### **Lab 9: Using Airgeddon to Create an Evil Twin and Capture Login Credentials**

**Objective:** Learn how to use the Airgeddon script to create an Evil Twin network and capture Wi-Fi login credentials.

**Purpose:** This lab demonstrates the use of Airgeddon, a Wi-Fi auditing tool that simplifies the process of configuring various Wi-Fi penetration testing tools. By using Airgeddon, users can automate many tasks that would otherwise require manual configuration.

**Tools Used:**

* Kali Linux 2024.4 (running in a VM)
* Alfa AWUS036ACHM External wireless card (supporting monitor mode)

**Key Steps in the Lab:**

1. **Setup:**
   * Install Airgeddon on Kali Linux using GitHub.
   * Verify and install necessary dependencies through the script's automated checks.
   * Configure the external wireless card for monitor mode.
2. **Initiating the Evil Twin Attack:**
   * Use the Evil Twin attacks menu in Airgeddon and select the captive portal option.
   * Discover available Wi-Fi networks and select the target network.
3. **Deauthentication and Handshake Capture:**
   * De-authenticate devices from the target network to force reconnections.
   * Use Airgeddon to capture the WPA/WPA2 handshake (if possible).
   * Spoof the MAC address for anonymity.
4. **Setting up the Captive Portal:**
   * Configure the portal language (English in this case) and begin the attack.
   * Allow Airgeddon to display a fake login page for capturing user credentials.
5. **Simulating a Victim Device:**
   * Connect a device to the Evil Twin network.
   * Observe how users are prompted to enter Wi-Fi credentials in the captive portal.
6. **Credential Capture:**
   * Confirm the captured credentials are displayed in plain text on the terminal.
   * End the attack after verifying the credentials.

**Outcomes:**

* Successfully created an Evil Twin network using Airgeddon.
* Captured Wi-Fi credentials through a simulated phishing attack.
* Practiced ethical Wi-Fi auditing techniques, emphasizing the importance of securing wireless networks.

**Takeaways:**

* Airgeddon simplifies the use of multiple Wi-Fi penetration tools.
* Monitor mode and a proper external wireless card are essential for effective network auditing.
* Understanding vulnerabilities in Wi-Fi networks helps enhance cybersecurity measures.