Cracking Wi-Fi Passwords Using Aircrack-ng

21BCY10019 - Siddharth Dayal
21BCY10123 - Harshitaa Ashish

Introduction

Wi-Fi security is a critical aspect of modern networking, as wireless networks are ubiquitous and serve as the backbone for internet connectivity in homes, offices, and public spaces. Aircrack-ng is a powerful suite of tools designed for auditing wireless networks. In our presentation, we demonstrated how Aircrack-ng can be used to test the security of Wi-Fi networks by attempting to crack Wi-Fi passwords.

Overview of Aircrack-ng

Aircrack-ng is an open-source tool suite that includes features for monitoring, attacking, testing, and cracking Wi-Fi networks. It supports various encryption standards such as WEP, WPA, and WPA2. The suite includes several key tools:

- **Airmon-ng**: Enables and disables monitor mode on wireless interfaces.
- **Airodump-ng**: Captures raw 802.11 frames.
- **Aireplay-ng**: Injects frames and generates traffic for capture.
- **Aircrack-ng**: Performs the actual cracking by analyzing captured data.

Cracking Process

The process of cracking a Wi-Fi password using Aircrack-ng involves several steps:

1. Preparing the Environment

Before starting, it's essential to have the necessary hardware and software:

- A computer running a Linux distribution (e.g., Kali Linux).
- A wireless network adapter capable of packet injection.
- Aircrack-ng suite installed.

2. Enabling Monitor Mode

Using **Airmon-ng**, we set the wireless network adapter to monitor mode, which allows it to capture all wireless traffic within range.

sh

airmon-ng start wlan0

3. Capturing Data Packets

Next, we used **Airodump-ng** to capture data packets from the target network. This step involves identifying the target network and capturing the handshake, which is crucial for WPA/WPA2 cracking.

sh

airodump-ng wlan0mon

We noted the BSSID (MAC address) and channel of the target network and then focused our capture on that specific network.

sh

airodump-ng --bssid [BSSID] --channel [CH] --write capture wlan0mon

4. Deauthentication Attack

To speed up the process of capturing the WPA/WPA2 handshake, we performed a deauthentication attack using **Aireplay-ng**. This forces connected clients to reconnect, capturing the handshake in the process.

sh

aireplay-ng --deauth 10 -a [BSSID] wlan0mon

5. Cracking the Password

With the handshake captured, we used **Aircrack-ng** to attempt cracking the password. This step requires a wordlist, which contains potential passwords.

sh

aircrack-ng -w [wordlist] -b [BSSID] capture-01.cap

The tool goes through the wordlist, trying each entry until the correct password is found or the list is exhausted.

Ethical Considerations

It's crucial to emphasize the ethical implications of using Aircrack-ng. Unauthorized access to Wi-Fi networks is illegal and unethical. The primary purpose of this tool is to help network administrators test the security of their own networks to ensure they are protected against unauthorized access. During our presentation, we highlighted that our demonstration was conducted in a controlled environment with full permission.

Conclusion

Aircrack-ng is a robust tool for understanding and improving Wi-Fi security. Our demonstration provided a practical overview of how Wi-Fi passwords can be cracked, underscoring the importance of strong passwords and other security measures such as WPA3, which offers enhanced security features. By leveraging tools like Aircrack-ng ethically, we can better secure wireless networks against potential threats.