Wi-Fi & Aircrack Mastery Guide (Day 1-30)

This guide covers Wi-Fi security testing using Aircrack-ng and related tools, organized day-by-day for progressive learning.

Day 1: Install Aircrack-ng Suite

- **Command:** Install via package manager: `apt install aircrack-ng`
- **Purpose:** Set up Aircrack-ng tools for Wi-Fi testing.

Day 2: Understand Wi-Fi Security Types

- **Task:** Learn differences between WEP, WPA, WPA2, WPA3.
- **Purpose:** Identify attack methods appropriate for each encryption type.

Day 3: Enable Monitor Mode

- **Command:** `airmon-ng start wlan0`
- **Purpose:** Prepare wireless adapter for packet capturing.

Day 4: Scan Nearby Networks

- **Command:** `airodump-ng wlan0mon`
- **Purpose:** Identify available networks, channels, and encryption types.

Day 5: Analyze Network Details

- **Task:** Observe ESSID, BSSID, channel, encryption, clients.
- **Purpose:** Gather target information.

Day 6: Focus Capture on Target Network

- **Command:** `airodump-ng -c <channel> --bssid <BSSID> -w capture wlan0mon`
- **Purpose:** Capture packets from a specific network.

Day 7: Monitor Signal Strength

- **Task:** Observe signal quality to ensure effective packet capture.
- **Purpose:** Optimize capture process.

Day 8: Save Capture Files

- **Task:** Save .cap files for later cracking.

- **Purpose:** Preserve handshake data.

Day 9: Test Packet Injection Capability

- **Command:** `aireplay-ng --test wlan0mon`
- **Purpose:** Verify adapter supports packet injection.

Day 10: Deauthenticate Clients

- **Command:** `aireplay-ng --deauth 10 -a <BSSID> -c <Client MAC> wlan0mon`
- **Purpose:** Force reconnections to capture WPA handshakes.

Day 11: Capture Handshakes

- **Task:** Ensure handshake packets are captured during reconnections.
- **Purpose:** Required for WPA/WPA2 password cracking.

Day 12: Verify Handshake Quality

- **Task:** Use Aircrack-ng to check handshake: `aircrack-ng capture.cap`
- **Purpose:** Ensure valid handshake for cracking.

Day 13: WPA/WPA2 Cracking with Dictionary

- **Command:** `aircrack-ng -w wordlist.txt -b <BSSID> capture.cap`
- **Purpose:** Attempt password recovery using dictionary attack.

Day 14: Capture Multiple Handshakes

- **Task:** Capture handshakes from multiple clients.
- **Purpose:** Increase chances of successful cracking.

Day 15: Crack WEP Networks

- **Command:** `aircrack-ng capture.cap`
- **Purpose:** Exploit WEP weaknesses to recover key.

Day 16: Analyze Encryption Weaknesses

- **Task:** Study captured packets and encryption type.
- **Purpose:** Determine attack approach.

Day 17: Advanced WPA Attack Techniques

- **Task:** Explore PMKID attacks, offline cracking.
- **Purpose:** Gain alternative methods to recover WPA keys.

Day 18: Automate Capture Process

- **Task:** Use scripts to capture multiple handshakes over time.
- **Purpose:** Save manual effort.

Day 19: Packet Analysis

- **Tool:** Wireshark or tcpdump.
- **Purpose:** Inspect packets for sensitive information.

Day 20: WPS Attack with Reaver

- **Command:** `reaver -i wlan0mon -b <BSSID> -vv`
- **Purpose:** Attempt recovery of WPA key via WPS PIN.

Day 21: WPS Attack with Bully

- **Command:** `bully -b <BSSID> -c <channel> wlan0mon`
- **Purpose:** Alternative WPS attack tool.

Day 22: Evil Twin Setup

- **Tool:** hostapd or Airbase-ng.
- **Purpose:** Create fake AP to capture credentials.

Day 23: Rogue AP Monitoring

- **Task:** Observe client connections and gather info.
- **Purpose:** Test network defense against rogue APs.

Day 24: PMKID Capture

- **Tool:** hcxdumptool.
- **Purpose:** Extract WPA/WPA2 PMKID without client handshake.

Day 25: Cracking PMKID Hashes

- **Tool:** hashcat with captured PMKID.
- **Purpose:** Recover WPA/WPA2 passwords offline.

Day 26: Analyze Client Traffic

- **Tool:** Wireshark.
- **Purpose:** Monitor unencrypted traffic and vulnerabilities.

Day 27: Combine Aircrack with Wireshark

- **Task:** Capture and analyze traffic simultaneously.
- **Purpose:** Gain deeper network insights.

Day 28: Automate Attacks with Scripts

- **Task:** Use Bash/Python scripts to automate scanning, capture, and cracking.
- **Purpose:** Increase efficiency.

Day 29: Documentation & Reporting

- **Task:** Log successful attacks, findings, and network analysis.
- **Purpose:** Prepare professional report.

Day 30: Safe Pentesting Practices

- **Task:** Review ethics, scope, and legality.
- **Purpose:** Ensure all Wi-Fi testing is authorized and legal.

Note: Only test Wi-Fi networks you own or are authorized to assess. Unauthorized Wi-Fi attacks are illegal.