Question 1 ***DHCP and ARP*** **()**

Recall that DHCP (Dynamic Host Configuration Protocol) is responsible for setting up configurations when a computer first joins a local network.

Assume that Alice wants to connect to the network, but she's missing a configuration. You want to supply a forged configuration to Alice, causing packets that she intends to send to the network to be sent to you instead.

For this part, assume that your computer has IP address 10.10.10.66 and the network's router and DHCP server have IP address 10.10.10.5. There are no other machines on the network and there are no reserved or private IP addresses.

Q1.1 Alice broadcasts a request for a configuration to everyone.

What values of the assigned IP address and the router's IP address could you include in your response to Alice in order to cause packets that she intends to send to the network to be sent to you instead?

Q1.2 Imagine that you supply the correct router's IP address in your forged configuration offer to Alice. What other vulnerabilities exist in the DHCP protocol that would still allow you to become a man-in-the-middle attacker?

Now recall that ARP, the Address Resolution Protocol, translates Layer 3 IP addresses into Layer 2 MAC addresses.

For this part, imagine that Alice has successfully obtained a configuration from the network's router and now she wants to communicate with Bob, whose computer is on the same LAN network.

Alice knows Bob's IP address but wants to learn his MAC address. You want to convince Alice that your MAC address (and not Bob's) corresponds to Bob's IP address, causing messages intended for Bob to be sent to you instead. You, Alice, and Bob are part of the same LAN network and, apart from the router, there are no other machines on the network.

Assume that your computer has IP address 10.10.10.66 and your MAC address is 66:66:66:66:66:66, Alice's IP address is 10.10.10.77 and her MAC address is 77:77:77:77:77:77, and Bob's IP address is 10.10.10.88 and his MAC address is 88:88:88:88:88:88. The network router's IP address is 10.10.10.5.

Q1.1 Alice broadcasts to everyone else on the LAN: "What is the MAC address of 10.10.10.88?" Recall that 10.10.10.88 corresponds to Bob's IP address.

What values for the IP and MAC address could you include in your response to Alice to cause her messages intended for Bob to be sent to you instead?

Q1.2 How would your spoofed response to Alice change if Bob was outside the LAN that you and Alice are both part of?

Q1.3 Which defenses exist against such an ARP-spoofing attack?

Q1.4 You decide to use a network switch to prevent further ARP spoof attacks.

Explain how a network switch prevents such attacks in the following two cases: (1) the switch knows Bob's IP to MAC address mapping and (2) the switch does **not** know Bob's IP to MAC address mapping.

Question 2 ***WPA2-PSK*** **()**

Recall that WPA2-PSK (Wi-Fi Protected Access: Pre-Shared Key) is a protocol that enables secure communications over a Wi-Fi network by encrypting messages with cryptography.

For each of the following questions, assume that Mallory is trying to attack a Wi-Fi network secured with the standard WPA2-PSK protocol.

Q2.1 How does the access point and the client derive the PSK (Pre-Shared Key)?

Q2.2 Assume that Mallory can observe the unencrypted data sent as part of the 4-way WPA handshakes between the clients and the access point. Which values does Mallory need to perform a brute-force search for the Wi-Fi password? Select all that apply.

- ☐ (G) ANonce
- ☐ (H) SNonce
- ☐ (I) PSK
- ☐ (J) PTK
- ☐ (K) GTK
- ☐ (L) The router's MAC address
- ☐ (M) The client's MAC address
- ☐ (N) The MICs

Q2.3 Now imagine that Mallory is trying to masquerade as the access point in order to launch a Man-in-the-Middle (MITM) against Alice, who is trying to join the Wi-Fi network. How can Mallory trick Alice into thinking that she is the access point?

Q2.4 What can Mallory do after successfully brute-forcing the Wi-Fi password? Select all that apply.

- ☐ (G) Perform on-path network attacks against victims in the same Wi-Fi network.
- ☐ (H) Decrypt network traffic encrypted with the PTK of a user who joins the network after you.
- ☐ (I) Decrypt network traffic encrypted with the GTK
- ☐ (J) Decrypt TLS network traffic.
- ☐ (K) None of the above.
- ☐ (L) ——

Q2.5 Assume that Mallory can brute-force the Wi-Fi password in roughly an hour. Which defenses would stop this attack? Select all that apply.

☐ (A) Changing the Wi-Fi password every day.

☐ (B) Using WPA2-Enterprise.

☐ (C) A modern NIDS system.

☐ (D) None of the above.

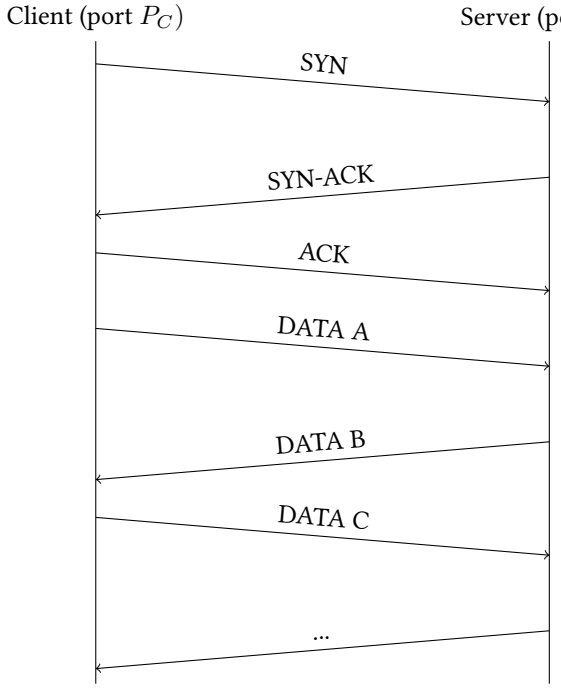
☐ (E) ——

☐ (F) ——

Q2.6 Does WPA-Enterprise offer forward secrecy? If it does, explain how forward secrecy is achieved. If it does not, explain how Mallory can recover the shared PTK (Pairwise Transport Key) after the handshake is complete?

Question 3 ***Attack on TCP*** **()**

Suppose that a client connects to a server, and then performs the following TCP handshake and initial data transfer:



1. Client sends initial SYN with sequence number A (usually random).
2. Server sends SYN-ACK with sequence number B (also usually random) and ACK $A + 1$.
3. Client sends ACK with sequence number $A + 1$ and ACK $B + 1$.
4. Client sends DATA A of length L_A with sequence number $A + 1$ and ACK $B + 1$.
5. Server sends DATA B of length L_B with sequence number $B + 1$ and ACK $A + 1 + L_A$.
6. Client sends DATA C of length L_C with sequence number $A + 1 + L_A$ and ACK $B + 1 + L_B$.
7. Data exchange continues until both sides are done sending data.

Q3.1 Assume that the next transmission in this connection will be DATA D from the server to the client. What will this packet look like?

Sequence number:	_____	ACK:	_____
Source port:	P_S	Destination port:	P_C
Length:	L_D	Flags:	ACK

Q3.2 You should be familiar with the concept and capabilities of a *man-in-the-middle* as an attacker who **can observe** and **can modify** traffic. There are two other types of relevant attackers in this scenario:

1. *On-path* attacker: **can observe** traffic but **cannot modify** it.
2. *Off-path* attacker: **cannot observe** traffic and **cannot modify** it.

Carol is an *on-path* attacker. Can Carol do anything malicious to the connection? If so, what can she do?

Q3.3 David is an *off-path* attacker. Can David do anything malicious to the connection? If so, what can he do?

Q3.4 The client starts getting responses from the server that don't make any sense. Inferring that David is attempting to hijack the connection, the client then immediately sends the server a **RST** packet, which terminates the ongoing connection. David wants to impersonate the client by establishing a new connection. How would he go about doing this?