Aircrack-ng Documentation

Introduction

Aircrack-ng is a comprehensive suite of tools for assessing Wi-Fi network security. It focuses on different areas of Wi-Fi security including monitoring, attacking, testing, and cracking. Aircrack-ng is an essential tool for penetration testers and security professionals working with wireless networks.

Features

- Packet capture and export of data to text files for further processing.
- Cracking WEP and WPA-PSK keys using dictionary attacks.
- Replay attacks, deauthentication, fake access points.
- Capture and injection of packets for analysis.
- Support for various drivers and platforms (Linux, Windows, macOS, etc).
- Integration with other tools like Wifite, Wireshark, and Hashcat.

Installation

Aircrack-ng can be installed on most Linux distributions and also supports Windows and macOS. On Linux, use the following commands:

Debian/Ubuntu:

sudo apt update

sudo apt install aircrack-ng

Kali Linux:

Already pre-installed.

From source:

1. git clone https://github.com/aircrack-ng/aircrack-ng.git

2. cd aircrack-ng

3. autoreconf -i

4. ./configure

5. make

6. sudo make install

Usage

Common usage examples of Aircrack-ng:

1. Capturing packets:

   sudo airodump-ng wlan0

2. Targeting a specific network:

   sudo airodump-ng --bssid [BSSID] -c [channel] -w capture wlan0

3. Cracking a captured handshake:

   aircrack-ng -w wordlist.txt -b [BSSID] capture.cap

4. Deauthentication attack:

   sudo aireplay-ng --deauth 100 -a [BSSID] wlan0

Each command requires a compatible wireless network adapter capable of monitoring and packet injection.

Disclaimer

Aircrack-ng should only be used on networks you own or have explicit permission to test. Unauthorized use of Aircrack-ng on third-party networks is illegal and unethical. Use this tool responsibly and within the bounds of the law.

Conclusion

Aircrack-ng is a powerful, flexible, and widely-used toolkit for wireless security auditing. Its modular design allows professionals to carry out complex attacks and penetration tests, making it a staple in any ethical hacker's toolkit.