تنبيه قانوني ♂ كل ما يلي يصلح فقط لاختبار شبكتك أو معمل خاص بك. أي إزعاج/قطع اتصال أو محاولة دخول على شبكة لا تملكها مخالف للقانون.

هل لازم USB Wi-Fi Adapter؟

لا، مش لازم في كل الحالات. قدامك 3 طرق بدون شراء أدابتور:

(A) الاعتماد على كارت اللابتوب الداخلي

- بعض الكروت تدعم **Monitor mode** وأحيانًا **Packet Injection**.
- افحص الدعم:

```
# اعرف اسم واجهة الواي فاي أولًا
ip link
# افحص قدراتها
iw list | sed -n '/Supported interface modes/,/Band/p'
```

ابحث عن `* monitor` ضمن "Supported interface modes". لو موجود، جرب التحويل لـ monitor:

```
sudo airmon-ng check kill   # يوقف خدمات تتعارض مع المونيتور
sudo airmon-ng start wlan0  # استبدل wlan0 بواجهتك الفعلية
# هينشئ غالبًا wlan0mon
```

لاختبار الحقن (Injection) في معملك فقط:

```
sudo aireplay-ng --test wlan0mon
```

ملاحظة: كثير من كروت Intel تدعم المونيتور جزئيًا؛ الحقن يعتمد على الموديل والسواق.

(B) معامـل افتراضي بالكامل (بدون أي عتاد) باستخدام mac80211_hwsim

ينشئ **راديوهات واي فاي افتراضية** داخل لينكس، فتقدر تتعلم/تتدرب بدون قطعة خارجية.

المتطلبات

- توزيعة لينكس (Kali/Ubuntu).
- الحزم: aircrack-ng, iw, hostapd, wpa_supplicant.

```
sudo apt update && sudo apt install -y aircrack-ng iw hostapd wpasupplicant
```

الخطوات

1) إنشاء راديوهين افتراضيين:

```
sudo modprobe mac80211_hwsim radios=2
# تأكد
iw dev
```

هتظهر مثلًا `wlan0` و`wlan1`.

2) ارفع الواجهات:

```
sudo ip link set wlan0 up
sudo ip link set wlan1 up
```

3) شغل نقطة وصول (AP) على `wlan0`: أنشئ ملف `/tmp/ap.conf`:

```
interface=wlan0
driver=nl80211
ssid=LabAP
hw_mode=g
channel=6
wpa=2
wpa_passphrase=Passw0rd123
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
```

ثم:

```
sudo hostapd /tmp/ap.conf
```

4) وصّل عميل على `wlan1`: في ترمينال آخر:

```
# توليد إعداد مؤقت والاتصال
wpa_passphrase LabAP Passw0rd123 | sudo tee /tmp/wpa.conf >/dev/null
sudo wpa_supplicant -i wlan1 -c /tmp/wpa.conf -B
```

5) جرّب المونيتور والالتقاط على واجهة ثالثة (افتراضية):

```
sudo airmon-ng start wlan1          # ينشئ wlan1mon
sudo airodump-ng wlan1mon           # راقب الشبكات/العميل/الـ APالافتراضيين
```

كده عندك AP وعميل وترافيك حقيقي داخل النظام—مناسب تمامًا للتعلم بدون أي قطعة.

(C) التدريب الأوفلاين على ملفات PCAP

- حمّل ملفات الترافيك اللاسلكي الجاهزة (Handshake/Management frames) وتدرّب على قراءتها بـ **Wireshark** أو تحليلها بـ **aircrack-ng**—ده تعليم بحت ومش محتاج عتاد.

مرجع الأوامر (مختصر + عملي)

1) airmon-ng — إدارة وضع المونيتور

```
sudo airmon-ng                  # يعرض الواجهات والكروت والسواقين
sudo airmon-ng check kill       # يوقف الخدمات المتعارضة (NetworkManager,
wpa_supplicant)
sudo airmon-ng start wlan0      # تحويل wlan0 إلى monitor (يخرج wlan0mon)
sudo airmon-ng stop wlan0mon    # إرجاعه لوضعه الطبيعي
```

نصائح حل المشاكل:

```
rfkill list                     # هل في حظر؟
sudo rfkill unblock all         # فك الحظر
sudo ip link set wlan0 down     # انزل الواجهة ثم ارفعها
sudo ip link set wlan0 up
```

2) airodump-ng — فحص الشبكات والتقاط الإطارات

```
sudo airodump-ng wlan0mon                           # مسح عام
sudo airodump-ng -c 6 wlan0mon                      # حصر القناة 6
sudo airodump-ng --bssid AA:BB:CC:DD:EE:FF -c 6
                 --write capture wlan0mon           # حفظ إلى capture.cap
```

أعلام مفيدة: - `--band abg` اختيار النطاق (2.4/5GHz) إن لزم. - `--manufacturer` و `--uptime` لعرض معلومات إضافية. - `--write-interval 1` يقلّل زمن التخزين. - `--ignore-negative-one` مفيد مع بعض السواقين عند مشاكل القناة.

3) aireplay-ng — اختبارات حقن/إعادة إرسال (للمعمل فقط)

⚠️ تحذير: بعض الأوامر قد تسبب قطع اتصال (DoS). استخدمها فقط داخل معملك الخاص.

اختبار الحقن:

```
sudo aireplay-ng --test wlan0mon
```

أعلام/أنماط شائعة (للمعرفة): - `--deauth <N>` إرسال إطارات Deauthentication (يستخدم فقط في معمل مغلق). - `-a <BSSID>` تحديد الراوتر المستهدف (داخل معملك). - `-c <ClientMAC>` تحديد عميل محدد.

4) crunch — توليد قوائم كلمات (Wordlists)

الصيغة العامة:

```
crunch <min> <max> [charset] [خيارات]
```

أمثلة عملية:

```
crunch 6 8 abc123 -o wordlist.txt        # توليد من حروف/أرقام محددة
crunch 8 8 -t @@%%!!!! -o patt.txt       # نمط: @ حرف صغير، , حرف كبير، % رقم، ! رمز
crunch 8 12 -f /usr/share/crunch/charset.lst mixalpha-numeric-all -o mix.txt
# تقسيم الملف لأجزاء 50MB
crunch 8 10 abc123 -o START -b 50m
```

أعلام مفيدة: - `-t` نمط مخصص. - `-o` إخراج إلى ملف. - `-b` split بالحجم. - `-p` كل التوافيق بدون تكرار. - `-d` منع تكرار حرف أكثر من عدد معين (مثال: `-d 2@`).

بيئة التشغيل

- **لينكس مفضل**. WSL لا يدعم monitor mode. إن احتجت بيئة جاهزة: استخدم **Kali Live USB** بدون تثبيت.
- تثبيت الحزم:

```
sudo apt update && sudo apt install -y aircrack-ng iw hostapd
wpasupplicant rfkill
```

استكشاف الأخطاء الشائعة

- واجهة بتتحول لاسم مختلف: استعمل `ip link` لتتأكد من الاسم الحالي.

- "fixed channel -1": جرّب `--ignore-negative-one` أو أوقف NetworkManager.
- لا أرى شبكات: تأكد من القناة/النطاق، ومن أن الكارت على المونيتور فعلًا (`iw dev`).

ماذا تفعل الآن بدون أدابتور؟

1) جرّب خيار (B) **hwsim** —أفضل طريقة تتعلم بيها الآن. 2) إن دعم كارتك الداخلي المونيتور، استخدمه في معمل مغلق لديك. 3) درّب عينك على تحليل إطارات 802.11 بملفات PCAP.

> لما تكون جاهز ماديًا لاحقًا، فكّر في شراء قطعة تدعم Monitor + Injection جيدًا (مثل شرائح Atheros/Mediatek/Realtek المناسبة)، لكن كبداية أنت مش محتاجها عشان تتعلم الأساسيات.