Wifite 2 - Advanced Kali Linux Guide

1. What is Wifite and Why Use It?

Wifite 2 is a Python-based wireless auditing tool designed to automate Wi-Fi hacking. It integrates several powerful tools like aircrack-ng, reaver, bully, and hcxdumptool. It automates capturing WPA handshakes, performing PMKID and WPS attacks, and cracking captured credentials.

This tool is ideal for ethical hackers, penetration testers, and security enthusiasts to test the robustness of wireless security configurations.

2. Installing & Updating Wifite

Kali Linux includes Wifite by default, but to get the latest version:

- Clone repo: git clone https://github.com/derv82/wifite2.git
- Navigate: cd wifite2
- Run: sudo python3 wifite.py

Dependencies: aircrack-ng, hcxdumptool, hashcat, reaver, bully, tshark

3. Wireless Adapter Setup

To use Wifite, your wireless card must support monitor mode and packet injection.

- Start monitor mode: sudo airmon-ng start wlan0
- Verify: iwconfig (look for wlan0mon)
- Optional: kill interfering processes with: airmon-ng check kill

Recommended chipsets: Atheros AR9271, Ralink RT5370, or Realtek RTL8812AU.

4. Getting Started

Launch the tool with: sudo wifite

It will scan for nearby access points and list their properties:

- Signal strength
- Encryption type (WPA/WPA2, WEP, WPS)
- WPS status

Select targets by typing numbers or press ENTER to attack all visible networks.

5. Attack Modes Explained

WPA Handshake: Disconnects a connected client, waits for reconnection to capture handshake.

PMKID Attack: Extracts PMKID directly from routers with RSN enabled without client interaction.

WPS PIN Brute Force: Attacks routers with WPS enabled using PINs to extract credentials.

Offline Cracking: After capturing .cap/.hccapx, Wifite can invoke Aircrack-ng or Hashcat with a wordlist.

6. Real-World Example - WPA2 Handshake Capture

1. sudo wifite
2. Select WPA2-secured network
3. Wait for handshake capture via deauth attack
4. Handshake saved to /root/wifite/

Crack with Aircrack-ng:

```
aircrack-ng -w /usr/share/wordlists/rockyou.txt captured.cap
```

7. Real-World Example - WPS Brute Force

1. sudo wifite --wps-only
2. Target routers with WPS active
3. Uses Reaver or Bully to brute force 8-digit PIN

This process may take hours depending on router lockouts. Use --timeout and --delay flags to avoid detection.

8. Real-World Example - PMKID Hash Extraction

1. sudo wifite --pmkid
2. PMKID hash captured automatically (requires hcxdumptool)
3. Hash is saved in .hccapx format

Crack with Hashcat:

```
hashcat -m 16800 pmkid.hccapx wordlist.txt
```

9. Useful Wifite Flags and Options

--no-wpa	Skip WPA/WPA2 networks
--wps-only	Attack only WPS-enabled routers
--pmkid	Enable PMKID hash attacks
--crack	Try to crack handshakes automatically

--dict <file>	Use custom dictionary
--kill	Kill conflicting services like NetworkManager

10. Where Files Are Stored

Wifite stores output in:

/root/wifite/

You will find:

- .cap files (handshakes)
- .pcap files (raw packets)
- .hccapx files (for hashcat)

Clean up old logs and organize your captures for future use.

11. Best Practices and Ethics

Only use Wifite on networks you own or have explicit permission to test. Unauthorized access to networks is illegal and unethical.

Respect privacy, document your work, and ensure you follow local laws and regulations. Use logging to record your tests and share findings responsibly.