CAYVORA
SECURITY
cayvora.com

PENTEST LAB SERIES — VOL. 03

# Wireless Penetration Testing

avec Airgeddon

Guide complet : capture de handshake WPA/WPA2, attaques Evil Twin, PMKID & cracking hors ligne. Usage strictement professionnel et éthique.

■ ~35 min de lecture
■ Intermédiaire — Avancé
■ Cayvora Security 2025

**AVERTISSEMENT LÉGAL**

Ce guide est destiné exclusivement aux pentesters professionnels disposant d'une autorisation écrite. Toute utilisation non autorisée constitue une infraction pénale (Loi 07-03 au Maroc). Cayvora opère toujours dans un cadre contractuel défini.

# 00 Table des Matières

## 01 Introduction & Contexte Professionnel

Dans le cadre d'une mission d'audit de sécurité sans fil, l'évaluateur cherche à mesurer la résistance du réseau Wi-Fi d'un client face aux vecteurs d'attaque les plus courants. **Airgeddon** est un framework bash open-source qui automatise et orchestre l'ensemble des phases d'un test d'intrusion wireless : reconnaissance, capture de handshake, cracking hors ligne, et attaques de type Evil Twin.

Ce guide couvre le workflow complet d'un audit Wi-Fi professionnel, de la configuration de l'environnement jusqu'à la récupération de la clé PSK — en passant par les techniques avancées comme la capture de PMKID sans client connecté.

**POURQUOI LE WI-FI RESTE CRITIQUE EN 2025 ?**
Malgré WPA3, la majorité des réseaux d'entreprises marocaines utilisent encore WPA2-PSK. Un réseau mal configuré ou avec un mot de passe faible peut être compromis en quelques minutes. Lors de nos audits Cayvora, nous détectons ce type de vulnérabilité dans plus de 60% des engagements.

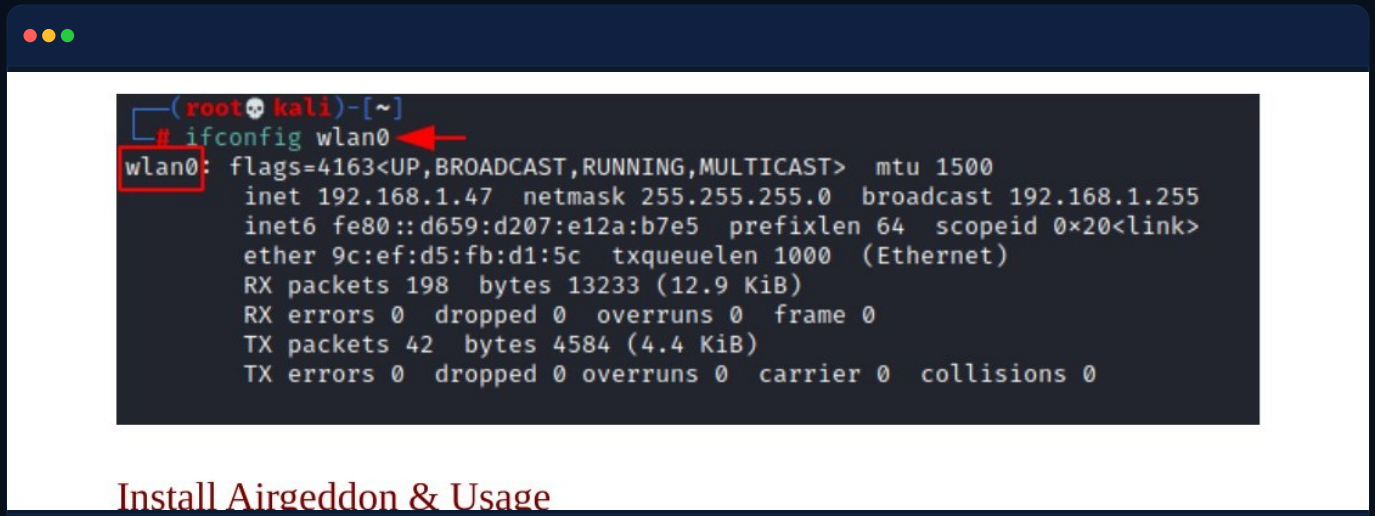
**Vecteurs d'attaque couverts dans ce guide :**

- Capture du 4-way Handshake WPA/WPA2 + cracking hors ligne
- Attaque Deauthentication pour forcer la ré-authentification des clients
- Evil Twin (Rogue AP) avec portail captif pour voler les credentials
- PMKID Attack — extraction sans client connecté (technique Jens Steube 2018)
- Cracking par dictionnaire, brute force et règles Hashcat GPU

## 02 Installation d'Airgeddon

Airgeddon s'installe via un simple clone git et s'exécute en tant que root. Au premier lancement, il vérifie et installe automatiquement toutes ses dépendances. Compatible avec Kali Linux, Parrot OS Security, BlackArch et la plupart des distributions orientées sécurité.

Commencez par identifier votre interface Wi-Fi avec **ifconfig wlan0**. L'interface doit afficher les flags **BROADCAST, RUNNING, MULTICAST** pour confirmer qu'elle est opérationnelle.




*ifconfig wlan0 — Interface en mode Managed, prête pour la configuration Airgeddon*

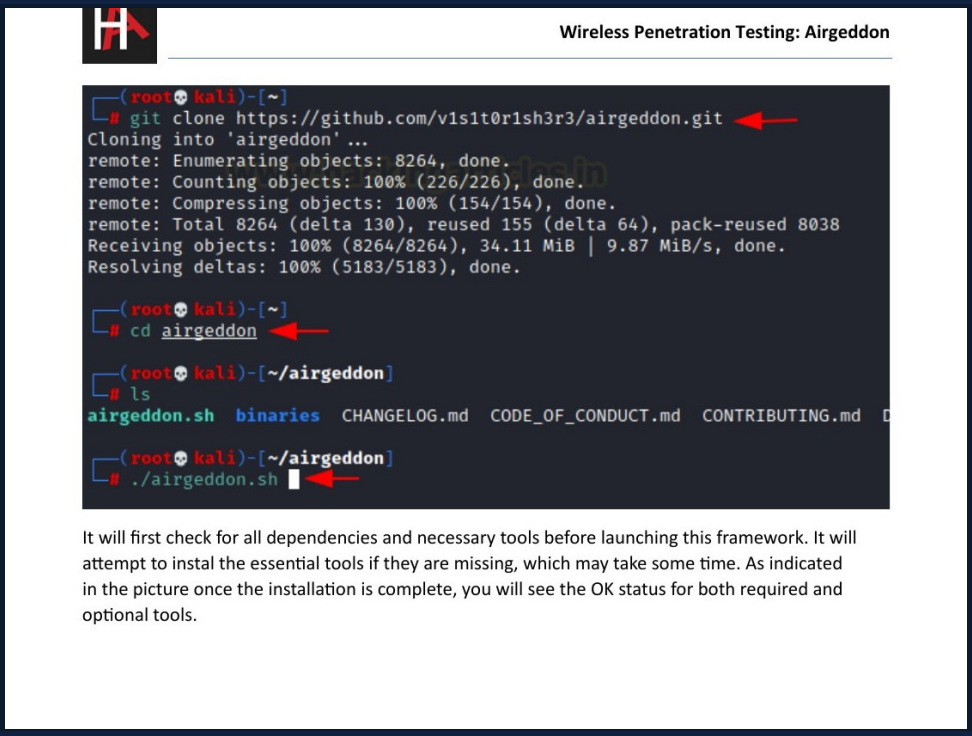
BASH — INSTALLATION

```bash
# Cloner le dépôt Airgeddon depuis GitHub
git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git

# Accéder au répertoire
cd airgeddon

# Lancer le script (root obligatoire)
sudo ./airgeddon.sh
```

Au premier lancement, Airgeddon effectue un contrôle exhaustif de ses dépendances. Tous les outils essentiels (airmon-ng, airodump-ng, aircrack-ng, xterm...) et optionnels (hashcat, bettercap, hostapd-wpe...) doivent afficher le statut **OK**.

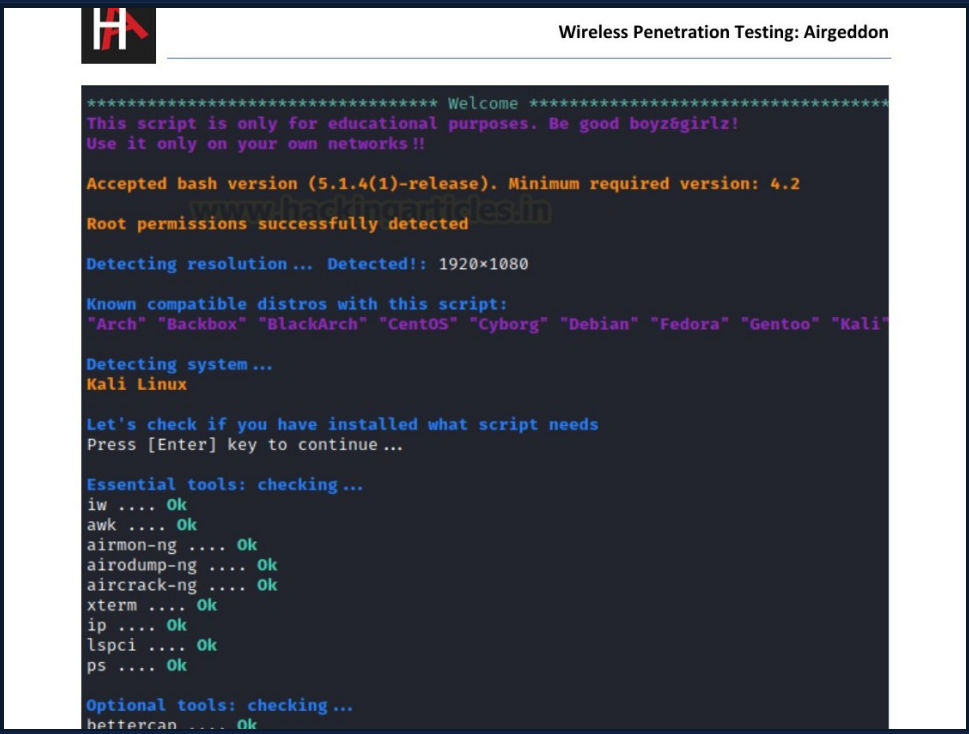



*Vérification des dépendances : tous les outils essentiels et optionnels marqués OK*

**CONSEIL CAYVORA — TERRAIN**
Utilisez un adaptateur Wi-Fi externe dédié (Alfa AWUS036ACH, Ralink RT5370) pour garantir la compatibilité complète avec le mode Monitor et l'injection de paquets. Les adaptateurs intégrés des laptops sont souvent limités.

## 03 Interface Wi-Fi & Mode Monitor

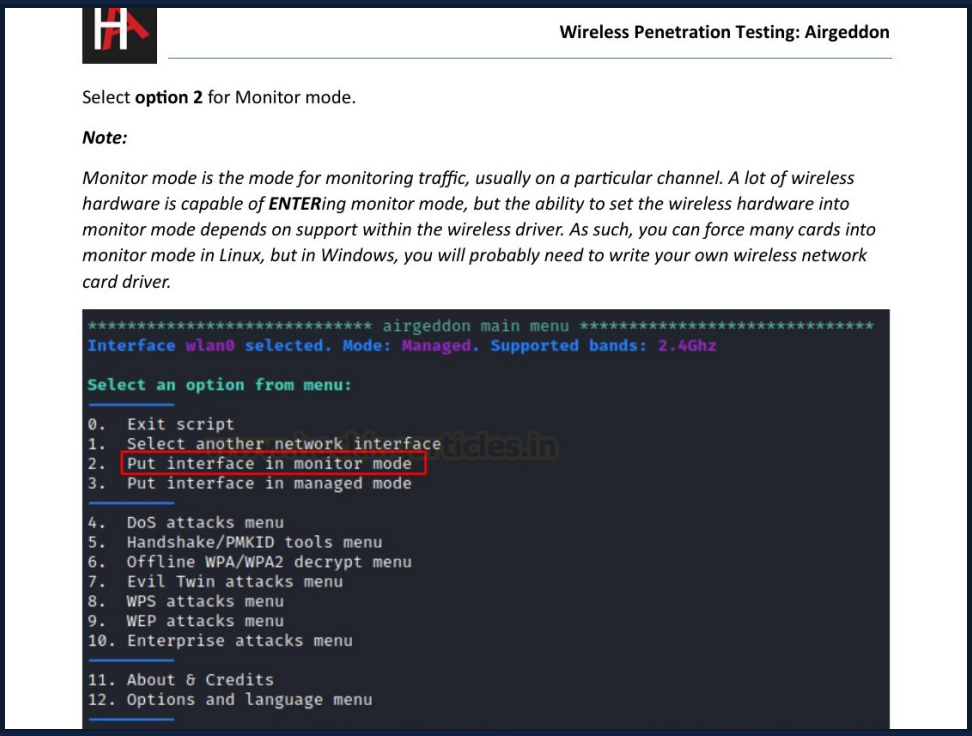
Après démarrage, Airgeddon liste toutes les interfaces réseau disponibles. Sélectionnez votre interface Wi-Fi (wlan0). Par défaut, la carte opère en mode **Managed** — elle ne traite que les trames destinées à votre machine. Pour capturer tout le trafic environnant, il faut passer en mode **Monitor**.




*Menu de sélection d'interface — wlan0 sur 2.4GHz, chipset Ralink RT5370*

## Activer le Mode Monitor

1. Au menu principal, sélectionnez Option 3 (votre interface wlan0 — vérifiez le chipset affiché)
2. Choisissez Option 2 — 'Put interface in monitor mode' pour activer la capture passive
3. L'interface est automatiquement renommée wlan0mon — le terminal confirme le succès
4. Vérifiez que le mode affiché passe de 'Managed' à 'Monitor' dans le bandeau supérieur



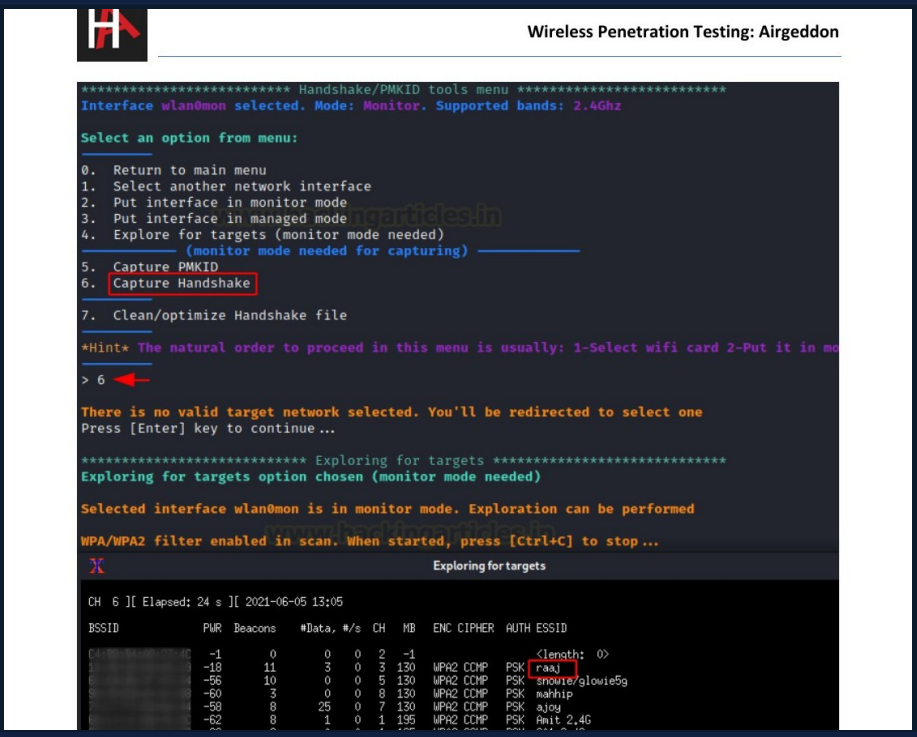

*Interface wlan0mon activée en Mode Monitor — prête pour la capture et l'injection de paquets*

**MODE MONITOR VS MODE MANAGED**
Managed : l'interface traite uniquement les trames qui lui sont destinées (connexion normale). Monitor : capture TOUTES les trames circulant sur l'air, quel que soit le destinataire. Ce mode désactive temporairement votre connexion Internet.

## 04 Capture du Handshake WPA/WPA2

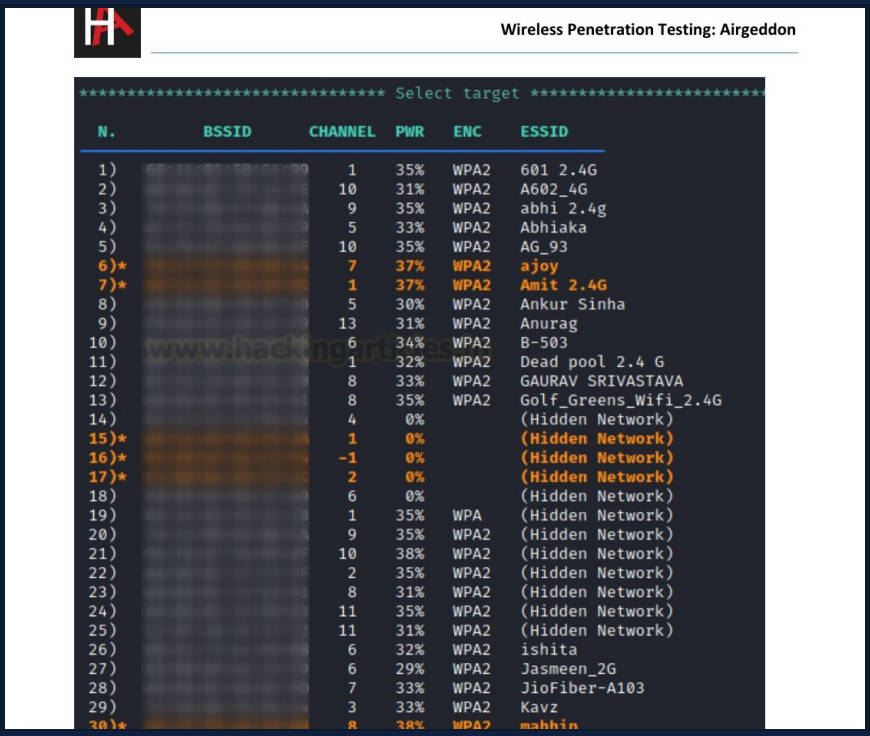
Le **4-way handshake WPA/WPA2** est l'échange cryptographique qui se produit lors de l'authentification d'un client sur un point d'accès. Cet échange contient suffisamment d'informations pour tenter de retrouver la clé PSK hors ligne, sans plus jamais interagir avec le routeur après la capture.

Depuis le menu principal → **Option 5** (Handshake/PMKID tools menu) → **Option 6** (Capture Handshake). Une nouvelle fenêtre s'ouvre et scanne tous les réseaux WPA/WPA2 à portée avec leur BSSID, canal, puissance et SSID.




*airodump-ng liste tous les réseaux WPA/WPA2 — réseaux marqués (*) ont des clients connectés*

Appuyez **CTRL+C** pour stopper le scan. La liste des cibles s'affiche avec leur numéro de série. Sélectionnez votre cible en entrant son numéro. Privilégiez les réseaux marqués **(*)** — ils ont des clients connectés et le handshake sera plus facile à capturer.




*Liste des cibles avec BSSID, canal, puissance et SSID — sélection par numéro de série*

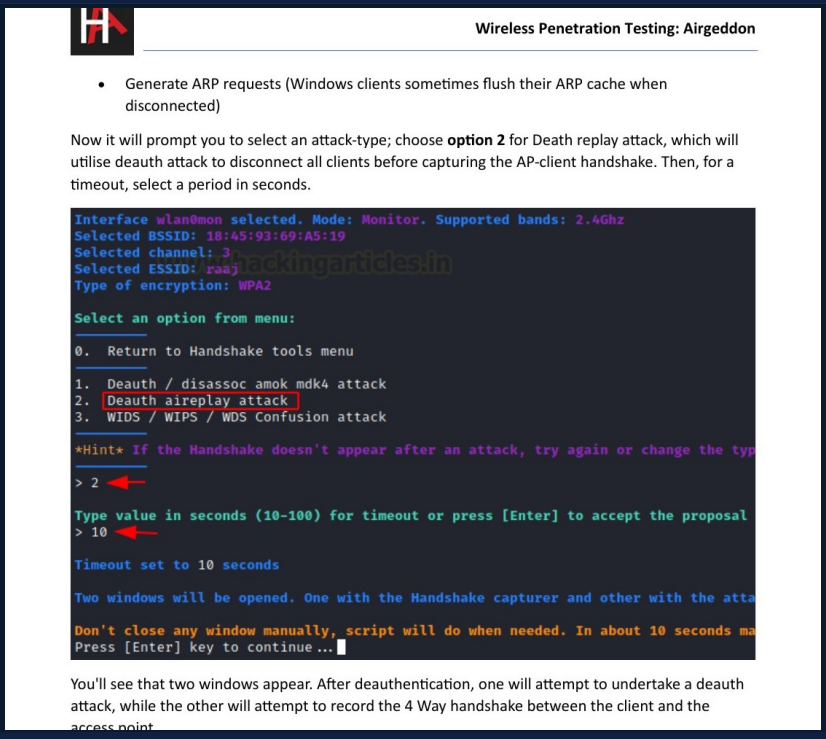
**CONFIRMATION DE CAPTURE**
Surveillez le coin supérieur droit de la fenêtre airodump-ng. L'apparition de 'WPA handshake: [BSSID]' confirme la capture réussie. Appuyez alors CTRL+C et sauvegardez le fichier .cap proposé par Airgeddon.

## 05 Attaque Deauthentication

Si aucun client ne s'authentifie naturellement, l'**attaque de deauthentication** force les clients déjà connectés à se déconnecter, puis à se ré-authentifier — générant le handshake nécessaire. Cette attaque exploite une faiblesse du protocole 802.11 : les trames de désassociation ne sont pas authentifiées.

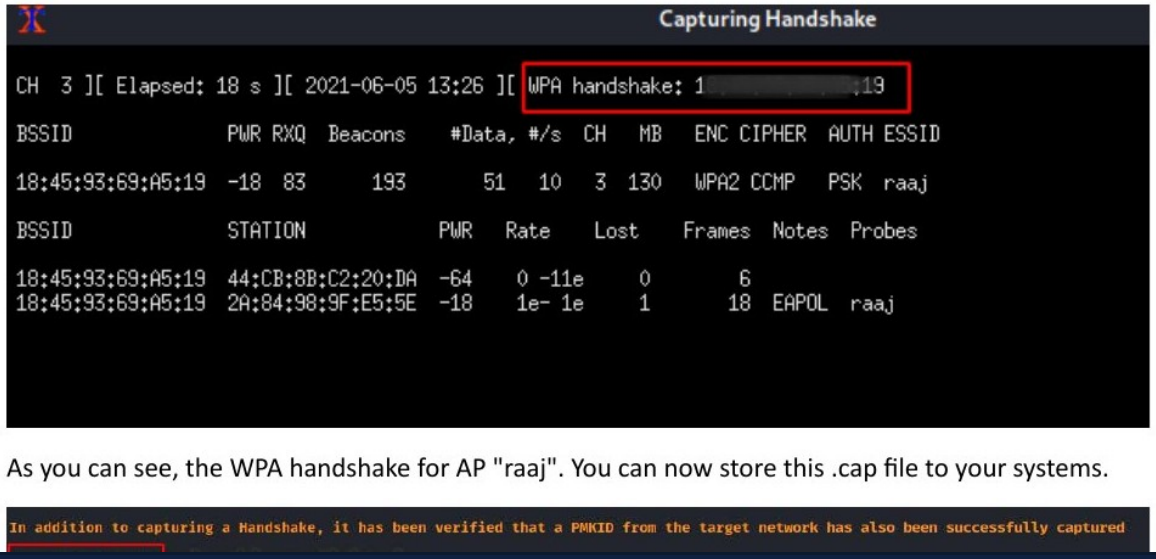
**IMPACT CLIENT — À DOCUMENTER DANS LE RAPPORT**
L'attaque deauth interrompt momentanément la connexion Internet des clients légitimes. En mission réelle, coordonnez avec le client pour choisir une plage horaire à faible impact (nuit, week-end). Documentez systématiquement cette action dans votre rapport de pentest.

Après sélection de la cible, choisissez **Option 2 — Deauth aireplay attack**. Définissez un timeout en secondes (10 à 100). Deux fenêtres s'ouvrent simultanément : l'une exécute l'attaque deauth (aireplay-ng), l'autre capture le handshake (airodump-ng).




*Deux fenêtres simultanées : aireplay-ng envoie les trames deauth + airodump-ng capture le handshake*

## Wireless Penetration Testing: Airgeddon



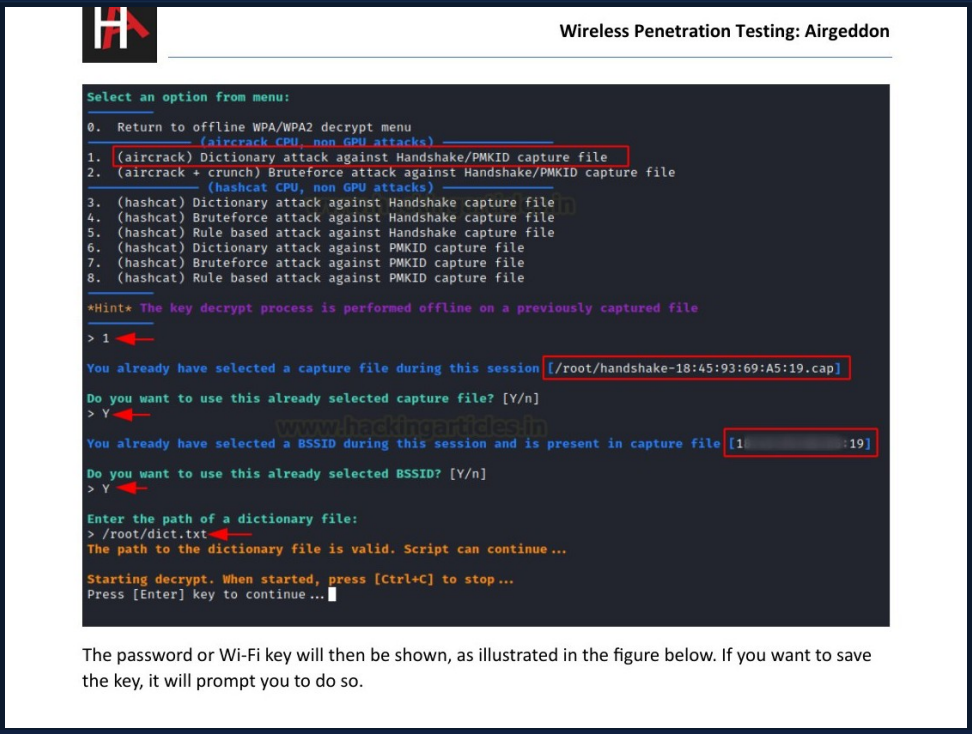

As you can see, the WPA handshake for AP "raaj". You can now store this .cap file to your systems.

*Handshake WPA2 confirmé — 'WPA handshake: [BSSID]' visible en haut à droite de la fenêtre*

## 06 Cracking Hors Ligne — 3 Méthodes

Le fichier .cap contient le handshake chiffré. Pour extraire la clé PSK, on utilise des attaques hors ligne — le routeur cible n'est plus impliqué. Airgeddon intègre trois moteurs de cracking selon le contexte de la mission.

Menu principal → **Option 6** (Offline WPA/WPA2 decrypt menu) → **Option 1** (Personal).



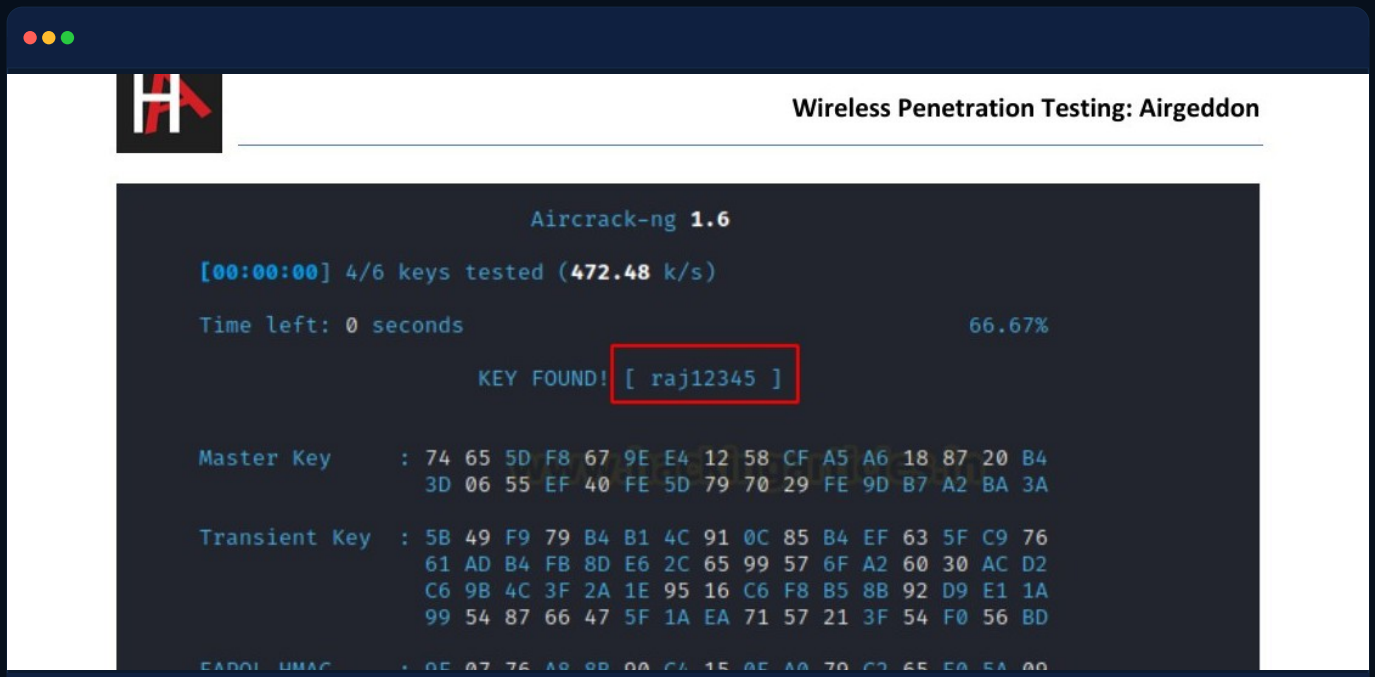

*Menu de décryptage WPA/WPA2 — 8 variantes : aircrack CPU + hashcat GPU en dict/bruteforce/rules*

## Méthode 1 — Dictionnaire avec Aircrack-ng

La méthode la plus rapide. Aircrack-ng teste chaque entrée d'une wordlist contre le hash du handshake. La wordlist **rockyou.txt** (14 millions de mots de passe) est le point de départ standard. Sélectionnez **Option 1** dans le sous-menu.

Aircrack-ng — Dictionary Attack

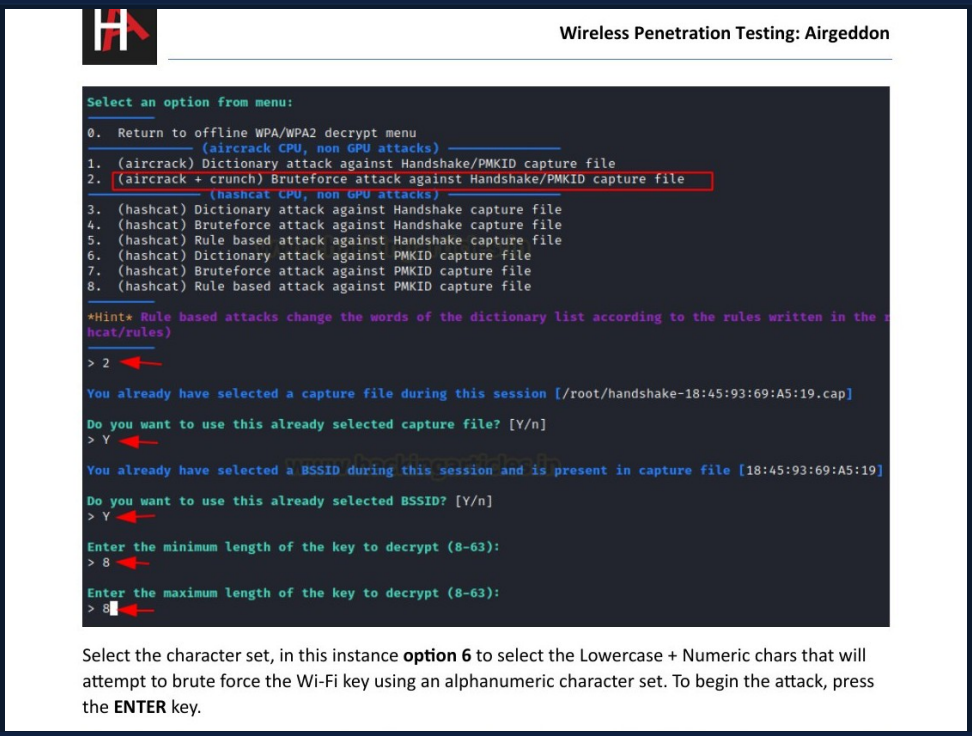
```
# Via Airgeddon : Option 6 > Option 1 > Option 1
# Ou en ligne de commande directement :
aircrack-ng -w /usr/share/wordlists/rockyou.txt \
            -b [BSSID_CIBLE] /root/handshake.cap
```




*KEY FOUND — Aircrack-ng affiche la clé PSK en clair + Master Key + Transient Key*

## Méthode 2 — Brute Force avec Aircrack + Crunch

Quand la wordlist échoue, Crunch génère toutes les combinaisons possibles selon un charset défini. Sélectionnez **Option 2**, définissez la longueur min/max, puis choisissez votre jeu de caractères.

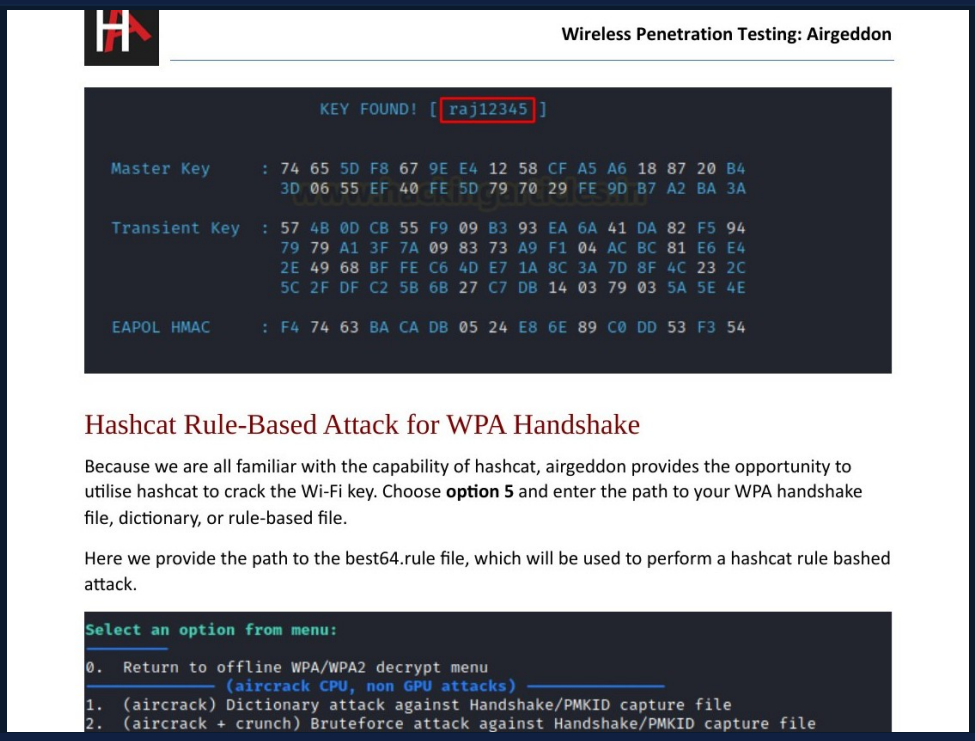



*Sélection du charset pour le brute force — Option 6 : lowercase + numeric [a-z0-9]*

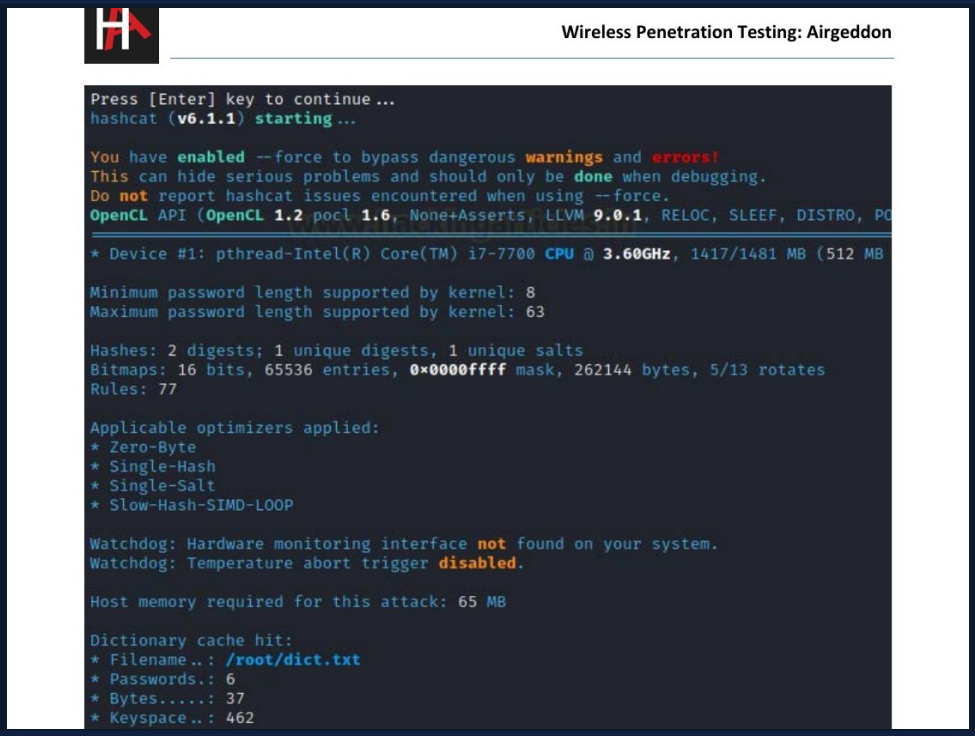
## Méthode 3 — Rule-Based avec Hashcat (GPU)

La méthode la plus puissante. Hashcat exploite le GPU pour des vitesses x50 à x100 vs CPU. Les règles (best64.rule) transforment les mots de la wordlist selon des patterns courants : capitalisation, substitutions leetspeak, ajout de chiffres.

Sélectionnez **Option 5** et fournissez le .cap, la wordlist et le fichier .rule.




*Configuration hashcat rule-based : fichier .cap + wordlist + best64.rule*




*Hashcat status: Cracked — vitesse GPU, progression et clé trouvée affichées*

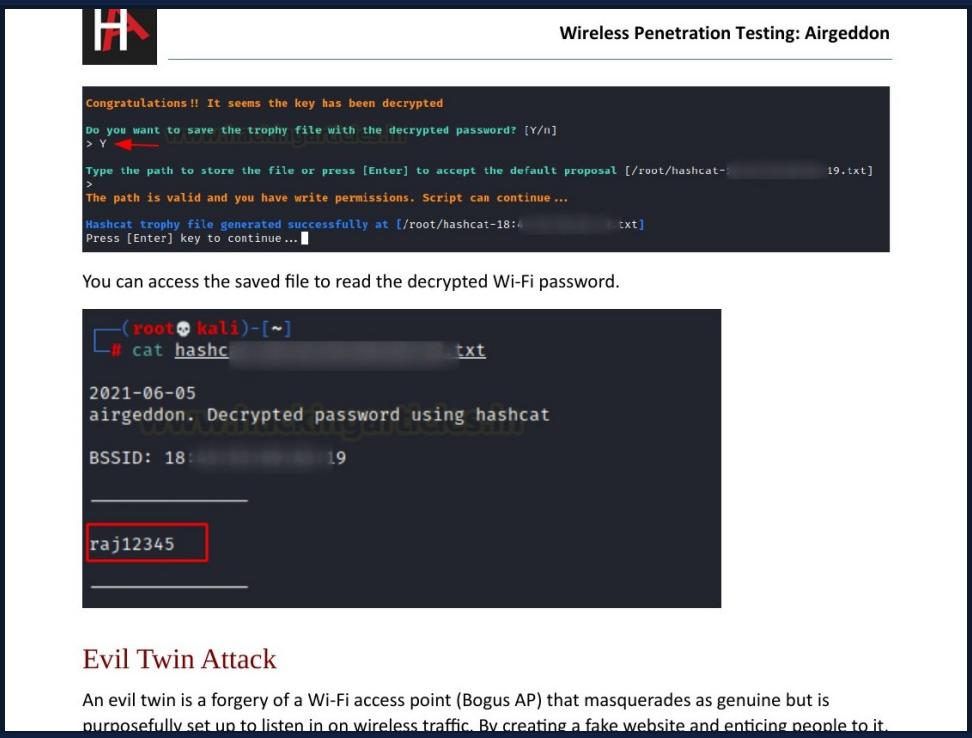
**STRATÉGIE DE CRACKING OPTIMALE — ORDRE CAYVORA**
1. Dictionnaire rockyou.txt (couvre ~80% des cas PME/agences) 2. Rule-based best64.rule sur rockyou (variations courantes) 3. Wordlists spécialisées (noms arabes, passwords marocains...) 4. Brute force ciblé (si longueur connue) — dernier recours.

## 07 Evil Twin Attack & Portail Captif

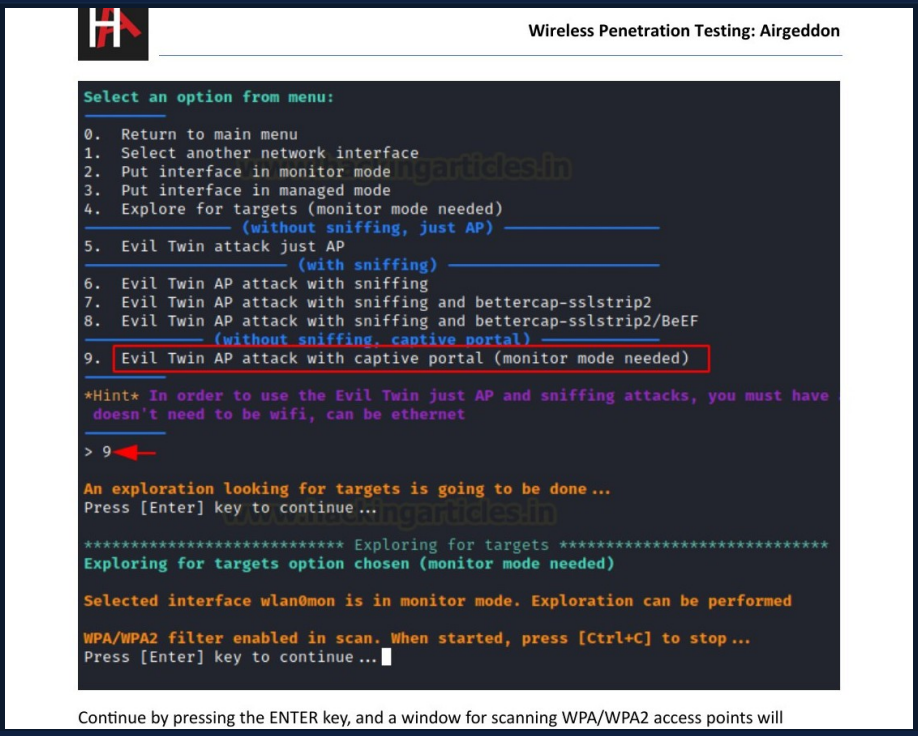
L'attaque **Evil Twin** (ou Rogue AP) crée un point d'accès jumeau malveillant portant le même SSID que la cible. En déconnectant simultanément les clients du vrai AP via deauth, on les pousse à se connecter au faux AP. Une fois connectés, ils sont redirigés vers un portail captif qui sollicite leur mot de passe Wi-Fi sous prétexte d'une 'mise à jour réseau'.

**IMPACT LÉGAL — CLAUSE CONTRACTUELLE OBLIGATOIRE**
L'Evil Twin est l'attaque wireless la plus intrusive : AP rogue + interception active. Ne jamais réaliser cette attaque sans clause contractuelle explicite. Au Maroc, cela peut constituer une infraction à la Loi 07-03 sur les STAD.

Menu principal → **Option 7** (Evil Twin attacks menu) → **Option 9** (Evil Twin AP attack with captive portal). Ce mode orchestre automatiquement 6 composants simultanés.



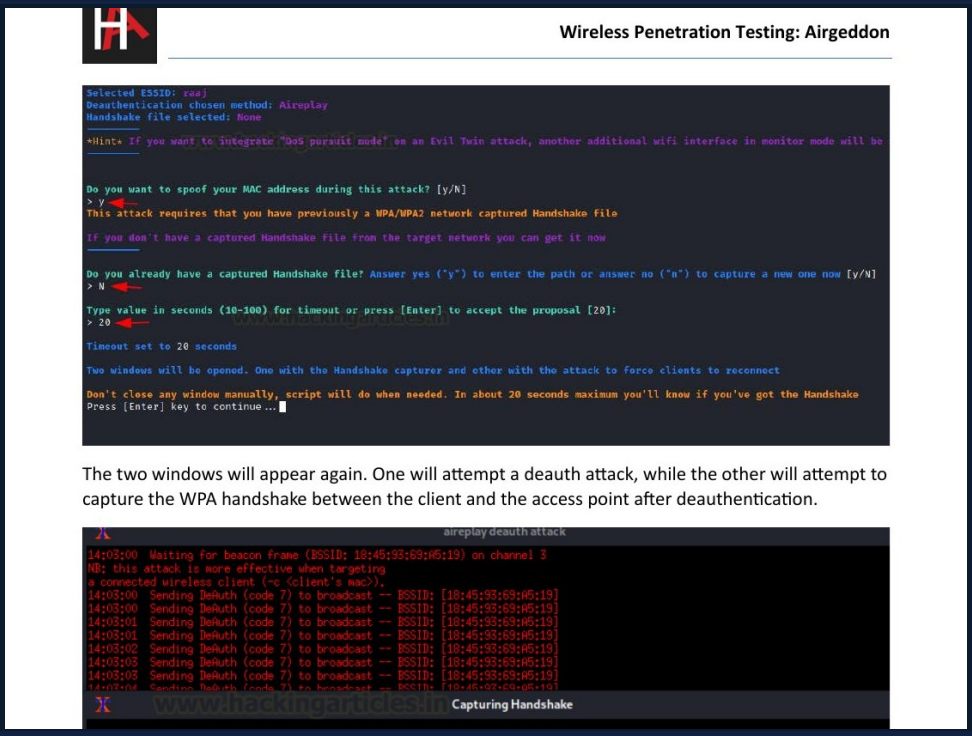

*Menu Evil Twin — Option 9 : captive portal mode (monitor mode requis)*




*Scan des APs pour sélectionner la cible Evil Twin — liste avec clients connectés (*)*

**Les 6 composants lancés simultanément par Airgeddon :**

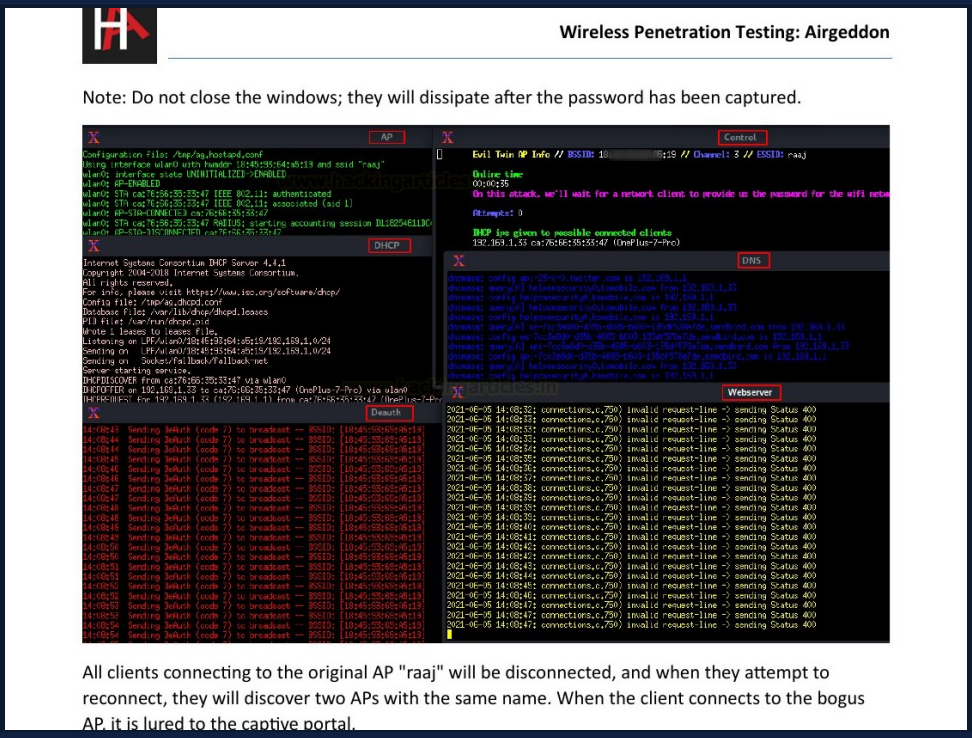
- AP : hostapd crée un AP ouvert avec le même SSID que la cible
- DHCP : dnsmasq distribue des IPs malveillantes aux clients connectés
- DNS : toutes les requêtes DNS sont redirigées vers notre portail captif
- Deauth : aireplay-ng maintient la pression pour forcer les clients vers le faux AP
- Webserver : héberge la page de phishing du portail captif
- Control : sniffe le mot de passe soumis et le vérifie contre le handshake capturé




The two windows will appear again. One will attempt a deauth attack, while the other will attempt to capture the WPA handshake between the client and the access point after deauthentication.



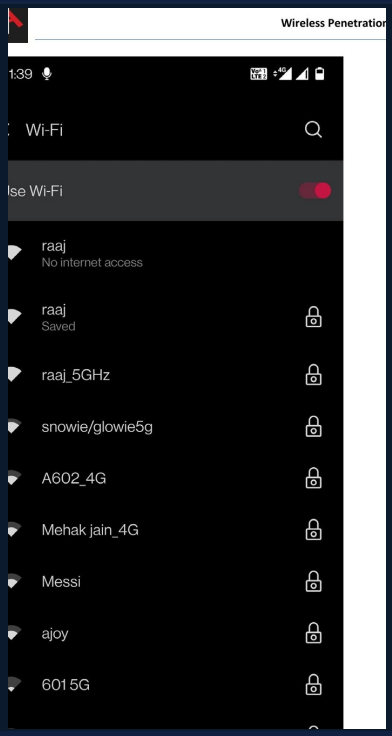

*6 fenêtres simultanées : AP · DHCP · DNS · Deauth · Webserver · Control*



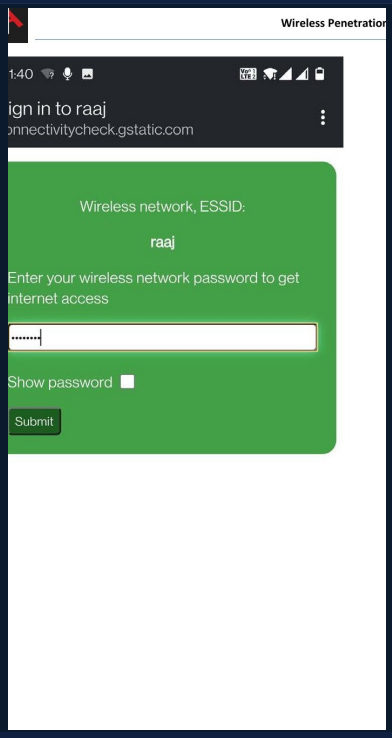

All clients connecting to the original AP "raaj" will be disconnected, and when they attempt to reconnect, they will discover two APs with the same name. When the client connects to the bogus AP, it is lured to the captive portal.

*Attaque en cours — le Control panel attend le mot de passe soumis par la victime*

Côté victime, le client voit deux réseaux portant le même nom. En se connectant au faux AP (ouvert, donc prioritaire), le portail captif s'affiche automatiquement.




*Vue côté victime — deux réseaux 'raaj' visibles : l'original et le faux AP ouvert*




*Portail captif affiché sur le téléphone — demande le mot de passe Wi-Fi pour 'accéder à Internet'*

Wireless Penetration Testing: Airgeddon

If the client gives the Wi-Fi key, the password will be captured in plaintext in the control window.


Additionally, save the password in the file you gave during the proposal.

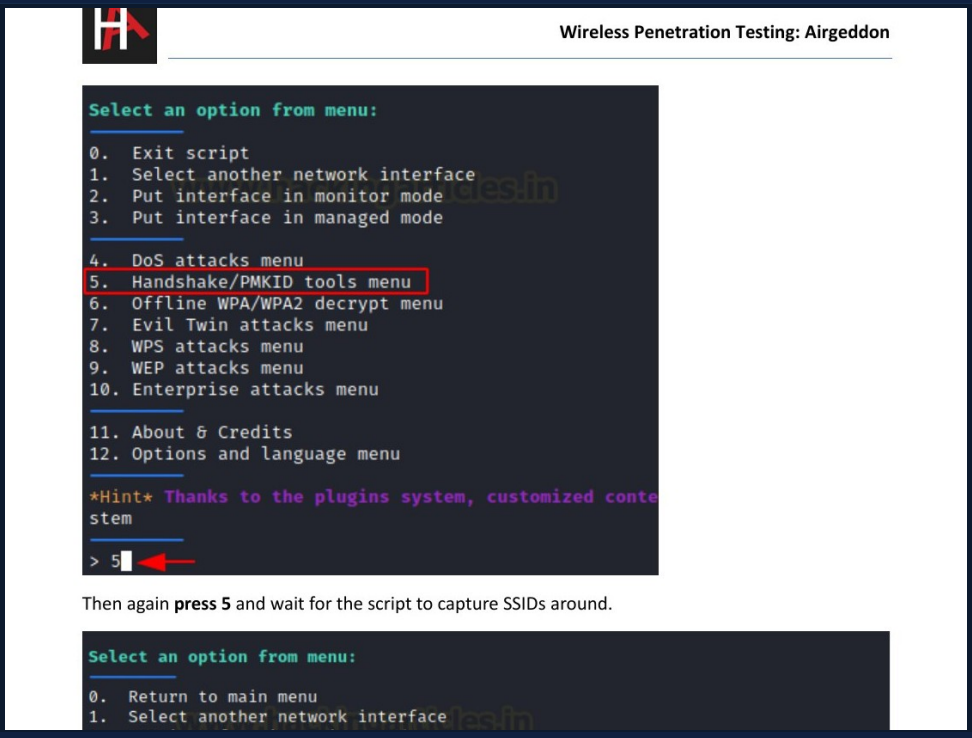

*Password captured — mot de passe affiché en clair dans la fenêtre Control d'Airgeddon*

## 08 PMKID Attack — Sans Client Connecté

La **PMKID Attack** (découverte par Jens Steube, auteur d'Hashcat, en 2018) est particulièrement redoutable : elle ne nécessite **aucun client connecté**. Le PMKID est un identifiant calculé par l'AP à partir du PMK, du MAC de l'AP et du MAC du client. Il est transmis directement dans la première trame EAPOL.

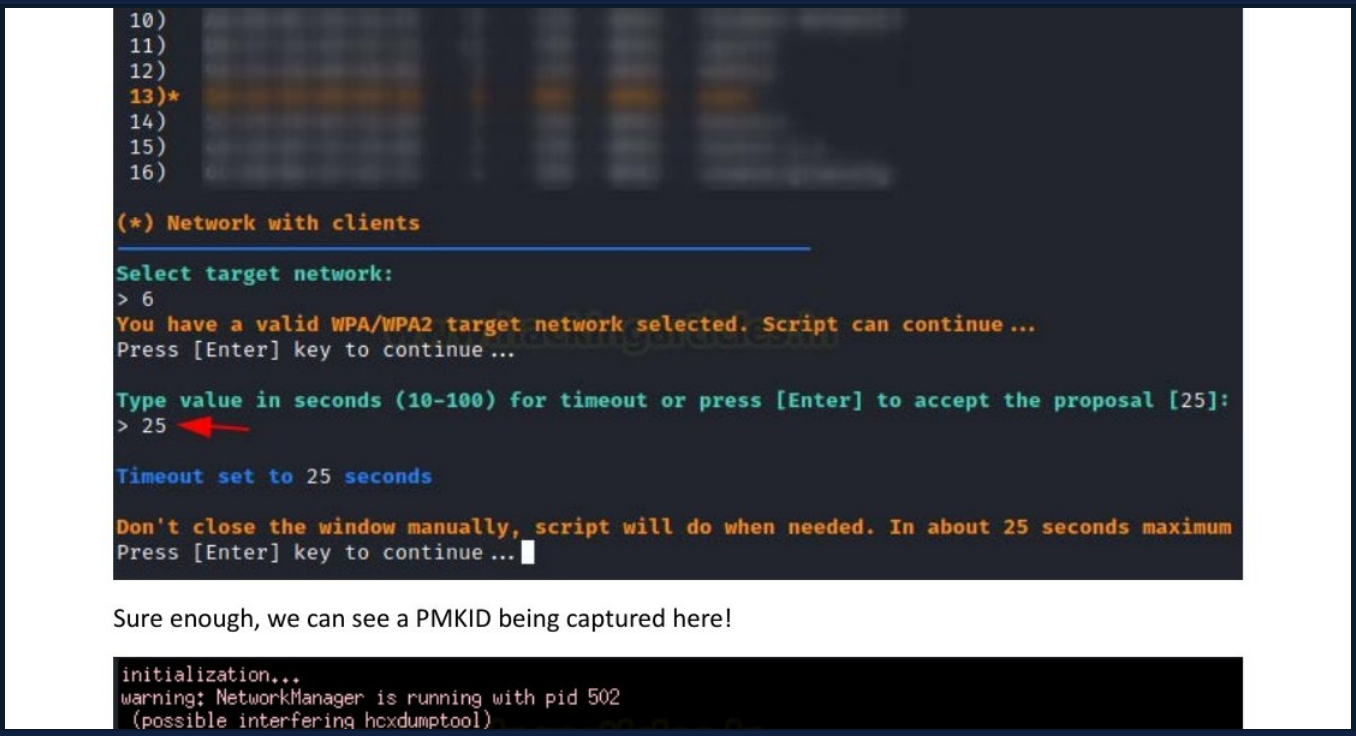
**FORMULE PMKID**
PMKID = HMAC-SHA1-128(PMK, 'PMK Name' || AP_MAC || Client_MAC). Cette valeur peut être capturée directement depuis l'AP sans interaction client. Avantage : si l'AP est vulnérable et le mot de passe faible, l'attaque aboutit sans attendre qu'un utilisateur se connecte.

Menu principal → **Option 5** (Handshake/PMKID tools menu) → **Option 5** (Capture PMKID — différent de Capture Handshake).

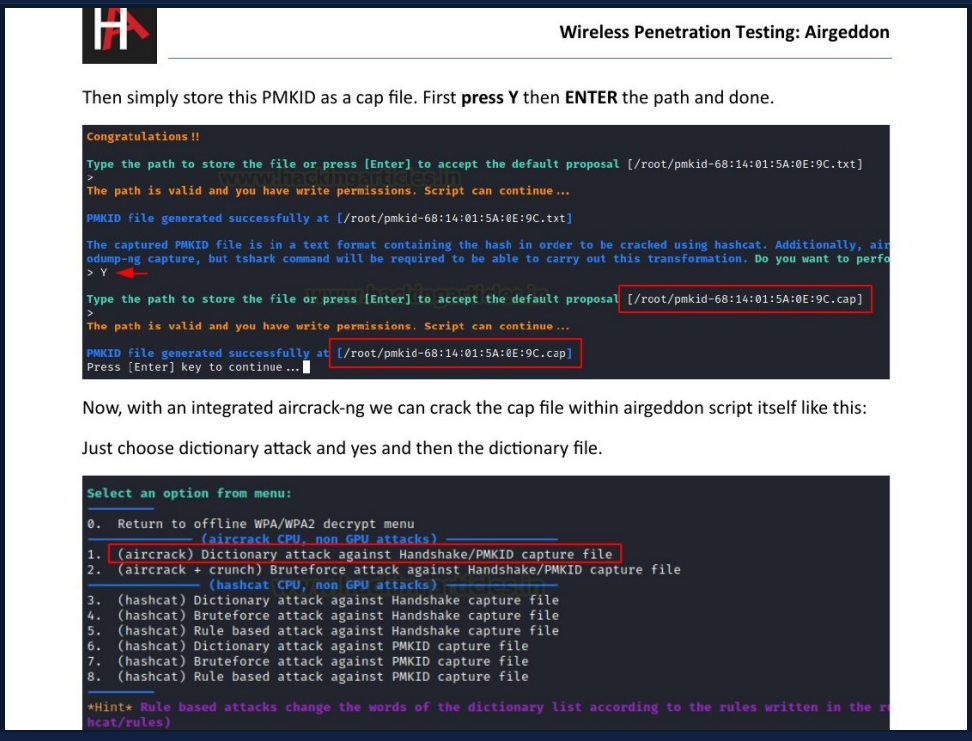



*Menu Handshake/PMKID — Option 5 : Capture PMKID (hcxdumptool requis)*

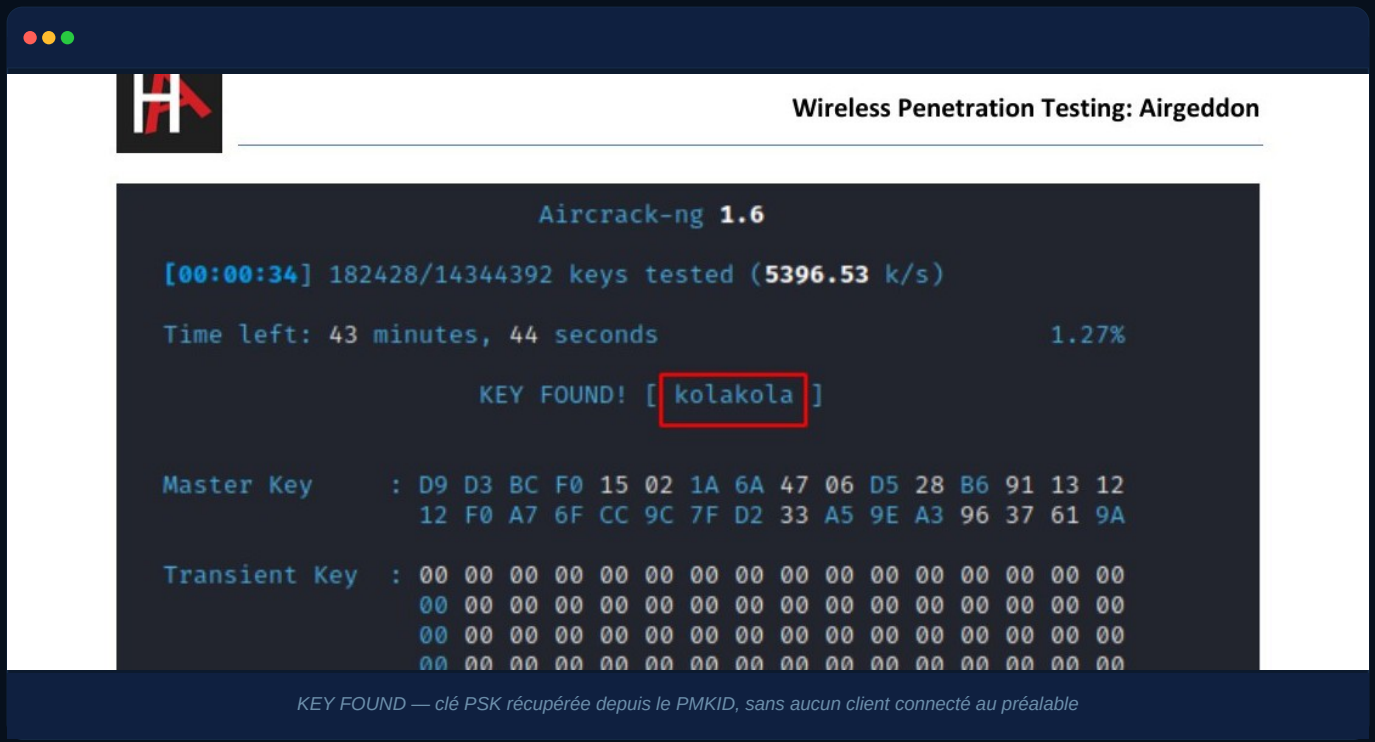
1. Airgeddon explore automatiquement les cibles — stoppez avec CTRL+C et sélectionnez la cible
2. Définissez un timeout de 25 secondes (généralement suffisant pour la capture PMKID)
3. hcxdumptool tente d'extraire le PMKID directement depuis les trames EAPOL de l'AP
4. Si capturé, sauvegardez en .txt puis convertissez en .cap pour la compatibilité aircrack
5. Lancez le cracking avec Option 1 (dictionary) — même workflow que pour le handshake




*hcxdumptool capture le PMKID — hash visible en dernière ligne [PMKIDROGUE:...]*




*Cracking du PMKID avec aircrack-ng et rockyou.txt — même processus que le handshake*




*KEY FOUND — clé PSK récupérée depuis le PMKID, sans aucun client connecté au préalable*

**LIMITES DE L'ATTAQUE PMKID**
Tous les AP ne sont pas vulnérables. Les firmware récents de certains équipements (Cisco, Fortinet, routeurs WPA3) n'incluent pas le PMKID dans leurs trames EAPOL. Dans ce cas, revenez à la capture de handshake classique.

## Votre réseau Wi-Fi est-il résistant à ces attaques ?

Un audit wireless professionnel Cayvora teste votre infrastructure contre l'ensemble de ces vecteurs — handshake, Evil Twin, PMKID — avec rapport détaillé et plan de remédiation concret. **contact@cayvora.com • cayvora.com**