MODULE 6 ASSIGNMENT – WIFI TRAINING

1) What are the pillars of Wi-Fi security?

1. **Encryption**:

- **Purpose**: Protects the data being transmitted over the network.
- **Example**: **WPA3** uses stronger encryption methods (like **AES**) to ensure that even if the data is intercepted, it cannot be read easily.
- **Why it's important**: Prevents eavesdropping by unauthorized users.

2. Authentication:

- **Purpose**: Ensures that only authorized users and devices can access the network.
- **Example**: **WPA3** uses **Simultaneous Authentication of Equals (SAE)** for more secure device authentication, preventing brute-force attacks.
- **Why it's important**: Ensures that only trusted devices can connect to the network.

3. Access Control:

- **Purpose**: Manages who can connect to the Wi-Fi network and what they can access once connected.
- **Example**: **MAC address filtering**, **802.1X** network access control for enterprise-level security.
- **Why it's important**: Restricts network access to specific, trusted devices.

4. Network Segmentation:

- **Purpose**: Divides the network into smaller, isolated segments for better control.
- **Example**: **Guest networks** for visitors, **IoT networks** separate from sensitive data networks.
- **Why it's important**: Limits the damage of a potential breach to a specific segment and keeps critical assets safe.

5. Integrity:

- **Purpose**: Ensures that the data hasn't been altered during transmission.
- **Example**: **Message Integrity Codes (MICs)** are used in WPA3 to ensure data integrity.
- **Why it's important**: Prevents data tampering and ensures the authenticity of communication.

6. Key Management:

- **Purpose**: Manages the secure exchange and refresh of encryption keys to maintain security.
- **Example**: **Dynamic encryption keys** in WPA3 to avoid the risks of reusing the same key.

- **Why it’s important**: Keeps encryption keys fresh and harder to crack over time.

2) Explain the difference between authentication and encryption in WiFi security.

Authentication:

- **Purpose**: Verifies the **identity** of devices or users trying to connect to the Wi-Fi network.
- **What it does**:
    - Ensures that only authorized devices or users can access the network.
    - Involves checking credentials (like a password, certificate, or device identifier).
- **Example**:
    - **WPA2/WPA3** use **Pre-Shared Key (PSK)** or **802.1X** for authentication to verify that the connecting device is allowed to join.
- **Why it's important**: Prevents unauthorized access and protects the network from being hijacked by unknown or malicious devices.

Encryption:

- **Purpose**: Protects the **data** being transmitted over the Wi-Fi network.
- **What it does**:
    - Scrambles the data being sent between devices and the router, making it unreadable to anyone who intercepts it.
    - Uses an encryption key (e.g., **AES** in WPA2/WPA3) to encode the data.
- **Example**:
    - **WPA2** and **WPA3** use **AES encryption** to secure the data sent between the device and the access point.
- **Why it's important**: Prevents **eavesdropping** and **data theft** by ensuring that intercepted data is unreadable.

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

Feature	WEP	WPA	WPA2	WPA3
Encryption	RC4	TKIP	AES	AES (stronger)
Authentication	Shared Key	PSK/802.1X	PSK/802.1X	SAE (stronger)
Security	Weak	Better than WEP	Strong	Strongest
Use Today	**Not recommended**	**Outdated**	**Common**	**Recommended**

4) Why is WEP considered insecure compared to WPA2 or WPA3?

1. Weak Encryption (RC4):

- **WEP** uses the **RC4 stream cipher** for encryption, which is **easy to break** using modern tools.
- **WPA2/WPA3** use **AES (Advanced Encryption Standard)**, which is **much stronger** and resistant to known attacks.

2. Static Encryption Keys:

- In **WEP**, the **encryption key** is **static** (doesn't change), meaning once it's cracked, **all data** can be decrypted.
- **WPA2/WPA3** use **dynamic key generation** (like **TKIP** for WPA and **AES** for WPA2/WPA3), making it much harder to crack and ensuring stronger **security over time**.

3. Vulnerable to Replay Attacks:

- **WEP** is vulnerable to **replay attacks**, where intercepted data can be **replayed** to the network to gain unauthorized access.
- **WPA2/WPA3** have improved **message integrity** (via **MIC** or **Integrity Check**), preventing this type of attack.

4. Short Key Length (Weaknesses in Key Management):

- **WEP** typically uses **40-bit or 104-bit keys**, which are **short** and **easily guessed** by modern computing power.
- **WPA2/WPA3** use **longer keys** and more sophisticated **key management** techniques to ensure the integrity and strength of encryption.

5. Vulnerability to Dictionary and Brute-Force Attacks:

- **WEP** is highly vulnerable to **brute-force attacks** (trying all possible keys) because of weak key management and low-key lengths.
- **WPA2/WPA3** use more advanced **authentication methods** (e.g., **SAE** in WPA3), which make brute-force or dictionary attacks much **harder**.

6. Lack of Modern Security Features:

- **WEP** lacks support for modern security techniques, such as **forward secrecy** (ensures session keys are not reused) and **improved authentication methods**.
- **WPA2/WPA3** introduce **stronger handshakes**, **automatic key rotation**, and more robust **encryption** for **data protection**.

5) Why was WPA2 introduced?

WPA2 was introduced to address the security weaknesses of **WPA** and **WEP**:

1. WEP's Weaknesses:

- **WEP** (Wired Equivalent Privacy) had **serious vulnerabilities** that made it **easy to crack** using modern tools, as its **RC4 encryption** was weak.
- **Static keys** in WEP made it easy for attackers to decrypt traffic once they captured enough data.
- **WEP** was not providing **sufficient protection** for the increasing demand for **secure Wi-Fi networks**.

2. WPA's Shortcomings:

- While **WPA** (Wi-Fi Protected Access) was an improvement over WEP, it still used the **TKIP (Temporal Key Integrity Protocol)**, which was also found to have **weaknesses** and was eventually phased out.
- WPA still did not offer the **strongest possible encryption**.

3. Introducing WPA2 with AES Encryption:

- **WPA2** replaced **TKIP** with **AES (Advanced Encryption Standard)**, which is much **stronger** and **more secure**.
- **AES** is a **government-approved encryption standard** and is far more resistant to attacks compared to RC4 (used in WEP) and TKIP (used in WPA).
- WPA2 was designed to **address the shortcomings** of WPA and provide **long-term security** for wireless networks.

4. Future-proofing Wi-Fi Security:

- WPA2 also supported **stronger authentication methods**, like **802.1X** for enterprise networks, which provided better user authentication and **network access control**.
- By adopting AES, WPA2 set a new **standard for Wi-Fi security** that would **last for many years** (until the introduction of WPA3 in 2018).

6) What is the role of the Pairwise Master Key (PMK) in the 4-way handshake?

What is the 4-Way Handshake?

The **4-way handshake** is a key exchange process used in **WPA2** (and **WPA3**) to **establish a secure connection** between a **client (supplicant)** and the **access point (AP)** after the device tries to connect to the Wi-Fi network.

Role of the Pairwise Master Key (PMK):

1. **PMK as the Root Key**:
    - The **Pairwise Master Key (PMK)** is a **shared secret key** that is derived during the **authentication process** (either from a **Pre-Shared Key (PSK)** in WPA2-Personal or **802.1X** in WPA2-Enterprise).
    - It's the starting point of the **4-way handshake** and is used to generate all further encryption keys for securing the session.
2. **Key Derivation**:
    - The PMK is used to generate additional keys during the handshake, specifically:
        - **PTK (Pairwise Transient Key)**: A key used for encrypting data traffic between the client and the AP.
        - **GTK (Group Temporal Key)**: A key used for group broadcast communication.
3. **Handshake Steps**:
    - **Step 1**: The client and AP already share the **PMK** (via PSK or 802.1X).
    - **Step 2**: The AP sends a **nonce (random number)** to the client.
    - **Step 3**: The client generates a **second nonce**, combines it with the **PMK**, and computes the **Pairwise Transient Key (PTK)**, which will be used for encrypting data between the client and AP.
    - **Step 4**: The AP and client confirm that they both have the same PTK and finalize the handshake.

7) How does the 4-way handshake ensure mutual authentication between the client and the access point?

Step 1: AP Sends a Nonce to the Client:

- The AP sends a **random number (nonce)** to the client. This **nonce** is used to ensure that the handshake is **unique** each time and prevents replay attacks.
- The AP doesn't yet authenticate the client — it's only sending information for **key generation**.
- **Step 2: Client Responds with its Nonce**:
- The client generates its own **random number (nonce)** and sends it back to the AP.
- This nonce is essential because it ensures the client is involved in the handshake, confirming it's not an attacker.
- **Step 3: AP and Client Derive the Pairwise Transient Key (PTK)**:
- The client combines the **AP's nonce**, **its own nonce**, and the **Pairwise Master Key (PMK)** (derived from the pre-shared key or 802.1X) to generate the **PTK**.

- The **AP also computes the same PTK**, using the same information. This step confirms that both parties know the same **PMK** (the shared secret).
- **Step 4: Final Confirmation**:
- Both the AP and client use the **PTK** to authenticate that they share the correct encryption keys.
- The client proves to the AP that it knows the correct **PMK** by encrypting a message with the **PTK**.
- Similarly, the AP proves to the client that it knows the correct **PMK** by sending an encrypted message.
- If both sides can successfully decrypt these messages, they know that the other side has the correct **PMK**, confirming mutual authentication.

8) What will happen if we put a wrong passphrase during a 4Way handshake?

1. The 4-Way Handshake Relies on the PMK:

- The **4-way handshake** process starts with the generation of the **Pairwise Master Key (PMK)**, which is derived from the **passphrase** (for WPA2-Personal) or through **802.1X** (for WPA2-Enterprise).
- If a **wrong passphrase** is entered by the client, the resulting **PMK** (Pairwise Master Key) will be incorrect.

2. Impact on the Key Derivation Process:

- **Step 1**: The client and AP both derive the **Pairwise Transient Key (PTK)** from the **PMK**, which is then used for encrypting the communication between the client and AP.
- If the **PMK** is incorrect (because of the wrong passphrase), the **PTK** derived by the client will **not match** the PTK that the AP derives.

3. Outcome: Failed Authentication:

- During the handshake, when the client and AP try to confirm the shared **PTK**, the encryption and decryption operations will **fail** because they both have **different keys**.
- This mismatch will cause the **4-way handshake to fail**, meaning the client will not be able to successfully authenticate and establish a secure connection with the AP.

4. No Connection Established:

- **No encryption**: Since the handshake fails, the client and AP will not have a valid encryption key, so no encrypted data will be exchanged.
- The client will either **receive an authentication failure message** or simply **not connect** to the network.

- In WPA2, the AP will reject the client's attempt to join the network.

5. User Feedback:

- The user will typically receive a **connection error** or **incorrect password message** from the device or Wi-Fi manager.
- In case of repeated incorrect passphrases, the client may **time out** or retry the connection.

9) What problem does 802.1X solve in a network?

The Problem 802.1X Solves:

In a network, especially in **enterprise environments** or public networks, **unauthorized access** is a significant threat. Without proper authentication, anyone can potentially connect to a network, which can result in:

1. **Unauthorized Devices Accessing Network Resources**:
    - In an **open network** (like public Wi-Fi), anyone within range can connect, often without needing to prove their identity. This exposes the network to unauthorized users and attackers.
2. **Weak Authentication Mechanisms in Legacy Networks**:
    - Traditional **WPA2-Personal (PSK)** is based on a **shared passphrase** for all users. If the passphrase is leaked or guessed, **every device** on the network becomes vulnerable.
    - In large networks, sharing a single key for all users doesn't provide proper **access control** or security.
3. **Lack of Fine-Grained Access Control**:
    - Without proper **authentication**, it's hard to implement **role-based access control** or **network segmentation**. For example, both guest devices and employees could have the same access, even though they should have different levels of network privileges.

How 802.1X Solves These Problems:

802.1X is a **network access control protocol** that enforces **strong authentication** and **fine-grained access control** for both **wired** and **wireless** networks. It solves these key issues:

1. Strong Authentication:

- **802.1X** enables **individual device authentication**, meaning that each device trying to connect to the network must **prove its identity** (usually via credentials like **username/password**, **digital certificates**, or **smartcards**).
- **EAP (Extensible Authentication Protocol)** used in 802.1X allows a variety of **authentication methods**, including **multi-factor authentication (MFA)**, to enhance security.

- Only **authenticated devices** can access the network, making it **much harder** for unauthorized users or attackers to gain access.

2. Dynamic Key Generation and Better Security:

- With **802.1X**, the authentication process generates **unique session keys** for each device connecting to the network. This ensures that:
    - Devices don't share a **static password** or encryption key.
    - If one device is compromised, only that device is affected — the rest of the network remains secure.
- In contrast, **WPA2-Personal** uses a **single static passphrase** for all devices, making it much easier to compromise.

3. Network Access Control and Segmentation:

- **802.1X** enables **network access control (NAC)** systems, allowing administrators to define **access policies**. For instance:
    - **Guest devices** can be given limited access (e.g., to the internet only), while **employees** can access internal resources.
    - Devices can be assigned to **specific VLANs** (virtual networks) based on their authentication type, ensuring proper **network segmentation**.
- This allows for **granular control** over **who** connects to the network, **what** resources they can access, and **how** they can interact with the network.

4. Scalability and Centralized Management:

- Unlike **WPA2-Personal**, which uses a **shared passphrase**, **802.1X** allows for **centralized management** of authentication credentials through an **authentication server** (typically **RADIUS**).
    - This allows for **easier scaling** in large networks, where each device can be authenticated using a centralized service, making it easier to manage user accounts and permissions.

10) How does 802.1X enhance security over wireless networks?

Device Authentication:

- **802.1X** ensures that **only authenticated devices** can connect to the network. Each device (or user) must present valid credentials before gaining access.
- Authentication methods supported by **802.1X** include:
    - **Usernames/passwords**
    - **Digital certificates**

        - **Smart cards**
        - **Two-factor authentication (2FA)**
    - This **strong authentication** prevents unauthorized devices from accessing the network, which is a major security concern for wireless networks.

2. **Per-Device Encryption**:
    - **802.1X** enables the use of **unique session keys** for each device that successfully authenticates. This means that the encryption keys used to protect data traffic are **not shared across devices**.
    - Each device has a **unique encryption key**, ensuring that:
        - Even if one device is compromised, the others remain secure.
        - **Encrypted communication** between devices and the access point (AP) ensures confidentiality and data integrity.
3. **Dynamic Key Management**:
    - In **WPA2-Personal** (with PSK), a **single static key** is shared across all devices, which means if one device is compromised, the entire network is vulnerable.
    - **802.1X** eliminates this risk by using **dynamic key generation**:
        - After authentication, the **Pairwise Transient Key (PTK)** is generated uniquely for each session.
        - The **PTK** is used to encrypt data between the client and AP, and it changes with each session.
        - This **dynamic keying** ensures that each session is **fresh** and protected, even if previous keys were exposed.
4. **Fine-Grained Access Control**:
    - With **802.1X**, the network can apply **role-based access control (RBAC)**. This means that users can be given access to **specific network resources** based on their **credentials**.
    - For example, a guest user may only have internet access, while an employee may have access to internal resources like file servers or databases.
    - **Network segmentation** (using **VLANs**) can also be enforced, ensuring that devices are placed in the correct virtual network segment with limited access.
5. **Protection Against Spoofing and Man-in-the-Middle (MitM) Attacks**:
    - **802.1X** helps prevent attacks like **spoofing** (where an attacker pretends to be a legitimate device) by ensuring that both the **client** and **AP** authenticate each other.

- The use of **digital certificates**, **mutual authentication**, and **nonces** (random numbers) ensures that both parties are verified and that an attacker cannot easily impersonate a legitimate device.
- This **mutual authentication** step ensures that:
    - The **client** is connecting to a legitimate AP, and
    - The **AP** is not being impersonated by an attacker.

6. **Centralized Authentication and Logging**:
    - With **802.1X**, authentication is typically handled by a centralized server (e.g., **RADIUS**), which:
        - Makes it easier to **manage user credentials** and access permissions.
        - Provides **detailed logging** of all authentication attempts, which helps identify suspicious activities.
    - This centralization makes it easier to enforce consistent security policies and track **who connected**, **when**, and **where**.