République Algérienne Démocratique et Populaire Ministère de l'Enseignement supérieur et de la Recherche Scientifique Université

ABDERRAHMANE MIRA - BEJAIA -

Faculté science exacte Département Informatique

Mémoire pour l'obtention du diplôme de master en informatique Option : Administration et Sécurité des réseaux

Thème :

Recueil de vulnérabilités réseau informatique pour l'audit

Réalisé par :

M. BOUKRARA Mohamed Anis

M. DJAMA Abdelaali

Encadré par :

M. MOKTFI Mohend

Devant le jury composé de :

Président du jury :	DR. SABRI Salima	MCA
Examinateur :	DR.HOUHA Amel	MCA

Promotion 2022/2023

Remerciements

Nous tenons tout d'abord à exprimer notre profonde gratitude envers notre encadrant de mémoire, le docteur Mohand Moktefi, pour son encadrement précieux, ses conseils éclairés et sa disponibilité tout au long de ce projet de recherche. Sa passion pour le domaine nous a inspiré et sa patience nous a permis de progresser dans notre réflexion et dans la rédaction de ce mémoire.
Nous adressons également nos sincères remerciements aux membres du jury, pour leur investissement dans l'évaluation de notre travail et pour leurs commentaires constructifs qui ont contribué à améliorer la qualité de ce mémoire.

Dédicace

Je dédie ce mémoire à ma mere, mon père et mes deux sœur Ines et Melissa qui m'ont soutenu et encouragé durant ces années d'études,
A tous mes amis en particulier Lydia et Fares. Sans oublier celle qui m'a donné plein de force de courage et d'amour lors de ces deux dernières années d'études et qui ma encourager à aller de l'avant et qui a toujours cru en moi toi SYRIA !

Boukrara Mohamed Anis

Je dédie ce mémoire à toutes les personnes qui ont été présentes à mes côtés tout au long de ce parcours. À ma famille, pour leur amour et leur soutien indéfectible. À mes amis, pour leurs encouragements constants et leur amitié précieuse. À mes enseignants et mentors, pour leur expertise et leur guidance inspirante. Je tiens également à exprimer ma reconnaissance envers les professionnels du domaine de la sécurité informatique qui ont partagé leurs connaissances avec générosité. Merci à toutes les personnes qui ont contribué à la réalisation de ce mémoire, ainsi qu'à tous les chercheurs et experts anonymes dont les travaux ont enrichi ma compréhension. Votre soutien et votre confiance ont été essentiels. Ce mémoire est dédié avec une profonde gratitude à vous tous.

Djama Abdelaali

Table des matières

I. INTRODUCTION GENERALE ..... - 1 -

CHAPITRE I SECURITE INFORMATIQUE ..... - 2 -

II.1. INTRODUCTION ..... - 3 -

II.2. DEFINITION D'UN SYSTEME D'INFORMATION ..... - 3 -

II.3. DEFINITION D'UN RESEAU INFORMATIQUE ..... - 3 -

II.4. DEFINITION DE LA SECURITE INFORMATIQUE ..... - 4 -

II.4.1. OBJECTIFS DE LA SECURITE INFORMATIQUE ..... - 4 -

II.5. POLITIQUE DE SECURITE ..... - 5 -

II.5.1. STRATEGIE DE LA POLITIQUE DE SECURITE ..... - 6 -

II.5.2. ELABORATION DU DOCUMENT (POLITIQUE DE SECURITE) ..... - 8 -

II.5.3. OUTILS ASSOCIES A LA POLITIQUE DE SECURITE ..... - 9 -

II.6. DEFINITION DE VULNERABILITE ..... - 10 -

II.7. AUDIT INFORMATIQUE ..... - 11 -

II.7.1. ROLES ET OBJECTIFS D'UN AUDIT INFORMATIQUE ..... - 11 -

II.7.2. ETAPES D'UN AUDIT INFORMATIQUE ..... - 11 -

II.8. CONCLUSION ..... - 12 -

CHAPITRE II PRESENTATION DE L'ORGANISME D'ACCUEILLE ..... - 12 -

III.1. INTRODUCTION : ..... - 13 -

III.2. PRESENTATION DU GROUPE CEVITAL : ..... - 13 -

III.3. DESCRIPTION DE CEVITAL : ..... - 13 -

III.4. L'ORGANISATION GENERALE DES COMPOSANTES ET LES MISSIONS DES DIRECTIONS : ..... - 14 -

III.4.1 STRUCTURE DE L'ENCADREMENT : (ORGANIGRAMME) ..... - 14 -

III.4.2 MISSIONS ET SERVICES DES COMPOSANTES DE LA DG : ..... - 14 -

III.5. VULNERABILITE AU QUELLE NOUS AVONS PU ASSISTER : ..... - 19 -

III.6. CONCLUSION **:** ..... - 20 -

CHAPITRE III RECENSEMENT DES ATTAQUES, DES OUTILS DE SECURITE RESEAUX ET DES VULNERABILITES ..... - 21 -

IV.1. INTRODUCTION ..... - 22 -

IV.2. DIFFERENTS TYPES D'ATTAQUANTS [8] ..... - 22 -

IV.2.1. HACKERS WHITE HATS (PIRATE CHAPEAU BLANC) ..... - 22 -
IV.2.2. HACKERS GREY HATS (PIRATES CHAPEAUX GREY) ..... - 22 -
IV.2.3. HACKERS BLACK HATS (PIRATES CHAPEAUX NOIR) ..... - 23 -

IV.3. DIFFERENTS TYPES D'ATTAQUES [2] ..... - 23 -

IV.3.1. ATTAQUES PERMETTANT DE DEVOILER LE RESEAU ..... - 23 -
IV.3.2. ATTAQUES PAR IDENTIFICATION DES SYSTEMES RESEAU ..... - 23 -
IV.3.3. ATTAQUE PAR TRAVERSEE DES EQUIPEMENTS FILTRANTS ..... - 25 -
IV.3.4. ATTAQUES PERMETTANT D'ECOUTER LE TRAFIC RESEAU ..... - 26 -
IV.3.5. ATTAQUES PERMETTANT D'INTERFERER AVEC UNE SESSION RESEAU ..... - 28 -
IV.3.6. ATTAQUES PERMETTANT DE METTRE LE RESEAU EN DENI DE SERVICE ..... - 31 -

IV.4. OUTILS DE SECURITE RESEAUX ..... - 32 -

IV.4.1. PARES-FEUX ..... - 32 -
IV.4.2. DMZ ..... - 33 -
IV.4.3. PROXY ..... - 33 -
IV.4.4. IDS (INTRUSION DETECTION SYSTEM) ..... - 34 -
IV.4.5. IPS (INTRUSION PREVENTION SYSTEM) ..... - 37 -

IV.5. OUTILS DE DETECTION DE VULNERABILITES ..... - 38 -

IV.5.1. NESSUS PRO ..... - 38 -
IV.5.2. NMAP « NETWORK MAPPER » ..... - 39 -
IV.5.3. SNORT ..... - 39 -
IV.5.4. METASPLOIT ..... - 40 -
IV.5.5. YERSINIA ..... - 40 -

IV.6. CONCLUSION : ..... - 41 -

CHAPITRE IV RECUEIL DES VULNERABILITES ..... - 41 -

V.1. INTRODUCTION AU CVSS ..... - 42 -

V.2. FONCTIONNEMENT DU CVSS ..... - 42 -

V.3. LES COMPOSANTES DU CVSS ..... - 42 -

V.4. L'ECHELLE DE NOTATION ..... - 42 -

V.5. TABLEAU DE NOTATION CVSS ..... - 43 -

V.6. CONCLUSION ..... - 44 -

RECUEIL DES VULNERABILITES .....- 45 -

VI. CONCLUSION GENERALE.....- 74 -

BIBLIOGRAPHIE .....- 75 -

Liste des figures

Figure I.1. Piliers de s´sécurité informatique et réseau ……...……..... - 5 -

Figure I.2. Composants d'une politique de sécurité …….……... - 6 -

Figure I.3. Stratégie de la politique de sécurité. ……... - 7 -

Figure II.1. Organigramme globale de l'entreprise CEVITAL. ……...…. - 14 -

Figure III.1. Fonctionnement de la commande ping. ……..…. - 24 -

Figure III. 2. Fonctionnement du balayage TCP. ……. - 24 -

Figure III.3. Traversée d'un pare-feu en fixant le port source. ……... - 25 -

Figure III.4. Traversée d'un pare-feu en fixant le port source. ……...…… - 26 -

Figure III.5. Fonctionnement de l'attaque VLAN Hopping. ……. - 27 -

Figure III.6. Fonctionnement de l'attaque par sniffing. ……... - 28 -

Figure III.7. Attaque Man In The Middle. ……..... - 29 -

Figure III.8. Attaque ARP spoofing. ……. - 29 -

Figure III.9. Attaque IP spoofing. ……. - 30 -

Figure III.10. Attaque par déni de service distribué. ……... - 31

Figure III.11. Attaque smurf et fraggle par amplification de l'inondation. …….. - 31 -

Figure III.12. Représentation de l'emplacement d'un par-feux 'firewall' ……..... - 32 -

Figure III.13. Représentation de l'emplacement d'une DMZ. …….. - 33 -

Figure III.14. Architecture d'un proxy. ……..... - 33 -

Figure III.15. Architecture classique d'un IDS ….……..... - 34 -

Figure III.16. Fonctionnement d'un IDS……...……..... - 35 -

Figure III.17. Emplacement d'un IDS…...……..... - 35 -

Figure III.18. Logo du logiciel Nessus pro……..... - 37 -

Figure III.19. Logo du logiciel Nmap. …….. - 38 -

Figure III.20. Logo du logiciel de Metasploit. ……...… - 39 -

Liste des tableaux

Tableau IV.1. Echelle de notation CVSS ..…….... - 43 -

Tableau IV.2. Notation CVSS ..…….…….... - 43 -

Liste des abréviations

Ack: acsknowledgement.

Arp: address resolution protocol.

Cvss: Common Vulnerability Scoring System.

Ddos: distributed denial of service.

Dtp : dynamique trunking protocol.

Icmp : internet contrôle message protocole.

Ids: intrusion detection system.

Ip: internet protocole.

Ips: intrusion prevention system.

Ipv4: internet protocole version 4.

Ipv6: internet protocole version 6.

Lan: local area network.

Mac: media access contrôle.

Man: metropoliténe area network.

Nmap: network mapper.

Stp : spanning tree protocole.

Syn : syncronisation.

Tcp : transmision contrôle protocole.

Udp: user datagram protocole.

Vlan: virtuelle local area network.

Vtp: vlan trunking protocol.

Wan: wide area network.

I. Introduction générale

À l'ère où les réseaux informatiques se sont imposés comme des outils incontournables pour un large éventail d'organisations, la sécurité des systèmes d'information s'est érigée en une préoccupation primordiale. Les vulnérabilités réseaux représentent une porte d'entrée potentielle pour des individus malveillants, lesquels peuvent ainsi accéder à des informations confidentielles ou perturber le bon déroulement des réseaux. En conséquence, les audits de sécurité informatique revêtent une importance cruciale, permettant de détecter et de rectifier les failles de sécurité avant qu'elles ne soient exploitées. Dans cette perspective, cette étude se penchera sur l'importance de l'identification des vulnérabilités au sein des réseaux informatiques dans le cadre des audits de sécurité.

Actuellement, les systèmes d'information font face à un dilemme majeur : ils doivent fournir des données pertinentes et utiles aux utilisateurs tout en assurant la fiabilité, la sécurité, et la confidentialité de ces informations. La sécurité s'impose comme un enjeu majeur dans le domaine des systèmes informatiques, car les menaces, aussi bien internes qu'externes, planent sur les données stockées et traitées par ces systèmes. Les entreprises doivent ainsi mettre en place des dispositifs de sécurité adéquats, tels que des pare-feux, des antivirus, et des systèmes de gestion d'identité et d'accès, afin de protéger leurs données contre les cyberattaques et les erreurs humaines.

Ce mémoire a pour but de fournir une vue d'ensemble exhaustive des vulnérabilités potentielles présentes au sein des réseaux informatiques d’une entreprise. Les vulnérabilités, représentant des failles de sécurité, peuvent être exploitées par des attaquants en vue d'accéder illicitement à des données sensibles ou de compromettre le fonctionnement du réseau.

Chapitre I

Sécurité informatique

II.1. Introduction

De nos jours, les systèmes d'information sont de plus en plus ouverts à internet, ce qui a fait qu'ils sont de plus en plus sujets à des attaques et menaces. C'est pour cela que leur sécurisation est devenue plus que primordiale afin d'éviter au maximum qu'ils soient atteints, ainsi que de déceler les vulnérabilités de nos systèmes le plus tôt possible pour mieux les sécuriser.

Dans ce premier chapitre, nous allons présenter les systèmes d'information et les réseaux informatiques ainsi que des notions et objectifs de la sécurité informatique, tout en définissant ce que sont que des vulnérabilités et nous allons finir par la présentation d'un audit informatique.

II.2. Définition d'un système d'information

Un système est un ensemble d'éléments reliés qui forment une entité, un système d'information (SI) représente l'ensemble des données ainsi que des ressources logiciel et matérielles partagées d'une l'entreprise. Il permet de stocker, de faire circuler les ressources qu'il contient et représente également le réseau d'acteurs qui interviennent dans cette dernière.

Un système d'information représente le noyau d'une entreprise, c'est pour cela qu'il est primordial de le sécuriser de la meilleure manière possible et en continue pour éviter toute attaque émanent de l'extérieur tout comme de l'intérieure. [1]

II.3. Définition d'un réseau informatique

Un réseau informatique est un ensemble d'objets interconnectés les uns avec les autres. Permettent de faire circuler des éléments entre chacun de ces entités selon des règles bien définies. Ces transmissions de données peuvent être des échanges de messages entre utilisateurs, un accès à distance à des bases de données ou bien encore le partage de fichiers. Nous pouvant citer trois types de réseaux qui sont [2] :

- **LAN (Local Area Network) :** il représente un réseau local permettant l'échange de données et le partage de ressources relient des ordinateurs et des serveurs ;
- **MAN (Metropolitan Area Network) :** c'est un réseau dit métropolitain qui permet d'assurer la connexion de plus grande distance que le LAN (regroupent plusieurs LAN) ;
- **WAN (Wide Area Network) :** c'est un réseau pouvant être représenté à l'échelle d'un pays. Le plus connu des WAN est Internet.

II.4. Définition de la sécurité informatique

La sécurité informatique représente l'ensemble des moyens mis en œuvre, qu'ils soient techniques, juridiques, organisationnels ou humains pour réduire la vulnérabilité d'un système contre toutes les menaces quelles soit accidentelles ou bien intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité. [5]

II.4.1. Objectifs de la sécurité informatique

La sécurité informatique vise généralement à protéger les informations contre toutes divulgation, altération ou destruction ainsi que de garantir que les ressources matérielles et logicielles d'un système soient utilisées dans un cadre prévu. Parmi ces objectifs, on cite : [4]

- **La confidentialité :** elle consiste à s'assurer que les informations confidentielles ne soient accessibles que par les personnes autorisées ;
- **L'intégrité :** elle consiste à garantir que les données protégées ne peuvent être modifiées que par les personnes autorisées ;
- **La disponibilité :** elle consiste à garantir l'accès à un service ou à une ressource pour les personnes autorisées ;
- **La non-répudiation :** il s'agit de s'assurer qu'un correspondant participant dans une transaction ne peut nier son implication ;
- **L'authentification :** elle permet de s'assurer de l'identité d'un utilisateur donné. C'est-à-dire garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

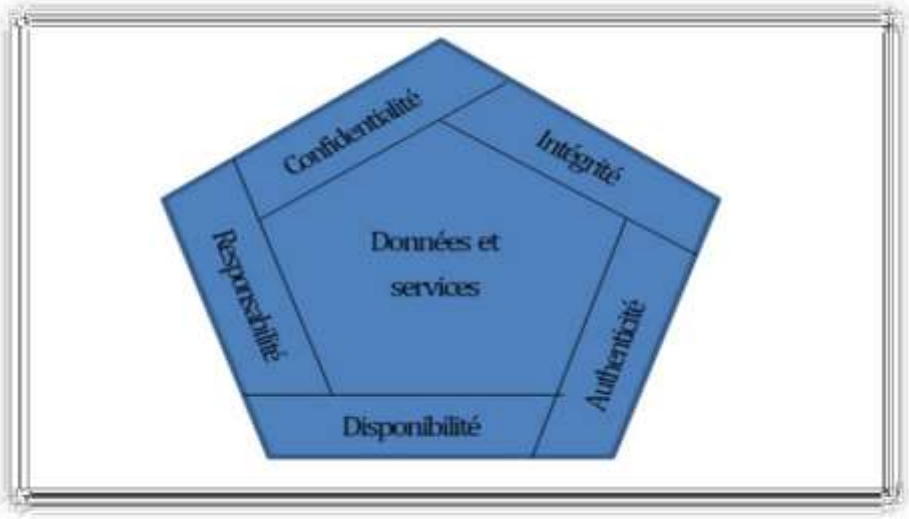


Figure I.1. Piliers de la sécurité informatique et réseau

II.5. Politique de sécurité

La politique de sécurité est un ensemble de règles, de procédures et de mesures mises en place pour protéger les informations et les systèmes d'une organisation contre les menaces et les risques potentiels. Elle a pour objectif de garantir la confidentialité, l'intégrité et la disponibilité des données, ainsi que de prévenir les incidents de sécurité [3].

Voici les principaux éléments qui composent une politique de sécurité :

- **Objectifs de sécurité :** il s'agit des objectifs que l'organisation souhaite atteindre en matière de sécurité. Ces objectifs doivent être clairement définis et compris par tous les membres de l'organisation ;
- **Responsabilités de sécurité :** il est important de définir les rôles et les responsabilités de chacun en matière de sécurité, afin que chaque personne sache ce qu'elle doit faire pour contribuer à la sécurité de l'organisation ;
- **Procédures de sécurité :** les procédures de sécurité décrivent les actions à entreprendre pour protéger les informations et les systèmes de l'organisation. Ces procédures doivent être claires, précises et faciles à suivre ;
- **Sensibilisation à la sécurité :** il est important de sensibiliser tous les membres de l'organisation à la sécurité de l'information et de leur apprendre à adopter des comportements sécurisés ;

- **Gestion des incidents de sécurité :** la politique de sécurité doit également inclure des procédures pour gérer les incidents de sécurité, tels que les attaques informatiques ou les violations de données ;
- **Surveillance de la sécurité :** la surveillance de la sécurité doit être mise en place pour détecter les menaces et les risques potentiels, afin de prendre des mesures préventives en temps utile.

En résumé, la politique de sécurité est un élément clé de la protection des informations et des systèmes d'une organisation. Elle doit être élaborée de manière claire et précise, et comprendre les objectifs de sécurité, des responsabilités, des procédures, de la sensibilisation à la sécurité, la gestion des incidents de sécurité et la surveillance de la sécurité (Fig.I.2).

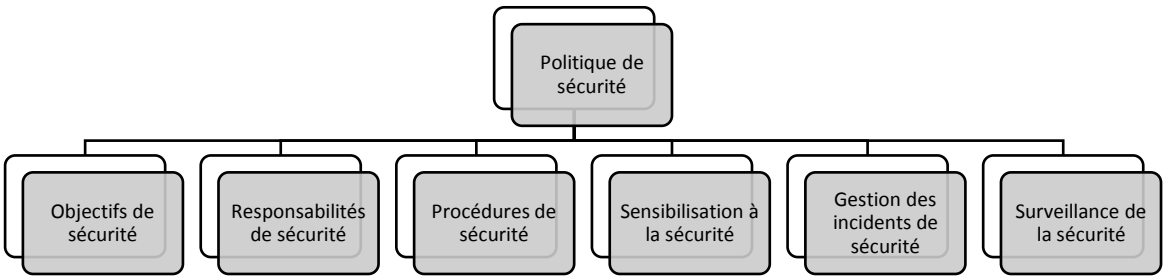


Figure I.2. Composants d'une politique de sécurité [3].

II.5.1. Stratégie de la politique de sécurité

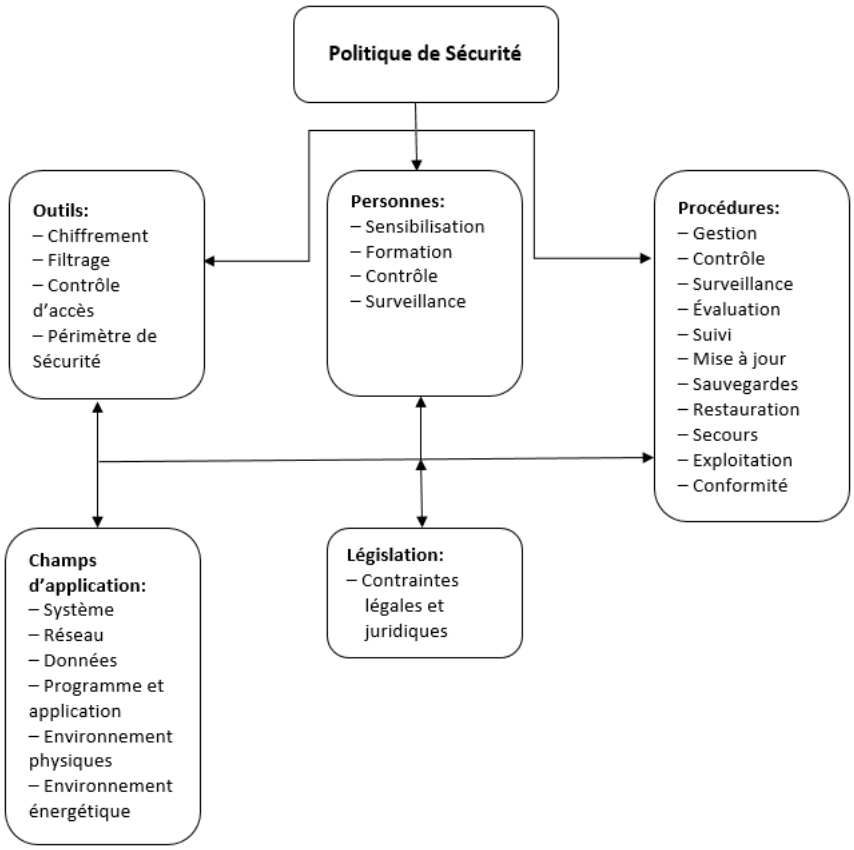
La stratégie de la politique de sécurité informatique est la planification de l'approche globale de la sécurité informatique de l'organisation. Elle comprend les objectifs de sécurité, les processus de gestion des risques et les plans d'action pour répondre aux menaces potentielles. [3]

Voici quelques éléments clés que devrait inclure une stratégie de politique de sécurité :

- **Objectifs de sécurité :** les objectifs de sécurité définissent les objectifs généraux de l'organisation en matière de sécurité informatique. Ils peuvent inclure la protection des données, la conformité réglementaire, la disponibilité des systèmes, la réduction des risques et la prévention des pertes financières ;
- **Processus de gestion des risques :** la gestion des risques est le processus d'identification, d'évaluation et de traitement des risques pour l'organisation. Cela peut

inclure l'identification des actifs à protéger, l'analyse des menaces et des vulnérabilités, l'évaluation des risques, le choix des contre-mesures et la mise en œuvre de plans d'action ;

- **Plan d'actions :** un plan d'actions est une feuille de route détaillée pour la mise en œuvre de la stratégie de sécurité informatique de l'organisation. Il peut inclure des actions telles que l'installation de technologies de sécurité, la formation des employés, la mise en place de politiques de sécurité et la création d'un plan de réponse aux incidents ;
- **Gestion des incidents :** la gestion des incidents est le processus de réponse aux incidents de sécurité informatique tels que les attaques de virus, les pertes de données et les violations de la sécurité. Les organisations doivent avoir des plans de réponse aux incidents en place pour minimiser les dommages causés par ces événements ;
- **Mise en place de la politique de sécurité :** les politiques de sécurité sont des règles et des procédures qui définissent les règles de sécurité de l'organisation. Les politiques doivent être claires et applicables à tous les employés, et doivent être régulièrement mises à jour pour refléter les



changements dans les technologies et les menaces.

Figure I.3. Stratégie de la politique de sécurité [3].

II.5.2. Elaboration du document (politique de sécurité)

L'élaboration d'un document de politique de sécurité informatique est un processus important pour garantir la sécurité et la protection des systèmes, des données et des informations de l'organisation. [3]

Voici les étapes clés pour élaborer un tel document :

- **Identifier les objectifs de sécurité :** avant de commencer à écrire la politique de sécurité, il est important de définir les objectifs de sécurité de l'organisation. Les objectifs peuvent varier en fonction des besoins spécifiques de l'entreprise, mais ils doivent être alignés sur les meilleures pratiques de l'industrie et les réglementations en vigueur ;
- **Identifier les actifs à protéger :** il est important de savoir quels sont les actifs critiques à protéger. Les actifs peuvent inclure les données de l'entreprise, les systèmes, les applications, les équipements et les infrastructures. Il est important de déterminer leur importance, leur valeur et leur sensibilité pour l'organisation ;

- **Élaborer les politiques de sécurité :** les politiques de sécurité définissent les règles et les procédures que les employés de l'organisation doivent suivre pour garantir la sécurité des systèmes et des données. Cela peut inclure des politiques pour la gestion des mots de passe, l'accès aux systèmes, la gestion des patchs, la gestion des sauvegardes et la gestion des logs ;
- **Définir les responsabilités :** il est important de définir les rôles et les responsabilités pour la sécurité informatique. Cela peut inclure la désignation d'un responsable de la sécurité informatique, la définition des rôles et des responsabilités pour les utilisateurs finaux, les administrateurs de systèmes, les développeurs et les fournisseurs tiers ;
- **Définir les procédures de réponse aux incidents :** les incidents de sécurité sont inévitables, il est donc important de définir des procédures de réponse aux incidents pour minimiser les dommages causés par ces derniers. Les procédures doivent inclure des instructions claires sur la façon de signaler les incidents, comment les gérer et comment les documenter ;
- **Réviser et mettre à jour régulièrement :** la politique de sécurité doit être régulièrement révisée et mise à jour pour garantir qu'elle reste pertinente et efficace. Les changements dans les technologies, les menaces et les pratiques de sécurité peuvent nécessiter des ajustements à la politique de sécurité.

En fin de compte, l'élaboration d'un document de politique de sécurité est un processus continu qui nécessite une attention constante pour garantir que les mesures de sécurité sont adéquates pour protéger les actifs de l'organisation.

II.5.3. Outils associés à la politique de sécurité

Il existe de nombreux outils associés à la politique de sécurité informatique, qui aident à mettre en œuvre et à renforcer les mesures de sécurité de l'organisation [3]. Voici quelques exemples :

- **Pare-feu :** un pare-feu est un dispositif de sécurité qui contrôle le trafic réseau entrant et sortant pour protéger les systèmes contre les attaques externes. Il est souvent utilisé comme première ligne de défense pour empêcher les intrusions.
- **Logiciels de détection d'intrusions :** les logiciels de détection d'intrusions surveillent le réseau pour détecter les comportements suspects ou malveillants. Ils peuvent alerter les administrateurs de systèmes en cas d'activité suspecte ;

- **Antivirus et antimalware :** les programmes antivirus et antimalware protègent les systèmes contre les logiciels malveillants et les virus. Ils scannent régulièrement les fichiers pour détecter les menaces potentielles et les supprimer ;
- **Systèmes de gestion des identités et des accès :** les systèmes de gestion des identités et des accès permettent de contrôler l'accès aux systèmes et aux données en définissant les autorisations pour les utilisateurs et les groupes. Ils permettent également de suivre l'utilisation des ressources informatiques par les utilisateurs ;
- **Systèmes de sauvegarde et de récupération des données :** les systèmes de sauvegarde et de récupération des données permettent de récupérer les données en cas de panne de système, de corruption de données ou d'autres incidents ;
- **Formation et sensibilisation à la sécurité :** les programmes de formation et de sensibilisation à la sécurité aident à éduquer les utilisateurs finaux sur les meilleures pratiques de sécurité, les menaces potentielles et les comportements à risque. Ils peuvent aider à réduire les erreurs humaines qui peuvent compromettre la sécurité ;
- **Services de sécurité gérés :** les services de sécurité gérés fournissent des services de sécurité avancés pour les organisations qui n'ont pas les ressources internes nécessaires pour mettre en place et gérer les mesures de sécurité. Ils peuvent fournir une surveillance continue, une analyse de sécurité, des alertes de sécurité et des rapports de conformité.

Ces outils peuvent être utilisés ensemble pour mettre en œuvre les mesures de sécurité appropriées pour l'organisation. Il est important de choisir les outils appropriés en fonction des besoins et des exigences spécifiques de l'organisation.

II.6. Définition de vulnérabilité

Une vulnérabilité représente une faiblesse ou une faille qui peut être exploitée par un attaquant pour effectuer des actions non autorisées. Il peut s'agir d'une modification, d'une suppression ou d'une divulgation au sein d'un ordinateur ou d'un système réseau sur lequel il n'a aucune juridiction [7]**.**

Nous pouvons citer trois catégories de vulnérabilité qui sont :

- **Vulnérabilités liées aux domaines physiques :** ces vulnérabilités représentent le manque de ressources au niveau des équipements ainsi qu'une mauvaise gestion et accès aux salles informatiques et aux bases de données ;

- **Vulnérabilités liées aux domaines organisationnels :** ces vulnérabilisées sont dites humaines et sont dues au manque de qualification du personnel d'une société ;
- **Vulnérabilités liées aux domaines technologiques :** ces vulnérabilités regroupent tous ce qui est systèmes d'exploitation, logiciels, failles ainsi que l'architecture des réseaux et principalement leur mauvaise gestion et le manque des mises à jour et des correctifs.

II.7. Audit informatique

Un audit informatique de sécurité est un processus d'examen systématique et approfondi de la sécurité d'un SI, pour identifier les vulnérabilités et les risques potentiels. Il peut être effectué soit par une équipe interne de sécurité ou bien par une entreprise extérieure spécialisée en sécurité informatique. Sa mission consiste à mesurer le niveau d'application des règles préalablement rédigées sur le système d'information par rapport aux règles qui devraient être effectivement appliquées selon les processus édictés. Ce dernier permet de prendre des décisions éclairées sur les opérations de l'organisation auditée [6].

II.7.1. Rôles et objectifs d'un audit informatique

La réalisation d'un audit a plusieurs objectifs parmi lesquels, nous citons :

- **Évaluation de la conformité :** permet de déterminer si les pratiques de l'organisation sont conformes aux normes et aux lois en vigueur ;
- **Identification des** risques : les risque de fraude, les risques opérationnels, les risque financiers et les risques de conformité ;
- **Amélioration des processus :** permet de vérifier si les processus sont efficaces et répondent aux objectifs de l'organisation et des recommandations pour améliorer et aider l'organisation à atteindre ses objectifs ;
- **Respect de exigences légales :** permet la conformité aux exigences légales telles que la sécurité des données, la protection de la vie privé et d'autre domaines ;
- **Proposition d'action :** vise l'amélioration du niveau de sécurité du système d'information.

II.7.2. Etapes d'un audit informatique [6]

L'exécution d'un audit informatique passe par les étapes suivantes :

- **Définition de la charte de l'audit et sa préparation :** cette phase consiste en la définition des objectifs de l'audit, les ressources nécessaires, les échéances, les personnes impliquées dans l'audit ainsi que la collecte d'informations sur le système ou les processus à auditer

- **Evaluation des risques** : durant cette phase, l'auditeur a pour objectif d'évaluer les risques associés aux actifs du système, notamment les données, les logiciels et les matériels. Cette étape permet de déterminer les vulnérabilités et les menaces potentielles.
- **Test de vulnérabilité :** lors de cette phase, l'auditeur va utiliser des outils d'analyse de vulnérabilités pour identifier les failles de sécurité dans le système et pour vérifier l'efficacité des mesures de sécurité en place tout en sensibilisant les acteurs de l'audit.
- **Rapport d'audit et recommandations** : à la fin de ces étapes, l'auditeur ou bien l'expert SI va élaborer un rapport qui décrit les résultats de l'audit, les conclusions et les recommandations d'amélioration ainsi qu'un cahier des charges permettant d'appliquer ces recommandations dans le but d'améliorer la sécurité du système.

II.8. Conclusion

Dans ce chapitre, nous avons présenté les réseaux et systèmes d'information ainsi que la sécurité informatique et ses objectifs principaux qui sont : la confidentialité, l'intégrité, la disponibilité, la non-répudiation, l'authentification et les objectifs d'audit informatique.

Chapitre II

Présentation de l'organisme d'accueille

III.1. Introduction :

Afin de nous familiariser avec l'environnement de l'entreprise, nous allons définir certaines activités du groupe CEVITAL, ses différentes divisions qui la constituent ainsi que les taches associées à chaque division.

Ce chapitre est ainsi, une introduction à l'environnement de l'entreprise CEVITAL ainsi qu'à son étude globale.

III.2. Présentation du groupe CEVITAL :

CEVITAL est un groupe industriel algérien qui opère dans plusieurs secteurs d'activité, tels que l'agroalimentaire, l'électronique, l'automobile, la sidérurgie, le verre et l'emballage et considérer comme la Première entreprise privée algérienne à avoir investi dans des secteurs d'activités diversifiés.

Fondé en 1998, le groupe CEVITAL s'est construit au fil des investissements, autour de l'idée forte de constituer un ensemble économique est aujourd'hui l'un des plus importants groupes industriels d'Afrique Porté par 18 000 employés répartis sur 3 continents, il représente le fleuron de l'économie algérienne, et œuvre continuellement dans la création d'emplois et de richesses.

III.3. Description de CEVITAL :

Vision, Mission et Valeurs du groupe CEVITAL :

- **Vision :**

  Forts de notre esprit entrepreneurial, nous saisissons des opportunités de croissance et de diversification rentables pour devenir un acteur majeur en Afrique, en Europe et dans le bassin Méditerranéen.

- **Mission :**

  Contribuer au développement économique de l'Algérie et servir nos concitoyens.

- **Valeurs :**

  Nos règles d'or sont : **Intégrité-Respect-Initiative-Solidarité**, s'inscrivent dans une philosophie et une pratique quotidienne de développement humain, de création de richesse et de protection de l'environnement au bénéfice de toutes les parties prenantes internes et externes de CEVITAL ».

III.4. L'organisation générale des composantes et les missions des directions :

III.4.1 Structure de l'encadrement : (organigramme)

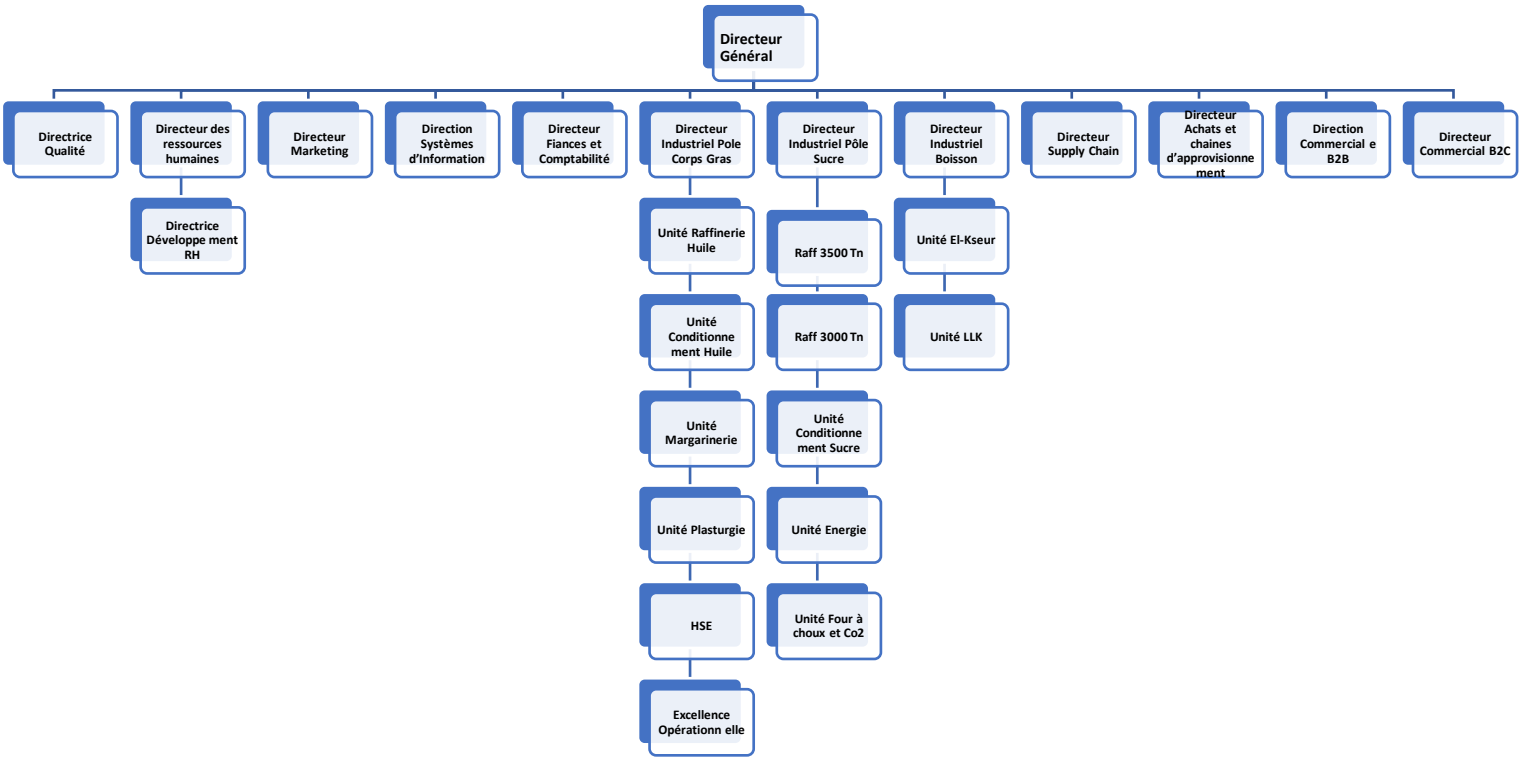


Figure II.1. Organigramme globale de l'entreprise CEVITAL.

III.4.2 Missions et services des composantes de la DG :

L'organisation mise en place consiste en la mobilisation des Ressources humaines matérielles et financières pour atteindre les objectifs demandés par le groupe**.**

La Direction générale est composée d'un secrétariat et de 19 directions :

- **La direction Marketing :**

Pour atteindre les objectifs de l'Entreprise, le Marketing CEVITAL pilote les marques et les gammes de produits. Son principal levier est la connaissance des consommateurs, leurs besoins, leurs usages, ainsi que la veille sur les marchés internationaux et sur la concurrence. Les équipes marketing produisent des recommandations d'innovation, de rénovation, d'animation publi-promotionnelle sur les marques et métiers CEVITAL. Ces

recommandations, validées, sont mises en œuvre par des groupes de projets pluridisciplinaires (Développement, Industriel, Approvisionnement, Commercial, Finances) coordonnés par le Marketing, jusqu'au lancement proprement dit et à son évaluation.

- **La direction des Ventes & Commerciale :**

Elle a en charge de commercialiser toutes les gammes des produits et le développement du Fichier clients de l'entreprise, au moyen d'actions de détection ou de promotion de projets à base de hautes technologies.

En relation directe avec la clientèle, elle possède des qualités relationnelles pour susciter l'intérêt des prospects.

- **La direction Système d'informations :**

Elle assure la mise en place des moyens des technologies de l'information nécessaires pour supporter et améliorer l'activité, la stratégie et la performance de l'entreprise.

Elle doit ainsi veiller à la cohérence des moyens informatiques et de communication mises à la disposition des utilisateurs, à leur mise à niveau, à leur maîtrise technique et à leur disponibilité et opérationnalité permanente et en toute sécurité.

Elle définit, également, dans le cadre des plans pluriannuels les évolutions nécessaires en fonction des objectifs de l'entreprise et des nouvelles technologies.

- **La direction des Finances et Comptabilité :**

Préparer et mettre à jour les budgets Tenir la comptabilité et préparer les états comptables et financiers selon les normes Pratiquer le contrôle de gestion Faire le Reporting périodique

- **La direction Industrielle :**

Chargé de l'évolution industrielle des sites de production et définit, avec la direction générale, les objectifs et le budget de chaque site.

Analyse les dysfonctionnements sur chaque site (équipements, organisation...) et recherche les solutions techniques ou humaines pour améliorer en permanence la productivité, la qualité des produits et des conditions de travail.

Anticipe les besoins en matériel et supervise leur achat (étude technique, tarif, installation...).

Est responsable de la politique environnement et sécurité Participe aux études de faisabilité des nouveaux produits.

- **La direction des Ressources Humaines :**

Définit et propose à la direction générale les principes de Gestion ressources humaines en support avec les objectifs du business et en ligne avec la politique RH groupe.

Assure un support administratif de qualité à l'ensemble du personnel de CEVITAL food

Pilote les activités du social.

Assiste la direction générale ainsi que tous les managers sur tous les aspects de gestion ressources humaines, établit et maitrise les procédures.

Assure le recrutement.

Chargé de la gestion des carrières, identifie les besoins en mobilité.

Gestion de la performance et des rémunérations.

Formation du personnel Assiste la direction générale et les managers dans les actions disciplinaires Participe avec la direction générale à l'élaboration de la politique de communication afin de développer l'adhésion du personnel aux objectifs fixés par l'organisation

- **La direction Approvisionnements :**

Dans le cadre de la stratégie globale d'approvisionnement et des budgets alloués (investissement et fonctionnement).

Elle met en place les mécanismes permettant de satisfaire les besoins matière et services dans les meilleurs délais, avec la meilleure qualité et au moindre coût afin de permettre la réalisation des objectifs de production et de vente.

- **La direction Logistique :**

Expédie les produits finis (sucre, huile, margarine, Eau minérale, …), qui consiste à charger les camions à livrer aux clients sur site et des dépôts Logistique.

Assure et gère le transport de tous les produits finis, que ce soit en moyens propres (camions de CEVITAL), affrétés ou moyens de transport des clients.

Le service transport assure aussi l'alimentation des différentes unités de production en quelques matières premières intrants et packaging et le transport pour certaines filiales du groupe (MFG, SAMHA, Direction Projets, NUMIDIS, …).

Gère les stocks de produits finis dans les différents dépôts locaux (Bejaia et environs) et Régionaux (Alger, Oran, Sétif, …).

- **La direction des Silos :**

Elle décharge les matières premières vrac arrivées par navire ou camions vers les points de stockage.

Elle stocke dans les conditions optimales les matières premières ; Elle Expédie et transfère vers les différents utilisateurs de ces produits dont l'alimentation de raffinerie de sucre et les futures unités de trituration.

Elle entretient et maintient en état de services les installations des unités silos

- **La direction des Boissons :**

Le Pôle Boissons et plastiques comprend trois unités industrielles situées en dehors du site de Bejaia :

- Unité LALLA KHEDIDJA domiciliée à Agouni-gueghrane (Wilaya de TIZI OUZOU) a pour vocation principale la production d'eau minérale et de boissons carbonatées à partir de la célèbre source de LLK Unité plastique, installée dans la même localité, assure la production des besoins en emballages pour les produits de Margarine et les Huiles et à terme des palettes, des étiquettes etc.
- Unité COJEK, implantée dans la zone industrielle d'El Kseur, Cojek est une SPA filiale de CEVITAL et qui a pour vocation la transformation de fruits et légumes frais en Jus, Nectars et Conserves. Le groupe ambitionne d'être Leader dans cette activité après la mise en œuvre d'un important plan de développement

- **La direction Corps Gras :**

Le pole corps gras est constitué des unités de production suivantes : une raffinerie d'huile de 1800 T/J, un conditionnement d'huile de 2200T/J, une margarinerie de 600T/J qui sont toutes opérationnelles et une unité inter estérification – Hydrogénation –pate

chocolatière –utilités actuellement en chantier à El kseur. Notre mission principale est de raffiner et de conditionner différentes huiles végétales ainsi que la production de différents types de margarines et beurre. Tous nos produits sont destinés à la consommation d'où notre préoccupation est de satisfaire le marché local et celui de l'export qualitativement et quantitativement.

- **La direction Pôle Sucre :**

Le pôle sucre est constitué de 04 unités de production : une raffinerie de sucre solide 2000T/J, une raffinerie de sucre solide 3000T/J, une unité de sucre liquide 600T/J, et une unité de conditionnement de sucre 2000 T/J qui sera mise en service en mars 2010.Sa vocation est de produire du sucre solide et liquide dans le respect des normes de qualité, de la préservation du milieu naturel et de la sécurité des personnes. Nos produits sont destinés aux industriels et aux particuliers et ce pour le marché local et à l'export. »

- **La direction QHSE :**

Met e en place, maintient et améliore les différents systèmes de management et référentiels pour se conformer aux standards internationaux Veille au respect des exigences règlementaires produits, environnement et sécurité Garantit la sécurité de notre personnel et la pérennité de nos installations Contrôle, assure la qualité de tous les produits de CEVITAL et réponse aux exigences clients

- **La direction Energie et Utilités :**

C'est la production et la distribution pour les différentes unités, avec en prime une qualité propre à chaque Process : D'environ 450 m3/h d'eau (brute, osmosée, adoucie et ultra pure) ; de la vapeur Ultra haute pression 300T/H et basse pression 500T/H. De l'Electricité Haute Tension, Moyenne Tension et Basse Tension, avec une capacité de 50M W. /

- **La direction Maintenance et travaux neufs :**

Met en place et intègre de nouveaux équipements industriels et procédés Planifie et assure la Maintenance pour l'ensemble des installations.

Gère et déploie avec le Directeur Industriel et les Directeurs de Pôles les projets d'investissement relatifs aux lignes de production, bâtiments et énergie/utilité (depuis la

définition du processus jusqu'à la mise en route de la ligne ou de l'atelier) Rédige les cahiers des charges en interne.

Négocie avec les fournisseurs et les intervenants extérieurs.

III.5. Vulnérabilité au quelle nous avons pu assister :

- **Vulnérabilité N°1 :** Détection ports ouverts sur un système cible, c'est une attaque par balayage TCP cette faille permet facilement de se faire exploiter car elle permet de détecter les ports ouverts sur un système cible et parmi les impacts que cela peut avoir sur notre système nous pouvant citer la Révélation d'informations sensibles sur le système, la préparation d'une attaque ainsi que la surcharge du réseau. On considère son niveau de gravité comme étant élevé

Afin de palier à ce problème nous invitent les administrateur réseaux. A configurer des pare-feux pour limiter les connexion suspecte et de fermer les ports inutilisés tout en configurant les systèmes de manier à limiter les tentatives de connexion anormalement élevés et bien évidemment sensibiliser les utilisateurs sur les bons pratiques à suivre.

- **Vulnérabilité N°2 :** Vulnérabilité dans la mise en œuvre SNMP du réseau local sans fil, c'est une faille de sécurité dans la mise en œuvre du protocole SNMP (Simple Network Management Protocol) utilisé dans les réseaux locaux sans fil. Cette vulnérabilité peut permettre à un attaquant distant d'exécuter du code arbitraire ou de provoquer un déni de service en envoyant des paquets SNMP spécialement conçus. Parmi les impacts que cela peut avoir sur notre système nous pouvant citer la pertes financières, l'atteinte à la réputation un déni de service ainsi qu'une compromission des données. Ont considéré sont niveau de gravité comme étant modéré.

Afin de palier a cette faille il est recommandé d'effectuer régulièrement des mises a jours des équipements réseaux, de segmenter le réseau afin d'isoler les systèmes sensibles des réseaux sans fille et d'effectuer des audits de sécurité régulièrement pour identifier les potentielles faille au niveaux des équipements réseaux.

- **Vulnérabilité N°3 :** ARP Spoofing, cette vulnérabilité fait référence à l'exploitation du protocole ARP (Address Resolution Protocol) pour effectuer une usurpation d'identité au sein d'un réseau local. Cette vulnérabilité est considérée comme étant élevé car elle permet à l'attaquant d'intercepter le trafic de manipuler les données en cours de transmission tout comme il lui est permis d'altérer les données échanger

Dans l'optique de faire face à cette vulnérabilité il est recommandé d'utiliser des mécanismes de sécurités supplémentaire tel que les VPN et VLAN ainsi que l'authentification des adresses MAC et l'utilisation de protocole de sécurités réseau tel que le Secure ARP.

III.6. Conclusion :

Ce stage au sein de CEVITAL a été une expérience enrichissante pour nous. Nous avons pu mettre en pratique nos connaissances théoriques et acquérir de nouvelles compétences.et également assister à un vrai test sur la sécurité de l'audit au sein de l'entreprise.

Nous tenons à remercier toutes les personnes de l'équipe informatique qui nous ont accompagné tout au long de ce stage, ainsi que l'ensemble du personnel de CEVITAL pour leur accueil chaleureux et leur disponibilité.

Chapitre III

Recensement des attaques, des outils de sécurité réseaux et des vulnérabilités

IV.1. Introduction

De nos jours, les réseaux informatiques sont sujets à de multiples attaques de la part de différents hackers (pirates informatique), dans l'objectif d'écouter, de modifier ou bien même de détruire le réseau que ce soit du côté logiciel ou bien matériel. Par conséquent, des outils de sécurité réseaux ont été mis en œuvre afin de minimiser les dégâts car aucun système ne peut être entièrement sécurisé.

Dans ce chapitre, nous allons identifier les différents types d'attaquants ainsi que les attaques les plus recensées en finissant par les outils qui sont mis en œuvre afin de maximiser la sécurité.

IV.2. Différents types d'attaquants [8]

Nous pouvons citer trois chapeaux d'attaquant qui sont :

IV.2.1. Hackers white hats (pirate chapeau blanc)

En général, les actions qui sont menées par les hackers white hats sont dans le but de mieux sécuriser un réseau informatique pour une société et d'avertir les auteurs des vulnérabilités qui ont été détectées, car ce ne sont véritablement que des experts en sécurité informatique et ne font pas en sorte de tirer profit de manière illicite avec leur actions contrairement aux black hats.

Les white hacks font en sorte de divulguer les vulnérabilités et les menaces qu'ils ont découvert afin que des experts en sécurité informatique puissent les sécuriser contrairement aux black hats qui dissimulent et gardent ce genre d'informations. De plus, les pirates à chapeaux blanc partagent même les codes qui permettent de corriger une faille.

Cependant, même si les actions des hacker white hats sont à but de prévention, leurs actions sont répréhensibles par la loi.

IV.2.2. Hackers grey hats (pirates chapeaux grey)

Ils représentent un compromis entre les white hats et les black hats, c'est-à-dire qu'il font en sorte de divulguer les failles et vulnérabilités détectées avant même que les personnes concernées soit mis au courant de ces dernières. Ceci laisse le temps à des individus étrangers de procéder à des manœuvres contre ces réseaux défaillants dans le but de nuire à ces derniers en divulguant des informations qui peuvent être très compromettantes vis-à-vis du réseau et de ses membres.

Parmi leurs motivations, on cite leur curiosité à découvrir et à explorer de nouvelles failles et vulnérabilités, ce qui est complètement illégal.

IV.2.3. Hackers black hats (pirates chapeaux noir)

Ces hackers ont généralement des buts bien précis, notamment la recherche de gains financiers ou encore de de nuire à une entreprise ou organisation, ce qui est qualifié de cyberterrorisme. Les black hats ont généralement les mêmes connaissances et utilisent les mêmes techniques que les white hats et les grey hats. La principale différence entre ces trois hackers est que les black hats sont considérés comme des individus révoltés contre le système qui ne se limitent pas aux barrières légales et sont très souvent à l'origine de virus et de logiciels espions. De plus, il arrive que certaines entreprises fassent appel aux black hats pour travailler en étroite collaboration avec elles dans le but de mieux sécuriser leurs réseaux ou bien même de nuire à d'autres entreprises rivales.

IV.3. Différents types d'attaques [2]

La connaissance des différents types d'attaques réseau est essentielle pour prévenir les incidents de sécurité et renforcer la résilience des infrastructures informatiques. Elles sont tellement nombreuses qu'il serait impossible de toutes les énumérer. Cependant, nous allons en présenter certaines, qui sont :

IV.3.1. Attaques permettant de dévoiler le réseau

Ici, sont regroupées les attaques permettant de dévoiler le réseau et qui peuvent fournir aux attaquants des informations précieuses sur l'architecture, les systèmes et les ressources du réseau.

IV.3.2. Attaques par identification des systèmes réseau

L'attaque par identification des systèmes réseau est une technique utilisée par les attaquants pour découvrir les hôtes actifs et les services disponibles sur un réseau. Elle permet à l'attaquant de recueillir des informations précieuses sur la topologie et la configuration du réseau cible.

Cette attaque peut être réalisée de différentes manières, notamment par le biais de balayages ICMP (Internet Control Message Protocol) et de balayages TCP (Transmission Control Protocol). Voyons comment ces techniques fonctionnent :

- **Attaque par balayage ICMP**

L'attaque par balayage ICMP repose sur l'envoi de paquets ICMP Echo Request (ping) à différentes adresses IP du réseau cible. L'attaquant analyse les réponses ICMP Echo Reply pour déterminer si les adresses IP sont actives ou non. Ainsi, il peut dresser une liste des hôtes actifs sur le réseau (Fig II.1.).

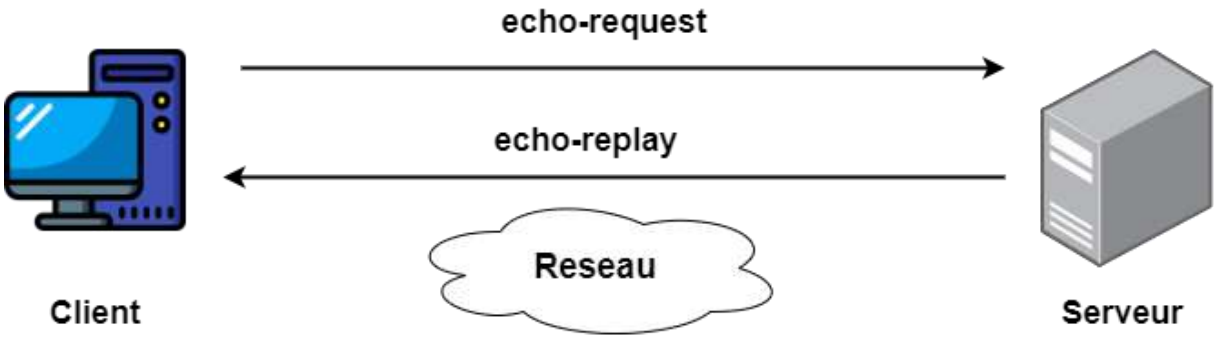


Figure III.1. Fonctionnement de la commande ping [3]

- **Attaque par balayage TCP**

L'attaque par balayage TCP vise à découvrir les ports ouverts sur les systèmes du réseau. L'attaquant envoie des paquets TCP SYN (synchronisation) à différentes adresses IP et ports. Il analyse les réponses SYN/ACK (synchronisation/accusé de réception) pour déterminer si le port est ouvert, fermé ou filtré par un pare-feu. Cette technique permet à l'attaquant de dresser une liste des services disponibles sur les hôtes du réseau.

Schéma de l'attaque par balayage TCP :

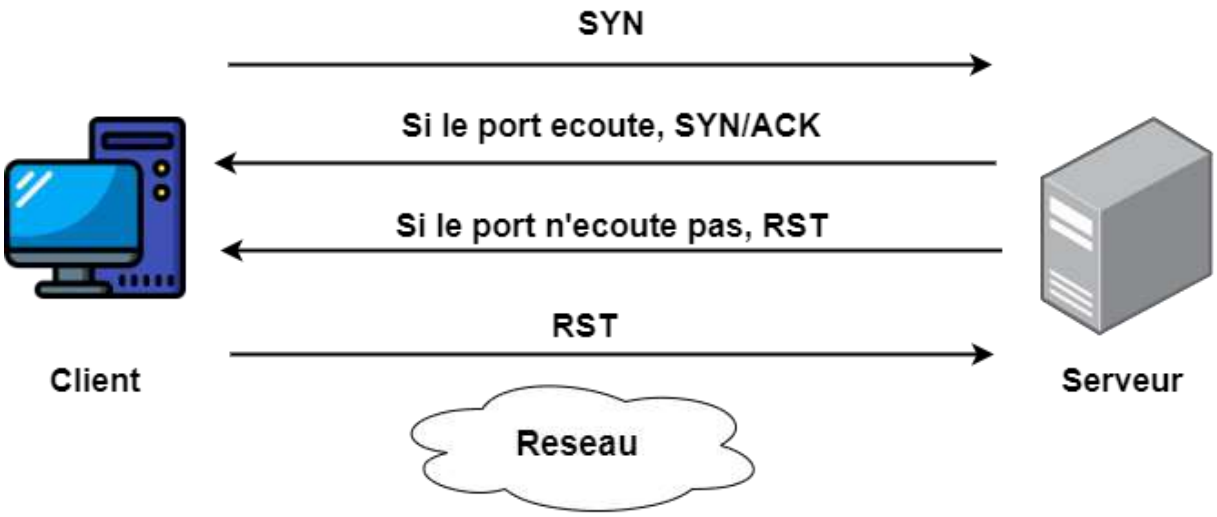


Figure III.2. Fonctionnement du balayage TCP [3]

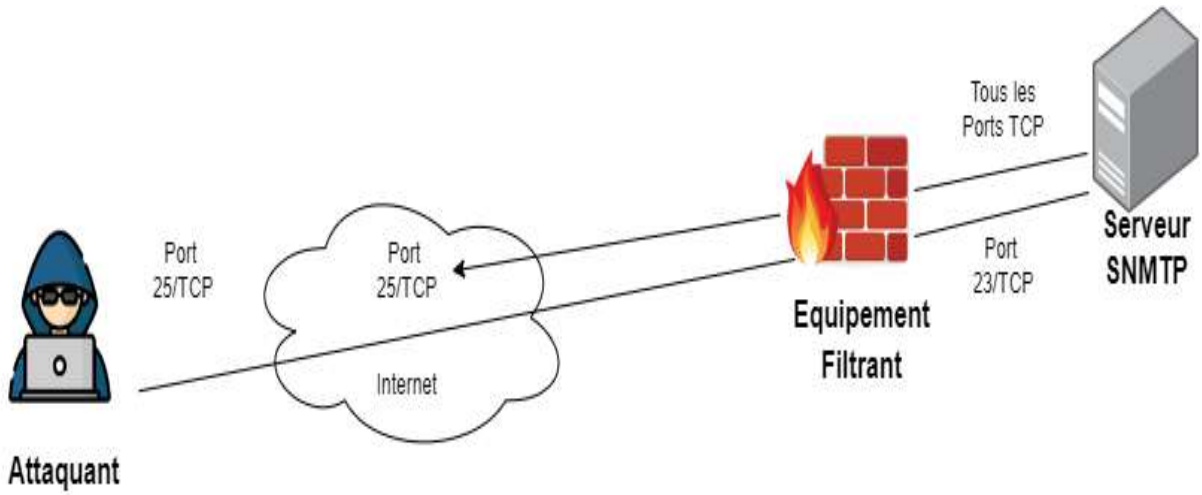
IV.3.3. Attaque par traversée des équipements filtrants

L'attaque par traversée des équipements filtrants, également connue sous le nom d'attaque par contournement des pares-feux, est une technique utilisée par les attaquants pour contourner les mesures de sécurité mises en place sur un réseau, telles que les pares-feux, les filtres de paquets et les dispositifs de sécurité réseau. Elle permet également à un attaquant d'accéder à des ressources normalement inaccessibles.

Il existe différentes techniques d'attaque par traversée des équipements filtrants, dont les deux plus courantes sont les suivantes :

- **Attaque par modification du port source**

L'attaquant modifie le numéro de port source des paquets qu'il envoie, de manière à tromper le pare-feu ou le filtre de paquets. En utilisant un numéro de port autorisé ou en faisant partie d'une plage de ports autorisés, l'attaquant peut masquer son trafic et le faire



passer à travers les équipements de sécurité sans être détecté.

Figure III.3. Traversée d'un pare-feu en fixant le port source [3]

- **Attaque par Fragment de paquet IP (Overlapping)**

L'attaquant fragmente les paquets qu'il envoie de manière à ce qu'ils se chevauchent lors de leur réassemblage par le destinataire. Cette technique exploite les règles de filtrage qui inspectent chaque fragment de manière individuelle sans prendre en compte leur position relative. Ainsi, l'attaquant peut introduire du trafic malveillant ou non autorisé en utilisant des fragments qui semblent être conformes aux règles de filtrage.

Schéma de l'attaque par fragmentation de paquet IP (overlapping) :

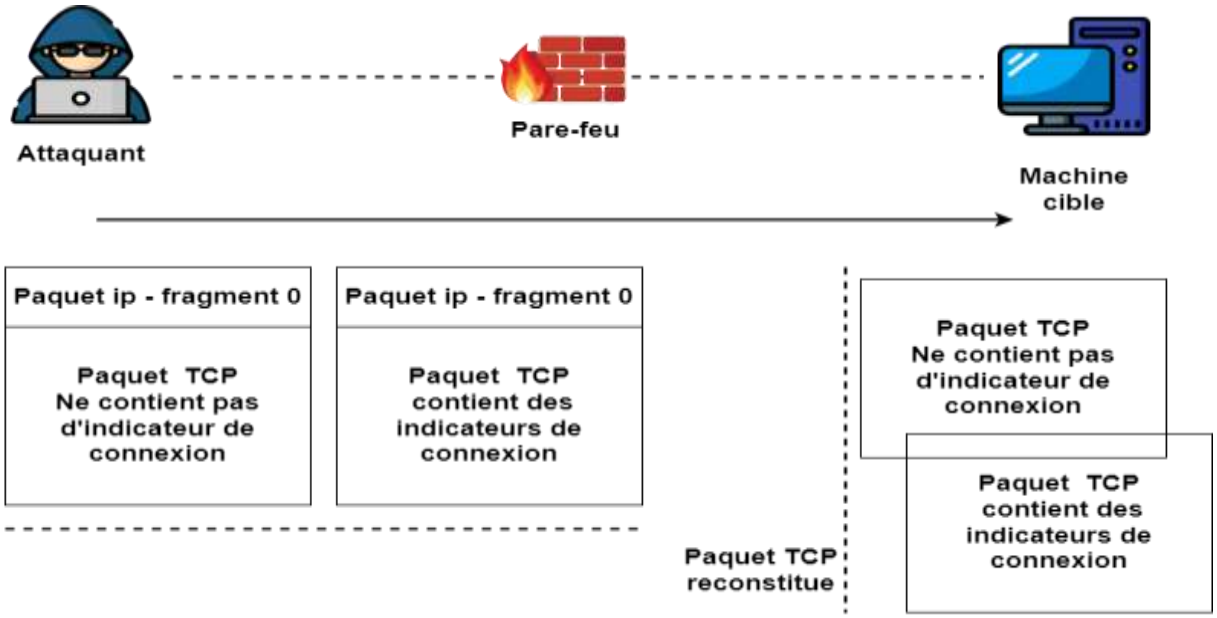


Figure III.4. Traversée d'un pare-feu en fixant le port source [3]

IV.3.4. Attaques permettant d'écouter le trafic réseau

Les attaques permettant d'écouter le trafic réseau, également connues sous le nom d'attaques d'écoute passive, sont des techniques utilisées par les attaquants pour intercepter et surveiller le trafic circulant sur un réseau. L'objectif principal de ces attaques est de collecter des informations sensibles, telles que des mots de passe, des données confidentielles ou des communications privées, sans être détectés.

Il existe différentes méthodes d'attaque permettant d'écouter le trafic réseau, parmi lesquelles les plus courantes sont les suivantes :

- **Attaque de commutateur**

L'attaquant exploite les vulnérabilités ou les faiblesses des commutateurs réseau pour intercepter le trafic. Par exemple, l'attaquant peut utiliser des techniques telles que le MAC flooding ou le VLAN hopping pour obtenir l'accès à des paquets qui ne lui sont pas destinés. Cela lui permet de capturer et d'analyser le trafic réseau afin d'extraire des informations sensibles.

Schéma de l'attaque de commutateur :

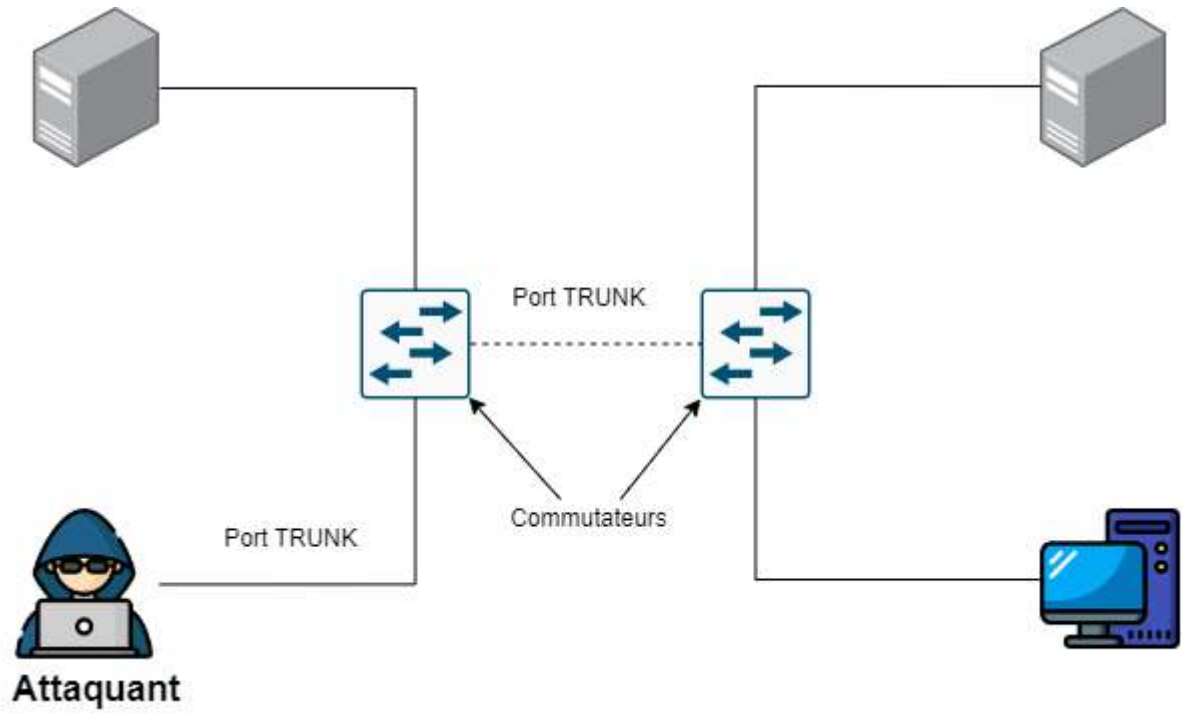


Figure III.5. Fonctionnement de l'attaque VLAN Hopping

- **Attaque par sniffing**

L'attaquant utilise des outils de sniffing pour capturer et analyser le trafic réseau. Ces outils permettent à l'attaquant d'intercepter les paquets de données qui transitent sur le réseau, de les décoder et d'extraire les informations sensibles qu'ils contiennent. Cette attaque peut être réalisée en étant directement connecté au réseau (par exemple, en étant sur le même réseau local) ou en utilisant des techniques telles que l'ARP poisoning pour rediriger le trafic vers l'attaquant.

Schéma de l'attaque par sniffing :

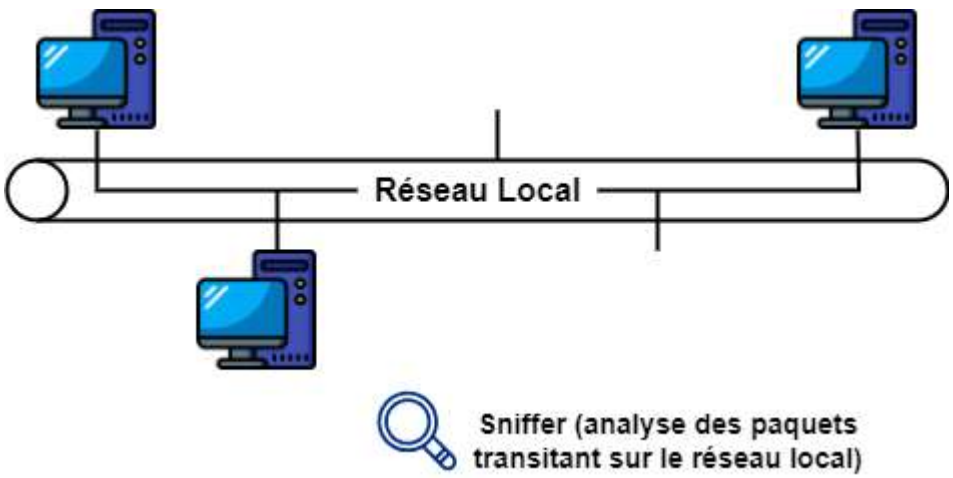


Figure III.6. Fonctionnement de l'attaque par sniffing

IV.3.5. Attaques permettant d'interférer avec une session réseau

Les attaques permettant d'interférer avec une session réseau sont des techniques utilisées par les attaquants pour perturber ou manipuler les communications entre deux entités ou systèmes sur un réseau. L'objectif principal de ces attaques est de compromettre l'intégrité, la confidentialité ou la disponibilité des données échangées au sein d'une session réseau.

Voici quelques exemples d'attaques permettant d'interférer avec une session réseau :

- **Attaque man-in-the-middle**

L'attaquant se positionne entre deux entités qui communiquent sur un réseau et intercepte ou modifie les données échangées entre elles. L'attaquant agit comme un relais invisible, ce qui lui permet de lire ou d'altérer les informations transmises sans que les entités ne s'en rendent compte.

Schéma de l'attaque man-in-the-middle :

Figure III.7. Attaque Man In The Middle [12]

- **Attaque ARP spoofing**

L'attaquant usurpe l'adresse MAC d'un autre périphérique sur le réseau en envoyant des fausses réponses ARP (Address Resolution Protocol) aux autres hôtes. Cela lui permet de rediriger le trafic réseau destiné à la victime vers sa propre machine, ce qui lui permet d'intercepter, modifier ou bloquer les données échangées dans la session.

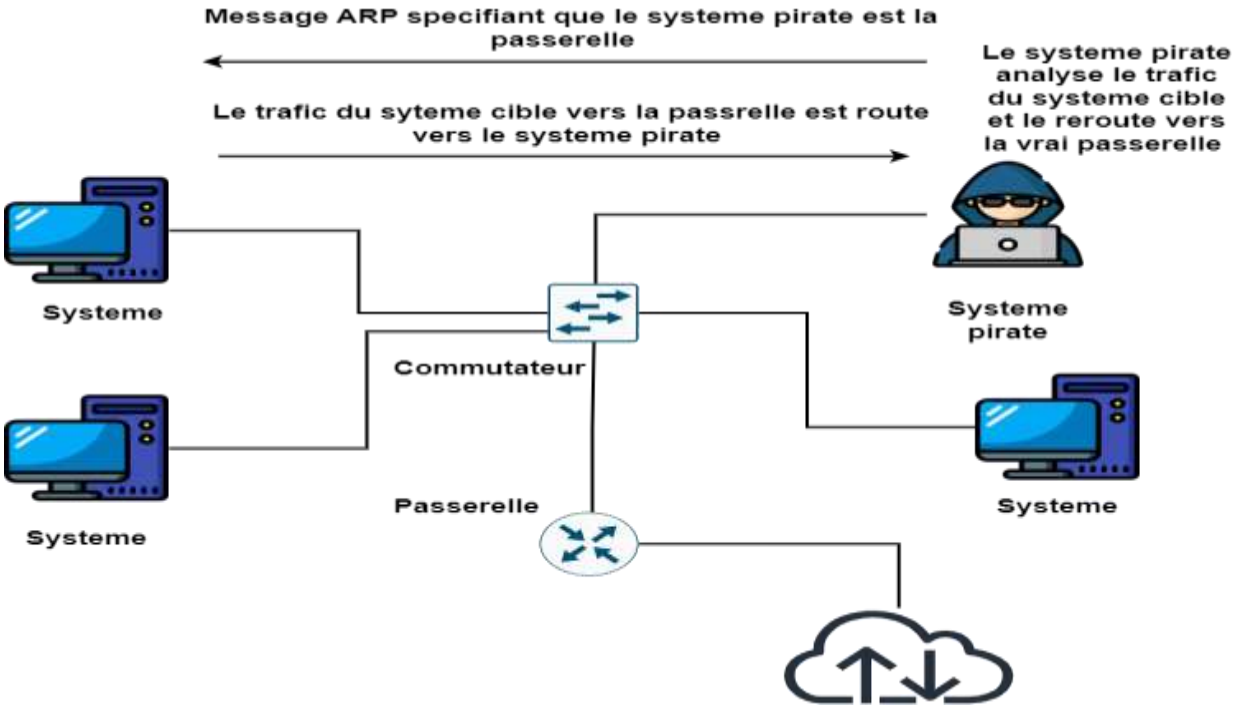


Schéma de l'attaque ARP spoofing :

Figure III.8. Attaque ARP spoofing [3]

- **Attaque IP spoofing**

L'attaquant falsifie l'adresse IP source dans les paquets qu'il envoie, ce qui lui permet de se faire passer pour une autre machine sur le réseau. Cela peut être utilisé pour tromper les systèmes de filtrage ou de contrôle d'accès basés sur l'adresse IP ou pour lancer des attaques en utilisant une fausse identité.

Schéma de l'attaque IP spoofing :

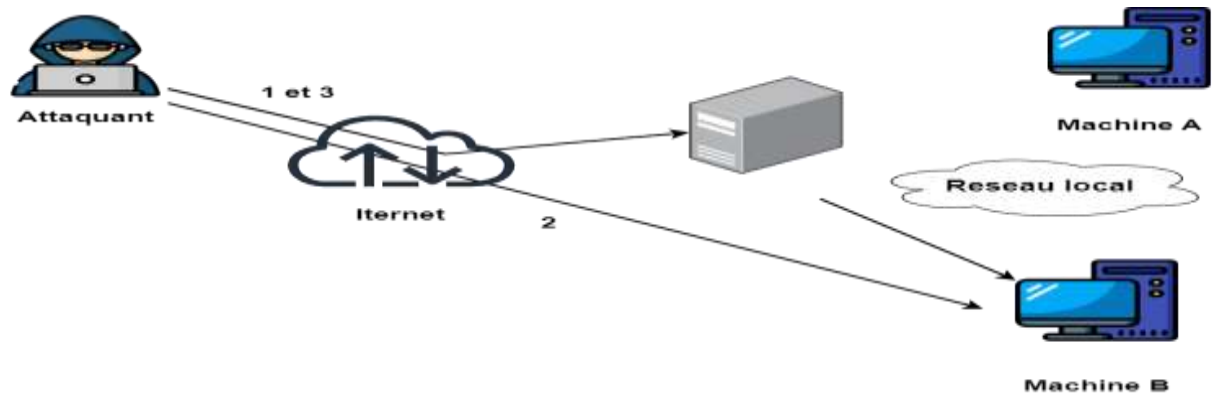


Figure III.9. Attaque IP spoofing [3]

IV.3.6. Attaques permettant de mettre le réseau en déni de service

Les attaques permettant de mettre le réseau en déni de service (Denial of Service - DoS) sont des techniques utilisées pour saturer ou épuiser les ressources d'un réseau, rendant les services ou les systèmes indisponibles pour les utilisateurs légitimes. L'objectif principal de ces attaques est de perturber ou de paralyser les opérations normales du réseau, entraînant une interruption du service ou une dégradation significative des performances.

Voici quelques exemples d'attaques permettant de mettre le réseau en déni de service :

- **Attaques par déni de service distribué (DDoS)**

Les attaques par déni de service distribué (Distributed Denial of Service - DDoS) sont des formes sophistiquées d'attaques visant à paralyser les services en ligne en inondant un système cible avec un trafic réseau excessif provenant de multiples sources. Contrairement aux attaques par déni de service classiques, les attaques DDoS impliquent la coordination d'un grand nombre de machines infectées ou compromises, appelées "botnets", qui agissent comme des agents malveillants pour envoyer un flux constant de requêtes vers la cible.

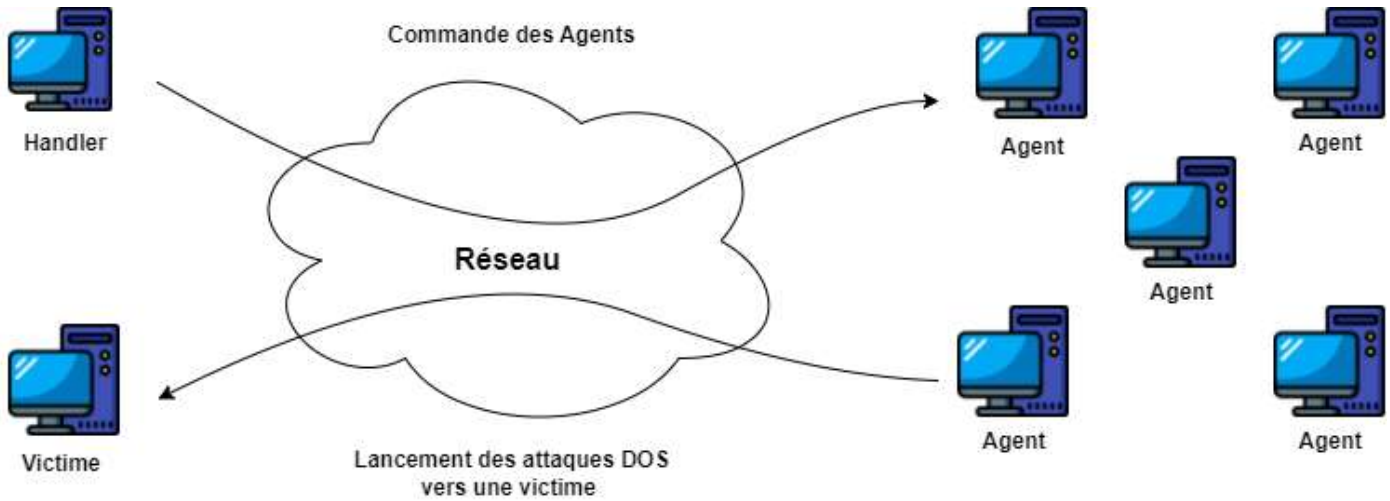


Schéma des attaques par déni de service distribué (DDoS) :

Figure III.10. Attaque par déni de service distribué [3]

- **Attaques smurf et fraggle par amplification de l'inondation**

Ces attaques exploitent des protocoles de diffusion comme ICMP (Internet Control Message Protocol) ou UDP (User Datagram Protocol) pour amplifier le trafic en envoyant des

requêtes falsifiées à un réseau ou à un sous-réseau. Cela provoque une surcharge des systèmes cibles, générant ainsi un déni de service.

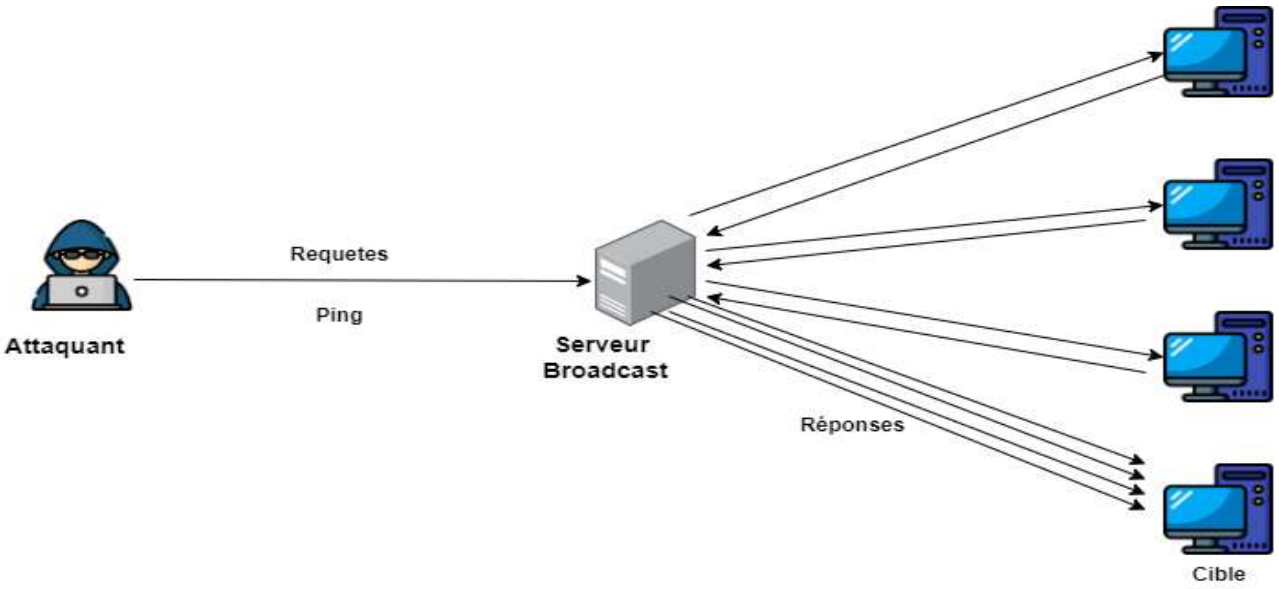


Schéma des attaques smurf et fraggle par amplification de l'inondation :

Figure III.11. Attaque smurf et fraggle par amplification de l'inondation [12]

IV.4. Outils de sécurité réseaux

Dans le but de renforcer la sécurité des réseaux informatiques et des données qui y circulent, il est nécessaire de faire appel à des outils de sécurité informatique qu'ils soient de nature logicielle ou bien matérielle que nous allons dans cette partie.

IV.4.1. Pares-feux

Un pare-feu est un système logiciel et matériel qui se trouve entre un réseau fiable et un réseau non fiable. Son objectif principal est de filtrer et d'empêcher le trafic non désiré de traverser la limite du pare-feu. Parmi les critères de filtrage nous pouvons citer l'origine du paquet, son adresse et son port. Afin d'être efficace, un pare-feu doit répondre à certaines exigences qui sont [9] :

• Être résistant aux attaques ;

• Être le seul point de transit entre deux réseaux ;

• Assurer l'application de la stratégie de contrôle d'accès de l'organisation ;

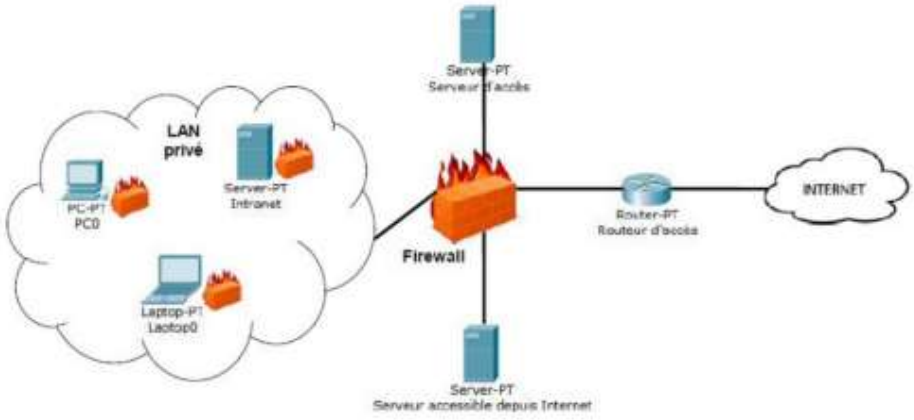


Figure III.12. Représentation de l'emplacement d'un pare-feu 'firewall'

IV.4.2. DMZ

La DMZ dite aussi zone démilitarisée représente un sous-réseau privé isolé qui sépare le LAN, d'un autre réseau tel qu'internet. Il est isolé par un pare-feu qui dispose de règles de filtrage qui sont moins oppressifs.

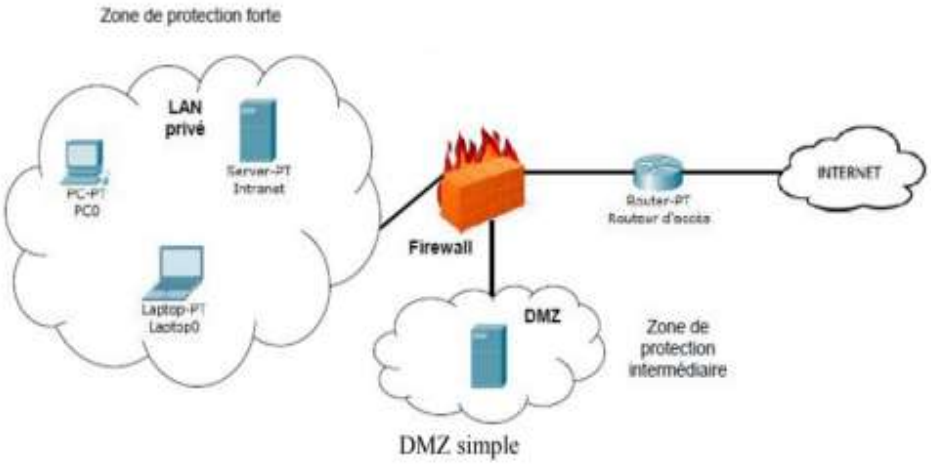


Figure III.13. Représentation de l'emplacement d'une DMZ

IV.4.3. Proxy

Un serveur proxy appelé aussi (serveur mandataire) est un serveur intermédiaire qui va permettre à une machine ou ensemble de machines d'accéder à internet. Dans ce cas, l'utilisateur va d'abord se connecter au serveur proxy et lui envoyer sa requête et c'est le serveur proxy qui va à son tour transmettre le message à des serveurs distants.

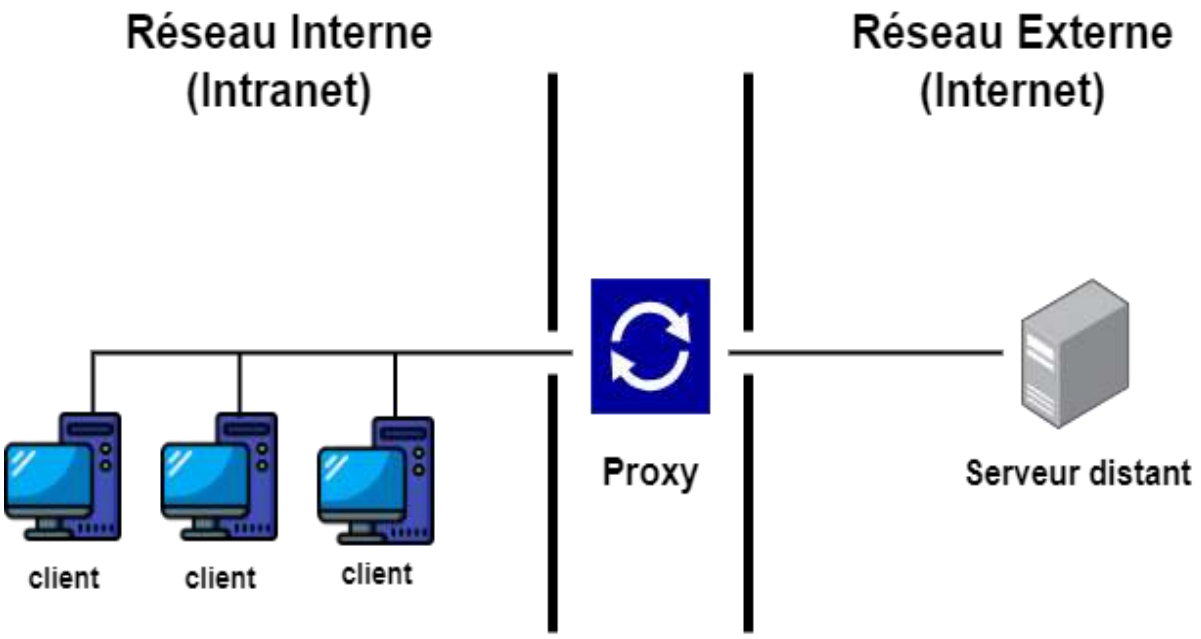


Figure III.14. Architecture d'un proxy

IV.4.4. IDS (Intrusion détection System)

IDS s'agit d'un mécanisme qui a pour objectif de repérer tous types de trafics partiellement malveillants qui transitent sur le système tels que les tentatives d'intrusion, les attaques virales ainsi que les débits trop importants. Cependant, IDS se contente de lancer une alerte et n'arrête pas le système. C'est un système de détection d'intrusions qui convient parfaitement pour réaliser cette tâche [11].

- **Architecture d'un IDS :**

Plusieurs architectures ont été proposées pour décrire les différents éléments constituant le système de détection d'intrusions. L'architecture la plus simple est composée de trois modules : le capteur, l'analyseur et le manager.

Cette architecture est montrée dans la figure suivante :

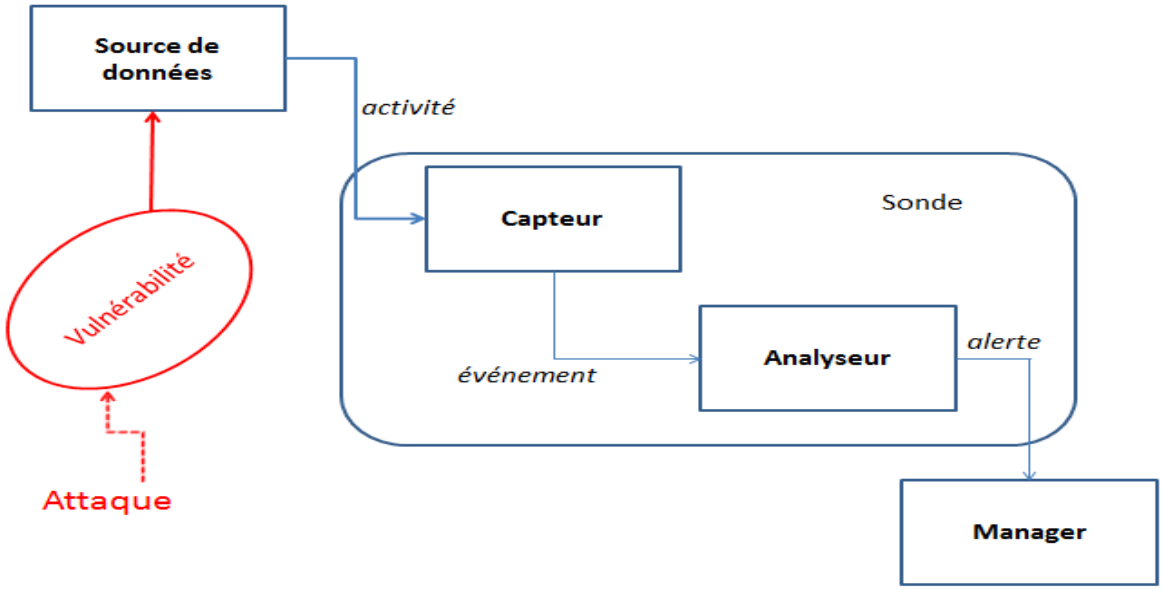


Figure III.15. Architecture classique d'un IDS [11]

- **Capteur :** chargé de collecter, filtrer et formater les informations brutes envoyées par la source de données concernant l'évolution de l'état du système. Le résultat de traitement est un message formaté appelé « événement » ;
- **Analyseur :** permet d'analyser les événements générés par le capteur en détectant toute activité malveillante qui peut se produire à partir d'un sous-ensemble de ces événements, et donc envoyer une alerte qui sera stockée dans les journaux du système ou bien utilisée pour lutter contre les attaques selon le type d'IDS ;
- **Manager :** permet de collecter et notifier les alertes envoyées par l'analyseur. Éventuellement, le manager est chargé de la réaction à adopter qui peut être :l'isolement de l'attaque pour réduire les dégâts, la suppression d'attaque, la restauration du système dans un état sain ou l'identification du problème qui a engendré cette attaque.

- **Principe de fonctionnement d'un IDS :** Le fonctionnement d'un IDS et le processus de détection d'intrusions sont illustrés dans la figure suivante :

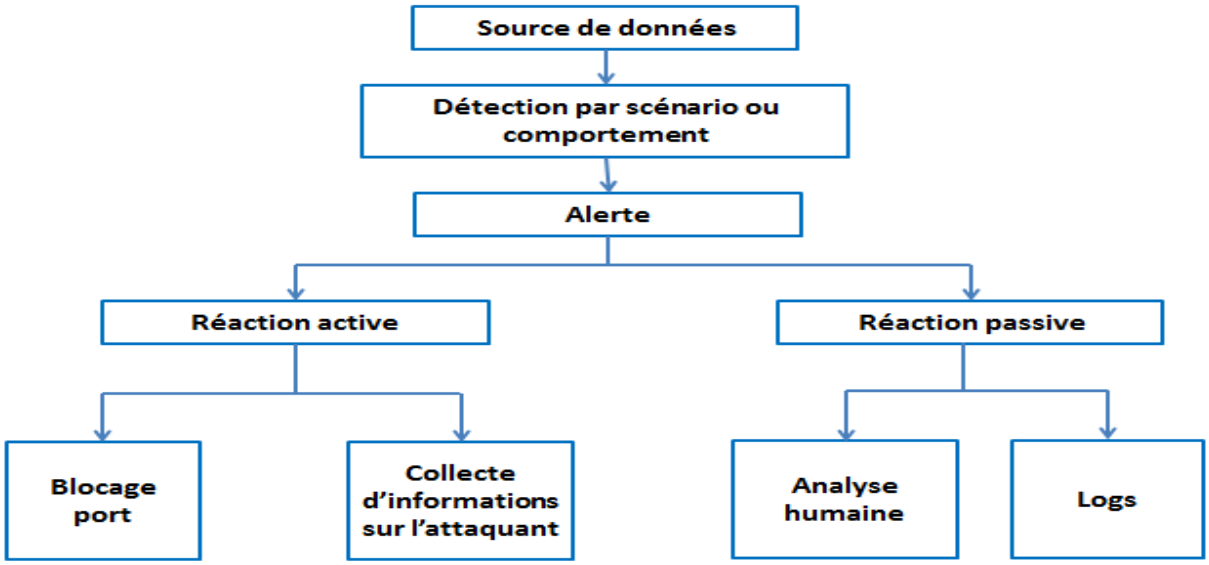
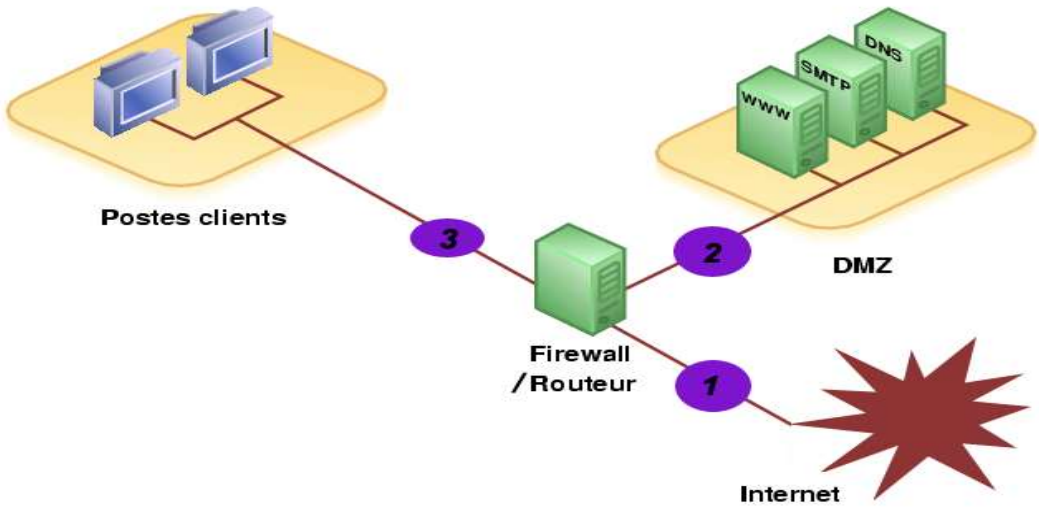


Figure III.16. Fonctionnement d'un IDS [11]

- **Emplacement des IDS**

Figure III.17. Emplacement d'un IDS [11]

Il existe plusieurs endroits stratégiques où il convient de placer un IDS pour atteindre le



niveau de protection attendu selon la politique de sécurité choisie.

Le schéma suivant illustre un réseau local ainsi que les trois positions que peut prendre un IDS

- **Position 1 :** lorsque l'IDS prend cette position, son rôle sera de détecter l'ensemble des attaques frontales, provenant de l'extérieur, vers le pare-feu. Par conséquent,

plusieurs alertes seront remontées ce qui rendra les logs difficilement consultables ;

- **Position 2 :** si l'IDS est placé sur la DMZ, il détectera les attaques qui n'ont pas été filtrées par le pare-feu et qui relèvent d'un certain niveau de compétence. Les logs seront ici plus clairs à consulter puisque les attaques bénignes ne seront pas recensées ;

- **Position 3 :** l'IDS dans cette position a pour objectif de rendre compte des attaques internes, provenant du réseau local de l'entreprise. Il peut être judicieux d'en placer un à cet endroit étant donné le fait que 80% des attaques proviennent de l'intérieur. De plus, si des trojans ont contaminé le parc informatique (navigation peu méfiante sur internet) ils pourront être ici facilement identifiés pour être ensuite éradiqués.

IV.4.5. IPS (intrusion prévention system)

L'IPS est un outil de protection et sécurité des systèmes d'information contre les intrusions, similaire aux IDS, à la différence que IPS prend des mesures en stoppant le trafic suspect en bloquant les ports ainsi que les flux [10].

➢ Fonctionnement des IPS

Les principes de fonctionnement de l'IPS sont :

- Surveillance et analyse en temps réel du trafic réseau : comment les IPS analysent le flux de données pour détecter les anomalies ;
- Détection des comportements suspects : identification des schémas de trafic malveillants ou inhabituels ;
- Utilisation des bases de données de signatures : comment les IPS repèrent les attaques connues en comparant les signatures ;
- Application des politiques de sécurité : comment les IPS bloquent ou préviennent les attaques en fonction des politiques définies.

➢ Les avantages des IPS :

Parmi les avantages de l'IPS, on cite :

- Détection proactive des menaces et des attaques en temps réel : comment les IPS agissent rapidement pour identifier et contrer les intrusions ;
- Prévention des attaques grâce à des mesures de blocage automatique : comment les IPS réagissent de manière proactive pour empêcher les attaques de réussir ;
- Protection des données sensibles et des systèmes critiques : comment les IPS

contribuent à maintenir l'intégrité et la confidentialité des informations ;

- Réduction du temps de réponse aux incidents de sécurité : comment les IPS permettent une réponse rapide et efficace aux attaques ;

IV.5. Outils de détection de vulnérabilités

Les outils de détections de failles et de vulnérabilités réseaux sont nombreux, chacun possédant sa propre méthode de fonctionnement et sa capacité à détecter et à recenser des failles. Il est également à noter qu'ils sont tout aussi bien utilisés pour effectuer des attaques. Parmi ces outils nous pouvons citer certains qui sont : Metrsoliot, Ethercap,Yersinia, Dirbuter, Acuntex, Nmap, Nessus pro,Burp suite pro, Script d'exploit, Appscan, Hping 3,Goldene eyc , Hulk, Go pish, Kali, Fiercce, Wpscan, Skip fish, Ens map, Fluxion. Dans ce qui suit, nous allons donner une brève définition de certains outils ainsi que leur méthode de fonctionnement.

IV.5.1. Nessus pro

Nessus pro est un outil de sécurité informatique, développé par la société Tenable qui est basé sur une architecture client/serveur. C'est un scanner de vulnérabilités qui permet d'effectuer des tests de sécurité et de détecter les failles et vulnérabilités des réseaux qu'elles soient de type IPv4, IPv6 ou bien même hybride. Par ailleurs, il prend en compte les appareils (pare-feu, routeurs, commutateurs), permet de corriger les erreurs de configuration, de scanner les ports et d'analyser des codes [13].

Figure III.18. Logo du logiciel Nessus pro

- **Méthode de fonctionnement de Nessus pro**

Tout d'abord après l'installation, l'utilisateur doit appliquer une configuration initiale telle que les plages d'adresses IP à analyser puis créer une politique de scan afin de spécifier les tests de sécurité souhaités. Après le lancement des tests, il doit collecter les informations sur les cibles exploitées et identifier les vulnérabilités et les failles de sécurité potentielles. Une

fois le rapport sur les vulnérabilités généré, l'utilisateur peut procéder à la mise en œuvre de mesures afin de les corriger.

IV.5.2. Nmap « network mapper »

Nmap développé par Fyodor, est considéré comme un outil d'exploration réseau et un scanner de port. Il est utilisé dans les audits de sécurité informatique ainsi que pour détecter les ports ouverts et les systèmes d'exploitation disponibles sur le réseau, tout en fournissant des informations sur la sécurité des réseaux. [14]

Figure III.19. Logo du logiciel Nmap

- **Méthode de fonctionnement de Nmap**

Comme pour tout autre outil de détection, l'utilisateur doit tout d'abord effectuer une configuration de base afin de spécifier les options de scan et les cibles à analyser que ce soit une seule adresse IP ou une plage d'adresses IP. Parmi les options de scan, il peut effectuer plusieurs types de scans tels que TCP SYN ou UDP qui vont lui permettre de générer des informations qui seront analysés par ces derniers. Parmi les informations obtenues, il peut y avoir les numéros des ports ouverts, les protocoles utilisés ainsi que des détails sur les systèmes d'exploitation. Enfin, Nmap va générer des rapports sur les résultats des scans effectués sous différents formats.

IV.5.3. Snort

Snort est un outil de détection d'intrusion (IDS) open-source développé par Sourcefire et maintenu par Cisco système. Il offre la possibilité d'effectuer des analyses en temps réel du trafic permettant ainsi de détecter tout paquet dangereux se trouvant dans le réseau. De plus il permet de faire l'analyse des protocoles et d'occasionnellement détecter une faille [15].

- Méthode fonctionnement de snort

Premièrement, l'utilisateur procède à une configuration initiale des outils de base ainsi qu'à la détermination des actions à effectuer en cas de détections de menaces. Snort fait en sorte d'analyser le trafic en temps réel afin de détecter de potentielles anomalies ou attaques. Lorsque c'est le cas, il effectue certaines actions selon la configuration initiale comme le blocage d'une connexion suspecte tout en enregistrant toutes les activités jugées suspectes.

IV.5.4. Metasploit

Metasploit est un outil en open-source développée par Rapid7 et utilisé pour la détection de failles et de vulnérabilités sur les réseaux informatiques. Il peut être utilisé de manière légale tout comme il peut être utiliseé de manière illégale. Il est initialement installé sur le système d'exploitation kali linux [16].

Figure III.20. Logo du logiciel de metasploit

- **Méthode de fonctionnement de metasploit**

Contrairement aux autres outils, Metasploit fait en sorte de collecter des informations sur la cible et de recueillir des vulnérabilités connues. Par la suite, il sélectionne des exploits préfabriqués en fonction des résultats obtenus lors de l'analyse précédente des vulnérabilités. Enfin, l'utilisateur peut passer à la dernière étape qui est le lancement de l'attaque sur la cible choisie tout en utilisant des techniques pour éviter la détection. A la fin de cette étape, Metasploit génère des rapports détaillés sur les résultats obtenus.

IV.5.5. Yersinia

Yersinia est un outil de sécurité informatique et de détection de vulnérabilités disponible en open-source. Il peut être utilisé pour effectuer des attaques sur des protocole réseaux afin de détecter les erreurs de configuration des équipements réseaux.

- **Méthode de fonctionnement de Yersinia**

Tout d'abord Yersinia détecte les protocoles réseaux actifs et disponibles tels que STP, DTP et VTP. Après cela, il recherche les vulnérabilités associées à ces protocoles et effectue des attaques en fonctions des vulnérabilités détectées. Pour cela, il utilise différentes techniques telles que l'usurpation d'identité, le déni de service ou l'injection de paquets. Une fois cette étape terminée, Yersinia analyse l'ampleur des dégâts et identifie les mesures de sécurité nécessaire afin de faire face à ces failles. Enfin, Yersinia génère un rapport détaillé des vulnérabilités détectées et met en place une panoplie de mesures de sécurité afin de renforcer la sécurité informatique.

IV.6. Conclusion :

A l'issu de ce chapitre, nous avons pu recenser six types d'attaquants différents, ainsi que les attaques réseaux les plus connues. Enfin, nous avons présenté des outils et des méthodes visant à renforcer la sécurité des réseaux informatiques.

Chapitre IV

Recueil des vulnérabilités

V.1. Introduction au CVSS [17]

Le Common Vulnerability Scoring System (CVSS) est un système d'évaluation des vulnérabilités largement utilisé dans le domaine de la cybersécurité. Il fournit une méthode normalisée et objective pour évaluer le niveau de risque associé à une vulnérabilité informatique. Le CVSS permet aux organisations de hiérarchiser les vulnérabilités, de prioriser les mesures de sécurité et de prendre des décisions éclairées pour atténuer les risques.

V.2. Fonctionnement du CVSS

Le CVSS attribue à chaque vulnérabilité un score qui reflète son impact potentiel sur la sécurité d'un système. Ce score est calculé en prenant en compte plusieurs aspects de la vulnérabilité, tels que sa complexité, sa portée, les impacts sur la confidentialité, l'intégrité et la disponibilité des données, ainsi que les contremesures disponibles. Le score CVSS est généralement accompagné de vecteurs de base, tels que l'accès requis, la complexité de l'exploitation et l'impact sur l'intégrité ou la confidentialité des données.

V.3. Les composantes du CVSS

Le CVSS est composé de trois métriques de base qui décrivent les caractéristiques de la vulnérabilité :

- **Métriques d'impact :** Elles évaluent les conséquences potentielles d'une exploitation réussie de la vulnérabilité. Elles mesurent l'impact sur la confidentialité, l'intégrité et la disponibilité des données.
- **Métriques d'exploitabilité** : Elles évaluent la facilité d'exploitation de la vulnérabilité, en prenant en compte des facteurs tels que la complexité de l'exploitation, les privilèges requis et les exigences d'interaction avec l'utilisateur.
- **Métriques de base :** Elles fournissent une évaluation de la sévérité de la vulnérabilité, en prenant en compte à la fois l'impact et l'exploitabilité.

V.4. L'échelle de notation

Le CVSS utilise une échelle de notation de 0 à 10 pour évaluer le niveau de risque d'une vulnérabilité. Un score de 0 indique un impact négligeable, tandis qu'un score de 10 représente un impact critique. Le score CVSS permet de classer les vulnérabilités en différentes catégories de risque, ce qui facilite la priorisation des mesures de sécurité.

Comme le représente le tableau ci-dessous :

Score CVSS	Niveau de risque	Description
0.0 - 3.9	Faible	Impact négligeable, peu de préoccupations majeures.
4.0 - 6.9	Modéré	Impact modéré, certaines préoccupations significatives.
7.0 - 8.9	Elevé	Impact important, des mesures de sécurité sont nécessaires
9.0 - 10.0	Critique	Impact critique, des actions immédiates sont nécessaires.

Tableau IV.1. Echelle de notation CVSS

Note :

L'échelle de notation CVSS est divisée en quatre niveaux de risque : Bas, Moyen, Élevé et Critique. Chaque niveau correspond à une plage de scores CVSS. Plus le score est élevé, plus le niveau de risque est élevé et plus l'impact potentiel de la vulnérabilité est grave. Ce tableau permet de catégoriser les vulnérabilités en fonction de leur niveau de risque global, ce qui aide les organisations à prioriser leurs actions de sécurité.

V.5. Tableau de notation CVSS

Voici un exemple de tableau de notation CVSS :

Métriques	Score	Description
Confidentialité	8.6	L'exploitation de la vulnérabilité peut Compromettre la confidentialité des données sensibles.
Intégrité	7.2	L'exploitation de la vulnérabilité peut Compromettre l'intégrité des données où des systèmes.
Disponibilité	9.3	L'exploitation de la vulnérabilité peut Entraîner une indisponibilité totale où partielle du système.
Exploitabilité	5.8	L'exploitation de la vulnérabilité Nécessite des compétences techniques avancées.
Impact	8.1	L'impact global de la vulnérabilité est considéré comme élevé.
Score CVSS	8.2	Le score global CVSS attribué à la vulnérabilité.

Tableau IV.2-notation CVSS

V.6. Conclusion

Le CVSS est un outil essentiel dans l'évaluation et la communication des risques liés aux vulnérabilités informatiques. Il fournit une méthode normalisée pour évaluer le niveau de risque associé à une vulnérabilité, en prenant en compte différents aspects de celle-ci. Le tableau de notation CVSS permet de synthétiser les métriques et de classer les vulnérabilités en fonction de leur niveau de risque. L'utilisation du CVSS aide les organisations à prendre des décisions éclairées en matière de sécurité et à mettre en place des mesures de mitigation appropriées.

Recueil des vulnérabilités

Vulnérabilité identifiée N°1-001	
Nom de la vulnérabilité	ICMP Echo Reply Flooding(Ping Flood)
Définition	Cette faille exploiter lors d'un balayage ICMP est que certains hôtes répondent différemment aux messages ICMP en fonction de leur disponibilité ou de leur état.
Impact potentiel	• Dégénérescence du réseau • Consommation excessive de la bande passante • Attaques par déni de service (DoS) • Falsification de la source IP • Perturbation de la connectivité
Niveau de gravite	**Modéré**
Exploitation	L'exploitation de la faille liée à l'attaque par balayage ICMP repose sur l'envoi de requêtes ICMP echo-request (pings) à une plage d'adresses IP et l'analyse des réponses obtenues. L'exploitation se fait en 4 étapes distinctives qui sont : I. L'attaquant sélectionne une plage d'adresse IP cible à balayer pour déterminer quels hôtes sont actifs ou disponibles sur le réseau. II. L'attaquant envoie des requêtes ICMP echo-request (pings) à chaque adresse IP de la plage ciblée grâce à des scripts personnalisées ou des outils de balayage réseau automatisés. III. L'attaquant analyse les réponses reçues suite à l'envoi des requêtes ICMP echo-request, les réponses en question sont : • **Réponse ICMP echo-reply :** cela indique que l'hôte est actif et disponible sur le réseau. • **Réponse ICMP time-exceeded :** Cette réponse indique la présence d'un équipement actif sur le chemin vers l'adresse IP ciblée. • **Pas de réponse ICMP :** Si un hôte ne répond pas du tout aux requêtes ICMP echo-request, cela peut indiquer qu'il est soit éteint, soit configuré pour ignorer ces types de requêtes. IV. En fonction des réponses reçues, l'attaquant compile une liste des adresses IP qui répondent aux requêtes ICMP. Ces informations peuvent être utilisées pour identifier les hôtes actifs sur le réseau et potentiellement cibler des attaques ultérieures.
Remédiation	Pour remédier à la faille exploitée par l'attaque par balayage ICMP, vous pouvez prendre les mesures suivantes : 1. **Filtrage des requêtes ICMP** : Configurez-les pare-feux et les équipements réseau pour filtrer les requêtes ICMP provenant de sources non autorisées. Bloquez les requêtes ICMP echo-request provenant d'adresses IP externes ou inconnues pour réduire la visibilité des hôtes actifs sur votre réseau. 2. **Désactivation des réponses ICMP :** Désactivez sélectivement les réponses ICMP echo-reply sur les hôtes qui n'en ont pas besoin. 3. **Utilisation d'outils de détection d'intrusion** : Mettez en place des outils de détection d'intrusion (IDS) ou de prévention des intrusions (IPS) pour surveiller les activités de balayage ICMP sur votre réseau. Ces outils peuvent détecter les schémas de balayage et générer des alertes pour vous permettre de prendre des mesures appropriées. 4. **Mise à jour régulière des systèmes :** Maintenez vos systèmes à jour avec les derniers correctifs de sécurité. Certaines vulnérabilités liées aux protocoles réseau peuvent être corrigées grâce à des mises à jour logicielles ou des correctifs fournis par les fournisseurs. 5. **Configuration des pare-feux** : Configurez les pare-feux pour limiter les taux de

	requêtes ICMP entrantes ou sortantes.

Vulnérabilité **identifiée** N°1-002	
Nom de la vulnérabilité	Détection ports ouverts sur un système cible
Définition	Lors d'une attaque par balayage TCP cette faille permet facilement de se faire exploiter car l'attaque ci-dessus permet de détecter les ports ouverts sur un système cible.
Impact potentiel	• Révélation d'informations sensibles • Préparation d'attaques • Évaluation de la sécurité • Surcharge réseau
Niveau de gravite	**Elevé**
Exploitation	L'exploitation de la faille dans l'attaque par balayage TCP se fait généralement en suivant les étapes suivantes : I. **Sélection des cibles :** L'attaquant choisit une ou plusieurs adresses IP ou plages d'adresses IP qu'il souhaite scanner pour identifier les ports ouverts. II. **Envoi de paquets SYN :** L'attaquant envoie des paquets SYN (synchronisation) vers des ports spécifiques de l'adresse IP cible. Ces paquets sont utilisés pour initier une demande de connexion TCP. III. **Analyse des réponses :** L'attaquant analyse les réponses reçues. Si le port est ouvert, le système cible renvoie un paquet SYN/ACK (synchronisation/accusé de réception) pour indiquer qu'il est prêt à établir une connexion. Si le port est fermé, le système cible envoie un paquet RST (réinitialisation) pour indiquer qu'il n'y a pas de service écoutant sur ce port. IV. **Enregistrement des résultats :** L'attaquant enregistre les ports qui ont renvoyé des réponses positives (SYN/ACK) pour identifier les services ouverts et potentiellement vulnérables. V. **Utilisation des informations collectées :** Les informations obtenues grâce au balayage TCP peuvent être utilisées à des fins malveillantes ultérieures. Par exemple, l'attaquant peut cibler des services connus pour des vulnérabilités spécifiques ou planifier des attaques plus ciblées.
Remédiation	1. **Configuration des pare-feu :** Configurez les pare-feu pour bloquer ou limiter les connexions entrantes non autorisées. Il est essentiel de fermer les ports inutilisés ou non nécessaires, réduisant ainsi les points d'entrée potentiels pour les attaques de balayage TCP. 2. **Filtres de paquets :** Utilisez des filtres de paquets pour contrôler le trafic réseau entrant et sortant. Ils peuvent être configurés pour bloquer les paquets SYN provenant d'adresses IP suspectes ou pour limiter le nombre de connexions SYN autorisées par seconde. 3. **Configuration des systèmes :** Configurez les systèmes pour limiter le nombre de tentatives de connexion SYN simultanées et définissez des seuils pour détecter les

	activités suspectes, comme des flux anormalement élevés de connexions SYN. 4. **Surveillance du réseau :** Mettez en place une surveillance du réseau pour détecter les activités de balayage TCP anormales. Cela peut inclure la surveillance des journaux de connexions TCP, l'utilisation de systèmes de détection d'intrusion (IDS) ou de prévention d'intrusion (IPS) pour détecter les schémas de trafic suspects. 5. **Utilisation de mécanismes de protection supplémentaires :** Il est possible de mettre en place des solutions de prévention d'intrusion, des systèmes de détection d'anomalies ou des services de répartition de charge pour gérer et filtrer le trafic réseau entrant. 6. **Sensibilisation à la sécurité :** Éduquez les utilisateurs sur les bonnes pratiques de sécurité, tels que l'utilisation de mots de passe forts, la sensibilisation aux techniques de phishing et la prudence lors de l'ouverture de pièces jointes ou de liens suspects.

Vulnérabilité identifiée N°1-003	
Nom de la vulnérabilité	IP Spoofing
Définition	Lors d'une attaque par modification du port source, l'attaquant exploite cette faille dans le processus de communication en utilisant des paquets réseau avec des adresses IP source et des ports source falsifiés.
Impact potentiel	• Contournement des mesures de sécurité • Altération de l'authentification • Difficulté de traçage
Niveau de gravite	**Elevé**
Exploitation	L'exploitation de la faille liée à l'attaque par modification du port source peut se dérouler de la manière suivante : I. **Sélection du port source :** L'attaquant choisit un port source spécifique dans le paquet qu'il envoie. Le port source est généralement un numéro de port aléatoire ou un numéro de port légitime qui est susceptible d'être autorisé à passer à travers les dispositifs de sécurité. II. **Envoi du paquet modifié :** L'attaquant envoie un paquet réseau vers la cible, en modifiant délibérément le port source du paquet pour qu'il semble provenir d'une source légitime ou autorisée. Cela peut tromper les systèmes de sécurité en leur faisant croire que le paquet provient d'une communication légitime. III. **Contournement des mécanismes de sécurité** : Étant donné que le paquet modifié semble provenir d'une source autorisée, il peut être autorisé à passer à travers les dispositifs de sécurité sans être bloqué ou filtré. Cela permet à l'attaquant de contourner les mécanismes de sécurité qui se basent sur les ports source pour autoriser ou bloquer le trafic. IV. **Attaques supplémentaires :** Une fois que le paquet modifié a réussi à passer les dispositifs de sécurité, l'attaquant peut utiliser cette opportunité pour mener d'autres attaques, telles que des attaques de déni de service (DoS), des attaques par injection de code malveillant ou des attaques d'usurpation d'identité.
Remédiation	Pour remédier à la faille liée à l'attaque par modification du port source, voici quelques mesures de sécurité recommandées : 1. **Authentification et autorisation :** Mettez en œuvre des mécanismes d'authentification et d'autorisation solides pour limiter l'accès aux services et aux ressources du réseau. Cela peut inclure l'utilisation de protocoles d'authentification forts, tels que le protocole RADIUS (Remote Authentication Dial-In User Service), et l'attribution de privilèges d'accès appropriés aux utilisateurs. 2. **Segmentation du réseau :** Divisez votre réseau en segments logiques pour limiter la propagation des attaques potentielles. Utilisez des sous-réseaux, des VLAN (Virtual Local Area Networks) et des listes de contrôle d'accès (ACL) pour restreindre le flux de trafic entre les segments et empêcher les attaquants d'atteindre facilement

	différentes parties du réseau. 3. **Sensibilisation à la sécurité :** Sensibilisez les utilisateurs et le personnel informatique aux bonnes pratiques de sécurité, notamment la prudence lors de l'ouverture de pièces jointes suspectes, l'utilisation de mots de passe forts et la surveillance des activités réseau inhabituelles. Une sensibilisation adéquate peut aider à prévenir les attaques et à minimiser les risques de modification du port source.

Vulnérabilité identifiée N°1-004	
Nom de la vulnérabilité	réassemblage de fragments IP
Définition	La vulnérabilité de réassemblage de fragments IP est une faiblesse présente dans les mécanismes de réassemblage des fragments de paquets IP lorsqu'ils sont transmis sur un réseau.
Impact potentiel	• Perturbation de la connectivité réseau • Exécution de code malveillant • Déni de service (DoS) • Fuite d'informations sensibles • Contournement des mécanismes de sécurité
Niveau de gravite	**Elevé**
Exploitation	L'exploitation de la vulnérabilité de l'attaque par fragmentation de paquets IP peut se faire de différentes manières, en fonction de la manière dont la vulnérabilité est exploitée. Voici quelques méthodes couramment utilisées pour exploiter cette faille : I. **Fragmentation malveillante :** Un attaquant peut fragmenter intentionnellement les paquets IP de manière malveillante en manipulant les en-têtes de fragmentation. Cela peut inclure la modification des champs d'offset et de longueur des fragments, ou la création de fragments incohérents. L'objectif est de provoquer un comportement inattendu ou erroné lors de réassemblage des fragments. II. **Attaque par débordement de tampon :** L'attaquant peut envoyer des paquets IP spécialement conçus avec des fragments mal formés, dans le but de provoquer un débordement de tampon lors de réassemblage des fragments. Cela peut conduire à l'exécution de code malveillant ou à un plantage du système vulnérable. III. **Attaque par saturation de ressources :** En exploitant la fragmentation De paquets IP, un attaquant peut envoyer un grand nombre de fragments avec des en-têtes spécialement conçus pour surcharger les ressources du système cible. Cela peut entraîner une saturation des capacités de traitement, de stockage ou de bande passante du système, provoquant ainsi une interruption de service. IV. **Attaque par confusion ou évitement des systèmes de détection :** L'attaquant peut utiliser des techniques de fragmentation de paquets pour tromper ou éviter les systèmes de détection d'intrusion ou les pare-feu. En fragmentant les paquets d'une manière spécifique, l'attaquant peut contourner les mécanismes de filtrage ou de surveillance du réseau, facilitant ainsi l'intrusion dans le système cible.
Remédiation	1. **Filtrage des fragments IP :** Configurez vos pare-feu et vos systèmes de filtrage pour bloquer ou filtrer les fragments IP indésirables ou suspects. Cela peut inclure la configuration de règles spécifiques pour détecter et bloquer les fragments mal formés ou potentiellement dangereux. 2. **Utilisation de solutions de prévention d'intrusion (IDS/IPS) :** Mettez en place des systèmes de prévention d'intrusion qui sont capables de détecter et de bloquer les attaques par fragmentation de paquets IP. Les IDS/IPS peuvent analyser le trafic réseau en temps réel et prendre des mesures pour contrer les attaques identifiées. 3. **Configuration sécurisée des routeurs :** Assurez-vous que vos routeurs sont correctement configurés et disposent des paramètres de sécurité appropriés pour gérer les fragments de paquets IP. Ceci peut inclure la désactivation de certaines fonctionnalités ou la configuration de seuils de fragmentation appropriés. 4. **Surveillance du trafic réseau :** Mettez en place des outils de surveillance du trafic réseau pour détecter toute activité suspecte ou anormale liée à la fragmentation de paquets IP. Une surveillance proactive vous permettra d'identifier rapidement les tentatives d'exploitation et de prendre des mesures pour y remédier.

Vulnérabilité identifiée N°1-005	
Nom de la vulnérabilité	Faiblesse dans WLAN pouvant conduire à un accès non autorisé
Définition	Cette vulnérabilité concerne les réseaux sans fil (WLAN) et est liée à des problèmes de sécurité dans la mise en œuvre du chiffrement WEP (Wired Equivalent Privacy). Elle peut permettre à un attaquant d'accéder de manière non autorisée au trafic réseau et de le lire ou de le modifier.
Impact potentiel	• L'attaque permet à un attaquant d'intercepter et de lire le trafic réseau sans fil. • Cela compromet la confidentialité des données transmises via le réseau sans fil. • L'attaquant peut accéder à des informations sensibles, telles que les identifiants de connexion et les données personnelles. • Il est possible de modifier le trafic réseau, ce qui peut entraîner l'injection de code malveillant ou la manipulation des données échangées. • L'ampleur de l'impact dépend du contexte d'utilisation du réseau sans fil et de la nature des données transitant par celui-ci.
Niveau de gravite	**Critique**
Exploitation	I. L'attaquant se trouve à proximité du réseau sans fil cible et utilise des outils spécialisés pour détecter les réseaux disponibles. II. L'attaquant identifie un réseau vulnérable qui utilise le protocole de chiffrement WEP (Wired Equivalent Privacy) ou qui utilise une implémentation incorrecte de ce protocole. III. L'attaquant utilise des techniques d'attaque, telles que l'injection de paquets ou l'utilisation d'outils de déchiffrement, pour intercepter le trafic réseau sans fil. IV. En exploitant les faiblesses du protocole WEP, l'attaquant peut récupérer les données transmises sur le réseau sans fil, y compris les informations sensibles telles que les identifiants de connexion, les données personnelles ou les informations confidentielles. V. L'attaquant peut également modifier le trafic réseau en injectant des paquets malveillants ou en manipulant les données échangées, ce qui peut avoir des conséquences néfastes.
Remédiation	1. **Utiliser des protocoles de chiffrement forts :** Évitez d'utiliser le protocole WEP (Wired Equivalent Privacy) qui est vulnérable. Privilégiez plutôt des protocoles de chiffrement plus robustes tels que WPA2 (Wi-Fi Protected Access 2) ou WPA3. 2. **Mettre à jour les équipements :** Assurez-vous que les points d'accès sans fil, les routeurs et les appareils clients sont équipés des derniers micro logiciels (firmwares) et des mises à jour de sécurité. Les fabricants publient régulièrement des correctifs pour corriger les vulnérabilités connues. 3. **Configurer correctement le réseau sans fil :** Utilisez des mots de passe forts pour le réseau sans fil et les points d'accès. Désactivez les fonctionnalités inutiles ou non sécurisées, telles que le WPS (Wi-Fi Protected Setup). 4. **Utiliser des méthodes d'authentification robustes :** Misez sur des méthodes d'authentification plus fortes telles que WPA2-Enterprise, qui utilise des certificats pour l'authentification des utilisateurs. 5. **Surveiller le trafic réseau :** Mettez en place des outils de surveillance du réseau pour détecter les activités suspectes ou les tentatives d'intrusion. Cela permet d'identifier rapidement les éventuelles attaques de sniffing. 6. **Segmenter le réseau :** Divisez le réseau en segments ou sous-réseaux plus petits, ce qui limite la propagation d'une éventuelle attaque de sniffing et réduit l'impact potentiel. 7. **Sensibiliser les utilisateurs :** Formez les utilisateurs sur les bonnes pratiques de sécurité, comme l'évitement de l'utilisation de réseaux Wi-Fi publics non sécurisés et la vérification des certificats lors de la connexion à un réseau sans fil

Vulnérabilité identifiée N°1-006	
Nom de la vulnérabilité	Vulnérabilité dans la mise en œuvre SNMP du réseau local sans fil
Définition	Elle concerne une faille de sécurité dans la mise en œuvre du protocole SNMP (Simple Network Management Protocol) utilisé dans les réseaux locaux sans fil. Cette vulnérabilité peut permettre à un attaquant distant d'exécuter du code arbitraire ou de provoquer un déni de service en envoyant des paquets SNMP spécialement conçus.
Impact potentiel	• Exécution de code arbitraire • Déni de service • Compromission des données • Altération ou suppression de données • Pertes financières • Atteinte à la réputation • Potentiel d'escalade de privilèges
Niveau de gravite	**Modéré**
Exploitation	I. L'attaquant identifie un réseau sans fil vulnérable utilisant le protocole SNMP. L'attaquant envoie des paquets SNMP spécialement conçus vers le réseau sans fil ciblé. II. Les paquets exploitent la vulnérabilité dans l'implémentation SNMP du réseau sans fil. III. L'exploitation réussie permet à l'attaquant d'exécuter du code arbitraire sur le système cible. IV. L'attaquant peut alors prendre le contrôle du système, accéder à des informations sensibles, modifier ou supprimer des données, ou provoquer un déni de service.
Remédiation	1. **Appliquer les correctifs :** Assurez-vous d'appliquer les correctifs et les mises à jour de sécurité fournis par les fabricants et les fournisseurs de votre équipement réseau, en particulier pour le protocole SNMP. Ces correctifs peuvent résoudre les failles de sécurité et renforcer la protection contre les attaques. 2. **Configuration sécurisée :** Configurez correctement votre réseau sans fil en utilisant les bonnes pratiques de sécurité. Cela peut inclure la désactivation ou la restriction de certaines fonctionnalités SNMP, l'utilisation de mots de passe forts et la limitation des autorisations d'accès. 3. **Surveillance du réseau :** Mettez en place des outils de surveillance et de détection des intrusions pour détecter les activités suspectes ou les tentatives d'exploitation de vulnérabilités. Cela vous permettra de prendre rapidement des mesures préventives en cas d'incident. 4. **Segmentation du réseau :** Utilisez des techniques de segmentation du réseau pour isoler les systèmes sensibles ou critiques des réseaux sans fil et limiter ainsi la surface d'attaque potentielle. 5. **Sensibilisation à la sécurité :** Sensibilisez vos utilisateurs et votre personnel à la sécurité des réseaux sans fil. Assurez-vous qu'ils comprennent les risques associés au sniffing et à d'autres attaques, et encouragez-les à adopter des pratiques de sécurité telles que l'utilisation de connexions chiffrées et l'évitement de l'envoi d'informations sensibles sur des réseaux non sécurisés. 6. **Audits de sécurité :** Effectuez régulièrement des audits de sécurité pour identifier les vulnérabilités et les failles potentielles dans votre infrastructure réseau.

Vulnérabilité identifiée N°1-007	
Nom de la vulnérabilité	Déni de service (crash du noyau) via un flux de paquets IP fragmentés
Définition	Cette vulnérabilité désigne une faille de sécurité qui permet à un attaquant de provoquer un déni de service sur un système en envoyant des flux de paquets IP fragmentés spécialement conçus.
Impact potentiel	• Déni de service • Instabilité du réseau • Perte de connectivité. • Risque de crash du noyau.
Niveau de gravite	**Modéré**
Exploitation	I. **Identification de la cible :** L'attaquant identifie un système cible qui est vulnérable à cette faille et accessible via le réseau. II. **Création de paquets IP fragmentés malveillants :** L'attaquant génère des paquets IP fragmentés spécialement conçus pour exploiter la vulnérabilité. Ces paquets peuvent contenir des paramètres malveillants, des valeurs incorrectes ou des anomalies qui perturbent le processus de reconstitution des fragments. III. **Envoi des paquets à la cible :** L'attaquant envoie ces paquets IP fragmentés malveillants à la cible, soit directement depuis sa propre machine, soit en utilisant des techniques d'usurpation d'adresse pour masquer l'origine de l'attaque. IV. **Traitement des paquets par la cible :** Lorsque la cible reçoit les paquets IP fragmentés, elle tente de les reconstituer pour leur traitement ultérieur. C'est à ce stade que la vulnérabilité est exploitée, car les paramètres malveillants ou incorrects des paquets peuvent provoquer des erreurs ou des comportements inattendus.
Remédiation	1. **Mettre à jour les systèmes :** Assurez-vous d'appliquer les derniers correctifs et mises à jour de sécurité disponibles pour les systèmes d'exploitation, les applications et les équipements réseau concernés. Les fournisseurs de logiciels publient régulièrement des correctifs pour corriger les vulnérabilités connues. 2. **Filtrer les paquets IP fragmentés :** Configurez les dispositifs de sécurité réseau, tels que les pare-feu et les passerelles, pour filtrer les paquets IP fragmentés entrants. Cela peut réduire la surface d'attaque en bloquant les paquets potentiellement malveillants. 3. **Utiliser des solutions de détection et de prévention d'intrusion (IDS/IPS) :** Mettez en place des systèmes d'IDS/IPS pour surveiller le trafic réseau à la recherche de comportements suspects ou de tentatives d'exploitation connues. Les IDS/IPS peuvent détecter et bloquer les attaques basées sur la fragmentation IP malveillante. 4. **Limiter les permissions et les accès :** Appliquez le principe du moindre privilège en limitant les permissions et les accès des utilisateurs et des applications aux ressources réseau. Cela peut réduire les possibilités d'exploitation en cas de compromission. 5. **Sensibilisation à la sécurité :** Sensibilisez les utilisateurs et le personnel à la sécurité des réseaux et des systèmes. Faites en sorte qu'ils comprennent les risques liés aux attaques par fragmentation IP et les meilleures pratiques pour se protéger, comme éviter l'ouverture de pièces jointes ou de liens suspects, et signaler tout comportement anormal.

Vulnérabilité identifiée N°1-008	
Nom de la vulnérabilité	OpenSSL CCS Injection Vulnerability (Heartbleed Bug)
Définition	Cette faille permet à un attaquant distant d'intercepter et de déchiffrer les communications sécurisées, compromettant ainsi la confidentialité des données transmises, elle affecte la bibliothèque OpenSSL, utilisée pour implémenter le protocole SSL/TLS dans de nombreux systèmes et applications.
Impact potentiel	1. Fuite de données sensibles 2. Risque pour la confidentialité des données 3. Impact sur la confiance et la réputation
Niveau de gravite	**Elevé**
Exploitation	I. **Établissement d'une connexion :** L'attaquant établit une connexion avec un serveur vulnérable qui utilise la version d'OpenSSL affectée par la faille. II. **Envoi de paquets "Heartbeat" :** L'attaquant envoie des paquets de requête "Heartbeat" au serveur vulnérable. Ces paquets contiennent une demande de réponse avec une longueur spécifique. III. **Réponse du serveur :** Le serveur vulnérable, en raison de la faille, répond au paquet "Heartbeat" en renvoyant les données demandées, mais sans vérifier la longueur des données réelles. IV. **Extraction de données sensibles :** L'attaquant peut alors extraire des données sensibles de la mémoire du serveur, telles que des clés de chiffrement, des identifiants d'utilisateur, des mots de passe ou d'autres informations confidentielles.
Remédiation	1. **Mettre à jour OpenSSL :** La première étape consiste à mettre à jour la version d'OpenSSL utilisée sur les systèmes vulnérables. Il est important d'installer les correctifs de sécurité fournis par les fournisseurs ou les développeurs d'OpenSSL pour résoudre la vulnérabilité. 2. **Remplacer les clés privées et les certificats :** Étant donné que la vulnérabilité Heartbleed peut potentiellement exposer des clés de chiffrement, il est recommandé de générer de nouvelles clés privées et de les remplacer sur les serveurs affectés. De même, les certificats associés doivent également être remplacés pour garantir l'intégrité des communications. 3. **Révoquer et renouveler les certificats :** Dans le cas où des certificats ont été exposés, il est essentiel de les révoquer et d'en demander de nouveaux auprès des autorités de certification respectives. Cela évite toute utilisation abusive des certificats compromis. 4. **Informer les utilisateurs et les clients :** Il est important de communiquer activement avec les utilisateurs et les clients pour les informer de la vulnérabilité et des mesures prises pour y remédier. Il est recommandé de fournir des conseils sur les actions à entreprendre, tels que la modification des mots de passe, afin de renforcer la sécurité des comptes des utilisateurs. 5. **Effectuer une analyse de sécurité complète :** Il est conseillé de réaliser une analyse de sécurité approfondie du système affecté pour détecter toute trace d'exploitation de la vulnérabilité et prendre les mesures appropriées pour remédier à toute compromission potentielle. 6. **Mettre en place une surveillance proactive :** Une surveillance continue du réseau et des systèmes peut aider à détecter toute activité suspecte ou tentative d'exploitation de la vulnérabilité. Des outils de détection d'intrusion, de surveillance des journaux et de gestion des vulnérabilités peuvent être utilisés pour renforcer la sécurité et réagir rapidement en cas d'incident.

Vulnérabilité identifiée N°1-009	
Nom de la vulnérabilité	Apache Struts Remote Code Execution Vulnerability (Apache Struts2 S2-045)
Définition	C'est une faille de sécurité qui affecte le framework Apache Struts version 2, elle permet à un attaquant distant de provoquer l'exécution de code arbitraire sur un serveur vulnérable.
Impact potentiel	• Compromission du serveur. • Exécution de code arbitraire. • Accès non autorisé aux données sensibles. • Modification ou suppression de données. • Exécution de commandes à distance. • Exploration du réseau. • Installation de logiciels malveillants supplémentaires. • Divulgation d'informations confidentielles. • Utilisation abusive des informations sensibles. • Impact sur la disponibilité du serveur. • Interruption de service. • Rendre le serveur inaccessible ou inutilisable.
Niveau de gravite	**Critique**
Exploitation	I. Identification d'une application Web utilisant Apache Struts2 vulnérable à la faille. II. Envoi d'une requête HTTP spécialement conçue à l'application Web, en exploitant la vulnérabilité présente dans la fonction de téléchargement de fichiers. III. Injection de code malveillant dans la requête, généralement en utilisant une injection d'expression OGNL (Object-Graph Navigation Langage). IV. Le serveur vulnérable traite la requête et exécute le code injecté, ce qui permet à l'attaquant d'exécuter des commandes à distance ou d'effectuer d'autres actions malveillantes sur le serveur.
Remédiation	1. **Mettre à jour Apache Struts2 :** Assurez-vous d'utiliser la dernière version stable d'Apache Struts2, qui inclut les correctifs de sécurité pour cette vulnérabilité. Suivez les recommandations du fournisseur pour la mise à jour du framework. 2. **Appliquer les correctifs de sécurité :** Si des correctifs spécifiques ont été publiés pour la vulnérabilité CVE-2017-5638, assurez-vous de les appliquer sur votre système. Suivez les instructions du fournisseur ou de l'organisme responsable de la sécurité pour appliquer ces correctifs. 3. **Configurer les pare-feux et les filtres de paquets :** Configurez-les pare-feux réseau pour bloquer les requêtes malveillantes et les tentatives d'exploitation de la faille. Utilisez des filtres de paquets pour limiter l'accès aux ressources sensibles et bloquer les requêtes suspectes. 4. **Surveiller les journaux et les activités réseau** : Mettez en place une surveillance régulière des journaux système et des activités réseau pour détecter les comportements anormaux ou les tentatives d'exploitation de la vulnérabilité. Réagissez rapidement en cas de détection d'activités suspectes. 5. **Sensibiliser et former les utilisateurs** : Sensibilisez les utilisateurs à l'importance de la sécurité des applications Web et aux risques associés à l'exploitation de cette vulnérabilité. Fournissez une formation adéquate sur les bonnes pratiques de sécurité pour réduire les risques d'attaque. 6. **Appliquer le principe du moindre privilège :** Limitez les privilèges des utilisateurs et des applications pour minimiser les dommages potentiels en cas de compromission. Accordez uniquement les privilèges nécessaires pour les tâches

	spécifiques. 7. **Utiliser des outils de sécurité et de détection des intrusions :** Mettez en place des outils de sécurité tels que des systèmes de détection des intrusions (IDS) ou des systèmes de prévention des intrusions (IPS) pour détecter et bloquer les tentatives d'exploitation de la vulnérabilité.

Vulnérabilité identifiée N°1-010	
Nom de la vulnérabilité	VLAN Hopping (Double Tagging)
Définition	C'est une faille de sécurité qui permet à un attaquant de contourner les mécanismes de segmentation de réseau basés sur les VLAN.
Impact potentiel	• Contournement de la segmentation VLAN • Accès non autorisé • Espionnage ou modification de données • Attaques ultérieures
Niveau de gravite	**Elevé**
Exploitation	I. **Identification des VLAN cibles :** L'attaquant recherche les VLAN du réseau qu'il souhaite cibler. Cela peut se faire en analysant le trafic réseau, en utilisant des outils d'exploration ou en exploitant d'autres vulnérabilités pour obtenir des informations sur l'infrastructure du réseau. II. **Création de paquets avec double étiquetage VLAN :** L'attaquant génère des paquets réseau spécialement conçus avec des en-têtes VLAN manipulés. L'objectif est de tromper les commutateurs réseau pour qu'ils transfèrent le trafic du VLAN cible vers le port de l'attaquant. III. **Envoi des paquets manipulés :** Les paquets modifiés sont envoyés sur le réseau, généralement à partir d'une interface réseau configurée de manière à paraître légitime. IV. **Réception du trafic du VLAN cible :** Si l'attaque réussit, l'attaquant recevra le trafic réseau provenant du VLAN cible, lui permettant ainsi d'intercepter, d'analyser ou de manipuler les données transitant sur ce VLAN.
Remédiation	1. **Mise en œuvre du protocole de sécurité VLAN :** Utilisez des protocoles de sécurité VLAN tels que VLAN Trunking Protocol (VTP) version 3 ou Port-based VLANs. Ces protocoles peuvent aider à empêcher l'ajout non autorisé ou la modification des étiquettes VLAN. 2. **Configuration appropriée des commutateurs réseau :** Assurez-vous de configurer correctement les commutateurs réseau pour limiter l'accès aux VLAN spécifiques aux ports autorisés uniquement. Désactivez les ports inutilisés et utilisez des listes de contrôle d'accès (ACL) pour restreindre le trafic entre les VLANs. 3. **Surveillance du trafic réseau :** Mettez en place des outils de surveillance du trafic réseau pour détecter les activités anormales ou suspectes, y compris les tentatives de VLAN Hopping. Utilisez des systèmes de détection d'intrusion (IDS) ou des systèmes de prévention d'intrusion (IPS) pour alerter et bloquer les attaques potentielles. 4. **Sensibilisation à la sécurité :** Sensibilisez le personnel informatique et les utilisateurs finaux aux risques liés au VLAN Hopping et aux bonnes pratiques de sécurité. Encouragez l'utilisation de mots de passe forts, la mise à jour régulière des appareils réseau avec les derniers correctifs de sécurité, et la surveillance proactive du trafic réseau. 5. **Mise à jour régulière du firmware :** Assurez-vous de maintenir à jour le firmware des commutateurs réseau pour bénéficier des dernières corrections de sécurité et des améliorations apportées aux mécanismes de contrôle d'accès et de gestion des VLANs.

Vulnérabilité identifiée N°1-011	
Nom de la vulnérabilité	VLAN Hopping (Switch Spoofing)
Définition	C'est une vulnérabilité qui permet à un attaquant de contourner les mécanismes de sécurité d'un réseau local virtuel (VLAN) pour accéder à des informations ou des ressources auxquelles il n'est normalement pas autorisé. La faille se produit lorsque des commutateurs réseau mal configurés ou vulnérables ne vérifient pas correctement l'appartenance VLAN des trames réseau.
Impact potentiel	• Accès non autorisé aux données sensibles. • Contournement des mesures de sécurité basées sur les VLANs. • Espionnage réseau et interception de données confidentielles. • Perturbation du réseau et des services. • Risque de déni de service.
Niveau de gravite	**Elevé**
Exploitation	I. **Identification d'un port réseau vulnérable :** L'attaquant recherche un port réseau configuré en mode trunk ou susceptible de transmettre le trafic VLAN. II. **Établissement d'une connexion illégitime :** L'attaquant envoie des trames Ethernet spécialement manipulées pour tromper le commutateur et se faire passer pour un hôte autorisé sur un VLAN spécifique. III. **Saut de VLAN :** En usurpant l'identité d'un hôte autorisé, l'attaquant peut accéder à des VLANs auxquels il n'est normalement pas autorisé, en contournant les restrictions de sécurité. IV. **Capture de données :** Une fois connecté au VLAN cible, l'attaquant peut capturer, modifier ou détourner le trafic réseau, y compris les données sensibles transitant sur le VLAN.
Remédiation	1. **Configuration appropriée des ports :** Configurez les ports réseau des commutateurs en utilisant des modes appropriés, tels que le mode d'accès pour les ports connectés aux périphériques finaux et le mode trunk pour les ports interconnectant les commutateurs. Veillez à limiter les ports en mode trunk aux VLANs nécessaires. 2. **Activation du protocole de sécurité VLAN :** Certains commutateurs prennent en charge des protocoles de sécurité VLAN, tels que VLAN Access Control Lists (VACL) ou Private VLANs (PVLAN). Ils permettent de restreindre la communication entre VLANs et de limiter les possibilités de saut de VLAN. 3. **Mise en œuvre de l'authentification :** Utilisez des mécanismes d'authentification, tels que IEEE 802.1X, pour valider l'identité des périphériques connectés aux ports réseau. Cela permet de s'assurer que seuls les hôtes autorisés peuvent accéder aux VLANs. 4. **Surveillance du trafic réseau :** Mettez en place des outils de surveillance du trafic réseau pour détecter toute activité suspecte ou des schémas de saut de VLAN. Les anomalies détectées peuvent être signalées et enquêtées pour

	prévenir les attaques potentielles. 5. **Mise à jour régulière des commutateurs :** Assurez-vous de maintenir les commutateurs à jour avec les dernières mises à jour de sécurité fournies par les fabricants. Les correctifs de sécurité peuvent inclure des améliorations de la gestion des VLANs et de la prévention des attaques.

Vulnérabilité identifiée N°1-012	
Nom de la vulnérabilité	VLAN Hopping (Switch VLAN Pruning)
Définition	C'est une faille de sécurité qui affecte certains commutateurs réseau, elle permet à un attaquant de contourner les mesures de sécurité mises en place pour isoler les VLANs et de passer d'un VLAN à un autre au sein d'un réseau local.
Impact potentiel	• Contournement des mesures de sécurité des VLANs • Accès non autorisé aux données sensibles • Compromission de la confidentialité et de l'intégrité des données • Risque de propagation des attaques • Impact sur la disponibilité du réseau
Niveau de gravite	**Elevé**
Exploitation	I. **Identification des ports accessibles :** L'attaquant commence par identifier les ports du commutateur réseau qui sont configurés en mode "trunk", c'est-à-dire ceux qui permettent le passage de plusieurs VLANs. II. **Envoi de trames spécialement formatées :** L'attaquant envoie des trames Ethernet spécialement formatées, généralement en utilisant des balises VLAN modifiées. Ces trames sont conçues pour tromper le commutateur et le faire croire qu'elles appartiennent à un VLAN spécifique, permettant ainsi à l'attaquant de passer d'un VLAN à un autre. III. **Manipulation des trames VLAN :** L'attaquant peut manipuler les trames VLAN en utilisant des techniques telles que le "double tagging". Cela implique d'ajouter une ou plusieurs balises VLAN supplémentaires aux trames, permettant à l'attaquant de tromper le commutateur et de les faire passer à travers des VLANs qui normalement ne devraient pas être accessibles. IV. **Capture ou modification des données :** Une fois que l'attaquant a réussi à accéder à d'autres VLANs, il peut capturer des données sensibles, intercepter des communications ou même modifier le contenu des trames. Cela lui donne la possibilité de voler des informations confidentielles, d'injecter du code malveillant ou de perturber le fonctionnement normal du réseau.
Remédiation	1. **Désactiver le mode "trunk" sur les ports non utilisés :** Les ports du commutateur qui ne sont pas nécessaires pour le passage de plusieurs VLANs devraient être configurés en mode "access" pour limiter l'accès aux VLANs spécifiques. 2. **Utiliser des listes de contrôle d'accès (ACL)** : Configurer des ACL sur le commutateur pour limiter le passage entre les VLANs. Cela permet de contrôler strictement quelles trames sont autorisées à passer entre les VLANs. 3. **Utiliser la fonction VLAN Native :** Configurer un VLAN Native sur les ports trunk pour spécifier un VLAN de gestion distinct qui n'est pas accessible depuis les autres VLANs. 4. **Mise en place d'un contrôle d'accès au port (Port Security) :** Activer la fonction Port Security pour limiter l'accès aux ports spécifiques en fonction des adresses MAC autorisées. Cela empêche les attaquants d'utiliser des adresses MAC falsifiées pour

	accéder à des VLANs non autorisés. 5. **Surveillance du trafic réseau :** Mettre en place des outils de surveillance du trafic réseau pour détecter les activités suspectes, telles que les tentatives de saut de VLAN. Cela peut inclure l'utilisation de systèmes de détection d'intrusion (IDS) ou de systèmes de prévention d'intrusion (IPS). 6. **Mises à jour et correctifs :** S'assurer que les commutateurs réseau sont régulièrement mis à jour avec les derniers correctifs de sécurité fournis par les fabricants. Ces correctifs peuvent résoudre les vulnérabilités connues, y compris celles liées à VLAN Hopping.

Vulnérabilité identifiée N°1-013	
Nom de la vulnérabilité	VLAN Hopping (Dynamic Trunking Protocol)
Définition	C'est une faille de sécurité qui affecte le protocole de tronçonnage dynamique (Dynamic Trunking Protocol, DTP) utilisé dans les réseaux VLAN. Cette faille permet à un attaquant de compromettre la sécurité des VLANs en exploitant les fonctionnalités de négociation automatique des ports des commutateurs Cisco.
Impact potentiel	• Contournement de l'isolation des VLANs • Accès non autorisé aux données sensibles • Possibilité de mener des attaques internes • Risque d'usurpation d'identité • Impact sur la confiance et la réputation
Niveau de gravite	**Elevé**
Exploitation	I. **Attaque de falsification de paquets DTP (Dynamic Trunking Protocol) :** L'attaquant envoie des paquets DTP falsifiés au switch pour le tromper et lui faire croire qu'un autre périphérique est un trunk (port de liaison) autorisé. Cela permet à l'attaquant de contourner les mécanismes de sécurité du VLAN et d'accéder à des VLANs non autorisés. II. **Attaque d'injection de VLAN :** L'attaquant envoie des paquets de trame Ethernet avec des étiquettes VLAN (VLAN tags) modifiées ou ajoutées. En utilisant des techniques d'injection de VLAN, l'attaquant peut faire passer son trafic par-dessus les VLANs existants et ainsi accéder à des VLANs non autorisés. III. **Attaque de reconfiguration de ports :** L'attaquant peut exploiter les vulnérabilités de configuration des ports du switch pour reconfigurer un port en tant que trunk non autorisé, permettant ainsi à l'attaquant d'accéder à plusieurs VLANs sur ce port. IV. **Attaque de manipulation de trames :** L'attaquant peut modifier ou manipuler les trames Ethernet envoyées sur le réseau, en modifiant les étiquettes VLAN ou en insérant des trames malveillantes dans des VLANs non autorisés.
Remédiation	1. **Désactiver le protocole DTP (Dynamic Trunking Protocol) :** Étant donné que le protocole DTP facilite les attaques de VLAN Hopping, il est recommandé de le désactiver sur tous les ports du switch. Cela empêche les attaquants d'exploiter ce protocole pour reconfigurer les ports en tant que trunks non autorisés. 2. **Configurer les ports en mode d'accès (Access Mode) :** Configurez les ports du switch en mode d'accès pour limiter leur fonctionnalité à un seul VLAN spécifique. Cela empêche les attaquants d'accéder à d'autres VLANs en modifiant les étiquettes VLAN. 3. **Utiliser les listes de contrôle d'accès (ACL) :** Configurez des ACL sur le switch pour limiter le trafic entre les VLANs et contrôler les communications autorisées. Cela permet de restreindre l'accès aux VLANs sensibles et d'empêcher les

	attaquants d'interagir avec des VLANs non autorisés. 4. **Mise à jour du firmware :** Assurez-vous de maintenir le firmware du switch à jour en installant les dernières mises à jour fournies par le fabricant. Les mises à jour du firmware peuvent inclure des correctifs de sécurité qui adressent les vulnérabilités connues, y compris celles liées au VLAN Hopping. 5. **Surveillance et détection des anomalies :** Mettez en place des systèmes de surveillance réseau pour détecter les activités anormales telles que la manipulation de trames VLAN, les changements de configuration des ports, ou les tentatives d'accès non autorisées à des VLANs sensibles. Cela permet une réponse rapide en cas d'attaque ou d'exploitation de la vulnérabilité.

Vulnérabilité identifiée N°1-014	
Nom de la vulnérabilité	VLAN Hopping (Dynamic Host Configuration Protocol)
Définition	C'est une vulnérabilité qui exploite le protocole de configuration dynamique des hôtes (DHCP) pour accéder à des VLANs auxquels un attaquant n'est normalement pas autorisé. Le DHCP est utilisé pour attribuer automatiquement des adresses IP et d'autres paramètres réseau aux appareils connectés à un réseau. Dans une attaque de VLAN Hopping basée sur le DHCP, l'attaquant exploite une faiblesse dans la configuration des serveurs DHCP et des commutateurs pour se faire passer pour un client légitime et obtenir un accès à un VLAN non autorisé.
Impact potentiel	• Accès non autorisé aux VLANs • Interception ou manipulation du trafic réseau • Menace sur la confidentialité • Menace sur l'intégrité des données • Perturbation du fonctionnement du réseau
Niveau de gravite	**Elevé**
Exploitation	I. **Spoofing de l'adresse MAC :** L'attaquant peut usurper l'adresse MAC d'un périphérique autorisé pour obtenir un accès non autorisé à un VLAN. II. **Attaque man-in-the-middle :** L'attaquant peut s'insérer entre le client et le serveur DHCP pour intercepter et manipuler les messages DHCP, afin de rediriger le client vers un VLAN non autorisé. III. **Attaque de reconnaissance :** L'attaquant peut envoyer des requêtes DHCP spécialement conçues pour identifier les VLANs actifs et découvrir les adresses IP disponibles. IV. **Exploitation de vulnérabilités DHCP :** Si des vulnérabilités existent dans les implémentations DHCP utilisées, un attaquant peut les exploiter pour obtenir un accès non autorisé aux VLANs.
Remédiation	1. **Désactiver les ports inutilisés :** Assurez-vous de désactiver les ports des commutateurs qui ne sont pas utilisés. Cela empêchera les attaquants de se connecter aux VLANs non autorisés via des ports inutilisés. 2. **Limiter l'accès aux ports VLAN :** Configurez les commutateurs pour n'autoriser l'accès qu'aux ports spécifiques qui doivent être connectés à des VLANs particuliers. Cela permet de restreindre l'accès aux VLANs aux seuls périphériques autorisés. 3. **Utiliser la séparation des VLANs :** Appliquez une stratégie de séparation stricte des VLANs pour empêcher les flux de données non autorisés entre les différents VLANs. Cela limite la propagation potentielle des attaques de VLAN Hopping. 4. **Utiliser des protocoles de sécurité** : Utilisez des protocoles de sécurité comme le 802.1X pour l'authentification des périphériques sur le réseau. Cela permet de

	s'assurer que seuls les périphériques autorisés peuvent accéder aux VLANs. 5. **Surveillance du réseau :** Mettez en place des outils de surveillance réseau pour détecter toute activité anormale ou tentative d'exploitation de la faille VLAN Hopping. Cela permet d'identifier rapidement les problèmes potentiels et de prendre des mesures appropriées. 6. **Mettre à jour les équipements réseau :** Assurez-vous de garder à jour les commutateurs et les périphériques réseau avec les derniers correctifs de sécurité et mises à jour du firmware. Cela permet de corriger les éventuelles vulnérabilités connues liées au VLAN Hopping

Vulnérabilité identifiée N° 1-015	
Nom de la vulnérabilité	ARP Spoofing
Définition	Elle fait référence à l'exploitation du protocole ARP (Address Resolution Protocol) pour effectuer une usurpation d'identité au sein d'un réseau local.
Impact potentiel	• Interceptation du trafic. • Manipulation des données en cours de transmission. • Attaques d'homme du milieu (MITM). • Atteinte à la confidentialité des données. • Altération de l'intégrité des données échangées.
Niveau de gravite	**Elevé**
Exploitation	I. Le pirate informatique envoie des requêtes ARP falsifiées sur le réseau local, en usurpant l'adresse MAC d'une autre machine légitime (généralement la passerelle par défaut). II. Les autres machines du réseau mettent à jour leur table ARP en associant l'adresse IP usurpée à l'adresse MAC falsifiée. III. Le pirate peut maintenant intercepter le trafic réseau entre les machines cibles en redirigeant les paquets vers sa propre machine. IV. Le pirate peut effectuer diverses attaques, telles que des attaques d'homme du milieu (MITM), où il peut surveiller, modifier ou injecter du trafic réseau entre les machines légitimes. V. En manipulant le trafic réseau, le pirate peut accéder à des informations sensibles, voler des identifiants, effectuer des attaques de déni de service, ou compromettre la confidentialité et l'intégrité des données échangées sur le réseau.
Remédiation	1. Utilisez des mécanismes de sécurité supplémentaires tels que les VLANs, les VPNs ou les réseaux privés pour isoler les segments de réseau et limiter la portée potentielle des attaques ARP Spoofing. 2. Mettez en place des configurations strictes au niveau des commutateurs (switches) et des routeurs pour empêcher les réponses ARP frauduleuses. Cela peut inclure l'utilisation de listes de contrôle d'accès (ACL) pour filtrer le trafic ARP ou la désactivation du protocole ARP sur les interfaces réseau non essentielles. 3. Utilisez des outils de détection d'ARP Spoofing qui peuvent surveiller le trafic ARP sur le réseau et détecter les anomalies, telles que des associations IP-MAC incorrectes ou des réponses ARP multiples pour une même adresse IP. 4. Mettez en œuvre des mesures de sécurité supplémentaires telles que l'authentification des adresses MAC, l'utilisation de protocoles de chiffrement

	pour le trafic réseau ou l'implémentation de protocoles de sécurité réseau tels que le Secure ARP (SARP) ou le Secure Neighbor Discovery (SEND) lorsque disponibles. 5. Sensibilisez les utilisateurs et le personnel informatique sur les risques de l'ARP Spoofing et les bonnes pratiques de sécurité réseau, tels que la vérification des adresses MAC lors de la configuration des machines ou l'utilisation de solutions de chiffrement pour les communications sensibles.

Vulnérabilité identifiée N° 1-016	
Nom de la vulnérabilité	ARP Cache Poisoning
Définition	C'est une technique utilisée par les attaquants pour tromper les hôtes du réseau en associant de fausses adresses IP à des adresses MAC valides.
Impact potentiel	• Interception du trafic réseau. • Attaques de type "man-in-the-middle". • Interruption des communications. • Attaques de déni de service. • Altération de la sécurité.
Niveau de gravite	**Modéré**
Exploitation	I. L'attaquant commence par analyser le réseau à la recherche de machines cibles. II. L'attaquant envoie des paquets ARP forgés pour usurper l'adresse IP d'une machine cible et associer cette adresse IP à sa propre adresse MAC. III. L'attaquant peut maintenant intercepter, modifier ou bloquer le trafic réseau destiné à la machine cible. IV. L'attaquant peut également envoyer de faux paquets ARP pour rediriger le trafic vers une autre machine ou pour créer des boucles réseau. V. L'exploitation réussie de cette vulnérabilité permet à l'attaquant de mener des attaques de type "man-in-the-middle", d'intercepter des données sensibles, d'altérer le trafic réseau ou de perturber la communication entre les machines cibles.
Remédiation	1. Utilisez des mécanismes d'authentification : Mettez en place des mécanismes d'authentification solides pour les appareils et les utilisateurs sur le réseau. Cela peut inclure l'utilisation de protocoles d'authentification tels que 802.1X, qui exigent une authentification avant d'accorder l'accès au réseau. 2. Surveillez le trafic ARP : Mettez en place une surveillance du trafic ARP sur le réseau pour détecter les anomalies ou les activités suspectes telles que des réponses ARP multiples pour une même adresse IP. 3. Utilisez des listes de contrôle d'accès (ACL) : Configurez des ACL sur les équipements réseau pour limiter les communications ARP entre les différents segments du réseau. Cela peut aider à prévenir les attaques ARP spoofing entre les sous-réseaux. 4. Mise à jour des logiciels et du firmware : Assurez-vous que tous les appareils réseau, y compris les commutateurs et les routeurs, disposent des dernières mises à jour de logiciels et de firmware. Les fournisseurs publient souvent des correctifs de sécurité pour résoudre les vulnérabilités connues, y compris celles liées à l'ARP spoofing. 5. Configuration des appareils réseau : Configurez les appareils réseau pour

	désactiver la réponse aux requêtes ARP provenant de sources non autorisées ou inattendues, comme la mise en place de la fonctionnalité "ARP Inspection" sur les commutateurs. 6. Utilisation de VLANs : Séparez les différents groupes d'utilisateurs et les appareils sur le réseau en utilisant des VLANs (Virtual Local Area Networks). Cela peut limiter la propagation des paquets ARP malveillants entre les différents segments du réseau. 7. Utilisation de chiffrement : Si possible, utilisez des protocoles de chiffrement tels que IPsec pour sécuriser le trafic réseau et empêcher l'interception ou la modification des paquets ARP. 8. Sensibilisation des utilisateurs : Éduquez les utilisateurs sur les risques liés à l'ARP spoofing et encouragez-les à signaler toute activité suspecte sur le réseau.

Vulnérabilité identifiée N° 1-017	
Nom de la vulnérabilité	Java Applet Rhino Script Engine Remote Code Execution Vulnerability
Définition	C'est une faille de sécurité qui affecte le moteur de script Rhino dans Java, elle permet à un attaquant d'exécuter du code à distance en exploitant une vulnérabilité dans la façon dont le moteur de script gère certaines opérations.
Impact potentiel	• Prise de contrôle de la machine cible. • Vol d'informations sensibles. • Propagation de logiciels malveillants. • Perturbation des services.
Niveau de gravite	**Elevé**
Exploitation	I. L'attaquant crée un fichier Flash malveillant contenant du code spécialement conçu pour exploiter la vulnérabilité. II. Le fichier Flash est distribué via différents canaux, tels que des sites web compromis, des e-mails de phishing ou des liens malveillants. III. L'utilisateur ciblé est incité à ouvrir ou à charger le fichier Flash sur son système. IV. Lorsque le fichier Flash est ouvert ou chargé par un lecteur Flash vulnérable, le code malveillant est exécuté. V. Le code malveillant tire parti de la vulnérabilité pour accéder à des privilèges ou pour exécuter du code arbitraire sur le système cible. VI. Une fois que l'attaquant a réussi à exploiter la vulnérabilité, il peut prendre le contrôle du système affecté et mener d'autres actions malveillantes, telles que l'installation de logiciels malveillants, le vol d'informations sensibles ou la compromission du système.
Remédiation	1. Mettre à jour les logiciels : Assurez-vous que tous les logiciels concernés, tels que les lecteurs Flash, les navigateurs web et les systèmes d'exploitation, sont à jour avec les derniers correctifs de sécurité. Les fournisseurs publient souvent des mises à jour pour corriger les vulnérabilités connues, il est donc essentiel de les appliquer régulièrement. 2. **Désactiver ou limiter l'utilisation du Flash :** Étant donné que cette vulnérabilité concerne spécifiquement les fichiers Flash, une solution possible consiste à désactiver complètement Flash dans les navigateurs web ou à limiter son utilisation uniquement aux sites de confiance. De nombreux navigateurs modernes ont déjà désactivé Flash par défaut ou prévoient de le faire à l'avenir. 3. **Utiliser des solutions de sécurité** : Installez et maintenez à jour des solutions de sécurité telles que des antivirus, des pare-feu et des logiciels de détection des intrusions. Ces outils peuvent aider à identifier les fichiers Flash malveillants ou les activités suspectes sur votre système.

	4. **Sensibiliser les utilisateurs :** Éduquez les utilisateurs sur les risques associés à l'ouverture de fichiers provenant de sources non fiables ou inconnues, en particulier les fichiers Flash. Encouragez-les à être prudents lorsqu'ils naviguent sur Internet et à signaler tout comportement suspect ou toute activité anormale. 5. **Utiliser des alternatives sécurisées :** Si possible, envisagez d'utiliser des alternatives plus sécurisées aux technologies vulnérables. Dans le cas de Flash, de nombreuses plates-formes et sites web ont abandonné son utilisation au profit de technologies plus sûres, telles que HTML5.

Vulnérabilité identifiée N° 1-018	
Nom de la vulnérabilité	IP Source Routing Vulnerability
Définition	Cette faille permet à un attaquant de masquer sa véritable adresse IP en utilisant une adresse IP source usurpée, ce qui peut conduire à des attaques de spoofing, de déni de service ou de reconnaissance du réseau.
Impact potentiel	• Attaques de spoofing • Déni de service • Reconnaissance du réseau • Perturbation de la communication
Niveau de gravite	**Elevé**
Exploitation	I. **Spoofing d'adresse IP source :** L'attaquant modifie l'adresse IP source d'un paquet pour faire croire qu'il provient d'une autre machine, trompant ainsi les systèmes de sécurité et masquant son identité réelle. II. **Falsification de paquets :** L'attaquant peut modifier les en-têtes des paquets pour falsifier des informations telles que l'adresse IP source, l'adresse MAC, les numéros de séquence, etc., afin de tromper les systèmes de sécurité et d'induire en erreur les destinataires légitimes. III. **Utilisation de techniques de tunneling** : L'attaquant peut utiliser des techniques de tunneling pour dissimuler sa véritable adresse IP et faire apparaître les paquets comme provenant d'une autre source légitime. IV. **Attaques par rebond :** L'attaquant peut utiliser des machines intermédiaires, souvent compromises, pour relayer le trafic et masquer son identité réelle, rendant ainsi plus difficile le traçage de l'origine de l'attaque.
Remédiation	1. **Mise en place de la vérification de l'adresse IP source** : Les systèmes et les pare-feu doivent être configurés pour vérifier l'adresse IP source des paquets entrants afin de détecter toute falsification. Des techniques telles que l'analyse des en-têtes IP et la vérification des adresses MAC peuvent être utilisées pour détecter les paquets avec des adresses IP falsifiées. 2. **Mise en œuvre de l'authentification et du chiffrement** : L'utilisation de protocoles d'authentification robustes tels que IPsec peut aider à vérifier l'authenticité des paquets IP et à protéger les communications contre les attaques de falsification. De plus, le chiffrement des données peut être utilisé pour protéger la confidentialité des informations sensibles. 3. **Configuration appropriée des pare-feu et des routeurs : Les** pare-feu et les routeurs doivent être configurés pour bloquer les paquets avec des adresses IP sources non valides ou provenant de plages d'adresses non autorisées. Les règles de filtrage doivent être mises à jour régulièrement pour bloquer les

	adresses IP suspectes ou connues pour être utilisées dans des attaques de spoofing. 4. **Surveillance du trafic réseau** : La mise en place de systèmes de détection d'intrusion (IDS) ou de systèmes de prévention d'intrusion (IPS) peut aider à détecter les attaques IP spoofing en surveillant le trafic réseau et en identifiant les schémas suspects ou les paquets avec des anomalies. 5. **Sensibilisation et formation des utilisateurs** : Il est essentiel de sensibiliser les utilisateurs aux risques de l'attaque IP spoofing et de les former aux bonnes pratiques de sécurité, telles que la vérification de l'authenticité des sites Web et la prudence lors de l'ouverture de pièces jointes ou du partage d'informations sensibles en ligne.

Vulnérabilité identifiée N° 1-019	
Nom de la vulnérabilité	FragmentSmack
Définition	Elle permet à un attaquant distant d'envoyer des paquets IP spécialement conçus afin de provoquer une surcharge de la CPU du système cible.
Impact potentiel	• Déni de service (DoS) • Utilisation excessive de la CPU • Ralentissement des performances • Perturbation des opérations • Risque de divulgation d'informations • Impact sur la disponibilité des services
Niveau de gravite	**Modéré**
Exploitation	I. Identification de la cible : L'attaquant identifie un système vulnérable qui exécute un noyau Linux avec la vulnérabilité FragmentSmack. II. Création de paquets malformés : L'attaquant génère des paquets IP spécialement conçus pour exploiter la faille. Il fragmente les paquets de manière incorrecte en fournissant des valeurs incohérentes pour les fragments, les décalages, les longueurs, ou en utilisant des options non valides. III. Envoi des paquets à la cible : L'attaquant envoie les paquets malformés à la cible vulnérable. Les paquets peuvent être envoyés directement sur le réseau ou à travers des manipulations du trafic existant. IV. Traitement des paquets par la cible : Lorsque la cible reçoit les paquets malformés, le noyau Linux tente de reconstituer les fragments pour reconstituer le paquet original. C'est à ce moment-là que la vulnérabilité FragmentSmack est exploitée. V. Exploitation de la faille : L'exploitation de la vulnérabilité peut conduire à un déni de service (DoS) en entraînant une surcharge de traitement des fragments. L'attaquant peut envoyer un grand nombre de paquets malformés pour épuiser les ressources système de la cible, ce qui peut entraîner des plantages, un ralentissement du système ou une indisponibilité du service.
Remédiation	1. **Mettre à jour le système :** Assurez-vous que le système d'exploitation est à jour avec les derniers correctifs de sécurité. Les fournisseurs de systèmes d'exploitation publient régulièrement des correctifs pour corriger les vulnérabilités connues, y compris la vulnérabilité FragmentSmack. Appliquez ces correctifs dès qu'ils sont disponibles. 2. **Utiliser un pare-feu :** Configurer et maintenir un pare-feu peut aider à filtrer le trafic malveillant et à bloquer les paquets malformés exploitant la vulnérabilité. Configurez le pare-feu pour bloquer le trafic suspect et limiter l'accès aux ports et services nécessaires uniquement. 3. **Utiliser des solutions de détection d'intrusion** : Les solutions de détection d'intrusion (IDS) peuvent aider à identifier les attaques basées sur la vulnérabilité FragmentSmack. Configurez un IDS pour surveiller et détecter les tentatives

	d'exploitation de la faille, et configurez des alertes pour avertir les administrateurs en cas d'activité suspecte. 4. **Limiter l'exposition :** Réduisez l'exposition de vos systèmes en désactivant les fonctionnalités réseau non nécessaires et en appliquant le principe du moindre privilège. Limitez les droits d'accès et les privilèges des utilisateurs et des applications pour minimiser les risques. 5. **Suivre les meilleures pratiques de sécurité réseau :** Appliquez les bonnes pratiques de sécurité réseau, telles que l'utilisation de VPN pour les connexions distantes, la segmentation du réseau pour isoler les segments critiques, et la surveillance régulière du trafic réseau pour détecter les activités suspectes.

Vulnérabilité identifiée N° 1-020	
Nom de la vulnérabilité	Bad Neighbor (Death Redux)
Définition	Elle permet à un attaquant distant d'envoyer des paquets d'ICMPv6 spécialement conçus pour dépasser les limites de taille acceptables par le système d'exploitation cible.
Impact potentiel	• Risque de déni de service (DoS) • Indisponibilité ou inutilisabilité de la machine cible • Perturbation des services et de la productivité • Possibilité de perturbation des communications réseau • Conséquences négatives sur les utilisateurs légitimes
Niveau de gravite	**Elevé**
Exploitation	I. **Identification de la cible** : L'attaquant identifie une machine cible vulnérable qui utilise IPv6 et dispose d'une implémentation de protocole réseau vulnérable. II. **Création de paquets malveillants :** L'attaquant génère des paquets ICMPv6 spécialement conçus pour exploiter la faille de traitement des en-têtes IPv6. Ces paquets sont conçus pour déclencher un dysfonctionnement dans le traitement des en-têtes IPv6 du système d'exploitation cible. III. **Envoi des paquets malveillants :** L'attaquant envoie les paquets ICMPv6 malveillants à la machine cible. Les paquets peuvent être envoyés directement sur le réseau ou à travers des techniques d'ingénierie sociale pour tromper l'utilisateur et l'inciter à ouvrir des paquets malveillants. IV. **Exploitation de la faille :** Lorsque la machine cible reçoit les paquets malveillants, la faille de traitement des en-têtes IPv6 est exploitée. Cela peut conduire à un déni de service (DoS) sur la machine cible, la rendant indisponible ou provoquant son crash. V. **Conséquences de l'exploitation :** L'exploitation réussie de la vulnérabilité peut entraîner une interruption des services réseau, une perte de connectivité ou un dysfonctionnement général du système cible.
Remédiation	1. **Mettre à jour les systèmes :** Assurez-vous d'appliquer les dernières mises à jour de sécurité fournies par les fabricants de systèmes d'exploitation. Les fournisseurs peuvent avoir publié des correctifs pour résoudre cette vulnérabilité spécifique. 2. **Filtrer le trafic ICMPv6 :** Configurez des règles de pare-feu pour filtrer le trafic ICMPv6 malveillant. Cela peut aider à bloquer les paquets exploitant la faille de traitement des en-têtes IPv6. 3. **Désactiver IPv6 si non utilisé :** Si vous n'utilisez pas activement IPv6 dans

	votre réseau, envisagez de le désactiver. Cela peut réduire la surface d'attaque potentielle et éliminer la vulnérabilité liée à cette faille spécifique. 4. **Utiliser des solutions de sécurité réseau :** Déployez des dispositifs de sécurité réseau, tels que des pare-feu et des systèmes de détection d'intrusion, qui peuvent détecter et bloquer les tentatives d'exploitation de la vulnérabilité. 5. **Sensibilisation à la sécurité** : Éduquez les utilisateurs et le personnel informatique sur les risques liés à cette vulnérabilité et les meilleures pratiques de sécurité, comme éviter d'ouvrir des paquets non sollicités ou suspects.

Vulnérabilité identifiée N° 1-021	
Nom de la vulnérabilité	Oracle WebLogic
Définition	Cette faille de sécurité permet à un attaquant distant non authentifié d'exécuter du code arbitraire à distance sur le serveur WebLogic affecté
Impact potentiel	• Exécution de code à distance. • Prise de contrôle du serveur. • Vol de données sensibles. • Perturbation des opérations. • Risque de propagation des attaques.
Niveau de gravite	**Critique**
Exploitation	I. **Identification de la cible** : L'attaquant identifie une application Web utilisant Oracle WebLogic Server et qui est vulnérable à cette faille spécifique. II. **Analyse de la vulnérabilité :** L'attaquant analyse la vulnérabilité pour comprendre sa nature et sa portée. Cela peut inclure l'examen des détails du CVE, la recherche d'informations supplémentaires et l'identification des méthodes d'exploitation potentielles. III. **Préparation de l'attaque :** L'attaquant prépare les outils et les ressources nécessaires pour mener l'attaque. Cela peut impliquer la configuration d'un environnement d'attaque, la création de charges utiles malveillantes et l'identification des vecteurs d'attaque. IV. **Lancement de l'attaque :** L'attaquant envoie des requêtes spécialement conçues à la cible, exploitant la vulnérabilité CVE-2019-2725. Cela peut inclure l'injection de code malveillant, l'exploitation de la dé sérialisation d'objets ou l'utilisation de techniques de manipulation du trafic réseau. V. **Exécution de code arbitraire :** Si l'attaque est réussie, l'attaquant parvient à exécuter du code arbitraire sur le serveur cible. Cela lui permet de prendre le contrôle du serveur, d'accéder à des données sensibles, de voler des informations ou de causer d'autres dommages. VI. **Dissimulation de l'attaque :** Après avoir réussi l'attaque, l'attaquant peut tenter de dissimuler ses traces en effaçant les logs ou en utilisant d'autres techniques d'obfuscation pour éviter la détection.
Remédiation	1. **Mettre à jour :** Assurez-vous d'appliquer les correctifs de sécurité fournis par Oracle pour remédier à cette vulnérabilité. Effectuez régulièrement des mises à jour pour vous assurer que votre installation de WebLogic Server est à jour avec les derniers correctifs de sécurité. 2. **Configuration sécurisée :** Configurez correctement les paramètres de sécurité dans Oracle WebLogic Server en suivant les recommandations de sécurité d'Oracle. Cela peut inclure l'utilisation de mots de passe forts, la désactivation des fonctionnalités non nécessaires, la configuration appropriée des autorisations d'accès, etc.

	3. **Surveillance du trafic réseau :** Mettez en place des mécanismes de surveillance du trafic réseau pour détecter les activités suspectes et les attaques potentielles. Cela peut inclure l'utilisation de pare-feu, de systèmes de détection d'intrusion et de journaux de trafic réseau. 4. **Sécurité du réseau :** Appliquez des mesures de sécurité supplémentaires au niveau du réseau pour protéger votre infrastructure. Cela peut inclure l'utilisation de VLAN, de tunnels VPN, de chiffrement des données et de filtrage du trafic. 5. **Sensibilisation à la sécurité :** Sensibilisez vos utilisateurs et votre personnel à la sécurité informatique et aux meilleures pratiques en matière d'utilisation d'Oracle WebLogic Server. Encouragez-les à signaler toute activité suspecte ou tout comportement inhabituel. 6. **Audit de sécurité :** Effectuez régulièrement des audits de sécurité

Vulnérabilité identifiée N° 1-022	
Nom de la vulnérabilité	POODLE
Définition	Le POODLE permet à un attaquant de déchiffrer des informations sensibles, telles que des cookies d'authentification, échangées entre un client et un serveur.
Impact potentiel	• Divulgation d'informations sensibles • Risque de vol de données • Réduction de la confidentialité • Risque de manipulation de données
Niveau de gravite	**Faible**
Exploitation	I. L'attaquant intercepte la communication entre le client et le serveur. II. L'attaquant force la négociation d'une connexion sécurisée en utilisant une version obsolète du protocole SSL/TLS qui est vulnérable. III. L'attaquant procède ensuite à une série de tentatives en injectant des paquets spécialement conçus dans la communication. IV. Par le biais de ces attaques répétées, l'attaquant peut progressivement récupérer des fragments de données chiffrées. V. L'attaquant analyse ensuite ces fragments pour extraire des informations sensibles, telles que des cookies de session ou des mots de passe. VI. Une fois que l'attaquant a obtenu des informations suffisantes, il peut les utiliser pour accéder illégalement aux comptes des utilisateurs ou effectuer d'autres actions malveillantes.
Remédiation	1. Désactiver les anciennes versions du protocole SSL/TLS : La première mesure de prévention consiste à désactiver les versions vulnérables du protocole SSL/TLS, en particulier SSLv3. Cela peut être réalisé en configurant les serveurs et les clients pour n'utiliser que des versions plus récentes et sécurisées du protocole, telles que TLS 1.2. 2. Mettre à jour les logiciels : Assurez-vous que tous les logiciels utilisant SSL/TLS sont à jour avec les derniers correctifs de sécurité. Cela inclut les serveurs web, les clients web, les applications et les bibliothèques SSL/TLS. 3. Activer les algorithmes de chiffrement forts : Configurez les serveurs pour utiliser uniquement des algorithmes de chiffrement forts et sécurisés, en évitant les algorithmes obsolètes ou faibles. Les algorithmes tels que AES (Advanced Encryption Standard) et SHA-2 (Secure Hash Algorithm 2) sont recommandés. 4. Utiliser des mesures supplémentaires de sécurité : Il est conseillé de mettre en place des mesures supplémentaires de sécurité, telles que l'utilisation de protocoles de chiffrement avancés tels que Perfect Forward Secrecy (PFS), qui génèrent une clé de session unique pour chaque connexion, rendant plus difficile la récupération des informations chiffrées. 5. Sensibilisation des utilisateurs : Informez les utilisateurs sur les bonnes pratiques de sécurité en ligne, notamment l'importance de ne pas se connecter à des sites web non sécurisés ou suspectés d'être vulnérables à des attaques de type POODLE

Vulnérabilité identifiée N° 1-023	
Nom de la vulnérabilité	Buffer Overflow in NFS mountd
Définition	Cette vulnérabilité permet à un attaquant distant de provoquer un dépassement de tampon en envoyant une requête spécialement conçue à un serveur NFS vulnérable.
Impact potentiel	• Exécution de code malveillant • Compromission de l'intégrité du système • Impact sur la disponibilité • Risque de propagation
Niveau de gravite	**Modéré**
Exploitation	I. Identification d'une entrée utilisateur non vérifiée ou d'un tampon de mémoire vulnérable dans le code d'une application. II. Envoi intentionnel d'une entrée malveillante ou d'une charge utile Excessive à cette zone de mémoire vulnérable. III. Débordement du tampon, ce qui peut entraîner un écrasement de la mémoire adjacente ou l'exécution de code arbitraire. IV. L'attaquant peut utiliser cette exécution de code arbitraire pour prendre le contrôle du système, exécuter des commandes malveillantes, installer des logiciels malveillants, accéder à des informations sensibles, etc.
Remédiation	1. Mises à jour et correctifs : Assurez-vous que les systèmes d'exploitation, les logiciels et les bibliothèques utilisées sont à jour avec les derniers correctifs de sécurité. Les développeurs et les fournisseurs de logiciels publient régulièrement des correctifs pour corriger les vulnérabilités connues, y compris les débordements de tampon. 2. Validation des entrées : Mettez en place des mécanismes de validation rigoureux des entrées utilisateur et des données provenant de sources externes. Vérifiez la taille et le type des données reçues pour s'assurer qu'elles ne dépassent pas les limites autorisées. 3. Utilisation de fonctions de manipulation sécurisées : Utilisez des fonctions de manipulation de chaînes et de mémoire sécurisées qui effectuent des vérifications de limites pour prévenir les débordements de tampon. Par exemple, utilisez des fonctions telles que strncpy() au lieu de strcpy(), snprintf() au lieu de sprintf(), etc. 4. Gestion adéquate de la mémoire : Mettez en œuvre des pratiques de gestion de la mémoire sûres, notamment l'allocation et la libération de mémoire correctes, l'utilisation de pointeurs sûrs, l'éviction des variables globales, etc. 5. Analyse de sécurité et tests de pénétration : Effectuez des analyses de sécurité régulières et des tests de pénétration pour identifier les vulnérabilités potentielles, y compris les débordements de tampon. Ces tests peuvent aider à détecter les faiblesses du code et à les corriger avant qu'elles ne soient exploitées. 6. Sensibilisation à la sécurité : Sensibilisez les développeurs et le personnel concerné aux bonnes pratiques de sécurité en matière de développement de logiciels. Encouragez l'utilisation de directives de codage sécurisées et fournissez une formation régulière sur les meilleures pratiques de sécurité.

Vulnérabilité identifiée N° 1-024	
Nom de la vulnérabilité	Buffer Overflow in the Windows LSASS Service
Définition	C'est une faille de sécurité qui a affecté le service LSASS (Local Security Authority Subsystem Service) sur les systèmes d'exploitation Windows.
Impact potentiel	• Exécution de code arbitraire. • Compromission de la sécurité. • Potentiellement élevé. • Risque de propagation.
Niveau de gravite	**Elevé**
Exploitation	I. **Identification de l'application vulnérable** : L'attaquant identifie une application qui est vulnérable au dépassement de tampon. Cela peut être une application serveur, un logiciel client, un système d'exploitation ou tout autre composant logiciel. II. **Création d'une charge utile malveillante :** L'attaquant crée une charge utile spécialement conçue pour exploiter la vulnérabilité. Cette charge utile peut contenir un code malveillant, des instructions spécifiques pour corrompre la mémoire ou exécuter des commandes arbitraires. III. **Injection de la charge utile :** L'attaquant envoie la charge utile à l'application vulnérable, généralement en utilisant des entrées Utilisateur malveillantes ou des requêtes réseau manipulées. IV. L'application traite la charge utile sans vérifier correctement sa taille, ce qui entraîne un dépassement de tampon. V. **Corruption de la mémoire :** En raison du dépassement de tampon, des données indésirables sont écrites dans des zones de mémoire adjacentes. Cela peut provoquer des corruptions de la pile, des écrasements de variables, des écrasements de pointeurs ou d'autres comportements inattendus. VI. **Exécution du code malveillant :** Si l'attaquant a réussi à corrompre la mémoire de manière contrôlée, il peut exploiter cette situation pour exécuter du code malveillant. Cela peut lui donner un accès non autorisé au système, la possibilité de voler des informations sensibles, d'intercepter des communications ou d'effectuer d'autres actions malveillantes.
Remédiation	1. **Appliquer les correctifs et les mises à jour de sécurité :** Les fournisseurs de logiciels publient souvent des correctifs pour remédier aux vulnérabilités connues. Il est important de maintenir à jour les systèmes et les logiciels pour bénéficier de ces correctifs. 2. **Utiliser des outils de sécurité :** Des outils de sécurité tels que les pare-feu, les systèmes de détection d'intrusion et les systèmes de prévention des intrusions peuvent aider à détecter et à bloquer les tentatives d'exploitation de vulnérabilités. 3. **Adopter des pratiques de codage sécurisées :** Les développeurs doivent prendre en compte la sécurité lors de la conception et du développement des applications, en appliquant des techniques de codage sécurisées, en effectuant une validation adéquate des entrées utilisateur et en mettant en œuvre des mécanismes de défense contre les dépassements de tampon. 4. **Sensibiliser les utilisateurs** : Les utilisateurs doivent être conscients des risques liés aux attaques par dépassement de tampon et doivent être formés pour identifier les signes d'une telle attaque, tels que des messages d'erreur inattendus ou des comportements anormaux des applications.

Vulnérabilité identifiée N° 1-025	
Nom de la vulnérabilité	Drupal RCE (Remote Code Execution)
Définition	C'est une vulnérabilité critique qui affecte les versions du CMS Drupal antérieures à la version 7.58 et 8.3.9. Cette vulnérabilité permet à un attaquant distant non authentifié d'exécuter du code malveillant à distance sur un site Drupal vulnérable.
Impact potentiel	• Exécution de code à distance • Prise de contrôle complète du site • Risque de compromission des informations d'utilisateurs • Impact sur la réputation de l'organisation propriétaire du site
Niveau de gravite	**Modéré**
Exploitation	I. **Identification de la vulnérabilité :** L'attaquant identifie un site Web vulnérable utilisant la version spécifique du logiciel concerné par la vulnérabilité CVE-2018-6922. II. **Injection de code malveillant :** L'attaquant exploite la faille de sécurité en injectant du code malveillant dans le site Web. Cela peut se faire en exploitant une faiblesse de la logique de traitement des requêtes ou en exploitant une vulnérabilité connue du logiciel utilisé. III. **Exécution du code à distance :** Une fois que le code malveillant est injecté, il peut être exécuté à distance par l'attaquant. Cela lui permet de prendre le contrôle du site Web et d'exécuter des actions malveillantes, telles que la modification du contenu du site, l'accès à des informations sensibles ou la propagation de logiciels malveillants. IV. **Dissimulation de l'activité malveillante :** L'attaquant peut tenter de dissimuler son activité malveillante en effaçant les traces de son intrusion ou en utilisant des techniques d'obfuscation pour rendre le code malveillant plus difficile à détecter.
Remédiation	1. **Mettre à jour le logiciel :** Assurez-vous d'utiliser la version la plus récente du logiciel concerné par la vulnérabilité. Les fournisseurs de logiciels publient régulièrement des correctifs et des mises à jour pour remédier aux failles de sécurité connues. Vérifiez les annonces de sécurité du fournisseur et appliquez les correctifs recommandés. 2. **Effectuer des tests de sécurité :** Réalisez des tests de sécurité réguliers pour identifier les vulnérabilités potentielles dans votre système. Cela peut inclure des scans de vulnérabilités, des audits de sécurité ou des tests de pénétration. Ces tests peuvent aider à identifier les failles de sécurité et à les corriger avant qu'elles ne soient exploitées. 3. **Utiliser des pare-feux :** Configurez des pare-feux et des filtres de paquets pour bloquer le trafic malveillant. Les pare-feux peuvent aider à détecter et à bloquer les tentatives d'exploitation de la vulnérabilité CVE-2018-6922. 4. **Limiter les privilèges d'accès** : Accordez uniquement les privilèges nécessaires aux utilisateurs et aux applications. Limiter l'accès aux ressources critiques réduit le risque d'exploitation de la vulnérabilité. 5. **Sensibilisation à la sécurité :** Informez les utilisateurs et le personnel de l'importance de la sécurité des systèmes. Sensibilisez-les aux bonnes pratiques de sécurité, telles que l'utilisation de mots de passe forts, la mise à jour régulière des logiciels et la vigilance face aux attaques potentielles.

Vulnérabilité identifiée N° 1-026	
Nom de la vulnérabilité	Buffer Overflow in Sendmail MIME Conversion
Définition	C'est une faille de sécurité qui affecte le logiciel Sendmail, qui est largement utilisé pour la gestion des e-mails sur de nombreux systèmes Unix et Linux.
Impact potentiel	• Exécution de code arbitraire. • Prise de contrôle complète du système. • Accès non autorisé à des informations sensibles. • Compromission de la confidentialité des données. • Perturbation des services d'e-mail. • Risque de propagation d'autres attaques sur le réseau. • Possibilité d'envoi d'e-mails malveillants. • Risque de saturation de la bande passante. • Potentielles perturbations ou interruptions des services d'e-mail. • Risques pour la sécurité du réseau et des données.
Niveau de gravite	**Modéré**
Exploitation	I. L'attaquant envoie un e-mail spécialement conçu avec une charge utile malveillante au serveur de messagerie Sendmail. II. Le serveur de messagerie traite l'e-mail et tente de délivrer le message aux destinataires. III. En raison de la faille présente dans Sendmail, l'attaquant peut exploiter une vulnérabilité de dépassement de tampon ou une autre méthode pour injecter du code malveillant dans le processus de traitement de l'e-mail. IV. Le code malveillant est exécuté sur le système cible, ce qui peut entraîner la prise de contrôle complète de celui-ci par l'attaquant.
Remédiation	1. Mettre à jour le serveur de messagerie Sendmail avec les derniers correctifs de sécurité disponibles. Les fournisseurs de logiciels publient régulièrement des correctifs pour corriger les vulnérabilités connues. 2. Configurer et appliquer des politiques de sécurité strictes pour le serveur de messagerie. Cela peut inclure la désactivation de fonctionnalités inutiles, la limitation des droits d'accès et l'utilisation de listes blanches pour filtrer les adresses IP ou les domaines suspects. 3. Surveiller régulièrement les activités du serveur de messagerie et analyser les journaux pour détecter toute tentative d'exploitation ou d'intrusion. 4. Mettre en place une solution de sécurité réseau, telle qu'un pare-feu ou un système de détection d'intrusion, pour bloquer ou alerter sur les tentatives d'exploitation de la vulnérabilité. 5. Sensibiliser les utilisateurs et les administrateurs système aux bonnes pratiques de sécurité en matière de messagerie électronique, telles que l'identification des e-mails suspects, l'utilisation de mots de passe forts et la mise en œuvre de politiques de gestion des e-mails.

Vulnérabilité identifiée N° 1-027	
Nom de la vulnérabilité	SACK Panic
Définition	C'est une faille de sécurité qui affecte le protocole TCP (Transmission Control Protocol). Cette vulnérabilité a été découverte dans le noyau Linux et peut être exploitée par un attaquant distant.
Impact potentiel	• Déni de service (DoS) • Épuisement des ressources système • Perturbation des opérations commerciales • Risque pour la réputation
Niveau de gravite	**Elevé**
Exploitation	I. **Envoi de paquets malveillants** : L'attaquant envoie des paquets spécialement conçus pour exploiter la vulnérabilité du noyau Linux. Ces paquets contiennent des options SACK (Selective Acknowledgement) malformées ou excessivement nombreuses. II. **Surcharge des mécanismes de traitement des paquets :** En recevant ces paquets malveillants, le noyau Linux peut entrer dans un état de panique en raison d'un traitement incorrect des options SACK. Cela peut entraîner une surcharge des ressources système, notamment de la mémoire, du processeur et de la bande passante.
Remédiation	1. **Appliquer les correctifs :** Les fournisseurs de systèmes d'exploitation et de noyaux ont publié des correctifs pour atténuer cette vulnérabilité. Il est essentiel de mettre à jour les systèmes avec les derniers correctifs de sécurité pour éliminer cette vulnérabilité. 2. **Configurer les pare-feu et les filtres de paquets :** Il est recommandé de configurer des règles de pare-feu ou des filtres de paquets pour bloquer les paquets malveillants exploitant cette vulnérabilité. Cela peut inclure la mise en place de règles de filtrage spécifiques pour bloquer les paquets contenant des options SACK malformées ou excessivement nombreuses. 3. **Surveiller le trafic réseau :** La surveillance active du trafic réseau peut aider à détecter les activités suspectes, y compris les tentatives d'exploitation de la vulnérabilité. Des outils de détection d'intrusion (IDS) ou de prévention d'intrusion (IPS) peuvent être utilisés pour identifier les comportements anormaux et prendre des mesures préventives. 4. **Mettre en place des mesures de mitigation :** Il peut être utile de mettre en place des mécanismes de limitation des ressources pour atténuer l'impact d'une attaque exploitant cette vulnérabilité. Cela peut inclure la configuration de limites de bande passante, de seuils d'utilisation de la mémoire ou de règles de gestion du trafic pour empêcher la saturation des ressources système.

Vulnérabilité identifiée N° 1-028	
Nom de la vulnérabilité	HTTPoxy
Définition	C'est une faille de sécurité qui affecte les applications web. Elle permet à un attaquant de manipuler les variables d'environnement HTTP_PROXY et HTTPS_PROXY via une requête HTTP.
Impact potentiel	• Redirection du trafic vers un proxy malveillant. • Possibilité d'intercepter et de manipuler les communications entre l'utilisateur et le serveur. • Fuites potentielles d'informations sensibles. • Risque d'injection de code malveillant. • Atteinte à l'intégrité des données transmises. • Possibilité d'attaques en chaîne vers d'autres composants du réseau.
Niveau de gravite	**Elevé**
Exploitation	I. **Manipulation de l'en-tête "Proxy"** : L'attaquant envoie une requête HTTP contenant un en-tête "Proxy" spécialement conçu, visant à manipuler la variable d'environnement HTTP_PROXY sur le serveur cible. II. **Utilisation de la variable d'environnement HTTP_PROXY :** Si le serveur est mal configuré et ne filtre pas correctement les en-têtes HTTP, il peut utiliser la valeur de l'en-tête "Proxy" pour définir la variable d'environnement HTTP_PROXY. Cette variable est utilisée par de nombreuses bibliothèques et frameworks pour déterminer les paramètres de proxy à utiliser lors des requêtes sortantes. III. **Redirection du trafic sortant :** Une fois que l'attaquant a réussi à manipuler la variable HTTP_PROXY, il peut rediriger tout le trafic sortant du serveur vers un proxy contrôlé par l'attaquant. Cela permet à l'attaquant de surveiller ou de modifier le trafic réseau entre le serveur et d'autres systèmes externes.
Remédiation	1. **Mettre à jour les bibliothèques et les frameworks :** Assurez-vous que toutes les bibliothèques et les frameworks utilisés dans l'application sont à jour avec les correctifs de sécurité les plus récents pour éviter les vulnérabilités connues. 2. **Vérifier la configuration du serveur :** Assurez-vous que les serveurs et les services sont correctement configurés pour filtrer et neutraliser les en-têtes HTTP malveillants, notamment l'en-tête "Proxy". Vérifiez les paramètres de proxy configurés sur les serveurs et les systèmes concernés. 3. **Utilisation de variables d'environnement spécifiques :** Au lieu d'utiliser la variable d'environnement générique HTTP_PROXY, utilisez des variables d'environnement spécifiques pour les besoins de proxy, si possible. 4. **Sensibiliser les développeurs et les administrateurs :** Sensibilisez les développeurs et les administrateurs système aux risques de sécurité associés à la manipulation des en-têtes HTTP et aux bonnes pratiques pour éviter les attaques d'injection ou de manipulation d'en-têtes. 5. **Mise en place de pare-feu et de filtres :** Configurez des pare-feu et des filtres pour bloquer les requêtes malveillantes et les en-têtes HTTP potentiellement dangereux. 6. **Surveillance du trafic réseau :** Mettez en place des mécanismes de surveillance du trafic réseau pour détecter les activités suspectes, telles que des redirections inattendues vers des serveurs proxy non autorisés.

VI. Conclusion générale

En conclusion de ce mémoire sur la collecte des vulnérabilités réseau informatiques pour l'audit, il est clair que la sécurité des réseaux informatiques est une préoccupation majeure dans le paysage technologique actuel. Les vulnérabilités peuvent exposer les systèmes et les données sensibles à des attaques malveillantes, entraînant des conséquences potentiellement graves pour les organisations. L'audit des vulnérabilités réseau est une étape cruciale pour identifier et évaluer les faiblesses potentielles dans les infrastructures informatiques. Il permet de détecter les vulnérabilités connues, les configurations inappropriées et les erreurs de sécurité, offrant ainsi une base solide pour prendre des mesures correctives. La collecte de vulnérabilités réseau nécessite l'utilisation d'outils spécialisés tels que Nessus, Nmap, Metasploit, etc. Ces outils fournissent des fonctionnalités avancées pour scanner les réseaux, analyser les protocoles, détecter les failles de sécurité et évaluer la résistance des systèmes aux attaques. Cependant, les systèmes doivent être régulièrement audités et mis à jour pour maintenir un niveau de sécurité optimal.

Enfin, la collecte de vulnérabilités réseau pour l'audit est une étape essentielle dans la protection des infrastructures informatiques. Elle permet de détecter les faiblesses potentielles, de prendre des mesures préventives et de renforcer la sécurité globale des systèmes.

Bibliographie

[1] J-DORDOIGNE. (2013). Réseaux informatiques : notions fondamentales (4e édition).

[2] AIX-MARSEILLE.(2012).Formation reseau. Source de 28-Mars 2023. http://www.pedagogie.ac-aix-marseille.fr/upload/docs/application/pdf/2012-07/formation_reseau.pdf

[3] A. SAIDANE, – B. OUAZENE, « Audit de sécurité d'un système d'information ». Mémoire de maîtrise, université Abderrahmane Mira-Bejaia, Algérie (2022).

[4] J-F. CARPENTIER. (2012). La sécurité informatique dans la petite entreprise etat de l'art et bonne pratique. (2ème édition). Eni Editions

[5] A. BOUDJAADAR. Plateforme basée agents pour l'aide à la conception et la simulation des réseaux de capteurs sans fil, 2010.

[6] 4 étapes à suivre pour auditer vos systèmes d'information. (20 avril 2022). Codeur. Source de 02 Mai 2023, de www.codeur.com/blog/audit-systeme-information/

[7] J.-F. CARPENTIER. (2016). S´sécurité informatique dans la petite entreprise. (3eme édition). Eni Editions

[8] Z-du moulin neuf. (Octobre 2009), sécurité informatique - ethical hacking - apprendre l'attaque pour mieux se défendre. Eni Editions

[9] A. SADIQUI. (2019) Sécurité des réseaux informatiques. Iste group.

[10] D. BURGERMEISTER and J. KRIER. (2006) Les systèmes de détection d'intrusions.

[11] k. BELKHATMI. O. BENAMARA, et al. Mise en place d'un système de détection et de prévention d'intrusion. phd thesis, Universite de Bejaia,(2016).

[12] R. Messier. CEH v10 Certified Ethical Hacker Study Guide. Sybex, 2019

[13] Tenable. Consulté le 06 Mai 2023 à l'adresse https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/datasheets/nessus pro-%28ds%29-fr-v3.pdf

[14] Nmap. Nmap.org. consulté le 28 Mai 2023 à l'adresse https://nmap.org

[15] Snort : définition, fonctionnement, avantages. 02 Février 2023. B.Mathieu. Cyberuniversity. source de 30 Mai 2023 de https://www.cyberuniversity.com/post/snort-definition-fonctionnement-avantages

[16] Imperva. Consulté le 06 Mai 2023 à l'adresse https://www.imperva.com/learn/applicationsecurity/metasploit/#:~:text=the%20metasploit%20project%20is%20a,a%20us%2dbased%20cybersecurity%20firm.

[17] What are CVSS Scores. Balbix. Source de 31 MAI 2023 de https://www.balbix.com/insights/understanding-cvss-scores/