WI-FI TRAINING
MODULE 6 ASSESSMENT

1. **What are the pillars of Wi-Fi Security ?**

The security of a Wi-Fi network relies on several fundamental pillars that work together to protect data and prevent unauthorized access. Here are the key pillars of Wi-Fi security:

1. Authentication and Access Control

- **Purpose:** Verifies the identity of users and devices attempting to connect to the network and controls their level of access.
- **Mechanisms:**
    - **Passwords/Passphrases (Pre-Shared Key - PSK):** The most common method for home and small business networks. Users enter a password to gain access. Strong, unique passwords are crucial.
    - **802.1X Authentication:** An enterprise-level authentication framework that provides more robust security. It often involves a RADIUS (Remote Authentication Dial-In User Service) server to centrally manage user credentials and access policies. This allows for individual user accounts and more granular control.
    - **MAC Address Filtering:** While not a strong security measure on its own, it can add a minor layer of control by allowing only devices with pre-approved MAC (Media Access Control) addresses to connect. However, MAC addresses can be easily spoofed.
    - **Captive Portals:** Often used in public Wi-Fi hotspots, these require users to agree to terms of service or provide credentials via a web page before granting internet access.

2. Encryption

- **Purpose:** Protects the confidentiality of data transmitted over the wireless network by scrambling it, making it unreadable to unauthorized individuals.
- **Protocols (in order of increasing security):**
    - **WEP (Wired Equivalent Privacy):** An outdated and highly vulnerable protocol. It should no longer be used.
    - **WPA (Wi-Fi Protected Access):** An improvement over WEP but also has known vulnerabilities.
    - **WPA2 (Wi-Fi Protected Access 2):** The most widely used and generally considered secure protocol. It uses the Advanced Encryption Standard (AES) for strong encryption.
    - **WPA3 (Wi-Fi Protected Access 3):** The latest and most secure protocol, offering enhanced encryption (using Galois/Counter Mode Protocol - GCMP), stronger authentication (Simultaneous Authentication of Equals - SAE), and improved security for open networks (Opportunistic Wireless Encryption - OWE).

3. Network Segmentation

- **Purpose:** Divides a network into smaller, isolated segments to limit the impact of a security breach. If one segment is compromised, it prevents attackers from easily moving laterally to other critical parts of the network.
- **Implementation:** Creating separate networks for different user groups (e.g., employees, guests, IoT devices) or functions. This can often be achieved using features like VLANs (Virtual Local Area Networks).

4. Secure Network Design and Configuration

- **Purpose:** Minimizing vulnerabilities through careful planning and setup of the wireless infrastructure.
- **Best Practices:**
    - **Changing Default Credentials:** Always change the default username and password of the router's administrative interface.
    - **Disabling SSID Broadcast:** Hiding the network name (SSID) can offer a minor level of obscurity, but it doesn't prevent determined attackers.
    - **Strategic Placement of Access Points:** Optimizing coverage and minimizing signal leakage outside the intended area.
    - **Firewall Configuration:** Enabling and properly configuring the firewall on the wireless router to control incoming and outgoing network traffic.
    - **Disabling Remote Management:** Unless necessary, disable the ability to manage the router remotely from the internet.
    - **Keeping Firmware Updated:** Regularly updating the router's firmware to patch security vulnerabilities.

5. Monitoring and Intrusion Detection/Prevention

- **Purpose:** Detecting and responding to suspicious activity or unauthorized access attempts on the network.
- **Mechanisms:**
    - **Network Monitoring Tools:** Software or hardware that analyzes network traffic for anomalies.
    - **Intrusion Detection Systems (IDS):** Systems that passively monitor network traffic for malicious patterns and generate alerts.
    - **Intrusion Prevention Systems (IPS):** Systems that actively work to block or mitigate detected threats.
    - **Wireless Intrusion Prevention Systems (WIPS):** Specifically designed to detect and prevent threats in wireless environments, such as rogue access points.

6. Security Policies and Procedures

- **Purpose:** Establishing guidelines and best practices for users and administrators to maintain a secure wireless environment.
- **Examples:**

    - Password policies (complexity, rotation).
    - Acceptable use policies for the network.
    - Procedures for connecting new devices.
    - Incident response plans.
    - Regular security awareness training for users.
2. **Explain the difference between encryption and authentication in Wi-Fi security.**

The terms "encryption" and "authentication" represent two distinct but equally crucial pillars of Wi-Fi security.

Authentication: Verifying Who Can Join

- **Purpose:** Authentication is the process of verifying the identity of a user or device attempting to connect to your Wi-Fi network. It's like checking an ID card before allowing someone into a building.
- **Focus:** Ensuring that only authorized users and devices are granted access to the network.
- **Mechanism:** This is typically achieved through:
    - **Passwords/Passphrases (Pre-Shared Key - PSK):** The most common method, where a user must enter the correct password to gain access.
    - **802.1X Authentication:** A more robust, enterprise-level method that often uses a RADIUS server to verify user credentials, allowing for individual accounts and more control.
    - **MAC Address Filtering:** A less secure method that restricts access based on the physical address of a device's network adapter.
    - **Captive Portals:** Web pages that require users to log in or agree to terms before accessing public Wi-Fi. Think of a doorman at a club. Authentication is like the doorman checking your name against the guest list or verifying your membership card before letting you in.

Encryption: Protecting the Data Being Transmitted

- **Purpose:** Encryption is the process of scrambling the data transmitted over the Wi-Fi network to prevent unauthorized individuals from reading it, even if they manage to intercept the wireless signals. It's like sending a secret message written in code.
- **Focus:** Ensuring the confidentiality and privacy of the data being exchanged between connected devices and the wireless router.
- **Mechanism:** This is achieved through various encryption protocols, such as:
    - **WEP (Wired Equivalent Privacy):** An older, insecure protocol that should not be used.
    - **WPA (Wi-Fi Protected Access):** An improvement over WEP but has known vulnerabilities.
    - **WPA2 (Wi-Fi Protected Access 2):** The current standard for most networks, using strong AES encryption.
    - **WPA3 (Wi-Fi Protected Access 3):** The latest and most secure protocol, offering even stronger encryption and authentication methods

3. **Explain the differences between WEP, WPA,WPA2 and WPA3.**

1. WEP (Wired Equivalent Privacy)

- **Introduction:** The first widely adopted wireless security standard, ratified in **September 1999**.
- **Goal:** To provide data confidentiality comparable to wired networks.
- **Encryption:** Uses the RC4 (Rivest Cipher 4) stream cipher with a static key. Initially used 64-bit keys, later expanded to 128-bit.
- **Key Management:** Employs a static encryption key shared among all devices on the network. This key often remained unchanged for extended periods.
- **Security:** Highly insecure and easily crackable. Numerous vulnerabilities were discovered due to its short key lengths and the way keys were generated. Tools to crack WEP keys became widely available.
- **Status: Obsolete and should not be used**. The Wi-Fi Alliance officially retired WEP in 2004. Many modern devices no longer support it.

2. WPA (Wi-Fi Protected Access)

- **Introduction:** Introduced in **2003** as an interim security enhancement to address the significant weaknesses of WEP.
- **Goal:** To provide a more secure wireless connection than WEP without requiring hardware upgrades.
- **Encryption:** Primarily used TKIP (Temporal Key Integrity Protocol), which provided dynamic per-packet keys, making it more secure than WEP's static keys. It could also use WEP's RC4 cipher for backward compatibility.
- **Key Management:** Introduced dynamic key generation and integrity checks, making it harder for attackers to intercept and manipulate data.
- **Security:** A significant improvement over WEP but still has known vulnerabilities. TKIP was eventually found to be susceptible to certain attacks.
- **Status:** Largely superseded by WPA2 and WPA3. While more secure than WEP, it's recommended to use newer protocols if your devices support them.

3. WPA2 (Wi-Fi Protected Access 2)

- **Introduction:** Ratified in **2004** as the next-generation Wi-Fi security standard.
- **Goal:** To provide robust and secure wireless communication.
- **Encryption:** Primarily uses AES (Advanced Encryption Standard), a much stronger and more secure encryption algorithm than RC4. It also included CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for data integrity.
- **Key Management:** Continued using dynamic key generation and offered two modes:
    - **WPA2-Personal** (PSK - Pre-Shared Key)**:** Uses a shared password for authentication, common for home and small office networks.
    -
    - **WPA2-Enterprise:** Uses 802.1X authentication with a RADIUS server for more robust authentication and individual user credentials, suitable for larger organizations.

- **Security:** Generally considered secure and the most widely supported standard for many years. However, it was found to be vulnerable to the KRACK (Key Reinstallation Attack) in 2017. While patches were released to address this, it highlighted the need for further security advancements.
- **Status:** Remains a widely used and generally secure option, especially when devices don't support WPA3. Ensure your devices and router firmware are updated to address known vulnerabilities.

4. WPA3 (Wi-Fi Protected Access 3)

- **Introduction:** Announced by the Wi-Fi Alliance in 2018 to address the shortcomings of WPA2 and provide even stronger security.
- **Goal:** To simplify Wi-Fi security, provide more robust authentication, and increase cryptographic strength.
- **Encryption:** Uses GCMP (Galois/Counter Mode Protocol), offering stronger encryption than WPA2's CCMP. It also mandates the use of Protected Management Frames (PMF) to protect against disassociation attacks. It uses longer encryption keys (192-bit in Personal mode and 256-bit in Enterprise mode).
- **Key Management:** Introduces SAE (Simultaneous Authentication of Equals), a more secure handshake method that replaces PSK in Personal mode, offering better protection against brute-force and dictionary attacks, even if a weak password is used. It also offers individualized data encryption, providing a unique encryption key for each data transmission. For open networks, it offers OWE (Opportunistic Wireless Encryption), which automatically encrypts the connection between the device and the access point, enhancing privacy on public Wi-Fi.
- **Security:** The most secure Wi-Fi security protocol currently available, offering significant improvements in authentication and encryption compared to its predecessors. It provides enhanced protection against various attacks.
- **Status:** Adoption is growing, but compatibility issues with older devices can still be a factor. If your devices and router support WPA3, it is the recommended option for the best security.

4. Why is WEP considered insecure compared to WPA2 and WPA3?

WEP (Wired Equivalent Privacy) is considered highly insecure compared to WPA2 (Wi-Fi Protected Access 2) and WPA3 (Wi-Fi Protected Access 3) due to several fundamental weaknesses in its design.

1. Weak Encryption Algorithm (RC4):

- WEP relies on the **RC4 stream cipher**, which was found to have significant cryptographic flaws shortly after WEP's introduction.
- These flaws allow attackers to **predict the keystream** used for encryption, enabling them to decrypt data packets without needing the WEP key.

2. Short and Static Encryption Keys:

- WEP initially used **64-bit keys**, which were later expanded to **128-bit**. However, the effective key length was often shorter due to the inclusion of the Initialization Vector (IV).
- The **encryption key was static**, meaning it remained the same for all devices and all communication sessions. Once compromised, an attacker could decrypt all past and future traffic.

3. Predictable and Small Initialization Vector (IV):

- WEP uses a **24-bit Initialization Vector (IV)**, which is transmitted in plaintext with each encrypted packet. The IV is intended to prevent the reuse of keystreams.
- However, the **small size of the IV leads to frequent reuse**, especially on busy networks. Attackers can collect packets with the same IV and use statistical methods to determine the encryption key. This is the basis of well-known WEP cracking techniques.

4. Lack of Robust Key Management:

- WEP lacks a proper mechanism for **automatic key rotation or management**. Keys were often manually configured and rarely changed, increasing the window of opportunity for attackers.

5. Weak Integrity Checks (CRC-32):

- WEP uses a simple **CRC-32 checksum** for data integrity. This method is insufficient to prevent attackers from **altering data packets** and recalculating the checksum, allowing for packet injection and manipulation.

In contrast, WPA2 and WPA3 address these weaknesses significantly:

WPA2:

- **Stronger Encryption (AES):** WPA2 primarily uses the **Advanced Encryption Standard (AES)** with the **CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)**. AES is a much more robust and secure encryption algorithm than RC4 and is significantly harder to crack.
- **Dynamic Key Management:** WPA2 implements a **Temporal Key Integrity Protocol (TKIP)** (though sometimes still uses RC4 for backward compatibility) or, more securely, uses a robust **four-way handshake** to establish unique session keys for each connection and periodically re-key. This prevents a single compromised key from jeopardizing all communication.
- **Stronger Integrity Checks (MIC):** WPA2 uses a **Message Integrity Check (MIC)**, which is cryptographically stronger than CRC-32, making it much harder for attackers to tamper with data packets without detection.

WPA3:

- **Even Stronger Encryption (GCMP):** WPA3 uses **GCMP (Galois/Counter Mode Protocol)**, which offers enhanced encryption and authentication compared to

WPA2's CCMP. It also mandates the use of **Protected Management Frames (PMF)** to prevent disassociation attacks.

- **Improved Authentication (SAE):** WPA3 introduces **SAE (Simultaneous Authentication of Equals)**, also known as Dragonfly, which provides a more secure handshake process resistant to offline dictionary attacks, even with weak passwords.
- **Individualized Data Encryption:** WPA3 offers **individualized data encryption** for each connected device, enhancing privacy.
- **Enhanced Open (OWE):** For open Wi-Fi networks, WPA3 offers OWE (Opportunistic Wireless Encryption), which automatically encrypts the connection, providing a level of privacy not present in unencrypted open networks.

5. Why was WPA2 introduced?

WPA2 (Wi-Fi Protected Access 2) was introduced in 2004 primarily to address the significant and well-documented security vulnerabilities of its predecessor, WEP (Wired Equivalent Privacy).

1. Fundamental Weaknesses in WEP's Encryption:

- **Weak Encryption Algorithm (RC4):** WEP relied on the RC4 stream cipher, which cryptographers quickly discovered had significant flaws. These flaws allowed attackers to predict the keystream used for encryption, making decryption of data packets relatively easy once enough packets were captured.
- **Short and Static Encryption Keys:** WEP used short (64-bit or 128-bit) static keys. These keys remained the same for all devices and all communication, making them prime targets for cracking. Once the key was compromised, the entire network's traffic could be decrypted.
- **Predictable and Small Initialization Vector (IV):** WEP used a 24-bit IV, transmitted in plaintext. The small size led to frequent reuse of IVs on busy networks. Attackers could exploit this IV reuse to correlate encrypted packets and eventually deduce the WEP key. This was the basis of effective WEP cracking techniques.

2. Lack of Robust Key Management:

- WEP lacked a mechanism for automatic key rotation. Keys were often manually configured and rarely changed, increasing the risk of compromise over time.

3. Weak Integrity Checks (CRC-32):

- WEP used a simple CRC-32 checksum for data integrity, which was insufficient to prevent attackers from altering data packets and recalculating the checksum, allowing for packet injection.

In essence, WEP was designed with flawed cryptographic principles and lacked the necessary mechanisms to withstand even moderately sophisticated attacks. As these vulnerabilities became widely known and tools to exploit them became readily available, the need for a more secure standard became critical.

WPA2 was designed as a significant security upgrade, addressing WEP's weaknesses by:

- **Implementing Stronger Encryption (AES):** WPA2 primarily uses the Advanced Encryption Standard (AES) with the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES is a much more robust and secure encryption algorithm than RC4.
- **Introducing Dynamic Key Management:** WPA2 uses a four-way handshake to establish unique session keys for each connection and periodically re-key. This prevents a single compromised key from jeopardizing all communication.
- **Employing Stronger Integrity Checks (MIC):** WPA2 uses a Message Integrity Check (MIC), which is cryptographically stronger than CRC-32, making data tampering much more difficult to achieve without detection.

6. What is the role of Pairwise Master Key in the 4 way handshake?

- PMK (Pair-wise Master Key) is a cryptographic concept used in wireless networks to establish secure communication between devices. It plays a vital role in ensuring confidentiality and integrity of data transmission. PMK is derived from a pre-shared key (PSK) or another authentication mechanism, and it serves as the foundation for generating encryption keys for pairwise communication.
- In wireless networks, such as Wi-Fi, the PMK is primarily used in the IEEE 802.11i standard, also known as WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key). WPA2-PSK is a widely adopted security protocol that enables secure wireless communication for home and small business networks.
- The process of generating pairwise keys from the PMK involves a four-way handshake between the client and the AP.
- **PMK Generation:** Initially, during the network setup or configuration, the PMK is established. It can be a pre-shared key manually configured on both the client device and the AP or obtained through an authentication mechanism like EAP (Extensible Authentication Protocol).
- **Authentication:** When a client device wants to connect to an AP, it initiates the authentication process. The AP authenticates the client's identity using the PMK.
- **Four-Way Handshake:** Once the client is authenticated, a four-way handshake begins to establish the pairwise keys. This handshake involves a series of messages exchanged between the client and the AP.
- **a. Message 1 (Client to AP):** The client sends a message to the AP, indicating its intent to connect and initiating the handshake process. This message includes the client's identity, the authentication algorithm used, and a randomly generated value called the ANonce (Authenticator Nonce).
- **b. Message 2 (AP to Client):** The AP responds with a message containing its identity, the authentication algorithm used, a randomly generated value called the SNonce (Supplicant Nonce), and the Group Temporal Key (GTK).
- **c. Message 3 (Client to AP):** The client sends another message, which includes the PMKID (PMK Identifier), the ANonce, and the SNonce. This message is also protected by a key derived from the PMK.

- **d. Message 4 (AP to Client):** Finally, the AP sends the last message containing the GTK, encrypted using a key derived from the PMK. This message confirms the successful establishment of the pairwise keys.
- **Pairwise Key Derivation:** After the four-way handshake, both the client and the AP have exchanged the necessary information to derive the pairwise keys. These keys are generated using a key derivation function, which takes the PMK, the ANonce, the SNonce, and other parameters as inputs.
- The derived pairwise keys are used to encrypt and decrypt the data transmitted between the client and the AP. Each client-device pair has its unique pairwise key, ensuring that the communication is secure and isolated from other devices within the network.
- By using PMK and pairwise keys, WPA2-PSK provides a robust security mechanism for wireless networks. It ensures that even if an attacker gains access to one pairwise key, they cannot decrypt the communication of other devices in the network.

7. What happen if we put a wrong passphrase in a four way handshake?

If we enter the wrong passphrase during the four-way handshake in a WPA2 or WPA3 network, the authentication process will fail. Here's a breakdown of what happens at each step:

1. Initial Association: Your device will likely be able to *associate* with the Wi-Fi Access Point (AP). Association is the process of establishing a basic connection at the link layer, where your device and the AP agree to communicate. This step doesn't involve the passphrase yet.

2. Four-Way Handshake Initiation (Message 1): The AP sends an **ANonce** (Authenticator Nonce) to your device (the supplicant). Your device receives this.

3. Supplicant Response (Message 2): Your device now needs to prove it knows the correct passphrase (which is used to derive the PMK - Pairwise Master Key). It does the following:

* Derives a **PTK (Pairwise Transient Key)** using its stored PMK (derived from the incorrect passphrase), the ANonce from the AP, and its own random number called **SNonce** (Supplicant Nonce), along with the MAC addresses of both devices.

* Calculates a **Message Integrity Code (MIC)** over the message using a portion of the derived PTK (the Key Confirmation Key - KCK).

* Sends a message containing the SNonce and the MIC to the AP.

4. AP Verification (Message 3): The AP receives this message and performs the following:
* It also attempts to derive the PTK using *its* PMK (derived from the correct passphrase), the received ANonce and SNonce, and the MAC addresses.

* It calculates its *own* MIC over the received message using its derived PTK's KCK.

* Crucially, the AP compares the MIC it calculated with the MIC received from your device.

5. Authentication Failure (Message 3 and Beyond):

* Since the MICs don't match, the AP **knows** that your device doesn't possess the correct PMK (and therefore the correct passphrase).

* The AP will **not** proceed with the handshake. It will typically **not** send Message 3 (which contains the Group Transient Key - GTK for multicast/broadcast encryption).

* Your device will likely receive no further valid handshake messages.

* The authentication will **fail**, and your device will **not be granted access** to the network.