PostSkill-2

Step 1: Set Up Your Wireless Adapter

1. **Identify Your Wireless Adapter**:
   - Open a terminal and type:

     ```
     "iwconfig"
     ```

   - Identify the name of your wireless interface (e.g., `wlan0`).
2. **Enable Monitor Mode**:
   - To capture packets, you need to enable monitor mode on your wireless adapter:

     ```
     sudo ifconfig wlan0 down
     sudo iwconfig wlan0 mode monitor
     sudo ifconfig wlan0 up
     ```

   - Verify it's in monitor mode:

     ```
     iwconfig
     ```

Step 2: Start Airodump-ng

1. **Launch Airodump-ng**:
   - Start `airodump-ng` on your wireless interface to capture packets:

     ```
     sudo airodump-ng wlan0
     ```

2. **Observe the Output**:
   - Airodump-ng will start displaying data about nearby wireless networks and clients. The screen will be divided into two sections:
     - **Top Section**: Displays information about the networks (BSSID, ESSID, Channel, Encryption, etc.).
     - **Bottom Section**: Displays information about the clients connected to the networks.

Step 3: Analyze the Captured Data

1. **Understanding the Output**:
   - **BSSID**: The MAC address of the Access Point (AP).
   - **PWR**: Signal strength. The closer to zero, the stronger the signal.
   - **Beacons**: Number of beacons sent by the AP.
   - **#Data**: Number of captured data packets. For WEP, these are used to crack the key.
   - **#/s**: Number of data packets per second.
   - **CH**: Channel the AP is operating on.
   - **MB**: Maximum speed supported by the AP.
   - **ENC**: Encryption type (e.g., WEP, WPA, WPA2).
   - **CIPHER**: The encryption cipher used (e.g., TKIP, CCMP).

- **AUTH**: Authentication method (e.g., PSK, MGT).
- **ESSID**: The network name (SSID).
- **Station**: MAC addresses of the clients connected to the AP.

2. **Filtering for a Specific Network**:
   - To capture packets from a specific network, use the following command with the BSSID and channel number:

     ```
     sudo airodump-ng --bssid [Target_BSSID] --channel [Channel] --write capture wlan0
     ```

   - Replace `[Target_BSSID]` with the BSSID of the target network and `[Channel]` with the channel number.
3. **Interpreting Client Data**:
   - **STATION**: MAC address of the client device.
   - **Frames**: Number of frames (packets) sent to/from the AP.
   - **Probe**: If a client is probing for a specific network, the network's SSID will be displayed here.

Step 4: Save and Analyze Captured Data

1. **Saving Captured Data**:
   - Airodump-ng can save captured packets to a file:

     ```
     sudo airodump-ng --bssid [Target_BSSID] --channel [Channel] --write capture wlan0
     ```

   - The data will be saved in a `.cap` file that you can later analyze with tools like Wireshark or Aircrack-ng.
2. **Analyzing the Captured Data**:
   - Use `aircrack-ng` to analyze the captured `.cap` file for potential cracking, especially if you're targeting WEP:

     ```
     sudo aircrack-ng capture*.cap
     ```

3. **Viewing the Capture in Wireshark**:
   - For a more detailed analysis, open the `.cap` file in Wireshark:

     ```
     wireshark capture*.cap
     ```

   - Wireshark allows you to inspect each packet in detail, apply filters, and analyze the data.

Step 5: Interpret the Results

- **WEP**: If targeting a WEP network, look for the number of IVs captured (`#Data` field). Once enough IVs are captured, you can attempt to crack the key using `aircrack-ng`.
- **WPA/WPA2**: Focus on capturing a WPA/WPA2 handshake (look for EAPOL packets). These can be used to attempt a dictionary attack using tools like `aircrack-ng`.

Step 6: Clean Up

1. **Disable Monitor Mode**:
    - Once done, disable monitor mode and return your wireless adapter to its default mode:

```
sudo ifconfig wlan0 down
sudo iwconfig wlan0 mode managed
sudo ifconfig wlan0 up
```