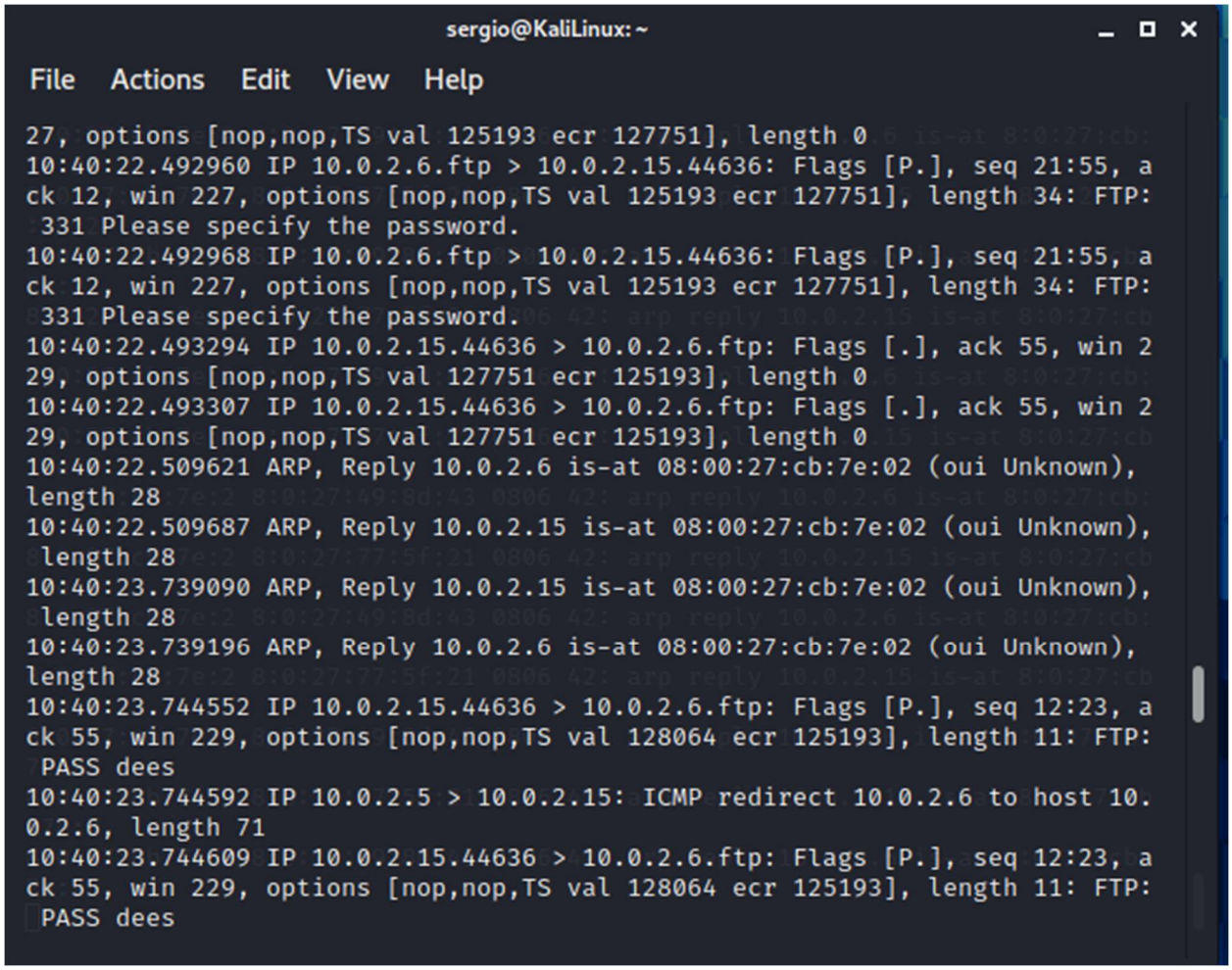
No, you cannot poison the ARP cache in IPv6 since there is no ARP in IPv6.

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

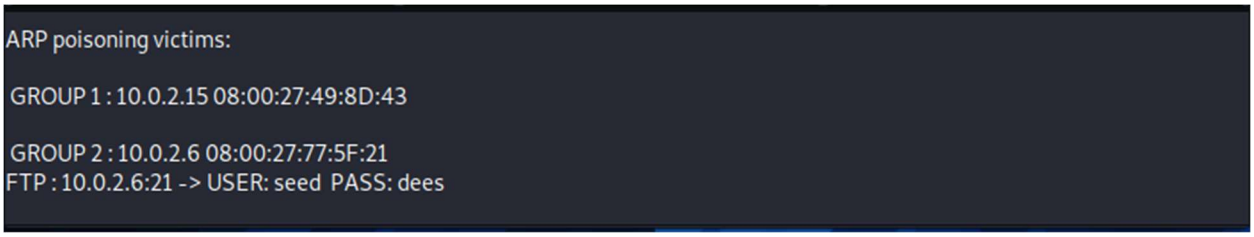
Use a virtual private network.

Avoid using IP trust relationships.

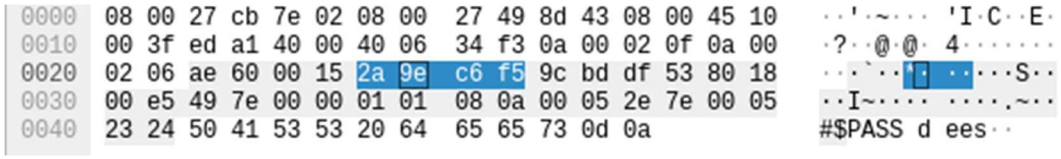
Screen Shot 1) Take a snip of the screen to show you found the password used to FTP using tcpdump.



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



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


0000 08 00 27 cb 7e 02 08 00 27 49 8d 43 08 00 45 10
0010 00 3f ed a1 40 00 40 06 34 f3 0a 00 02 0f 0a 00
0020 02 06 ae 60 00 15 2a 9e c6 f5 9c bd df 53 80 18
0030 00 e5 49 7e 00 00 01 01 08 0a 00 05 2e 7e 00 05
0040 23 24 50 41 53 53 20 64 65 65 73 0d 0a
#$PASS d ees