Here is a **professionally formatted study note breakdown** of the document *"Evil Twin Notes.docx"*, following your request for a **comprehensive, sentence-by-sentence analysis** with all critical information preserved and clearly formatted for pasting into Microsoft Word.

**Evil Twin Attack – Study Notes (CompTIA A+ 220-1102)**

**1. Concept Overview**

* An **Evil Twin** is a **fraudulent wireless access point** that mimics a legitimate Wi-Fi network.
* Its primary purpose is to **eavesdrop on wireless communication** and **intercept data**.
* In network defense, evil twins are often classified as **rogue access points**.

**2. Attack Simulation Walkthrough**

**A computer screen with blue arrows and icons

AI-generated content may be incorrect.**

* **Attacker's Setup Example**:
  + The attacker parks near a corporate building (e.g., “Big Corp”).
  + Configures an access point with the same SSID (network name) as the company’s Wi-Fi (e.g., “Big Corp wifi”).
* **Attracting Victims**:
  + The attacker broadcasts the **same SSID** but with a **higher signal strength** than the legitimate access point.
  + Performs a **deauthentication attack** to disconnect users from the real network.
* **Reconnection Behavior**:
  + When devices attempt to reconnect, they **automatically connect to the stronger evil twin** access point (same SSID).
  + Users continue normal activity while the attacker **captures all network traffic**.

**3. Data Capture and Exploitation**

* The attacker may:
  + **Provide Internet access** to avoid suspicion.
  + **Capture traffic**, especially on **unencrypted websites or services**.
  + **Modify data** or **record sessions** into a **PCAP file** (packet capture) for analysis.
  + **Harvest credentials** by observing usernames/passwords transmitted during login.

**4. KARMA Attack Overview (Evil Twin Variant)**

**A computer screen with a diagram

AI-generated content may be incorrect.**

* **KARMA Attack** is a **variant of evil twin**, exploiting:
  + Devices that lack proper **access point authentication** protocols.
  + The **Preferred Network List (PNL)** a list of SSIDs a device has previously trusted.
* **Execution of KARMA Attack**:
  + Devices broadcast their PNL looking for known networks.
  + Attackers listen to these broadcasts and **spoofs an SSID from the PNL**.
  + Victim device **auto-connects to attacker’s access point**, trusting it due to the matching SSID.

**5. Key Differences: Evil Twin vs. KARMA Attack**

| **Feature** | **Evil Twin** | **KARMA Attack** |
| --- | --- | --- |
| SSID Selection | Manually chosen by attacker | Chosen based on victim’s broadcast PNL |
| Victim Behavior | Victim selects network manually or by auto-reconnect | Victim’s device connects automatically |
| Authentication Exploited | User trust/familiarity | Device’s preferred SSID memory |

**6. Real-World Example: Airport Scenario**

* Attackers may deploy evil twin hotspots in high-traffic areas like **airports**.
* Common SSIDs used: **“SJU free wifi”**, **“JetBlue free wifi”**.
* Users looking for free internet unknowingly **connect to malicious APs**, giving attackers access to their data.

**7. Captive Portal Usage in Attacks**

* **Captive Portal**: A webpage requiring interaction before network access.
* Attackers use **fake captive portals** to:
  + Trick users into entering **Facebook or Google credentials**.
  + Exploit familiarity with **third-party authentication** to gain user trust.
* Result: Attackers harvest login credentials which may be reused in **further attacks**.

**8. Defense Recommendations**

* Users should **always use a VPN** when:
  + Connecting to **public or untrusted wireless networks**.
  + This encrypts their communication and **prevents interception** by evil twins.

**9. Exam Relevance – CompTIA A+ 220-1102**

* Evil Twin and KARMA attacks fall under:
  + **Objective 2.4**: Compare and contrast common types of attacks.
  + **Objective 2.6**: Explain common security concepts.
  + **Objective 2.7**: Compare wireless security protocols and authentication methods.
  + **Objective 4.2**: Summarize common security best practices.
* Key terminology to understand:
  + **Rogue Access Point**
  + **SSID spoofing**
  + **Deauthentication attack**
  + **KARMA attack**
  + **Captive portal**
  + **VPN (Virtual Private Network)**
  + **Credential harvesting**
  + **PCAP file**

**10. Real-Life Implementation Examples**

* **Penetration Testing Engagement**:
  + A security consultant simulates an evil twin near a company’s premises to test employee awareness.
  + Findings are used to improve wireless network policies.
* **Public Wi-Fi Exploits**:
  + Attackers set up fake hotspots in cafes, airports, or libraries to steal credentials or perform **Man-in-the-Middle (MitM)** attacks.
* **Security Awareness Training**:
  + Demonstrations of evil twin setups are used to train employees on spotting suspicious Wi-Fi behavior.

**11. Exam Inclusion Notification**

✅ **Included in CompTIA A+ 220-1102 Curriculum**

* Evil twin and rogue access point attacks are **explicitly referenced** in exam objectives.
* Understanding this concept is **essential** for questions about:
  + Wireless security vulnerabilities.
  + Secure network access practices.
  + Threat mitigation and end-user education.
* Frequently tested in **scenario-based questions**, requiring identification of symptoms, attack methods, or proper user guidance.