Q1 *Hackerman Visits the Voting Booth (FA20 Final Q11)* **(21 points)**

Your sketchy friend asks you to use your CS 161 skills to help him rig some sort of election. He hands you a business card with credentials for a Russian supercomputer.

Armed with massive computing power, you show up to the Caltopia polling center. It has a Wi-Fi network secured with standard WPA2-PSK.

Q1.1 (5 points) You observe a WPA 4-way handshake. Which values from the handshake are needed to perform a brute-force search for the Wi-Fi password? Select all that apply.

- ☐ (A) ANonce
- ☐ (B) SNonce
- ☐ (C) The router's MAC address
- ☐ (D) The client's MAC address
- ☐ (E) The MICs
- ☐ (F) None of the above

Q1.2 (4 points) What can you 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) None of the above
- ☐ (K) ——
- ☐ (L) ——

Q1.3 (3 points) Which defenses would stop your attack? Select all that apply.

- ☐ (A) Changing the Wi-Fi password every day
- ☐ (B) Using WPA2-Enterprise
- ☐ (C) None of the above
- ☐ (D) ——
- ☐ (E) ——
- ☐ (F) ——

You arrive at the New Blackwell City polling center. It also has a Wi-Fi network secured with standard WPA2-PSK.

You walk up to a poll worker, claim that you're a fellow poll worker, and ask for the Wi-Fi password. They write the password on a post-it note and give it to you.

Q1.4 (3 points) Which security principle is most closely related to your experience at this polling place?

- ◯ (G) Consider Shannon's maxim
- ◯ (H) Least privilege
- ◯ (I) Security is economics
- ◯ (J) Consider human factors
- ◯ (K) Defense in depth
- ◯ (L) Time of check to time of use

At the Campanile City polling center, you see a DHCP Discover message broadcast to everyone.

Assume your computer has IP address `10.10.10.142`, and the network's router and DHCP server have IP address `10.10.10.5`. Assume that there are no other machines on the network. Assume there are no reserved or private IP addresses.

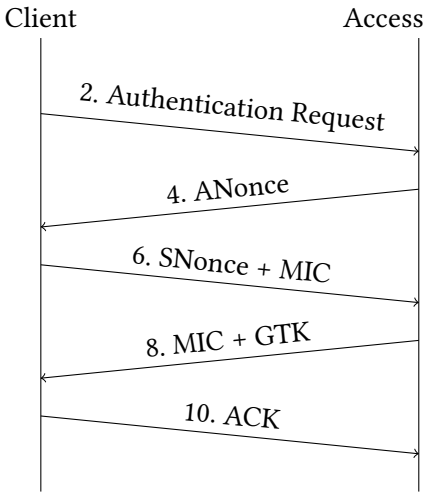
You want to return a malicious DHCP Offer that would make you a MITM. What values of the assigned IP address and the gateway IP address could you use in your response?

Q1.5 (3 points) Assigned IP address:

Q1.6 (3 points) Gateway IP address:

Q2 *I am Inevitable (SP22 Final Q10)* **(20 points)**

Recall the WPA 4-way handshake from lecture:



1. Client and AP derive the PSK from SSID and password.
3. AP randomly chooses ANonce.
5. Client randomly chooses SNonce and derives PTK.
7. AP derives PTK and verifies the MIC.
9. Client verifies the MIC.

For each method of client-AP authentication, select all things that the given adversary would be able to do. Assume that:

- The attacker does not know the WPA-PSK password but that they know that client's and AP's MAC addresses.
- For rogue AP attacks, there exists a client that knows the password that attempts to connect to the rogue AP attacker.
- The AMAC is the Access Point's MAC address and the SMAC is the Client's MAC address.

Q2.1 (5 points) The client and AP perform the WPA 4-way handshake with the following modifications:

- $\mathsf{PTK} = F(\mathsf{ANonce}, \mathsf{SNonce}, \mathsf{AMAC}, \mathsf{SMAC}, \mathsf{PSK})$, where F is a secure key derivation function
- $\mathsf{MIC} = \mathsf{PTK}$

☐ An on-path attacker that observes a successful handshake can decrypt subsequent WPA messages without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can trick the AP into completing a new handshake without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can learn the PSK without brute force.

☐ A rogue AP attacker can learn the PSK without brute force.

☐ A rogue AP attacker can only learn the PSK if they use brute force.

☐ None of the above

Q2.2 (5 points) The client and AP perform the WPA 4-way handshake with the following modifications:

- $\mathsf{PTK} = F(\mathsf{ANonce}, \mathsf{SNonce}, \mathsf{AMAC}, \mathsf{SMAC})$, where F is a secure key derivation function
- $\mathsf{MIC} = \mathsf{HMAC}(\mathsf{PTK}, \text{Dialogue})$

☐ An on-path attacker that observes a successful handshake can decrypt subsequent WPA messages without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can trick the AP into completing a new handshake without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can learn the PSK without brute force.

☐ A rogue AP attacker can learn the PSK without brute force.

☐ A rogue AP attacker can only learn the PSK if they use brute force.

☐ None of the above

Q2.3 (5 points) The client and AP perform the WPA 4-way handshake with the following modifications:

- Authentication: Client sends $\mathsf{H}(\mathsf{PSK})$ to AP, where H is a secure cryptographic hash.
- Verification: AP compares $\mathsf{H}(\mathsf{PSK})$ and to the value it received.
- AP sends: $\mathsf{Enc}(\mathsf{PSK}, \mathsf{PTK})$ to client, where Enc is an IND-CPA secure encryption algorithm.

☐ An on-path attacker that observes a successful handshake can decrypt subsequent WPA messages without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can trick the AP into completing a new handshake without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can learn the PSK without brute force.

☐ A rogue AP attacker can learn the PSK without brute force.

☐ A rogue AP attacker can only learn the PSK if they use brute force.

☐ None of the above

Q2.4 (5 points) The client and AP perform the WPA 4-way handshake with the following modifications:

- Authentication: Client conducts a Diffie-Hellman exchange with the AP to derive a shared key K.
- Client sends: $\mathsf{Enc}(K, \mathsf{PSK})$ to the AP.
- Verification: Check if $\mathsf{Dec}(K, \text{Ciphertext})$ equals the PSK
- Upon verification, AP sends: $\mathsf{Enc}(\mathsf{K}, \mathsf{PTK})$, where PTK is a random value, and sends it to the client.
- Assume that Enc is an IND-CPA secure encryption algorithm.

☐ An on-path attacker that observes a successful handshake can decrypt subsequent WPA messages without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can trick the AP into completing a new handshake without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can learn the PSK without brute force.

☐ A rogue AP attacker can learn the PSK without brute force.

☐ A rogue AP attacker can only learn the PSK if they use offline brute force.

☐ None of the above