**WLAN Threats**

**I. DoS Attacks**

- Improperly configured devices

- Malicious user

- Accidental interference

- Minimize risk:

+ Harden devices

+ Passwords secure

+ Create backups

+ Changes during off-hours

* **Definition:**
  + A DoS attack in a Wireless Local Area Network (WLAN) aims to disrupt or render the network or connected devices inaccessible to legitimate users.
  + The goal is to degrade or completely halt network service availability.
* **Common Attack Vectors:**
  + **Deauthentication (Deauth) Attacks:**
    - Involves sending forged deauthentication packets to disconnect devices from the Access Point (AP).
    - Attackers spoof MAC addresses of the AP or target devices.
    - Highly prevalent due to its simplicity and effectiveness.
  + **Flooding Attacks:**
    - Overwhelm the AP with a massive influx of packets, exhausting its resources.
    - Types include:
      * Forged packet floods.
      * Connection request floods.
  + **Jamming Attacks:**
    - Employs radio frequency (RF) interference to disrupt WLAN signals.
    - Uses specialized jamming devices to overpower legitimate transmissions.
    - **Rogue Access Points (Rogue APs):**
    - Attackers deploy fake APs with identical SSIDs to legitimate ones.
    - Users unknowingly connect, enabling attackers to perform DoS or data theft.
* **Impact of DoS Attacks:**
  + Service disruption and user inconvenience.
  + Degraded network performance.
  + Financial losses for organizations.
  + Data loss or compromise.
  + Facilitation of other malicious attacks.
* **Mitigation Strategies:**
  + Implement strong security protocols (WPA2/WPA3).
  + Maintain updated firmware for APs and client devices.
  + Deploy firewalls and Intrusion Detection Systems (IDS).
  + Monitor network traffic for anomalies.
  + Utilize rogue AP detection tools.
  + Change default SSIDs and AP passwords.
  + Reduce the AP transmit power when high power is unneeded.

**Important Notes:**

* DoS attacks primarily target availability, not confidentiality or integrity.
* WLANs are particularly vulnerable due to the open nature of wireless communication.
* Layered security is crucial for effective defense.
* Keeping the firmware of your routers up to date is extremely important.

II. Rogue Access Point

 **Definition:**

* Unauthorized wireless access points on a network.
* Not managed or approved by network administrators.

 **Purpose & Dangers:**

* **Malicious Intent:**
  + Intercept traffic, steal credentials, man-in-the-middle attacks.
  + "Evil twin" APs: mimic legitimate SSIDs.
  + Used for DoS attacks.
* **Unintentional Risks:**
  + Employee-installed personal routers.
  + Weak/default security settings.

 **How They Work:**

* Broadcast their own SSID.
* Devices connect, especially to familiar SSIDs.
* Capture transmitted data.

 **Threat Types:**

* **Data Interception:** sensitive information theft.
* **Man-in-the-Middle:** intercept/modify communication.
* **Network Intrusion:** backdoor access.
* **DoS Attacks:** network flooding, deauthentication.

 **Detection & Mitigation:**

* **WIDS (Wireless Intrusion Detection Systems):** monitor for unauthorized APs.
* **Regular Network Audits:** scan for unknown devices.
* **Centralized AP Management:** control authorized APs.
* **Employee Education:** risks of unauthorized devices.
* **802.1X Authentication:** verify device/user identities.
* **Physical Security:** control access to network closets.
* **SSID Broadcast Control:** (minor) hides SSID.

 **Key Points:**

* Significant WLAN security risk.
* Malicious & unintentional Rogue APs are threats.
* Proactive detection/mitigation is essential.

Revision:

Question 1: Which of the following is most likely NOT the source of a wireless DoS attack? => Rogue AP

Question 2: True or False: A rogue AP is a misconfigured AP connected to the network and a possible source of DoS attacks.

False

Question 3: What type of attack is an “evil twin AP” attack? => MITM