INSTITUT SUPERIEUR TECHNIQUE ADVENTISTE DE GOMA

B.P. 116 GOMA

ARRETE MINISTERIEL N 0 C 54/MINESU/CAB.MIN/SMM/KGN/JMB/2019 DU 14/02/2029

E-mail : uago2015@gmail.com
Web site : www.uagom.com

AUDIT D'UN SYSTEME D'INFORMATION AVEC KALI LINUX

''CAS DE L'UNIVERSITE ADVENTISTE DE GOMA''

« UAGO »

Par MUPENZI BATEYE Héritier

Mémoire présenté en vue de l'obtention du diplôme de licence en Informatique de Gestion

Directeur : **CT. KALEMA DJAMBA Josué**

SEPTEMBRE 2023

DECLARATION DE L'ETUDIANT

Je certifie, **MUPENZI BATEYE Héritier** que ce mémoire est original et qu'il n'a jamais été présenté en vue de l'obtention d'un quelconque grade académique dans une autre institution supérieure et universitaire.

J'ai consacré de nombreux mois à cette étude, faisant preuve de dévouement et de passion où j'ai fait preuve de rigueur et de persévérance. J'ai surmonté des obstacles et obtenu des résultats significatifs. Je souhaite exprimer ma gratitude envers Nos mentors, collègues et famille pour leur soutien. Je suis convaincu que notre recherche va apporter une contribution précieuse à notre domaine d'étude et j'espère que Nos résultats inspireront d'autres chercheurs. Merci pour votre attention.

Fait à Goma, le 21/09/2023

MUPENZI BATEYE Héritier

DECLARATION DU DIRECTEUR

Nous **CT. KALEMA DJAMBA Josué,** attestons avoir dirigée ce travail en qualité de Directeur pour le compte de l'Université Adventiste de Goma.

L'étudiant a réalisé un travail de recherche exceptionnel, démontrant un haut niveau de compétence, de détermination et de persévérance. Ses résultats sont significatifs et contribuent de manière importante à son domaine d'étude. Je suis fier de son travail et je le recommande fortement pour sa réussite et son engagement dans la recherche.

Fait à Goma, le 21/09/2023

CT. KALEMA DJAMBA Josué

EPIGRAPHE

« La recherche est le voyage qui mène à la découverte, et la mémoire en est le précieux témoignage »**.**

Jacques-Yves Cousteau

DÉDICACE

A nos très cher parents BATEYE et VICTORINE, et tous nos frères et sœurs.

MUPENZI BATEYE Héritier

REMERCIEMENTS

Je tiens à exprimer ma sincère reconnaissance envers les autorités académiques de l'UAGO /ISTAGO qui ont multipliés leurs efforts pour notre formation.

Je remercie en particulier notre directeur de mémoire, **CT. KALEMA DJAMBA Josué.** Votre expertise, votre enthousiasme et votre dévouement ont été essentiels à la réalisation de ce travail. Vos conseils éclairés, votre patience et votre disponibilité m'ont permis de surmonter les défis et de développer Nos compétences de recherche.

Enfin, je tiens à exprimer ma gratitude envers nos camarades de classe, nos amis, nos proches ; en particulier **Espoir FABIEN** et toutes les personnes qui m'ont apporté leur soutien tout au long de cette aventure académique. Je tiens à vous remercier pour les moments précieux que nous avons partagés. Nos discussions, nos échanges d'idées et notre soutien mutuel ont rendu cette expérience académique plus enrichissante et agréable. Votre collaboration et votre esprit d'équipe ont été d'une valeur inestimable, et je suis reconnaissant d'avoir eu la chance de travailler à vos côtés. Vos encouragements, votre compréhension et votre présence ont été une source d'inspiration et de motivation.

Je suis conscient que cette liste de remerciements ne saurait être exhaustive, mais je tiens à exprimer ma reconnaissance à tous ceux qui ont joué un rôle dans la réalisation de ce mémoire. Votre soutien indéfectible et votre confiance en moi resteront gravés dans ma mémoire.

MUPENZI BATEYE Héritier

SIGLE ET ABREVIATIONS

UAGO : Université Adventiste de Goma

CIA : Confidentialité, Intégrité, Disponibilité

DDoS : Déni de Service Distribué

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name Server

FTP: File Transfer Protocol

IP: Internet Protocol

IPS: Intrusion Prevention System

ISO: International Organization for Standardization

ISTAGO : Institut Technique Adventiste de Goma

IT : Information Technology (Technologie de l'information)

LAN: Local Area Protocol

MAC: Media Access Control

MAN: Metropolitan Area Network

MSF: Metasploit Framework

NAT : Network Address Translation

NIST : Institut National des NorNos et de la Technologie

SI : Système d'information

SSH : Secure Shell

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

WAN: Wide Area Network

TABLE DES MATIERES

LISTE DES FIGURES

LISTE DES TABLEAUX

RESUME

Ce présent travail traite sur l'audit d système d'information avec Kali Linux. Cette étude approfondie se concentre sur l'audit du système d'information (SI) avec Kali Linux. L'audit SI est essentiel pour évaluer la sécurité et l'efficacité des infrastructures informatiques. Kali Linux, dédié aux tests de pénétration et à l'audit de sécurité, offre des outils puissants pour cette tâche. Cette recherche explore les phases clés de l'audit SI, en mettant l'accent sur l'utilisation de Kali Linux pour détecter les vulnérabilités, analyser la sécurité et effectuer des audits de conformité.

Les résultats de l'audit du système d'information avec Kali Linux identifient les failles de sécurité et les vulnérabilités du réseau, offrant ainsi une compréhension claire des risques potentiels. Des recommandations spécifiques ont été fournies pour renforcer la sécurité du système et remédier aux problèmes identifiés, garantissant ainsi la protection des données et des ressources de l'entreprise (UAGO).

Les rapports d'audit générés facilitent la prise de décision des administrateurs réseau en leur fournissant des informations précieuses pour améliorer la sécurité globale du système d'information.

Mots clés : Audit du Système d'information, Kali Linux, Tests de Pénétration, Sécurité Informatique, Vulnérabilités, Audits de conformité, Mesures correctives, Administrateurs réseau.

ABSTRACT

This present work focuses on information system auditing with Kali Linux. This in-depth study focuses on the audit of information systems (IS) using Kali Linux. IS auditing is essential for assessing the security and efficiency of IT infrastructures. Kali Linux, dedicated to penetration testing and security auditing, offers powerful tools for this task. This research explores key phases of IS auditing, with a focus on using Kali Linux to detect vulnerabilities, analyze security, and perform compliance audits.

The results of information system auditing with Kali Linux identify network security flaws and vulnerabilities, providing a clear understanding of potential risks.

Specific recommendations have been provided to enhance system security and address identified issues, ensuring the protection of company data and resources (UAGO).

The generated audit reports facilitate network administrators' decision-making by providing valuable insights to improve overall information system security.

Keywords: Information System Audit, Kali Linux, Penetration Testing, Computer Security, Vulnerabilities, Compliance Audits, Corrective Measures, Network Administrators.

CHAPITRE PREMIER : INTRODUCTION

I.1. CONTEXTE DE L'ÉTUDE

Le système d'information est aujourd'hui un élément clé de la réussite de toute entreprise, organisation ou institution. Il permet non seulement de stocker et de traiter toutes les informations nécessaires à la prise de décisions, mais également de faciliter les communications, les échanges et la collaboration entre les différents acteurs de l'entreprise.

Avec l'évolution rapide des technologies de l'information et la transformation numérique des entreprises, la sécurité des systèmes informatiques est devenue un enjeu majeur pour les entreprises. Les cyberattaques représentent une menace constante et les conséquences peuvent être désastreuses pour les entreprises. Il est donc crucial pour les entreprises de s'assurer de la sécurité de leur système d'information. C'est dans ce contexte que l'audit de sécurité peut jouer un rôle important en identifiant les vulnérabilités du système d'information et en proposant des mesures de protection. **(Goffinet, s.d.)**

Cependant, comme tout système informatique, le système d'information est également vulnérable aux attaques malveillantes. Une attaque réussie peut non seulement causer des dommages financiers importants, mais également mettre en danger la confidentialité, l'intégrité et la disponibilité des données de l'entreprise.

C'est pourquoi il est crucial pour toute organisation de mettre en place des mesures de sécurité efficaces pour protéger son système d'information. Un audit du système d'information est une méthode très utile pour évaluer la robustesse de ces mesures de sécurité.

Kali Linux est un outil très puissant pour effectuer des audits de sécurité sur les systèmes d'information. L'université Adventiste de Goma est une institution d'enseignement supérieur qui traite un grande quantité d'informations sensibles. Par conséquent, il est important de mener un audit de sécurité pour protéger ses données et les informations de ses utilisateurs. (Amine, 2011)

Dans ce contexte, la présente recherche se propose d'étudier l'importance d'un audit du système d'information avec Kali Linux. Nous allons examiner les objectifs, les méthodes et les outils utilisés pour mener à bien un tel audit, ainsi que les avantages que ce type de vérification peut apporter à l'organisation.

Enfin, nous allons discuter des résultats obtenus lors d'un audit du système d'information avec Kali Linux, en détaillant les différents types de vulnérabilités et les mesures à prendre pour les corriger. Nous allons également discuter de la validité et de la fiabilité des résultats obtenus, ainsi que des possibles limites de cette approche. (Zahra, 2011)

I.2. PROBLÉMATIQUE

L'audit d'un système d'information avec kali linux dans le cas de l'université adventiste de Goma soulève plusieurs problématiques intéressantes, on peut dire que :

- Le système d'information de l'université adventiste de Goma n'est pas mis à jour régulièrement ; ce qui peut pousser à ce qu'un pirate peut s'introduire dans le système facilement.
- Au sein de l'UAGO, le scannage de réseau reste toujours une pratique qui met cette dernière dans une situation de manque de suivi des informations qui sont partagées dans leurs réseau et pourtant c'est une chose très capitale.

Cependant, pour y arriver, une questions suivante doit guider notre attention :

- Quelles solutions adéquates pour garantir les mesures de protection en vue de renforcer la sécurité ?

Cette problématique implique une étude approfondie de l'utilisation de Kali Linux dans le processus du contrôle d'un réseau LAN, en examinant ses avantages et ses limites, ainsi que les meilleures pratiques pour son utilisation. **(**Computer Land, 2015)

C'est pourquoi ce contrôle apportera l'augmentation des performances de notre réseau, l'audit doit également optimiser la sécurité de notre parc informatique en identifiant d'éventuels points faibles dans l'architecture réseau de l'université adventiste de Goma. (O'Gorman).

I.4. OBJECTIF DU TRAVAIL

I.4.1. Objectif général

L'objectif principal de cette recherche est d'auditer le système d'information avec kali linux au sein de l'université adventiste de Goma pour une bonne efficacité et sécurité des données confidentielles**.**

I.4.2. Objectifs spécifiques

- Identifier les vulnérabilités et les failles de sécurité dans le système d'information,
- Proposer des mesures de protection pour renforcer la sécurité du système d'information.

I.5. CHOIX ET INTERET DU SUJET

I.5.1. Intérêt général

L'usage et l'avantage de sécuriser son système d'information est de protéger les données confidentielles de l'entreprise contre les Hackers et les attaques malveillantes.

I.5.2. Intérêt personnel

Sachant que nos études faites nous obligent à être des informaticiens compétents et capables de résoudre des problèmes de sécurité informatique, nous avons choisi ce sujet pour nous aider à approfondir les notions de la cyber sécurité et aussi savoir comment on peut sécuriser son réseau contre les attaques malveillantes.

I.5.3. Intérêt scientifique

Ce travail va aider les administrateurs réseau de l'université à utiliser les résultats de ce travail comme un outil de la sécurité informatique.

I.6. DÉLIMITATION DU SUJET

Tout travail doit être limité dans le temps tout comme dans l'espace ; c'est pourquoi notre travail ne va pas se faire sur toutes les universités de la ville de Goma, mais seulement à l'Université Adventiste de Goma.

I.7. METHODE ET TECHNIQUES UTILISEES

Nous allons utiliser la méthode PERT et la méthode EBIOS

- ✓ **La méthode EBIOS**, méthode d'analyse de risque française de référence, permet aux organisations de réaliser une appréciation et un traitement des risques. (ANSSI, 2023)
- ✓ **La méthode PERT** : La méthode PERT (Program Evaluation and Review Technic) est un outil de management utilisé pour planifier. Mais c'est également une technique d'ordonnancement des tâches d'un projet sous la forme d'un réseau.

En effet, sa représentation se fait en s'inspirant du modèle du diagramme (le diagramme de PERT). Il vous permet de visualiser et représenter les étapes de votre projet, elles-mêmes reliées par des tâches. Mais également vos ressources !

- ✓ **Méthode Expérimental :** C'est donc la méthode qui permet véritablement d'expliquer les phénomènes étudiés en termes de relation de causalité.

Technique d'observation : Cette technique nous a permis de voir ceux qui se passent à l'UAGO pour ainsi comprendre le degré des problèmes auxquels les administrateurs du système font face.

Technique Documentaire : Pour atteindre les objectifs que nous nous sommes fixés dans ce travail, nous nous sommes documenté en faisant la lecture des différents travaux et mémoires. Nous avons aussi fait des recherches sur internet pour enrichir notre travail.

Technique d'interview libre : c'est la véritable conversation au cours de laquelle on pose des questions pour trouver des réponses, renseignements et informations importantes.

I.9. SUBDIVISION DU TRAVAIL

Chapitre premier : INTRODUCTION

Chapitre deuxième : REVUE DE LA LITTÉRATURE

Chapitre troisième : MÉTHODOLOGIE DE LA RECHERCHE

Chapitre quatrième : PRESENTATION DES RESULTATS

Chapitre cinquième : RECOMMANDATION ET ANALYSE D'IMPACT

CHAPITRE DEUXIÈME : REVUE DE LA LITTÉRATURE

II.0. INTRODUCTION

Cette revue de la littérature explore l'utilisation de Kali Linux dans l'audit du système d'information. Elle examine les avantages, les limites et les meilleures pratiques de cet outil, en mettant en évidence les études de cas et les résultats obtenus. L'objectif est de fournir une perspective complète sur son utilisation et d'identifier les défis potentiels liés à son déploiement. Les vulnérabilités peuvent être exploitées par des individus malveillants pour accéder à des données sensibles ou perturber les opérations. Kali Linux, une distribution Linux spécialisée dans la sécurité, offre des outils puissants pour analyser les vulnérabilités et les failles de sécurités pour y apporter une solution. Cette revue de littérature explore les défis spécifiques liés à cette pratique et met en évidence son importance dans la protection des systèmes informatiques.

II.1. REVUE EMPIRIQUE

Plusieurs études ont été menées sur le contrôle des logiciels avec Kali Linux. Dont on peut citer quelques-uns :

1. Selon **P. Praveena;** a fait un travail intitulé " *Penetration Testing of Network Security using Kali Linux"*, a montré comment Kali Linux pouvait être utilisé pour découvrir les vulnérabilités du réseau et effectuer des tests de pénétration. L'étude a révélé que Kali Linux était efficace pour identifier les failles de sécurité et proposer des Nosures correctives appropriées. (Praveena, 2017).
2. Une autre étude menée par **Khan**" *Détection des menaces de sécurité dans les réseaux Wi-Fi à l'aide de Kali Linux* ", a examiné comment Kali Linux peut être utilisé pour détecter les menaces de sécurité dans les réseaux Wi-Fi. L'étude a révélé que Kali Linux était un outil efficace pour détecter les vulnérabilités et les menaces de sécurité sur les réseaux Wi-Fi. (Khan).
3. Une étude menée par **Bora**." *Piratage matériel avec Kali Linux* ", s'est concentrée sur l'utilisation de Kali Linux pour le piratage, il a montré que cette distribution peut être utilisée aussi dans le but de **voler**, **détruire** et **corrompre** des documents électroniques d'un ordinateur cible.
4. Selon **Salifou KDNANE & zakaria KINDA** ont travaillés sur une ‘’ *mise en place d'un portail captif sur le réseau de l'UPB ‘’* : son objectif était de créer une passerelle entre un réseau interne et le réseau Internet. La finalité est de pouvoir déployer la solution dans toutes les structures de l'Université Polytechnique de Bobo-Dioulasso.

5. Selon **Justin KAZUNGU** lui a parlé sur ‘Une mise en place d’un portail d’accès sécurisé par un système d’authentification du réseau RADIUS dans un LAN’, il a montré comment se protéger contre les Hackers et comment on peut sécuriser son réseau LAN (voir son réseau sans fil)

Plusieurs études ont été réalisées pour évaluer l'efficacité de Kali Linux dans l'audit d'un système d'information. Par exemple, une étude menée par des chercheurs de l'université de technologie de Troyes a montré que Kali Linux pouvait être utilisé pour détecter les vulnérabilités des systèmes d'information, y compris les systèmes SCADA et les réseaux industriels. (KINDA, 2013)**.**

- **SCDA :** Un système de contrôle et d’acquisition de données en temps réel est un système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques

C’est pourquoi dans notre travail nous allons nous concentrer sur la sécurité de notre université en faisant l’audit de sécurité.

II.2. REVUES THÉORIQUES

La sécurité des systèmes d'information est un aspect crucial pour toute organisation, notamment les universités. Les audits de sécurité sont essentiels pour garantir la confidentialité, l'intégrité et la disponibilité des données. Kali Linux est un outil important pour les audits de sécurité, car il permet aux auditeurs de tester la sécurité du système et de détecter les vulnérabilités potentielles.

II.2.1. Système d’information :

Le système d’information (SI) c’est l’ensemble des ressources de l’entreprise qui permettent la gestion de l’information. Le SI est généralement associé aux technologies (matériel, logiciel et communication), aux processus qui les accompagnent, et aux hommes qui les supportent. D’abord simplement appelé informatique, cet ensemble a pris le nom de SI avec l’arrivée des nouvelles technologies qui ont élargi son domaine.

En outre, un SI est un environnement bien plus complexe. En effet, il faut le voir comme un ensemble de ressources, à la fois humaines**,** matérielles et immatérielles dont le rôle est de collecter, stocker, traiter et distribuer de l’information. (OpenClassroom, 2023).

Système informatique : Un ensemble interconnecté de matériels, de logiciels et de données qui travaillent ensemble pour effectuer des tâches informatiques spécifiques. Il englobe

l'infrastructure informatique d'une organisation, y compris les ordinateurs, les serveurs, les réseaux et les logiciels.

Système de pilotage : Un système qui contrôle et supervise les opérations d'un autre système ou d'un processus. Il peut s'agir d'un système logiciel ou matériel conçu pour prendre des décisions, ajuster les paramètres et surveiller le fonctionnement d'un système cible, tel qu'un système de contrôle industriel ou un système de gestion automatisée

II.2.2. Sécurité informatique

La sécurité des systèmes d'information (SSI)

La sécurité des systèmes d'information ou plus simplement sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système_d'information. Assurer la sécurité du système d'information est une activité du management du_système d'information.

La sécurité informatique protège l'intégrité des technologies de l'information comme les systèmes, les réseaux et les données informatiques contre les attaques, les dommages ou les accès non autorisés. Pour préserver leur compétitivité dans le contexte de la transformation numérique. (Red Hat, 2018)

La **sécurité informatique** vise généralement cinq principaux objectifs :

- **L'intégrité** : garantir que les données sont bien celles que l'on croit être
- **La disponibilité :** maintenir le bon fonctionnement du système d'information
- **La confidentialité :** rendre l'information inintelligible à d'autres personnes que les seuls acteurs d'une transaction.
- **La non répudiation :** garantir qu'une transaction ne peut être niée
- **L'authentification :** assurer que seules les personnes autorisées aient accès aux ressources.

La **sécurité informatique** s'appréhende sous trois aspects élémentaires et complémentaires : la prévention, la détection et la réaction.

Le plus souvent, prévenir le **risque informatique** se résume en cinq points

1. Analyser les risques
2. Définir une politique de sécurité
3. Mettre en œuvre une solution
4. Evaluer cette solution
5. Mettre à jour la solution et la politique au regard de l'évolution des risques

En fait, avec le développement de l'utilisation d'internet, nombre d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, elles sont plus au niveau de l'architecture trois tiers ou n-tiers. Il devient donc nécessaire de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système. En revanche, la sécurité est un compromis entre coûts, risques et contraintes. On comprendra mieux le poids d'un risque en se fiant à la formule suivante :

$$Risque = \frac{\textbf{Menace x Vulnerabilite}}{\textbf{Contre mesure}}$$

Risque : C'est la probabilité qu'une menace exploite une vulnérabilité. Autrement dit, c'est une possibilité qu'un fait dommageable se produise.

Vulnérabilité : C'est une faiblesse inhérente à un système (software ou hardware). Appelée parfois faille ou brèche, elle représente le niveau d'exposition face à la menace dans un contexte particulier.

Menace : C'est le danger (interne ou externe) tel qu'un hacker, un virus, etc.

Contre-mesure : C'est un moyen permettant de réduire le risque dans une organisation. (YENDE RAPHAEL Grevisse, 2018)

Malgré toutes les mesures de prévention, aucun système informatique n'est infaillible. D'où l'intérêt de mettre en place un système de détection fiable et performant. La détection suppose un suivi attentif et constant de l'état des systèmes notamment grâce à la diffusion d'alertes automatiques. (Wooxo, n.d.)

II.2.3. Auditer un système d'information :

Auditer un système est un processus de la collecte et l'évaluation des informations d'un système d'information.

Selon **l'Institut Ponemon**, un audit d'un système d'information est un processus de vérification et d'évaluation de la sécurité et de la qualité d'un système informatique.

Les audits de sécurité, scan des vulnérabilités et test d'intrusion découvrent les failles dans des systèmes qui permettent à des pirates de compromettre les opérations et voler les données confidentielles du système.

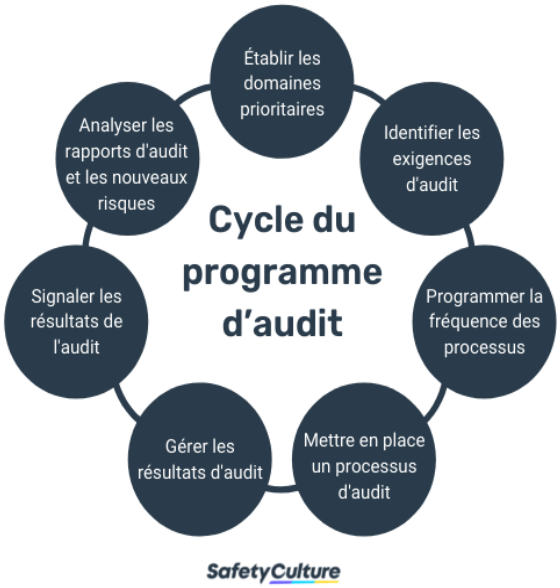


Figure 1: Cycle de programme d'audit

(NAVARRO, 2018)

II.2.4. Kali linux

Kali Linux est une distribution GNU/Linux sortie le 13 mars 2013, basée sur Debian. La distribution a pris la succession de BackTrack et est financée et maintenue à jour par Offensive Security.

- ✓ **Utilisation et Fonctionnement de kali linux**

Kali Linux est disponible sous forme de live DVD. Il est également possible de l'installer sur un disque dur, sur une clé USB, de mettre en place un démarrage PXE, ou encore de le virtualiser par-dessus son système d'exploitation grâce à des images_disque virtuelles proposées en téléchargement. Il est également possible de construire son propre DVD en utilisant les scripts Debian. (Kali, 2021.1)

L'un des avantages les plus importants de l'utilisation de Kali Linux pour l'audit d'un système d'information est sa grande communauté d'utilisateurs, qui fournit des mises à jour régulières et des conseils sur la façon de l'utiliser efficacement pour obtenir les meilleurs résultats**.** (Ponemon)**.**

Cette distribution est utilisée par des auditeurs en sécurité des systèmes d'information dans le cadre de l'audit automatisé de la sécurité intrinsèque d'un environnement. Les principes de sécurité de base tels que la gestion des mots de passe, l'authentification, le chiffrement et la gestion des autorisations sont importants pour assurer la sécurité des systèmes d'information. Les audits de sécurité peuvent aider les organisations à évaluer leur niveau de maturité en matière de sécurité et à identifier les domaines qui nécessitent une attention particulière. (WOOXO, n.d.)

En outre, une étude réalisée par des chercheurs de l'université de Malte a montré que Kali Linux pouvait également être utilisé pour les tests de pénétration sur les systèmes de sécurité des réseaux sans fil.
Il s'agit d'un outil d'analyse de sécurité à distance qui exécute plus de 1200 vérifications sur un ordinateur donné pour tester si l'une des attaques pourrait être utilisée pour s'introduire dans l'ordinateur ou lui nuire d'une autre manière.

- **Wireshark :** Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie. (Varonis, 2023)

Initialement nommé Ethereal, le projet a été renommé Wireshark en mai 2006 en raison de problèmes de marque. Wireshark est principalement utilisé pour capturer des paquets des données circulant sur un réseau (NIC) en mode promiscuité pour observer la plupart des trafics, même le trafic unicast, qui n'est pas envoyé à l'adresse MAC d'un contrôleur. (Le programmeur Marocain, 2023)

Wireshark est un multi plateforme et fonctionne sous Linux, MacOs, BSD, Solaris, certains autres systèmes d'exploitation de type Unix et Microsoft Windows.

II.2.5. La cryptographie

La cryptographie est un domaine fascinant qui remonte à l'Antiquité. Il s' agit de la pratique de cacher des informations en utilisant des techniques de codage et de décodage.
L'une des premières méthodes de cryptage connues était utilisée par les anciens égyptiens pour protéger les écrits sur les pyramides. En utilisant des hiéroglyphes, ils ont caché le sens réel derrière des symboles et des images que seuls les initiés pouvaient comprendre.
Durant la Seconde Guerre mondiale, la cryptographie joua un rôle majeur. Les Alliés ont pu casser les codes allemand s avec la machine à coder Enigma, ce qui a contribué à leur victoire. (la sécurité, s.d.)

- **Enigma** : est une machine électromécanique portative servant au chiffrement et au déchiffrement de l'information. Elle fut inventée par l'Allemand Arthur Scherbius, reprenant un brevet du Néerlandais Hugo Koch, datant de 1919.

Aujourd'hui, la cryptographie est utilisée dans le monde entier pour protéger les données, les communications et les transactions en ligne.

Des algorithmes sophistiqués sont utilisés pour chiffrer les informations que nous envoyons sur Internet ou stockons sur nos ordinateurs, pour empêcher les Hackers et les pirates informatiques d'accéder à ces documents. (Oracle, 2023)

En bref, la cryptographie est une discipline importante qui continue d'évoluer pour répondre aux besoins de la société moderne.

II.3. PRÉSENTATION DE L'ENTREPRISE

L'Université Adventiste de Goma (UAGO) a vu le jour 15 octobre 2000, en effet sous l'initiative des laïcs Adventiste de l'Association du Kivu Central (AKC) qui ont ressenti un besoin d'organiser une institution d'enseignement universitaire. A cette époque, l'effectif des membres de l'Eglise Adventiste dans l'AKC s'élevait à plus de 50.000, avec un grand nombre d'école primaire et secondaire. Avec tous les finalistes de ces écoles, le besoin d'une formation universitaire s'est fait ressentir.

Immédiatement, les activités académiques et les travaux de construction ont démarré sous la direction du premier Recteur a la personne de monsieur NIYONSENGA MBIZI Eliel. Deux facultés furent organisées : psychologie et sciences de l'éducation ; Sciences Economiques et de Gestion.

L'UAGO entretient des bonnes relations avec le ministre de l'enseignement supérieur et universitaire de la République Démocratique du Congo (RDC). Elle a été autorisée à fonctionner par l'arrêté départemental N°JURS/CABCD/023/99 du 18 octobre 1999.

Le cycle de licence en science de l'éducation et en science économiques fut confirmé par l'arrête départemental N°DEN/CABC/2002 et dont le début fut fixé au 1er décembre 2003.

L'arrêté ministériel n°1196/MINESU/CAB/SSM/2006 du 02/06/2006 portant agreement provisoire d'un établissement privé d'enseignement supérieur et universitaire dénommée « UNIVERSITE ADVENTISTE DE GOMA » fut octroyé.

Le décret présidentiel n°06/0106 du 12 juin 2006 de l'UAGO une personnalité juridique et les diplômes délivrés son homologue par le gouverneur congolais.

En 2004, la conférence générale de l'église adventiste a envoyé une mission d'inspection et l'UAGO est hissé au niveau de « pré-candidat ».

L'UAGO connait une progression remarquable depuis qu'elle a ouvert ses portes : elle a démarré avec deux facultés et un effectif de cinquante étudiants, aujourd'hui organise huit facultés avec cinq cent-neuf étudiants. Dès son début jusqu'à présent, l'UAGO a déjà délivré plus de 878 diplômes de gradué et plus de 608 de licence.

Ce bref parcours de l'UAGO augure un avenir plein d'espoir et avec l'appui du très hauts, nous attendons la voir hisser à un niveau des institutions d'éducation supérieur selon les critères de l'Eglise Adventiste.

Notre mission : la mission de l'église Adventiste du septième jour est d'appelé tout peuple à devenir des disciples de Jésus-Christ de proclamé l'évangile de l'éternel dans le contexte du message des trois anges Apocalypse 146-12 et de préparer le prochain retour de Christ.

Notre méthode : Guidé par la bible et le Saint-Esprit les Adventistes du septième jour poursuivent cette mission à travers une vie modelée par celle du christ en la communiquant en faisant des disciples en enseignant en guérissant et en servant.

Notre vision : Les Adventiste du septième jour voient la restauration de toute la création de Dieu en parfaite harmonie avec sa volonté et sa justice comme la finalité ultime du plan de Dieu et cela en harmonie avec la révélation biblique.

II.3.1. Mission, vision et objectif de l'université adventiste de Goma (Goma)

Mission

Promouvoir une éducation holistique qui rend les étudiants capables d'acquérir une connaissance pertinente et de capacité pratique fondées sur la vision biblique du monde envie de répondre aux besoins locaux.

Vision

Promouvoir la science qui harmonise avec la foi résultant le progrès qui honore Dieu et de focalisé sur le bien-être de l'humanité.

Valeur

- Non-violence
- Intégrité
- Créativité
- Travail en équipe

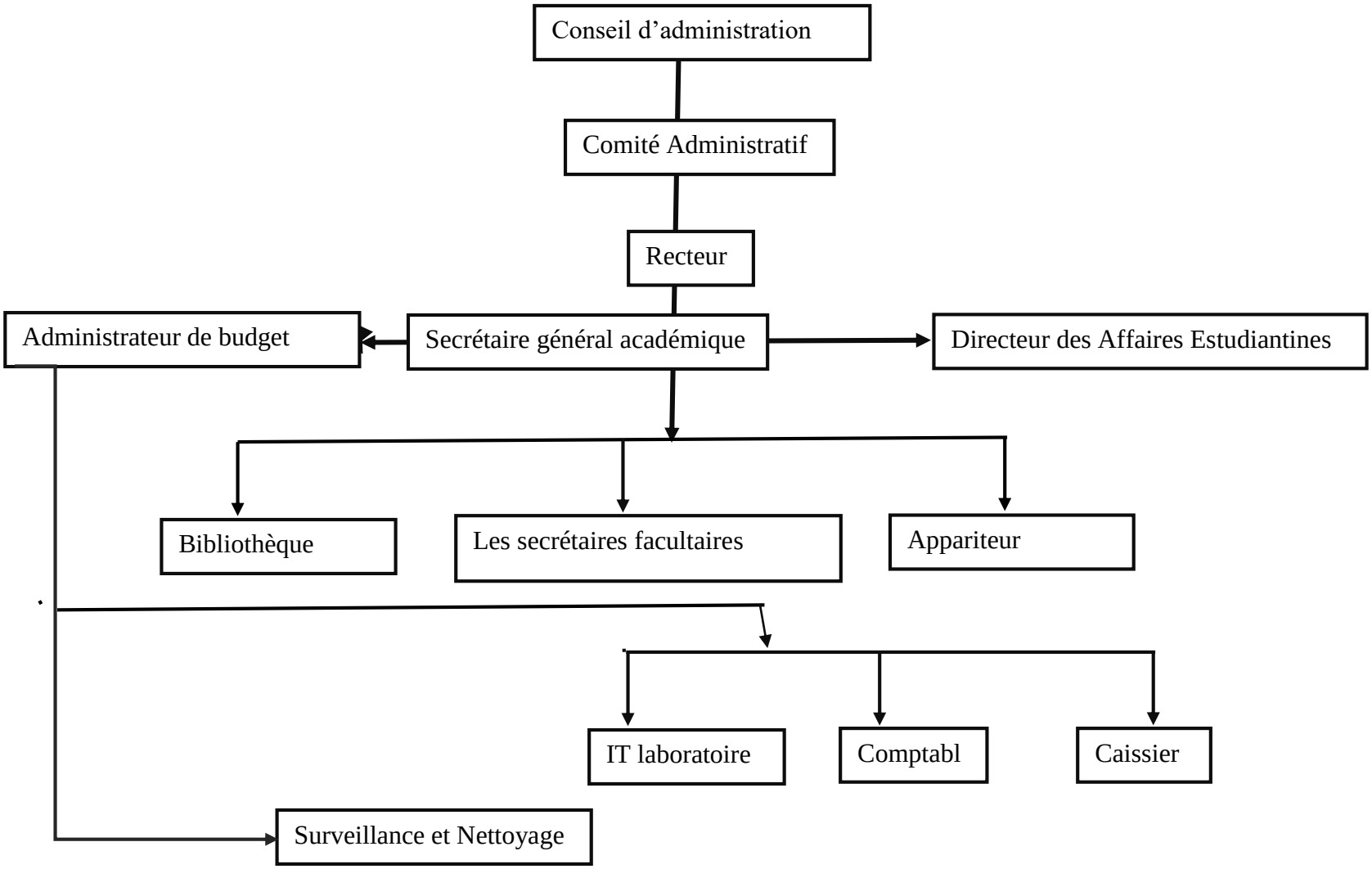
L'université Adventiste de Goma est une institution d'enseignement supérieur et universitaire privée, dirigée par l'église Adventiste du 7^{ième} jour. Etant qu'une Université Adventiste, ses objectifs sont les suivants :

- Participer au développement du pays à travers l'éducation dans certain domaine notamment : Gestion, agronomie, lettre, sante publique, science de l'éducation ;
- Initier ou appuyer la recherche développement.

- Rayonnement de transformer l'environnement et produire de diplômes adaptés à l'avenir, capable de transformer la société et de construire la société de demain telle que le peuple le souhaite. Source spécifiée non valide Au Nord : EP UZIMA
- A l'Est : Institut Maranatha
- Au Sud : La route Nationale N^0 2 (Route Goma Sake)
- A l'Ouest : Route vers l'entrée Présidentielle

ORGANIGRAMME

II.4.1. ORGANISATION ET FONCTIONNEME



II.4.2. Fonctionnement

1.Conseil d'administration

Le conseil d'administration est le principal comité universitaire responsable de l'ensemble des activités quotidiennes de l'université. Il s'agit à titre de responsable du traitement de toutes les questions relevant de la responsabilité du conseil universitaire. Il sert de manière législative, en tant que pouvoir déléguer, dans toutes les autres questions.

2.Comité Administratif

Ce comité prend ses décisions et recommandations d'une manière collégiale ;

Il est solidairement responsable devant le comité exécutif,

Il est chargé de, d':

- ✓ Assurer la gestion courante de l'U.A. GO & I.S.T.A. GO ;
- ✓ Recommander au comité exécutif les prévisions budgétaires préparer par le service de finance ;
- ✓ Préparer l'agenda du comité exécutif ;

Le comité Administratif a pour membre :

- Le recteur en même temps directeur général qui est le président du comité.
- Le secrétaire général administratif : secrétaire du comité
- Le secrétaire général académique : Membre
- Le secrétaire Général des affaires estudiantines : Membre

Le mandant pour les administrateurs de l'université est e 5 ans. Ce mandat est renouvelable une seule fois et l'intérim ne peut excéder une année.

3.Recteur

Le recteur doit être détenteur d'un doctorant à thèse avec moins le grade de professeur associé et a la charge de diriger l'ensemble de l'UAGO & ISTAGO d'en promouvoir par les moyens appropriés, l'unité, la collaboration et progrès. Outre ses qualifications spirituelles et membre de l'église adventiste du septième jour, parmi ces attributions nous avons :

- Diriger, promouvoir et coordonner toutes les activités de la communauté universitaire de l'UAGO et l'ISTAGO ;
- Représenter l'UAGO et l'ISTAGO auprès de tiers
- Présider les réunions du comité exécutif et administratif et veiller à l'application des décisions prises ;
- Etc….

4.Secrétaire Général Académique

Le Secrétaire Général Académique doit être détenteur d'un doctorant à thèse, et il est assiste le chef d'Etablissement dans ses fonctions. Le secrétaire général académique est membre du comité de gestion. Il supervise et coordonne les activités des services relevant de son ressort. Il fait rapport des activités de ses services au chef d'Etablissement dans les conditions prévues par le règlement organique.

A ce titre, parmi ces attributions il y'a :

- La gestion du personnel académique et scientifique qui s'occupe des dossiers de cette catégorie du personnel, leur carrière, leur promotion, leur appréciations, avancement de cours, etc. ;
- Suivre, au jour le jour, les activités de tout le secteur académique de l'établissement, en particulier les plans annuels des cours offerts par les facultés et les calendriers des cours avec l'aide des doyens des facultés.
- Présider les comités académiques ;
- Rédiger chaque semestre un rapport détaillé sur la vie académique de l'établissement ;
- Aider le corps enseignant à améliorer la qualité des enseignements et encourager la recherche ;
- Etc…

5.Secrétaire Général Administratif et Administrateur de Budget

Il est chargé de l'administration et de finances de l'UAGO et l'ISTAGO, il est directement responsable devant le recteur et le chef d'établissement. Il a la charge générale de l'administration financière de l'établissement, des biens physiques et des unités des productions.

Ses fonctions et responsabilités sont les suivantes :

- Il coordonne et supervises la gestion financière quotidienne de l'établissement dans le strict respect du règlement financier et des dispositions réglementaires en vigueur ;
- Rédige et commente, sous le couvert du comité de gestion, le rapport annuel de gestion financière.
- Supervise la comptabilité de l'établissement et suit les mouvements des comptes bancaires ;
- Préparer le budget annuel et veille au respect des règles budgétaires et à sa réparation dans les différents services de l'établissement ;
- Etc…

5.Directeur des Affaires Estudiantines

Le directeur des affaires estudiantines doit être au moins un détenteur d'une License (Maitrise). Il a comme attributions :

- Superviser les œuvres estudiantines ainsi que les espaces environnants ;
- Présider le comité mensuel des œuvres (gestion des homes, dortoirs et toutes autres infrastructures servant au logement des étudiants) ;
- Promouvoir la discipline et tenir le comité de discipline ;
- Etc…

6. Bibliothèque

La bibliothèque est un service base universitaire pour le personnel, les étudiants et les utilisateurs externes. Dans le but d'empêcher que la bibliothèque ne soit entrainée par des événements ou des enthousiasmes individuels, le bibliothécaire a l'obligation d'instituer des systèmes qui améliorent le fonctionnement de la bibliothèque et préservent le matériel d'information afin qu'il n'en soit pas perdu. Cela garantit que les informations sont identifiées, saisies, organisées et utilisées sous la forme de connaissances afin qu'aucune ne soit gaspillée et rendent les connaissances disponibles de sorte qu'aucune ne doive être privée dans les fonctions opérationnelles quotidiennes de la bibliothèque.

7. Apparitorat Central

L'appariteur est la porte d'entrée des étudiants pour entrer et sortir de l'université. En tant que département, ses principales fonctions sont : les admissions, la génération et la tenue des dossiers des étudiants, l'inscription et la remise des diplômes, la délivrance de certificats et de relevés de notes, la lettre de bourse et la délivrance de cartes d'étudiant aux étudiants.

8. Services de sécurité

Le département de de sécurité de l'UAGO et l'ISTAGO est chargé de la sécurité et de la protection des vies et biens de l'université et de la communauté universitaire, Nous prévenons les infractions de manière proactive et faisons tout ce qui est nécessaire pour réagir rapidement à une telle menace une fois remarquée.

9. Le Service de nettoyage

Ce service a été créé pour surveiller la propreté, fournir un environnement sur et sécurisé pour les étudiants, les employés et les visiteurs également pour prévenir la perte ou l'endommagement du bâtiment de l'université.

CHAPITRE TROISIEME : MÉTHODOLOGIE DE RECHERCHE

III.1. PLANNING PRÉVISIONNEL DU PROJET

III.1.1. Un Projet

Un projet est un objectif à réaliser, par des acteurs, dans un contexte précis, dans un délai donné, avec des moyens définis. (O'Shaughnessy, 1992)

Les principaux acteurs impliqués sur un projet sont généralement le chef de projet, le sponsor du projet, les membres de l'équipe, le client et les parties prenantes. Ces personnes sont amenées à travailler ensemble pour atteindre l'objectif fixé dans le cadre du projet.

Un projet doit avoir un début et une fin, cela nécessite la mise en œuvre de ressources humaines, financières et matérielles pour sa réalisation.

Un projet qui mène à terme est constitué de l':

- Etude de faisabilité du projet ;
- Elaboration du projet ;
- Exécution du projet ;
- Implantation du projet ;
- Son exploitation.

III.2. PLANIFICATION DU PROJET

La planification de projet correspond à l'organisation des tâches à réaliser sur une période donnée.

L'objectif de la planification est de :

- Déterminer le coût,
- Déterminer les ressources mobilisées et
- La meilleure manière d'ordonnancer toutes les tâches à effectuer.

III.3. MÉTHODE D'ORDONNANCEMENT

Il existe 3 méthodes pour l'ordonnancement :

- ✓ La méthode en barre ou Diagramme de GANTT,
- ✓ La méthode potentielle Métra (MPM) et
- ✓ La méthode Program Evaluation and Research Task (PERT)

Pour notre travail nous allons nous focaliser sur le diagramme PERT qui est un outil servant à analyser les différentes tâches qui entrent dans l'exécution d'un projet et permet de déterminer le temps requis pour chaque tâche.

PERT : est une méthode conventionnelle utilisable en gestion de projet, ordonnancement et planification développée aux États-Unis par la Navy dans les années 1950.

III.4. DÉLIMITATION DES TÂCHES

Pour établir un réseau PERT, la délimitation des tâches est la première étape pour déterminer les tâches, identifier et lister les tâches nécessaires à la construction effective du projet. Chaque tâche est associée à une durée estimée en unité de temps.

Ces différentes tâches sont retracées dans 4 paramètres :

- Codes tâches,
- Désignation de la tâche,
- Durée jours,
- Tâches précédentes.

Tableau 1: Délimitation des tâches

Code	Désignation de la tâche	Durée en jours	Tâches précédentes
A	Etude du projet	5	-
B	Conception du Projet	2	A
C	Contact et préparation du terrain	2	B
D	Etude préalables	5	C
E	Planification	3	D
F	Préparation ordinateur et installation du système Kali Linux	1	E
G	Installation logiciels (Nessus, Lynis. Etc….)	1	F
H	Audit proprement dit	10	G

I	Identification des vulnérabilités	8	H
J	Élaboration d'une fiche technique de diagnostic	1	I

III.4.1. ESTIMATION DES COUTS DE REALISATION DU PROJETS

Tableau 2: Estimation des coûts de réalisations du projet

Code	Désignation de la tâche	Tâches précédentes	Durée	Nbre/travailleurs	C.U en $	C.T en $
1	Etude du projet	-	5	3	15	225
2	Conception du Projet	A	2	3	10	60
3	Contact et préparation du terrain	B	2	2	12	48
4	Etude préalables	C	5	3	10	150
5	Planification	D	3	2	60	180
6	Préparation ordinateur et installation du système Kali Linux	E	1	2	50	100
7	Installation logiciels (Nessus, Lynis. Etc….)	F	1	1	30	30
8	Audit proprement dit	G	10	2	10	200
9	Identification des vulnérabilités	H	8	2	50	800
10	Élaboration d'une fiche technique de diagnostic	I	1	1	10	10
Total			**38**			**1803$**
Imprévus (10% du total)						**180.3$**
Coût total du projet						**1983.3$**

III.6. ELABORATION CHEMIN CRITIQUE

Pour calculer les dates on fait :

1. Calcul de la date au plus tôt (DAT) :
   DAT = Durée du début au plus tôt de la tâche précédente + Durée de la tâche suivante
2. Calcul de la date au plus tard (DPT) :
   DPT = Date au plus tôt de la tâche suivante – la durée de la tâche précédente

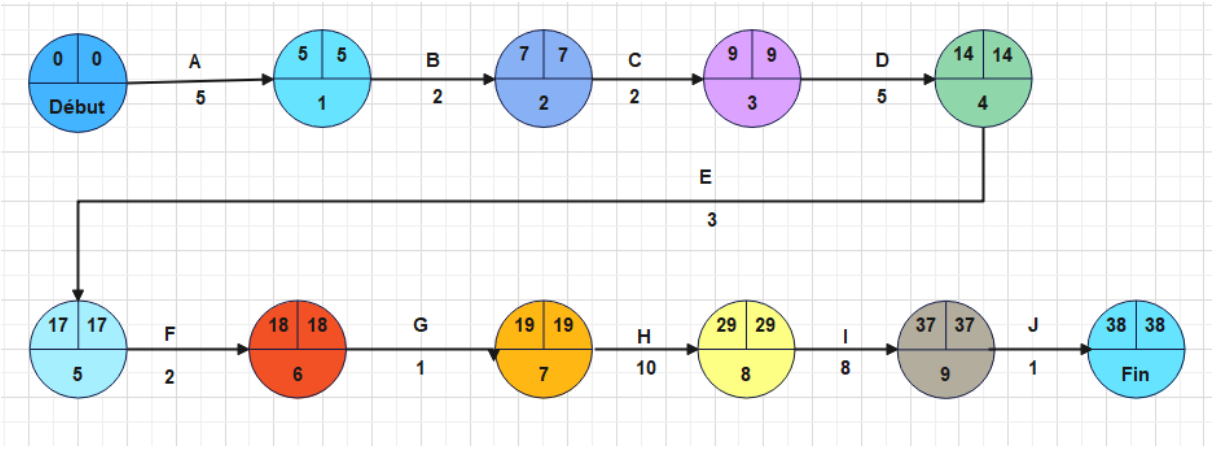


Figure 2: Graph

III.8. DÉTERMINATION DE LA MARGE LIBRE ET LA MARGE TOTAL

a. Marge libre ML(x)

Le champ Marge libre contient la durée de retard qu'une tâche peut prendre sans retarder successeur tâches. Si la tâche n'a aucun successeur, la marge libre représente la durée pendant laquelle une tâche peut être retardée sans retarder la date de fin du projet entier.

Formule :

ML= Durée au plus tard (nœud suivant) – Durée de la tâche – Date au plus tôt

b. Marge Total (x)

La marge totale d'une tâche est la marge qui peut être consommée sur cette tâche sans remettre en cause la fin du projet. Tout dépassement de délai, sur cette tâche, supérieur à la marge totale de la tâche provoquera un retard qui se répercute au moins en partie sur la fin de projet.

Formule :

MT= Date au plus tard – Date au plus tôt

III.8.1. Tableau pour les marges

Tableau 3: Marge

Tâche	Marge Libre	Marge Total
A	5-5-0=0	5-5-0=05-5-0=0
B	7-2-5=0	7-7=0
C	9-2-7=0	9-9=0
D	14-5-9=0	14-14=0
E	17-3-14=0	17-17=0
F	18-1-17=0	18-18=0
G	19-1-18=0	19-19=0
H	29-10-19=0	29-29=0
I	37-8-29=0	37-37=0
J	38-1-37=0	38-38=0

III.9. RECHERCHE DE CHEMIN ET TÂCHES CRITIQUES

On appelle chemin critique du réseau PERT, la succession des tâches pour lesquelles aucun retard n'est possible sans remettre en cause la durée optimale du projet. Donc la date au plus tôt est égale à la date au plus tard.

Dans notre travail, on n'a pas des tâches critiques car parmi toutes les tâches, aucune tâche qui va se réaliser avec retard. Donc toutes les tâches vont se réaliser comme prévu.

III.10. METHODE D'EVALUATION DE L'AUDIT DU SYSTEME EXISTANT

Pour auditer notre système nous allons utiliser la méthode EBIOS **(**Expression des besoins et identification des objectifs de sécurité) La méthode EBIOS est une méthode d'évaluation des risques en informatique, développée en 1995 par la Direction centrale de la sécurité des systèmes d'information et maintenue par l'Agence nationale de la sécurité des systèmes d'information qui lui a succédé en 2009.

Pour auditer un réseau avec la méthode EBIOS, il est recommandé de suivre les étapes suivantes

1. **Identifier les actifs à protéger** : Les actifs sont tout ce qui a de la valeur et que l'organisation possède. Dans notre cas on peut donner des exemples comme des serveurs, des ordinateurs portables, et d'autres équipements de réseau.
2. **Identifier les menaces** : il s'agit de recenser les événements qui peuvent compromettre la sécurité des actifs identifiés. Les menaces peuvent être internes ou externes… (Les malwares, le phishing, l'accès non autorisé. Etc…).
3. **Identifier les vulnérabilités** : il s'agit de recenser les faiblesses du système qui peuvent être exploitées par les menaces identifiées. On peut citer les vulnérabilités logicielles, les vulnérabilités matérielles, les vulnérabilités liées aux mots de passe, les vulnérabilités liées aux accès non autorisés. Etc…
4. **Évaluer les risques** : il s'agit d'évaluer la probabilité que les menaces exploitent les vulnérabilités identifiées et l'impact que cela pourrait avoir sur l'entreprise.
5. **Identifier les mesures de sécurité** : il s'agit de définir les Nosures de sécurité à mettre en place pour réduire les risques identifiés, on peut dire comme mettre à jour les logiciels et les équipements.

III.10.1. Identification des actifs à protéger

Lors de l'audit de notre réseau, on est parvenu à identifier les actifs à protéger dont les actifs peuvent inclure des données sensibles, des informations de connexion, des applications critiques, des équipements de réseau, des serveurs, des ordinateurs, des périphériques mobiles, des comptes d'utilisateurs, des groupes d'utilisateurs, des autorisations, des politiques de sécurité, des procédures de sauvegarde, etc.

III.10.2. Identification des menaces

Lors de l'audit du réseau de l'UAGO, on a trouvé que plusieurs menaces peuvent être identifiées. Voici une liste non exhaustive de ces menaces

- Les attaques par déni de service (DDoS) : ces attaques visent à saturer les serveurs et les équipements du réseau pour les rendre inaccessibles aux utilisateurs légitimes.
- Les attaques de phishing : ces attaques consistent à tromper les utilisateurs pour obtenir des informations sensibles, telles que des identifiants de connexion ou des informations bancaires.
- Les attaques de type "homme du milieu" : ces attaques consistent à intercepter les communications entre deux équipements pour les espionner ou les modifier.
- Les attaques par force brute : ces attaques consistent à tester toutes les combinaisons possibles de mots de passe pour accéder à un compte utilisateur.

- Les vulnérabilités logicielles : ces vulnérabilités permettent à un attaquant de prendre le contrôle d'un équipement ou d'accéder à des informations sensibles.
- Les erreurs de configuration : ces erreurs peuvent rendre les équipements du réseau vulnérables aux attaques.
- Les accès non autorisés : ces accès peuvent être réalisés par des utilisateurs malveillants ou par des utilisateurs légitimes qui ont des droits d'accès trop élevés.

III.10.3. Identification des vulnérabilités

Le Réseau de l'UAGO est victime des vulnérabilités suivantes :

- *Les vulnérabilités logicielles* : ces vulnérabilités peuvent être présentes dans les applications, les systèmes d'exploitation, les serveurs web, les bases de données, etc.
- *Les mots de passe faibles* : des mots de passe faibles ou facilement divisibles peuvent permettre à un attaquant d'accéder à un compte utilisateur.
- *Les ports ouverts* : des ports ouverts sur les équipements du réseau peuvent permettre à un attaquant d'exploiter des vulnérabilités pour prendre le contrôle de l'équipement.
- Les erreurs de configuration : des erreurs de configuration peuvent rendre les équipements du réseau vulnérables aux attaques.
- Les mises à jour manquantes : des mises à jour de sécurité manquantes peuvent laisser des vulnérabilités non corrigées sur les équipements du réseau.
- Les accès non autorisés : des utilisateurs ayant des droits d'accès trop élevés peuvent accéder à des informations sensibles ou compromettre la sécurité du réseau.

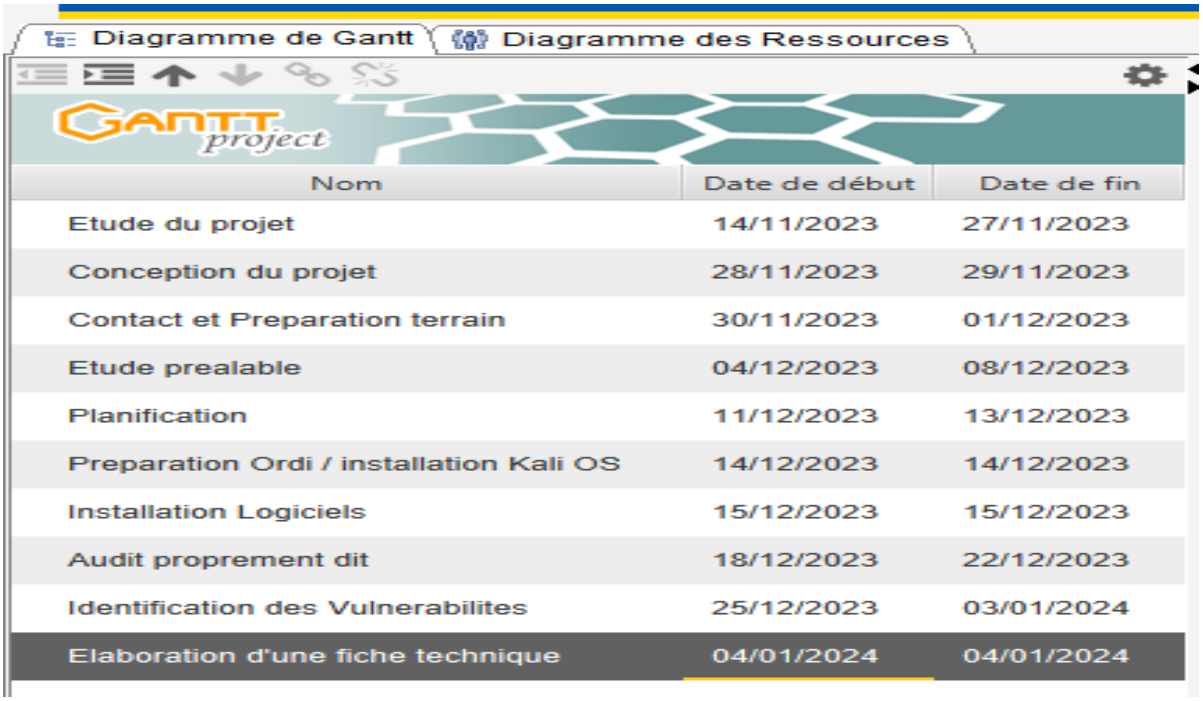
III.10.4. Identification des mesures de sécurité

Lors d'un audit de système d'information, plusieurs mesures de sécurité peuvent être identifiées pour protéger les actifs critiques de l'entreprise. Voici quelques exemples de mesures de sécurité qui peuvent être proposées lors d'un audit de système d'information :

- La mise en place de pare-feu : les pare-feu permettent de filtrer le trafic réseau pour bloquer les connexions non autorisées.
- La mise à jour régulière des logiciels : les mises à jour permettent de corriger les vulnérabilités présentes dans les logiciels.
- La mise en place de politiques de mots de passe forts : les politiques de mots de passe forts permettent de réduire les risques d'attaques par force brute.
- La mise en place de politiques de sécurité : les politiques de sécurité permettent de définir les règles à suivre pour protéger les actifs critiques de l'entreprise.
- La mise en place de solutions de chiffrement : le chiffrement permet de protéger les données sensibles contre les accès non autorisés.

- La mise en place de solutions de sauvegarde : les solutions de sauvegarde permettent de restaurer les données en cas de perte ou de corruption.
- La formation et la sensibilisation des utilisateurs : la formation et la sensibilisation permettent de réduire les risques d'attaques de phishing et d'accès non autorisés.

III.11. CALENDRIER DE RÉALISATION DU PROJET



Nom	Date de début	Date de fin
Etude du projet	14/11/2023	27/11/2023
Conception du projet	28/11/2023	29/11/2023
Contact et Preparation terrain	30/11/2023	01/12/2023
Etude prealable	04/12/2023	08/12/2023
Planification	11/12/2023	13/12/2023
Preparation Ordi / installation Kali OS	14/12/2023	14/12/2023
Installation Logiciels	15/12/2023	15/12/2023
Audit proprement dit	18/12/2023	22/12/2023
Identification des Vulnerabilites	25/12/2023	03/01/2024
Elaboration d'une fiche technique	04/01/2024	04/01/2024

Figure 3: Réalisation du projet

III.12. DIAGRAMME DE GANT

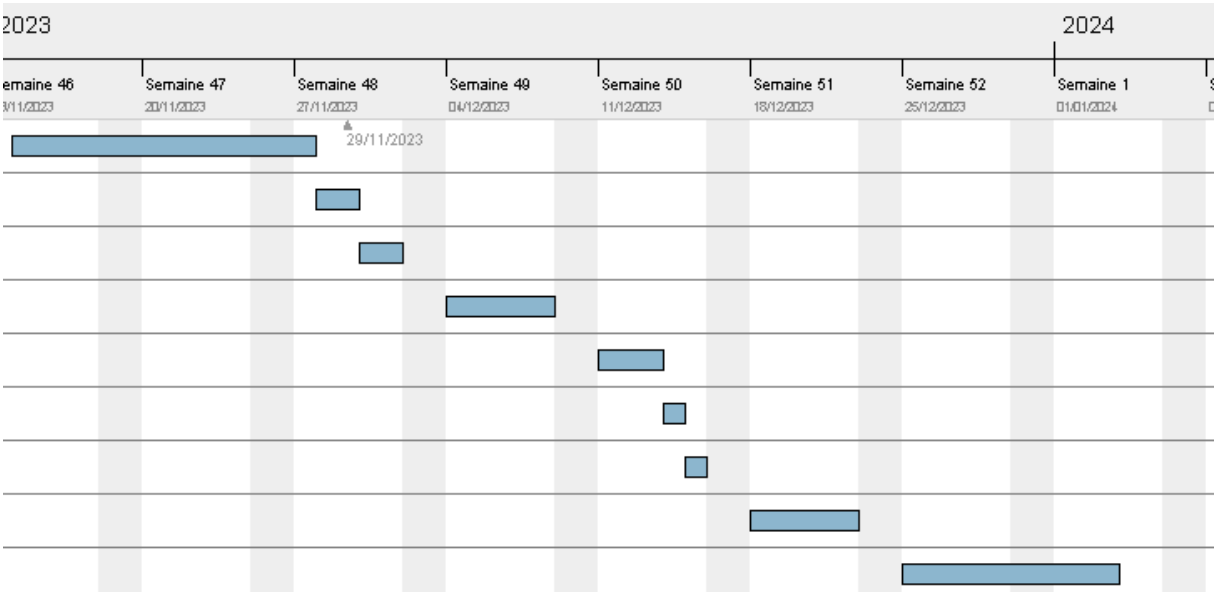


Figure 4: Diagramme de gant

III.13. ARCHITECTURE PHYSIQUE DE L'EXISTANT

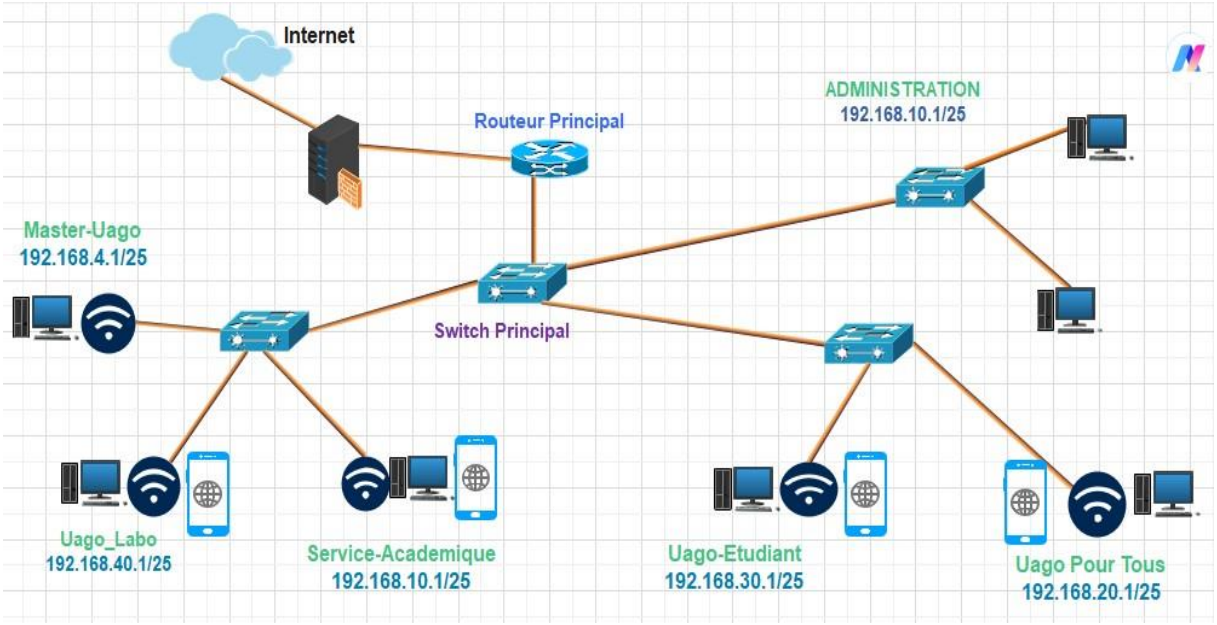


Figure 5: Architecture de l'existant

III.14. ARCHITECTURE LOGIQUE DE L'EXISTANT

Voici l'adressage du réseau à l'UAGO :

Tableau 4: Architecture de l'UAGO

N^0	Sous réseau	Adresse IP	Adresse réseau	Masque de sous réseau
01	Administration	192.168.10.1 - 192.168.10.16/25	192.168.10.0	255.255.255.0
02	Uago-Labo	192.168.40.1 – 192.168.40.26	192.168.40.0	255.255.255.0
03	Uago pour Tous	192.168.20.1 – 192.168.20.255	192.168.20.0	255.255.255.0
04	Master-Uago	192.168.4.1 – 192.168.4.26	192.168.10.0	255.255.255.0
05	Service-Académique	192.168.10.1 – 192.168.10.26	192.168.10.0	255.255.255.0
06	Uago-Etudiant	192.168.30.1 – 192.168.30.26	192.168.10.0	255.255.255.0

III.15. DIAGNOSTIQUE ET CRITIQUE DE L'EXISTANT

Après avoir fait une étude sur le système existant de notre université, il nous revient la tâche de ressortir ses défauts et qualités. Il ne s'agit pas de tout détruire sous prétexte que les nouvelles solutions seront proposées mais plutôt à dire ceux qui est réel.

Points Forts

- ✓ Chaque service exécute parfaitement son rôle et la distribution des taches est bien respectée
- ✓ La collaboration entre les agents est parfaite

Points Faibles

- ✓ En premier lieu nous avons manqué complètement le contrôle de logiciels se trouvant sur des machines connectées dans son réseau pour identifier les points faibles, les failles de sécurité, ceux qui donne que s'il y a un bon Hacker qui s'y introduisait dans le système ou serveur et détruire le système mais aussi voler les informations sensibles.
- ✓ En deuxième lieu nous avons constaté qu'il n'y a pas la séparation de salle informatique et la salle machine, qui peut causer à ce qu'une personne malveillante s'il trouver l'occasion de voler même un routeur il peut s'en aller avec, et pourtant seul l'administrateur du réseau pourrait avoir accès à ces équipements.

Proposition des solutions

Après avoir effectué un audit de sécurité, voici quelques propositions pour résoudre les problèmes identifiés :

1. Utilisation d'outils spécialisés,
2. Renforcer les mots des passes,
3. Utilisation d'outils spécialisés,
4. Veille technologique et mise à jour régulière,
5. Collaboration avec des experts en sécurité,
6. Intégration des résultats de l'audit dans les processus de gestion des risques.

Avantages :

1. Large éventail d'outils spécialisés,
2. Communauté active,
3. Facilité d'utilisation,
4. Flexibilité et personnalisation,
5. Renforcement de la sécurité.

Désavantages :

1. Courbe d'apprentissage requise,
2. Complexité des outils,
3. Risque d'utilisation inappropriée,
4. Contraintes matérielles,
5. Nécessité d'une évaluation approfondie en fonction des besoins spécifiques.

CHAPITRE QUATRIÈME : PRESENTATION DES RESULTATS

IV.0. Introduction :

Le quatrième chapitre de ce livre se concentre sur l'audit d'un système d'information à l'aide de Kali Linux. Kali Linux est une distribution Linux spécialisée dans les tests de pénétration et l'audit de sécurité. Dans ce chapitre, nous explorerons les étapes clés de l'audit, en mettant l'accent sur les outils et techniques spécifiques disponibles dans Kali Linux. Nous aborderons la collecte d'informations, l'analyse de vulnérabilités, l'évaluation des contrôles de sécurité et la génération de rapports. En comprenant et en utilisant ces outils, les professionnels de la sécurité informatique pourront mener des audits approfondis pour garantir la protection des systèmes d'information.

Matériels utilisés

- Ordinateur HP EliteBook 8460p i7
- Processeur Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz 2.50 GHz
- RAM : 6,00 Go
- HDD : 500 Go
- Système d'exploitation : Kali Linux

Les logiciels Kali /Linux utilisés

- **Lynis :** Lynis est un outil d'audit pour renforcer les systèmes basés sur GNU / Linux. Il analyse la configuration du système et crée une vue d'ensemble des informations système et des problèNos de sécurité utilisables par des auditeurs professionnels. Il peut aider à des audits automatisés. (SICOSFY, 2023)
- **Nikto :** Nikto est un scanner de vulnérabilité en ligne de commande logiciel gratuit qui analyse les serveurs Web à la recherche de fichiers/CGI dangereux, de logiciels serveur obsolètes et d'autres problèNos. Il effectue des vérifications génériques et spécifiques au type de serveur. (wiki-ubuntu.fr, s.d.)
- **Nmap :** Nmap est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de Nmap fournit des indications sur la sécurité d'un réseau. Il est disponible sous Windows, Mac OS X, Linux, BSD et Solaris. Le code source de Nmap est disponible sous la licence GNU GPL jusqu'à la version 7.90. Il est désormais distribué sous la Nmap Public Source License (NPSL), qui est basée sur la GPLv2 mais ajoute des restrictions qui la rendent non-libre. (Nmap.org, s.d.)

- **Nessus :** Nessus est le scanner de vulnérabilité réseaux propriétaire développé par Tenable, qui est utilisé pour identifier les vulnérabilités potentielles pour un système et prioriser les problèNos critique pour éliminer les chemins d'attaque. Par rapport aux autres scanners de vulnérabilité, Nessus a la particularité d'être basé sur une architecture client/serveur et d'être compatible avec Windows et Linux. (Tenable, 2023)

IV.2. ARCHITECTURE DU NOUVEAU SYSTÈME

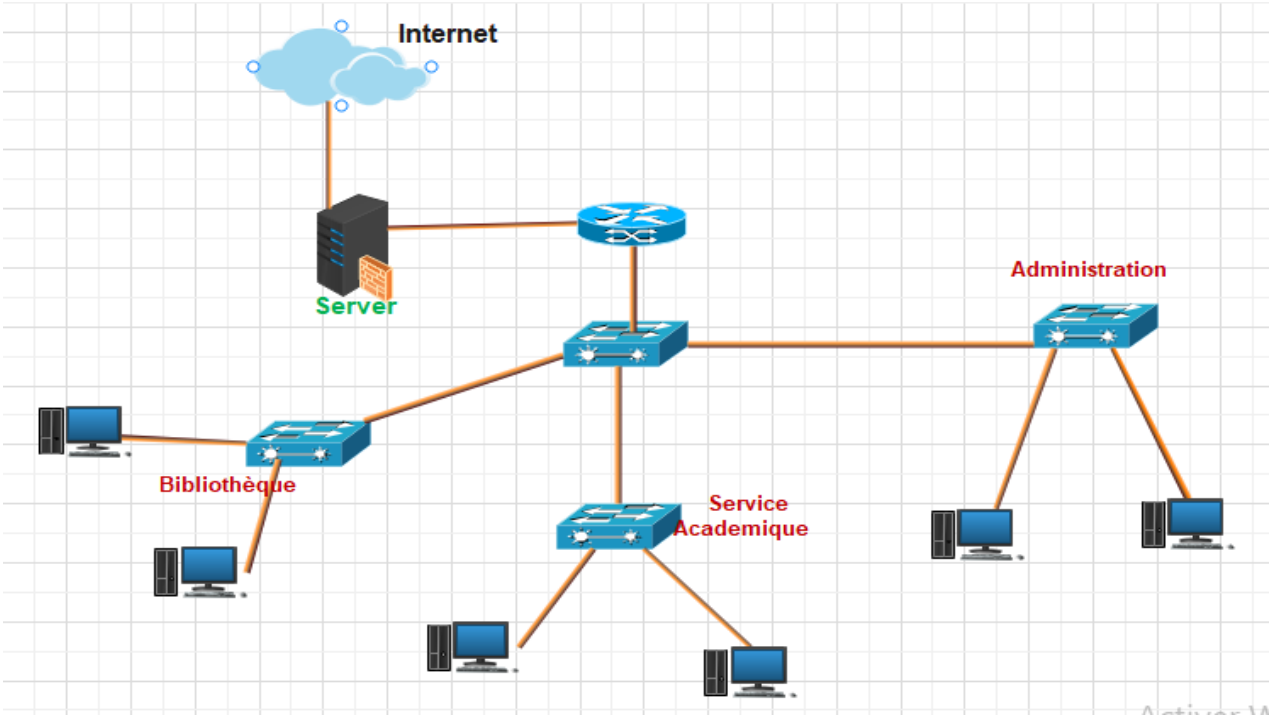


Figure 6: Architecture du nouveau SI

IV.3. INSTALLATION ET CONFIGURATION DE NESSUS

Nessus est le scanner de vulnérabilité réseaux de Tenable Network Security. Par rapport aux autres scanners de vulnérabilité, Nessus a la particularité d'être basé sur une architecture client/serveur et d'être compatible avec Windows et Linux.

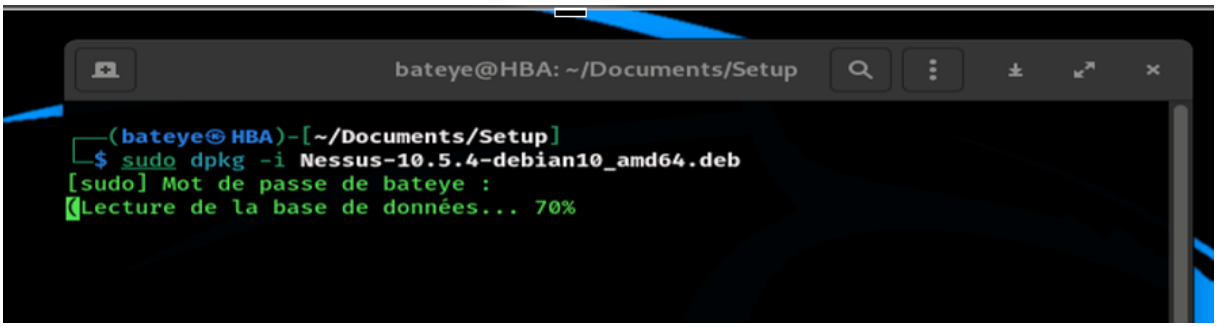


Figure 7: Installation de Nessus

b. Ici on va démarrer le service Nessus pour faire une configuration complète et commencer à scanner les vulnérabilités

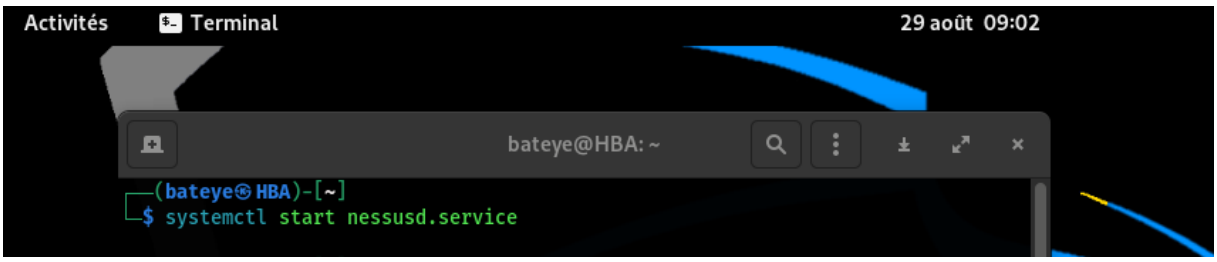


Figure 8: Démarrage du service Nessus

c. C'est le login pour se connecter au compte Nessus et commencer à faire des scans de vulnérabilités

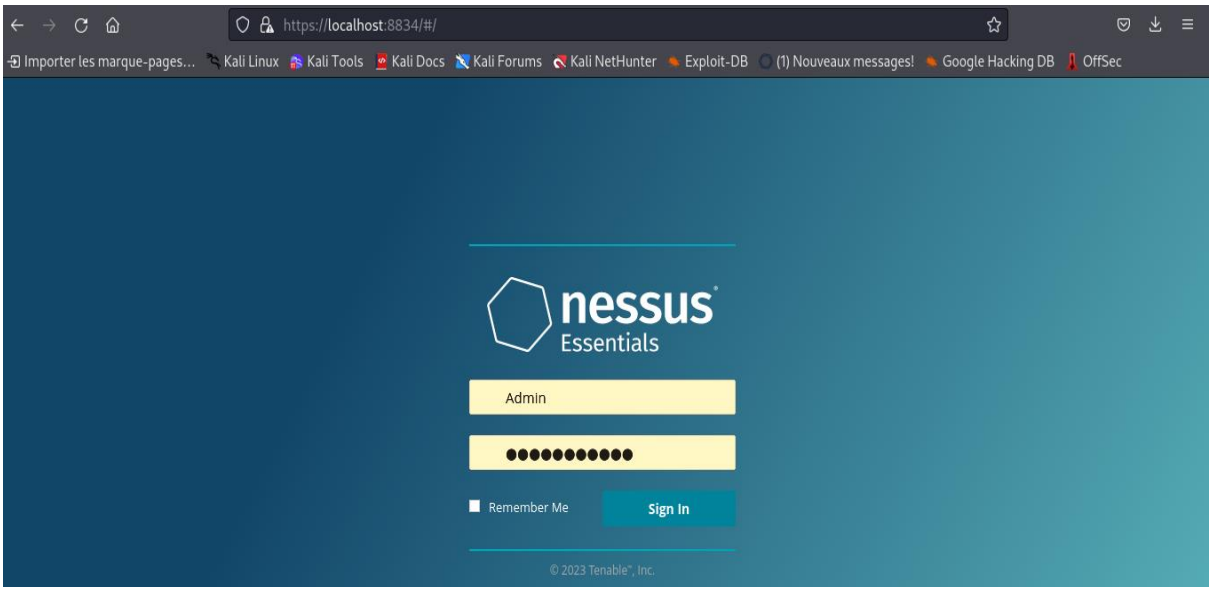


Figure 9: Nessus Login

d. scan des hôtes qui donne une liste des adresses IP qui sont connecté sur le réseau 192.168.1.0/24

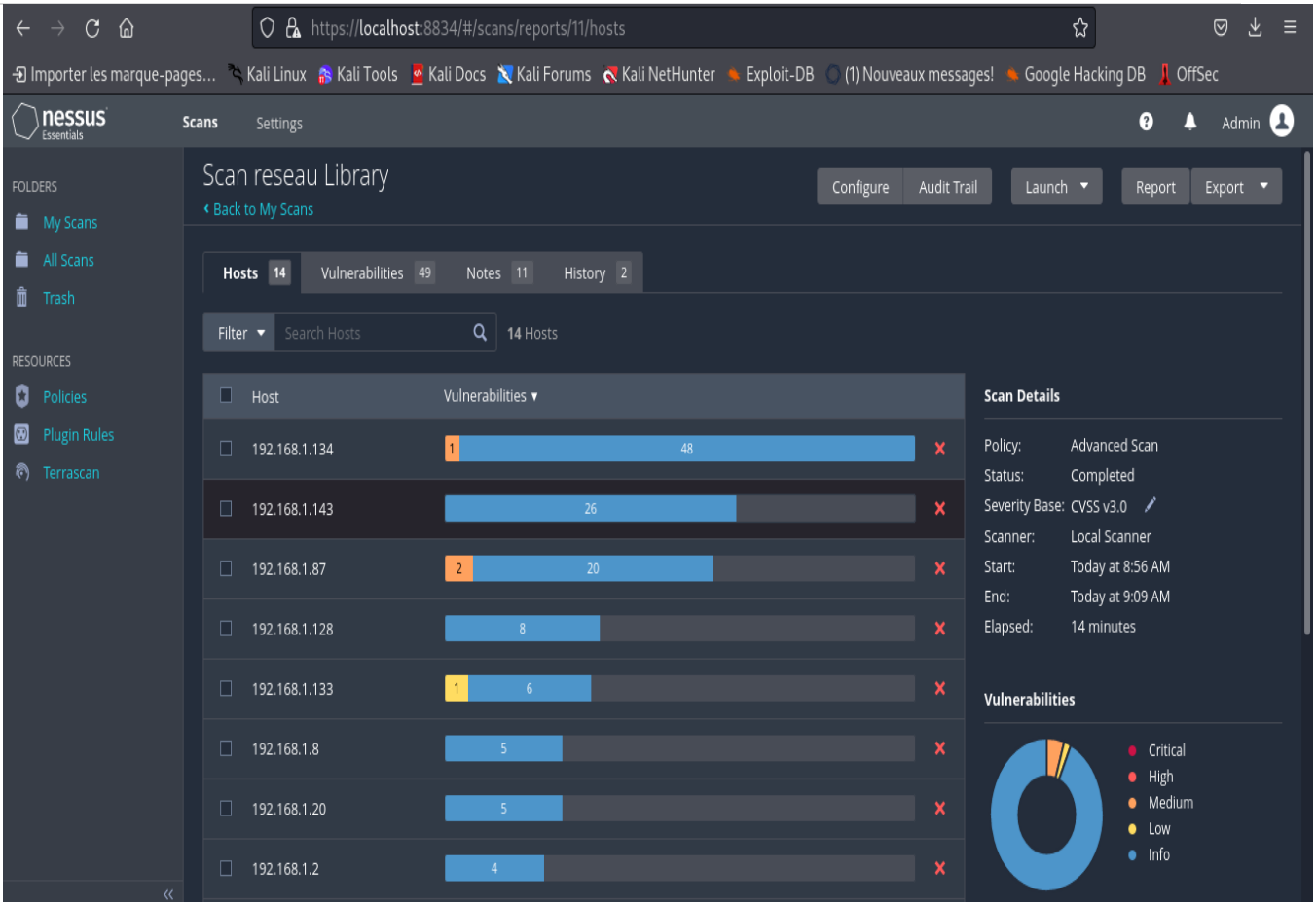


Figure 10: Scan Nessus

IV.3.1. IDENTIFICATION DES VULNERABILITES AVEC NESSUS

e. Ce plugin rassemble les adresses MAC découvertes à la fois lors de l'analyse à distance de l'hôte (par exemple SNMP et NetBIOS) et lors de l'exécution de vérifications locales (par exemple ifconfig). Il consolide ensuite les adresses MAC en une liste unique, unique et uniforme.

SNMP qui est un protocole de gestion de réseau qui est largement utilisé pour surveiller et gérer des dispositifs réseau. SNMP permet aux administrateurs réseau de collecter les informations sur l'état et les performances des appareils réseau, ainsi que de configurer et de contrôler ces appareils à distance.

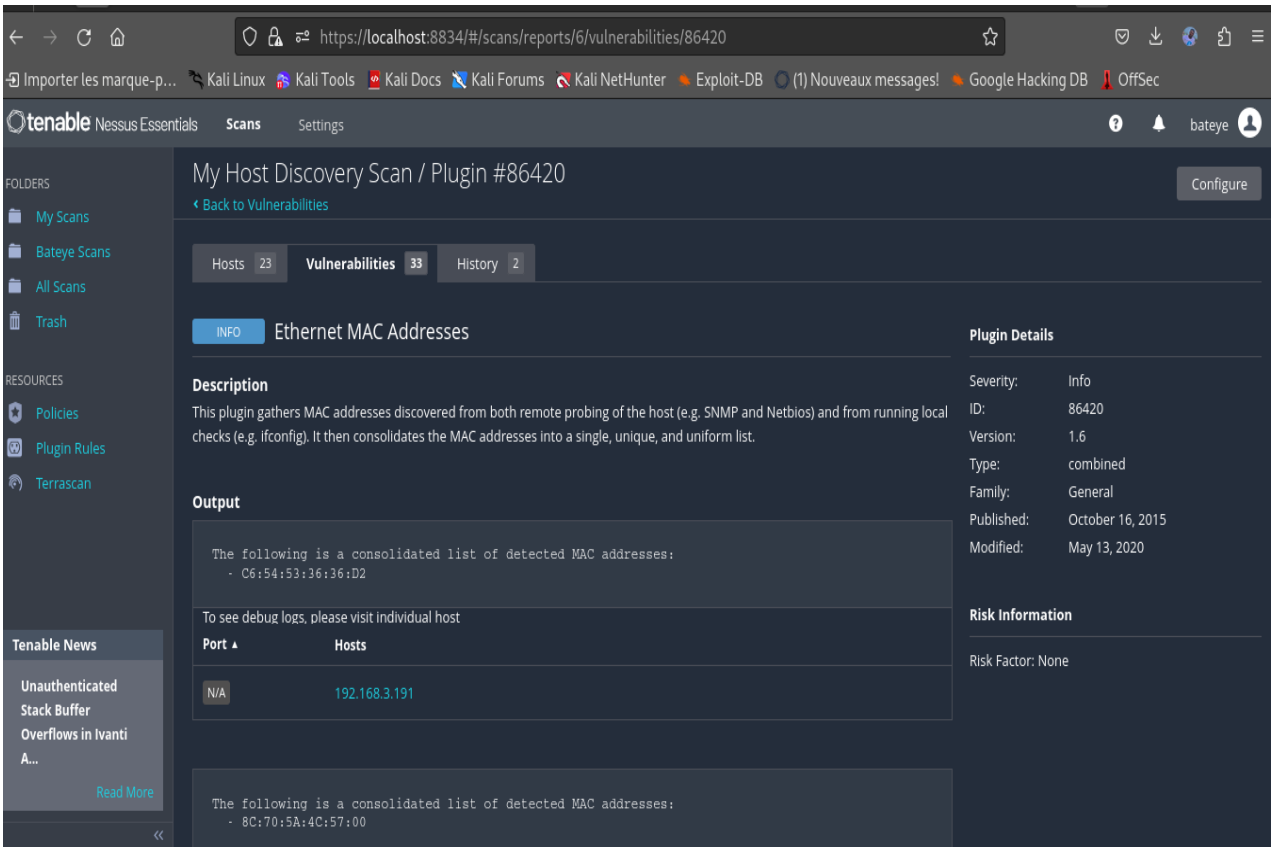


Figure 11: Scan avec Nessus 1

f. Nessus a pu énumérer les interfaces réseau configurées avec des adresses IPv4 en se connectant à l'hôte distant via SSH à l'aide des informations d'identification fournies.

Solution : Désactivez toutes les interfaces IPv4 inutilisées.

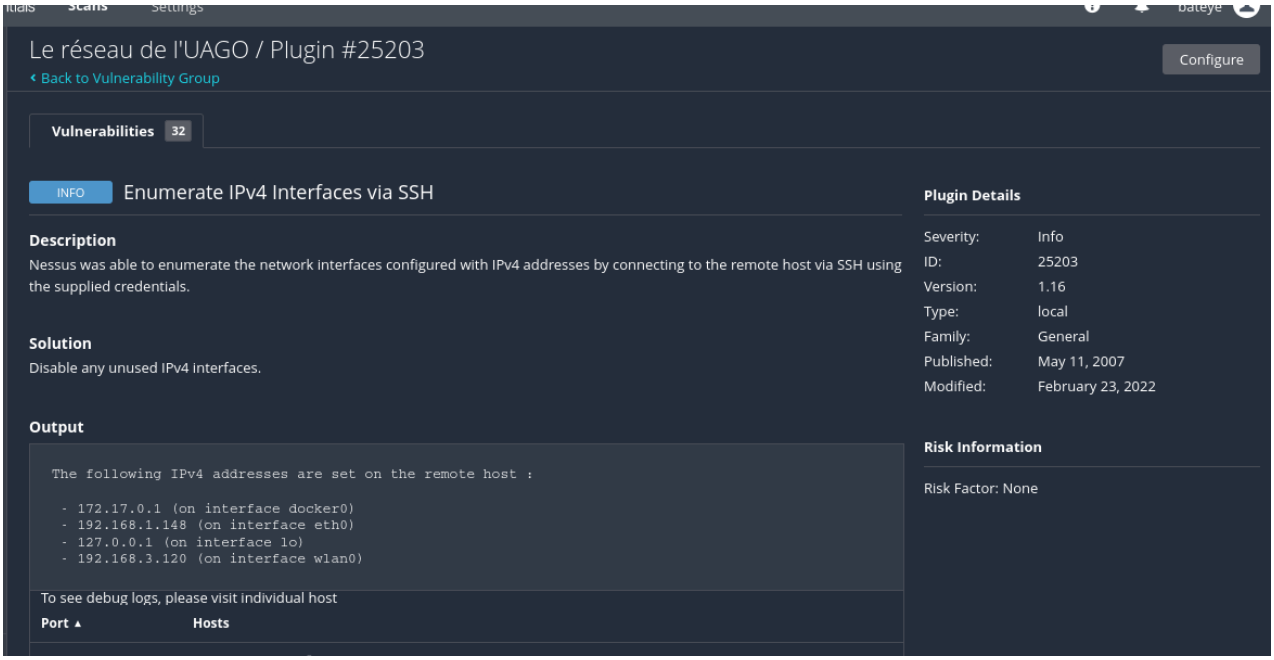


Figure 12: Scan Nessus 2

g. Ce script contacte le serveur DHCP distant (le cas échéant) et tente de récupérer des informations sur la configuration du réseau.

Solution : *Appliquez un filtrage pour conserver ces informations hors du réseau et supprimez toutes les options qui ne sont pas utilisées.*

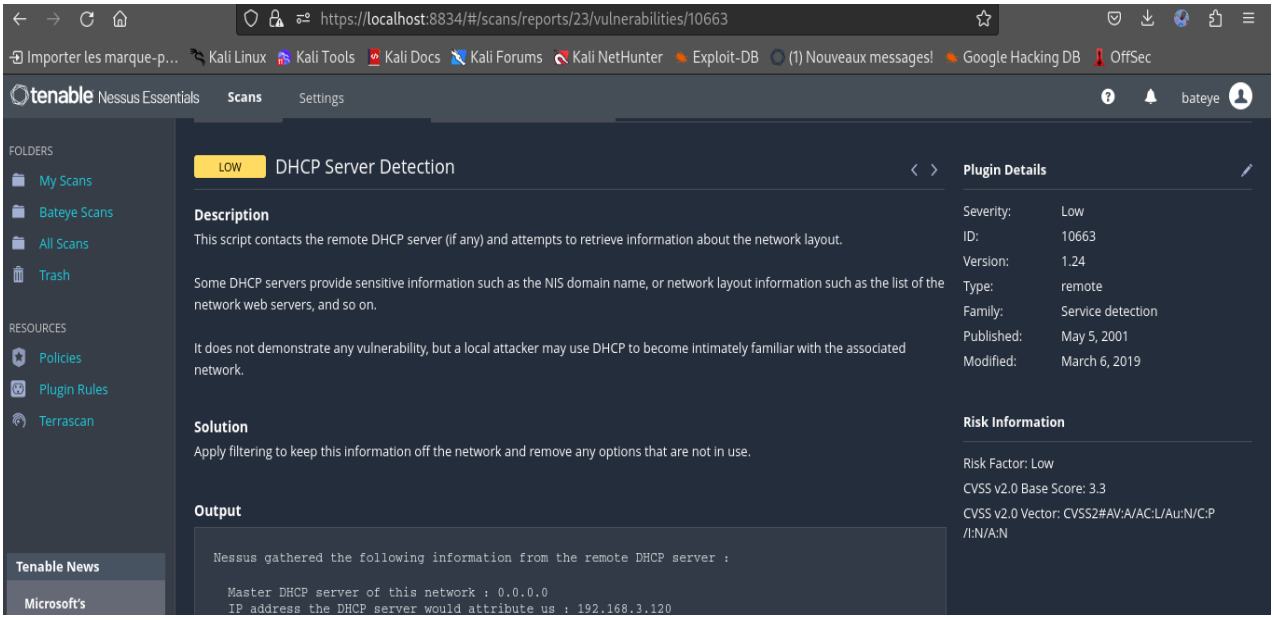


Figure 13: Scan Nessus 3

h. Cette vulnérabilités montre que le certificat X.509 du serveur n'est pas fiable. Cette situation peut se produire de trois manières différentes, dans lesquelles la chaîne de confiance peut être rompue, comme indiqué ci-dessous :

Solution : Achetez ou générez un certificat SSL approprié pour ce service.

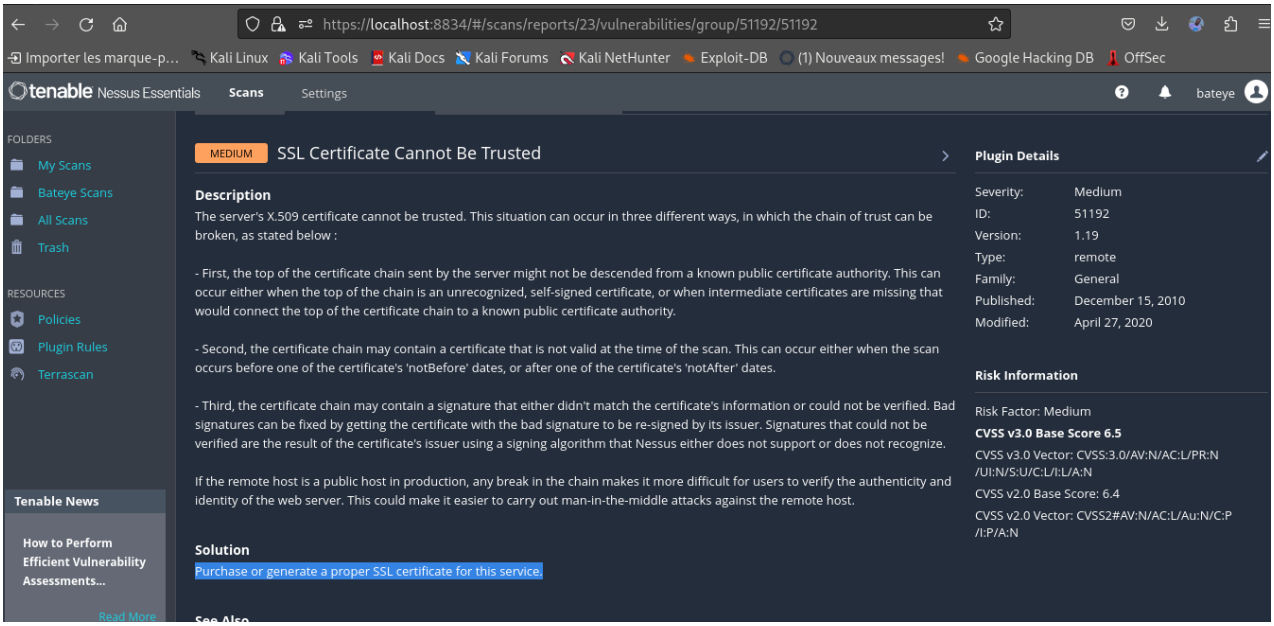


Figure 14: Scan Nessus 4

Cette vulnérabilité montré ci-dessous montre que la version de PostgreSQL installée sur l'hôte distant est potentiellement affectée par une vulnérabilité de divulgation d'informations. Dans PostgreSQL, un serveur modifié et non authentifié peut envoyer une chaîne non terminée lors de l'établissement du chiffrement de transport Kerberos. Dans certaines conditions, un serveur peut provoquer une lecture excessive d'un client libpq et signaler un message d'erreur contenant des octets non initialisés.

Solution : Mise à niveau vers PostgreSQL 12.14/13.10/14.7/15.2 ou version ultérieure

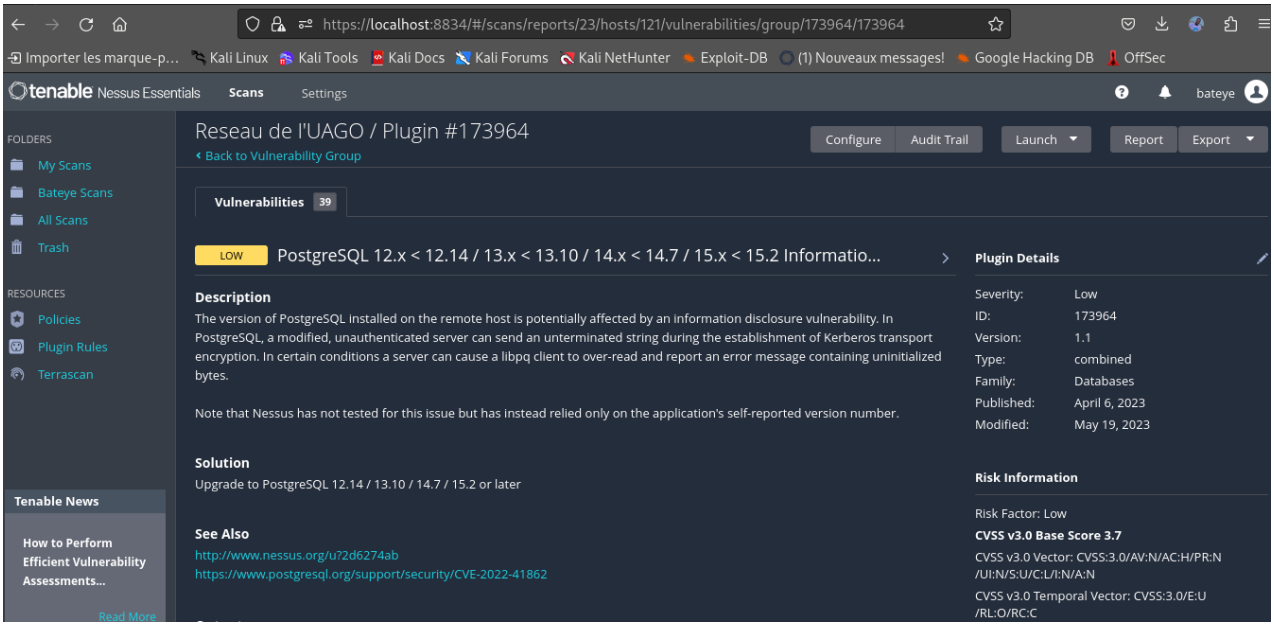


Figure 15 : Scan Nessus 5

IV.4. SCAN DES PORTS (Nmap et Zenmap)

Résultats de scan avec Nmap et Zenmap dans kali

Ce type de scan nous fournit beaucoup d'information très importante

-A : signifie (scan Agressif)

-O : besoin d'afficher le détail du système d'exploitation

a. Nmap est souvent utilisé pour déterminer les hôtes actifs dans un réseau, les ports ouverts sur ces hôtes, les services fonctionnant sur ces ports ouverts et l'identification de la version de ces services sur ces ports.

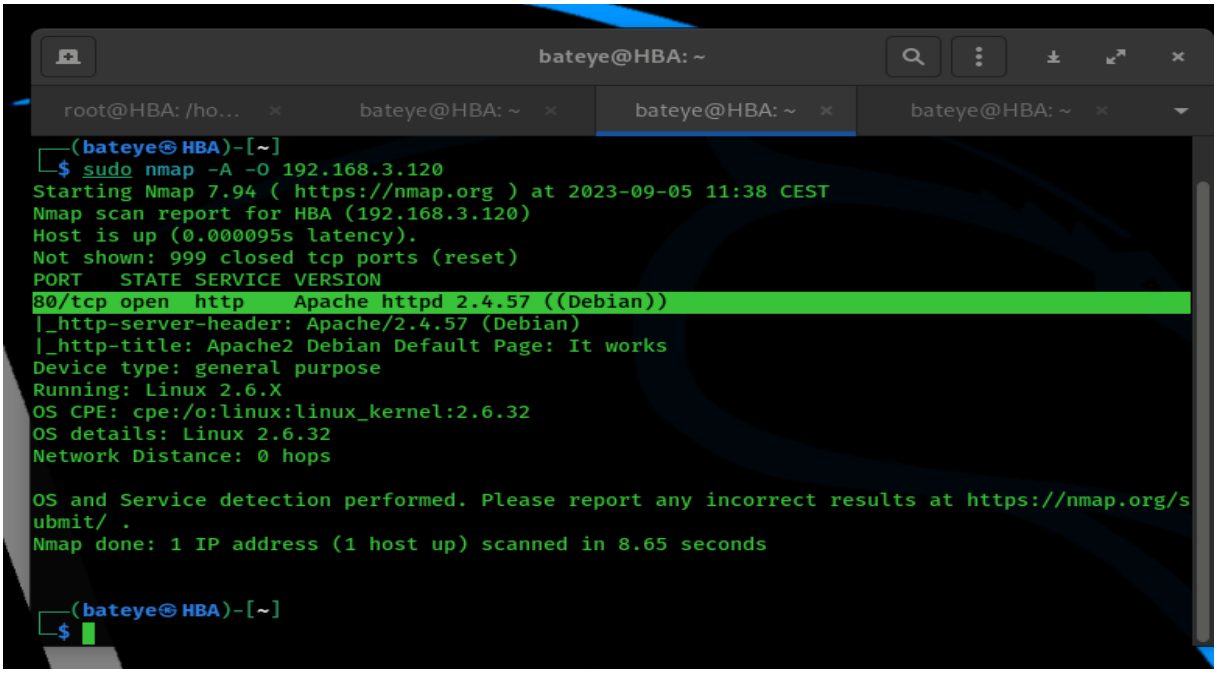


Figure 16: Scan Nmap1

b. Zenmap aussi fait des scans comme ceux de Nmap, il trouve aussi des services qui sont démarrés sur l'hôte cible mais aussi les ports qui sont ouverts, fermés pourquoi pas, l'adresse MAC etc…

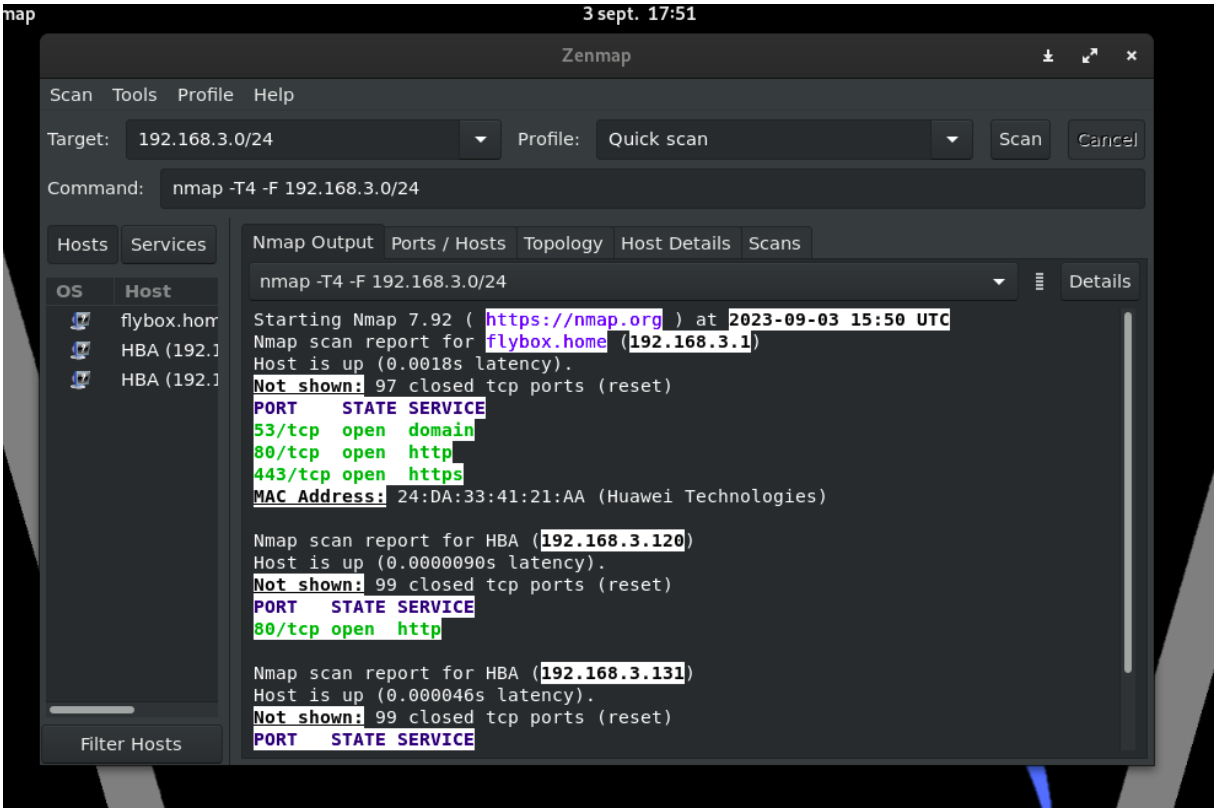


Figure 17: Scan avec znmap1

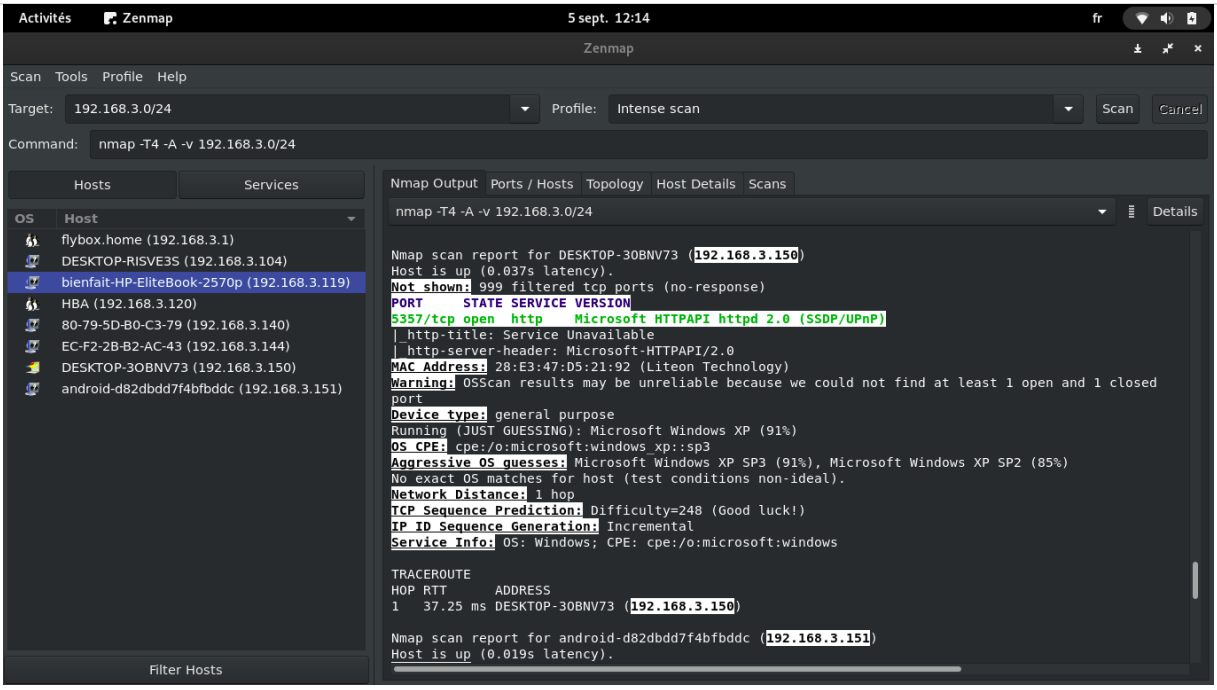


Figure 18: scan znmap2

Ici on nous donne la possibilité de voir le nombre de port ouverts, les ports filtrés, les ports fermés

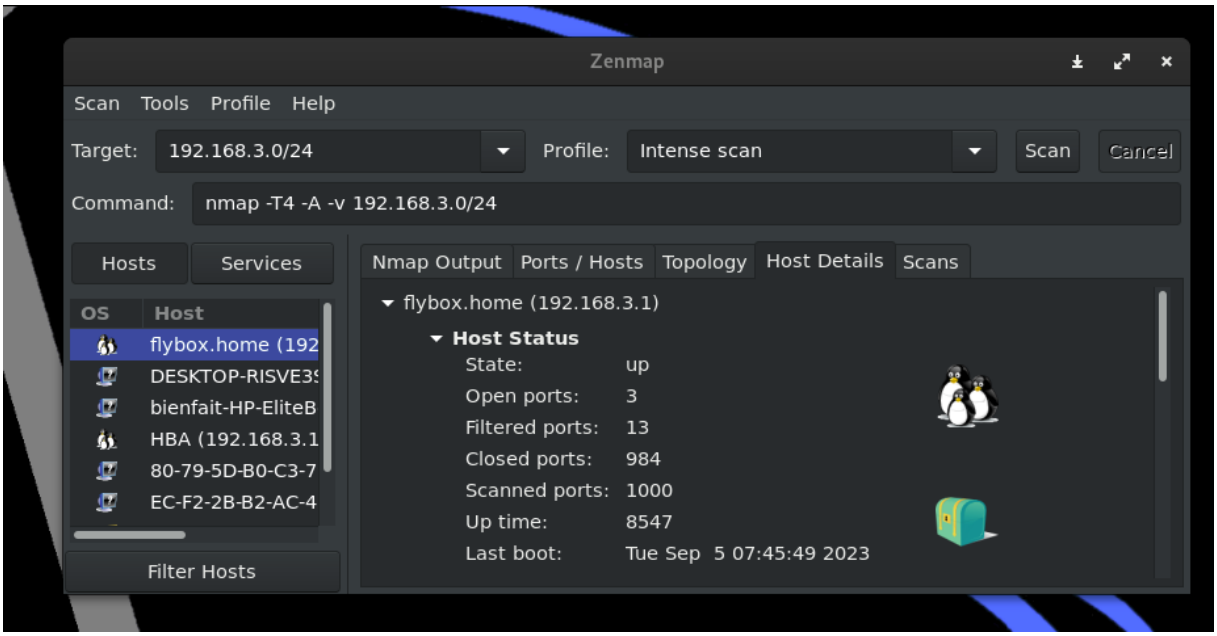


Figure 19: Scan avec znmap3

IV.6. UTILISATION DE NIKTO

Nikto est un scanneur des vulnérabilités et il analyse les serveurs Web à la recherche de fichiers/CGI dangereux, de logiciels serveur obsolètes et d'autres problèNos. Il effectue des vérifications génériques et spécifiques au type de serveur.

a. On va utiliser la commande **nikto -host «** adresse IP du serveur **»**

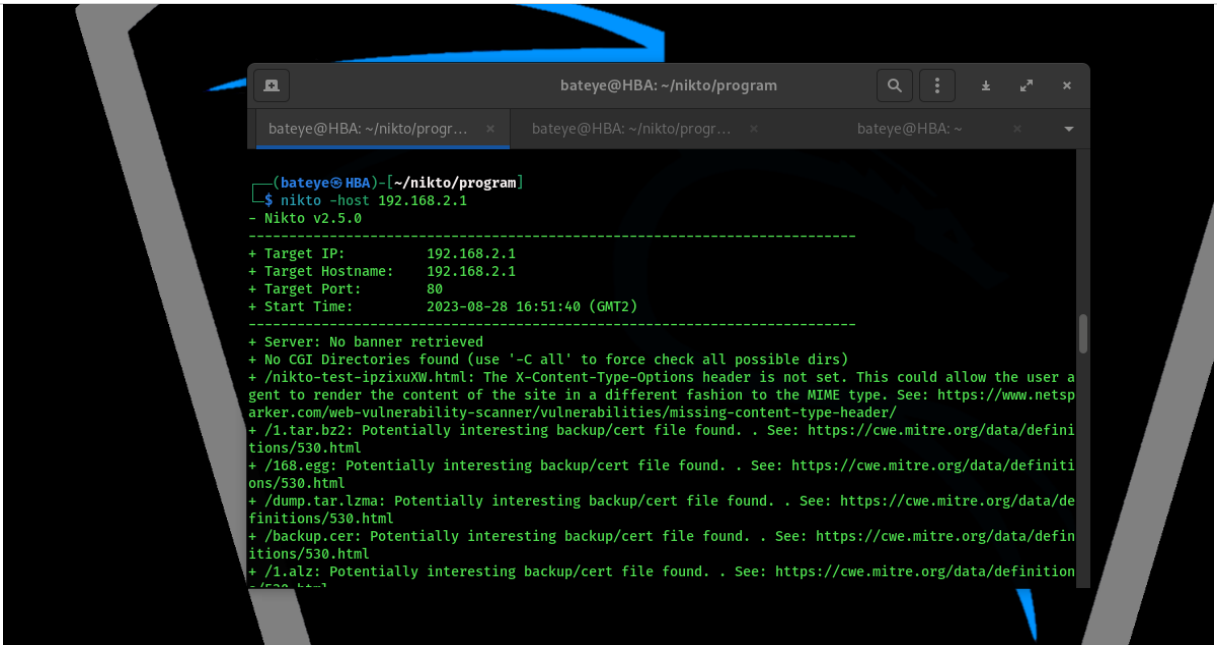


Figure 20: Scan avec Nikto

Figure 21: Fichiers/CGI dangereux

IV.7. UTILISATION DE WIRESHARK

a. Capture d'une série de trame

Après avoir lancé le logiciel Wireshark, la séquence suivante illustre la capture d'une série des trames :

1. Sélectionner Capture puis Options.

2. La ligne Filtre de capture pour les interfaces sélectionnées permet de préciser un filtrage à priori. La syntaxe de ce filtrage est identique à celle de la commande tcpdump

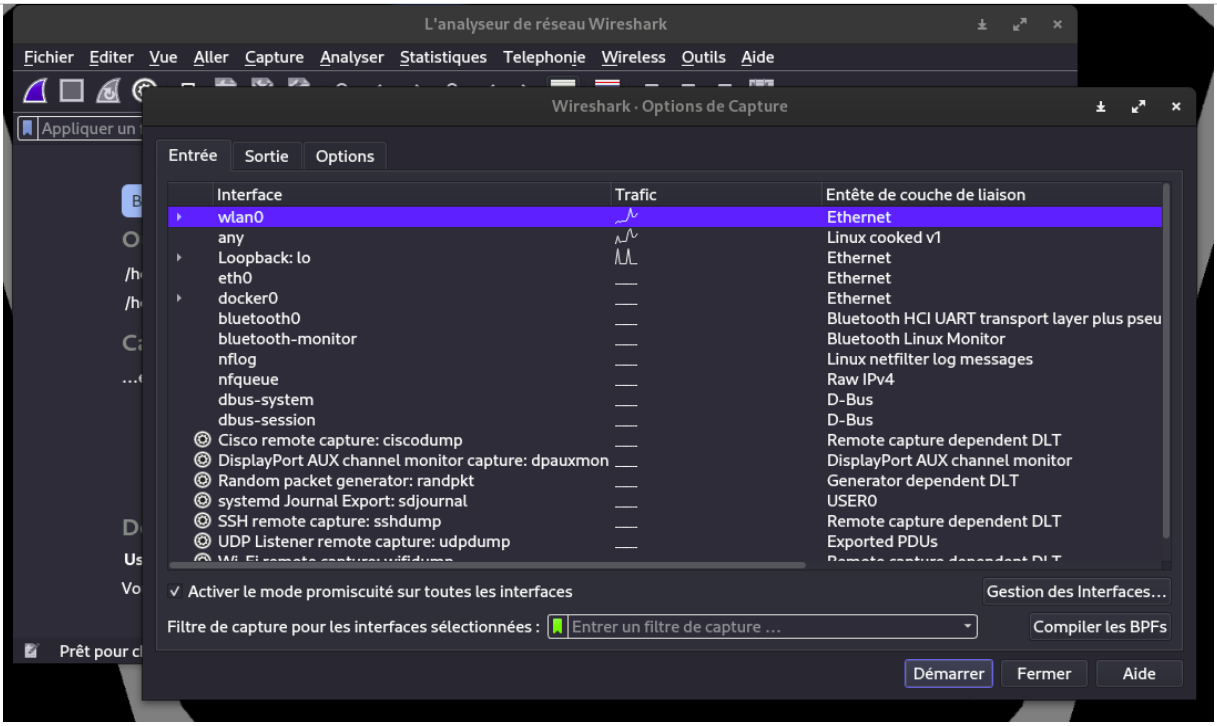


Figure 22: Choix de l'interface et filtrage avant capture

3. La rubrique Options permet de fixer plusieurs critères d'arrêt en fonction du nombre de traNos et / ou du volume de données capturées.

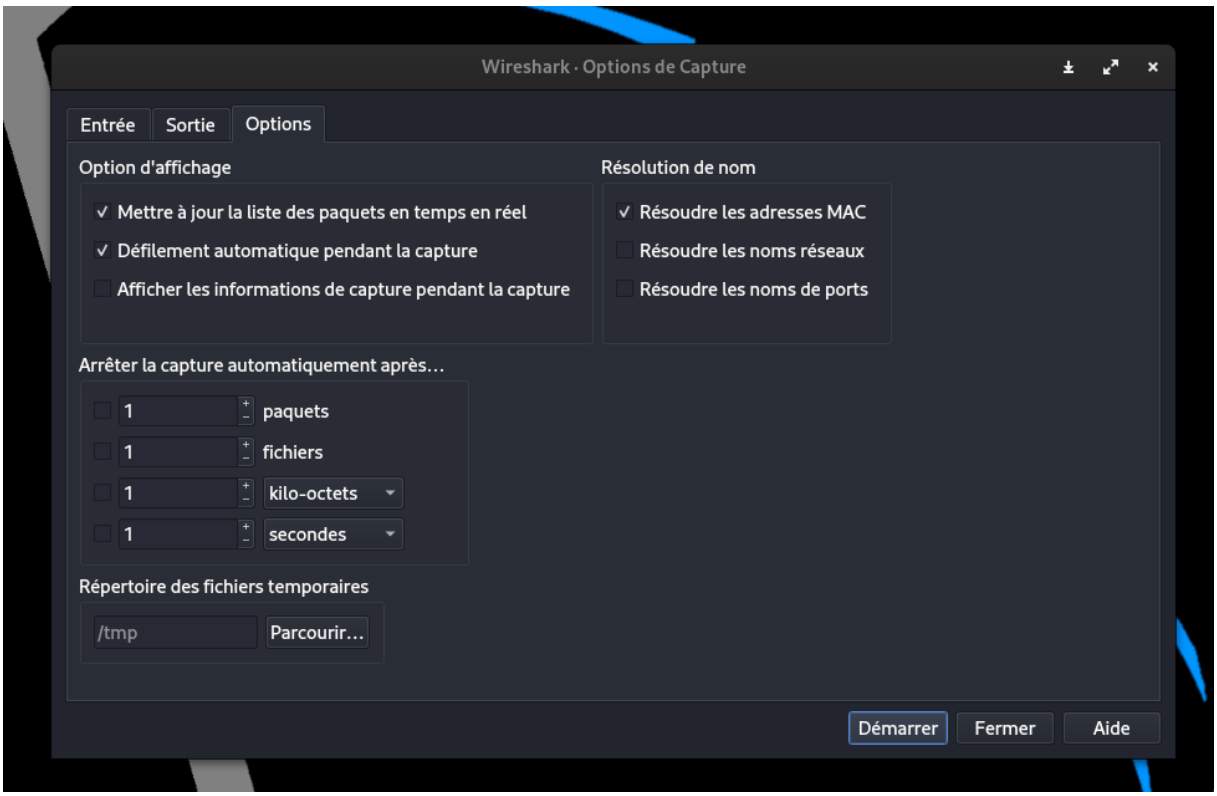


Figure 23: Choix des options d'arrêt des captures

4. Interface des captures des paquets du **wlan0**

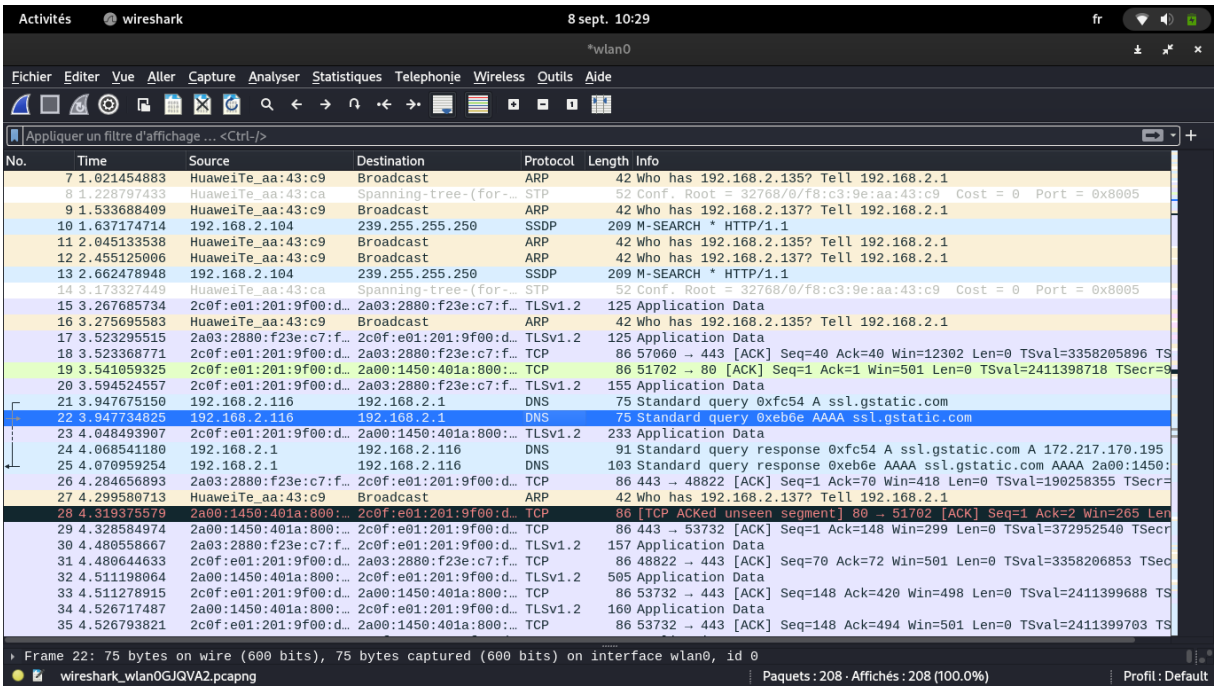


Figure 24: Capture des paquets du wlan0

5. Ici c'est le paquet 920

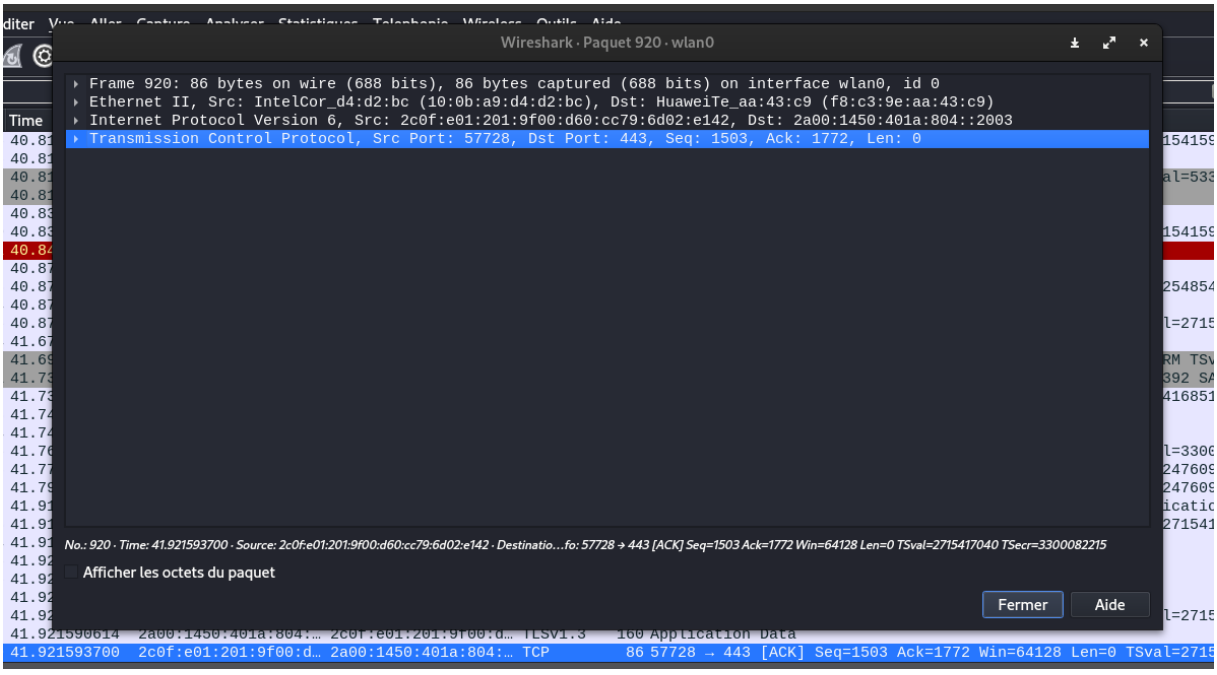


Figure 25: Protocoles

IV.8. AUDIT AVEC LYNIS

Lynis est un outil d'audit de sécurité pour les systèmes Linux, MacOs et Unix. Il effectue une analyse de santé approfondie de votre système pour soutenir le durcissement du système et les tests de conformité

a. Vous recevrez des suggestions détaillées en vue d'améliorer votre sécurité, ainsi qu'une synthèse finale précisant l'emplacement du fichier journal

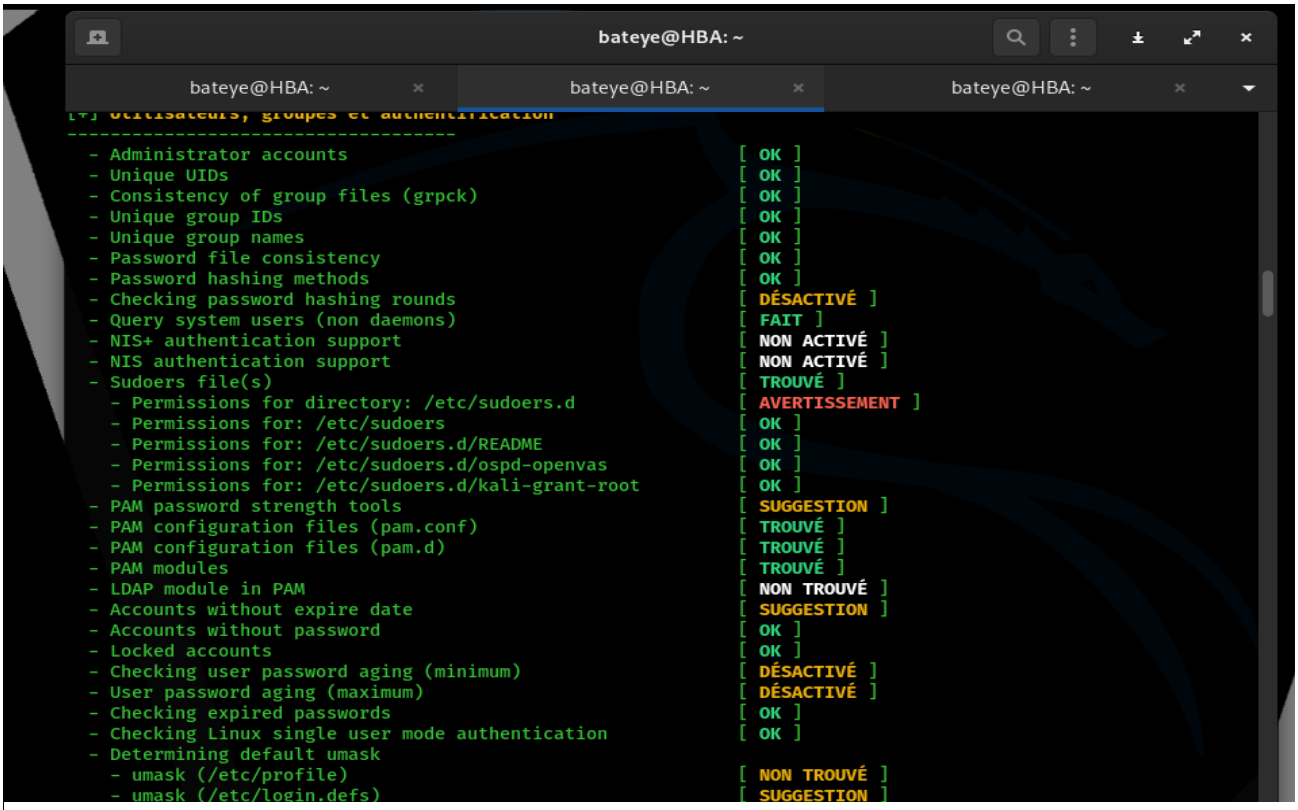


Figure 26: Etat du SI

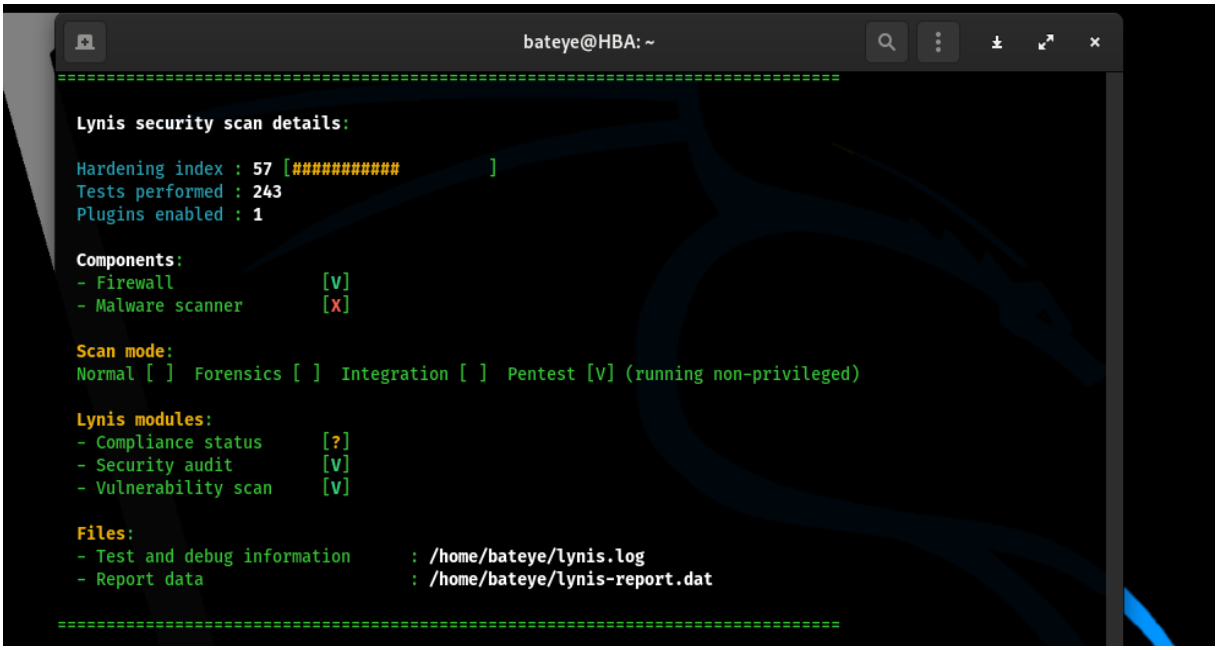


Figure 27: Scan Lynis

b. lynis propose aussi les méthodes à appliquer pour réduire les vulnérabilités

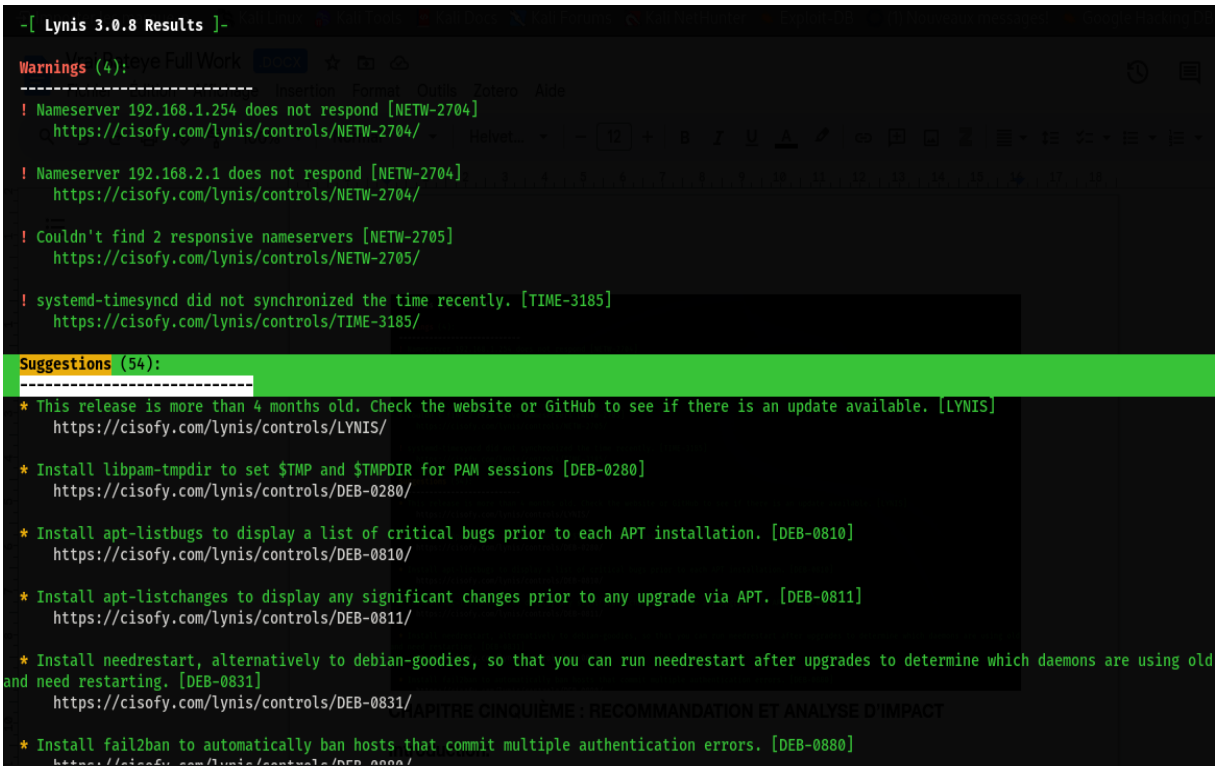


Figure 28: Suggestion Lynis

CHAPITRE CINQUIÈME : RECOMMANDATION ET ANALYSE D'IMPACT

V.0.Introduction:

Dans ce chapitre, nous aborderons les recommandations et l'analyse d'impact suite à l'audit du système d'information avec Kali Linux. Après avoir identifié les vulnérabilités et les faiblesses du système, il est essentiel de proposer des recommandations pour améliorer la sécurité et d'analyser l'impact de ces recommandations sur le système d'information.

V.1 Recommandations de sécurité :

Sur la base des résultats obtenus lors de l'audit du système d'information, il est important de formuler des recommandations spécifiques pour améliorer la sécurité globale. Ces recommandations peuvent inclure :

1. *Mise à jour régulière des systèmes et des applications* : Il est essentiel de maintenir tous les systèmes et les applications à jour avec les derniers correctifs de sécurité pour atténuer les vulnérabilités connues.
2. *Renforcement des mots de passe :* Les politiques de gestion des mots de passe doivent être mises en place, exigeant des mots de passe forts, un changement régulier et l'utilisation de l'authentification à deux facteurs lorsque cela est possible.
3. *Configuration sécurisée des pare-feu et des routeurs :* Les règles de pare-feu et de routage doivent être correctement configurées pour limiter l'accès non autorisé à l'infrastructure.
4. *Sensibilisation à la sécurité :* Il est important de former et de sensibiliser régulièrement les employés aux bonnes pratiques de sécurité, telles que la détection des attaques de phishing, la protection des informations sensibles, etc.
5. *Surveillance continue :* La mise en place d'un système de surveillance et de détection des incidents permet de détecter rapidement les activités suspectes et de réagir rapidement en cas d'incident de sécurité.
6. *Gestion des accès privilégiés :* Les accès privilégiés aux systèmes et aux applications doivent être strictement contrôlés et surveillés pour réduire les risques de compromission.

V.2. Analyse d'impact

Avant de mettre en œuvre les recommandations de sécurité, il est important de réaliser une analyse d'impact pour évaluer les conséquences possibles sur le système d'information. Cette analyse permet de comprendre comment les recommandations pourraient affecter les opérations, les performances, les coûts et les utilisateurs du système.

L'analyse d'impact devrait prendre en compte les éléments suivants :

1. **Opérations :** Évaluer comment les recommandations pourraient affecter les processus et les opérations existantes. Par exemple, certaines recommandations pourraient nécessiter des modifications dans les procédures de travail ou des ajustements dans les flux de données.
2. **Performances :** Déterminer si les recommandations pourraient avoir un impact sur les performances du système d'information. Par exemple, l'implémentation de Nosures de sécurité supplémentaires pourrait ralentir certaines opérations, ce qui doit être pris en compte.
3. **Coûts** : Évaluer les coûts associés à la mise en œuvre des recommandations. Cela peut inclure les coûts de formation, les coûts matériels ou logiciels supplémentaires, les coûts de maintenance, etc. Il est important de peser ces coûts par rapport aux risques potentiels d'incident de sécurité.
4. **Utilisateurs** : Analyser comment les recommandations pourraient affecter les utilisateurs du système d'information. Cela peut inclure des changements dans les habitudes de travail, l'accès à certaines fonctionnalités ou la nécessité de nouvelles formations.

V.3. POLITIQUE DE SECURITE

Cette politique de sécurité vise à assurer une utilisation responsable de Kali Linux pour l'audit des systèmes d'information, tout en garantissant la confidentialité, l'intégrité et la disponibilité des informations sensibles.

1. ***Objectif :***
   - Assurer la confidentialité, l'intégrité et la disponibilité des informations pendant l'audit du système d'information.
   - Identifier et réduire les risques potentiels liés à la sécurité.
   - Protéger les actifs informatiques de l'organisation.
   - Respecter les lois et réglementations en vigueur.
2. ***Responsabilités :***
   - Les auditeurs sont responsables de mener l'audit conformément aux procédures et aux normes établies.
   - L'équipe de sécurité est chargée de fournir un soutien et des conseils aux auditeurs.
   - La direction est responsable de l'approbation des recommandations émises à la suite de l'audit.
   - Les utilisateurs doivent coopérer avec les auditeurs et respecter les politiques de sécurité en place.

3. ***Accès et autorisation :***
    - Les auditeurs doivent avoir un accès limité et contrôlé aux systèmes et aux données nécessaires à l'audit.
    - Les privilèges d'accès doivent être accordés sur la base du principe du moindre privilège.
    - Les informations sensibles doivent être protégées et accessibles uniquement aux personnes autorisées.
4. ***Protection des données :***
    - Les données collectées pendant l'audit doivent être traitées avec confidentialité et protégées contre toute divulgation non autorisée.
    - Des mesures de sécurité appropriées, telles que le cryptage des données, l'utilisation de pare-feu et la mise en œuvre de contrôles d'accès, doivent être mises en place.
    - Les sauvegardes régulières doivent être effectuées pour prévenir la perte de données.
5. ***Conformité légale :***
    - L'audit doit être mené conformément aux lois, réglementations et normes applicables en matière de confidentialité, de protection des données et de sécurité informatique.
    - Les droits des utilisateurs et la vie privée doivent être respectés lors de la collecte et du traitement des données.
6. ***Rapport et suivi :***
    - Un rapport d'audit détaillé doit être préparé, incluant les résultats, les recommandations et les mesures correctives.
    - Les délais et les destinataires du rapport doivent être définis.
    - Les mesures correctives recommandées doivent être mises en place dans des délais convenus.

      Un suivi régulier doit être effectué pour vérifier la mise en œuvre des mesures correctives et assurer l'amélioration continue de la sécurité du système d'information
7. ***Application :***

Tout utilisateur en violation de cette politique s’expose à des mesures disciplinaires pouvant aller jusqu’au licenciement. Tout partenaire ou entrepreneur tiers en infraction pourra voir sa connexion réseau interrompue.

8. Définitions :

Ce paragraphe définit les termes techniques utilisés dans cette politique.

- *Liste de contrôle d'accès (ACL)* : Une liste d'entrées de contrôle d'accès (ACE) ou de règles. Chaque ACE dans une ACL identifie un ayant droit et spécifie les droits d'accès autorisés, refusés ou audités pour cet ayant droit.
- *Base de données* : Une collection organisée de données, généralement stockées et accessibles électroniquement à partir d'un système informatique.
- *Chiffrement :* Processus de codage d'un message ou d'autres informations afin que seules les parties autorisées puissent y accéder.
- *Pare-feu :* Une technologie utilisée pour isoler un réseau d'un autre. Les pare-feu peuvent être des systèmes autonomes ou être inclus dans d'autres appareils, tels que des routeurs ou des serveurs.
- *Ségrégation du réseau* : La séparation du réseau en unités logiques ou fonctionnelles appelées zones. Par exemple, vous pouvez avoir une zone pour le support technique et une autre zone pour la recherche, chacune ayant des besoins techniques différents.
- *Contrôle d'accès basé sur les rôles (RBAC)* : Un mécanisme de contrôle d'accès neutre en termes de politique, défini autour des rôles et des privilèges.
- *Serveur :* Un programme informatique ou un périphérique qui fournit des fonctionnalités à d'autres programmes ou périphériques, appelés clients.
- *VLAN (LAN virtuel) :* Un regroupement logique de périphériques dans le même domaine de diffusion.

V.4. PERSPECTIVE

L'audit du système d'information avec Kali Linux permet de réaliser des tests de sécurité approfondis et de détecter les vulnérabilités potentielles dans les infrastructures informatiques. En exploitant les nombreuses fonctionnalités et outils de Kali Linux, les auditeurs peuvent effectuer des scans de ports, des analyses de vulnérabilités, des attaques simulées et des tests de pénétration pour évaluer la robustesse de la sécurité du système.

L'utilisation de Kali Linux offre à l'auditeur la possibilité d'utiliser des outils spécialisés tels que Nmap, Metasploit, Wireshark et d'autres, qui sont préinstallés dans la distribution. Ces outils permettent d'identifier les points faibles du système, de vérifier la configuration des pare-feu, de détecter les faiblesses des protocoles de sécurité, et d'évaluer la résistance du système face aux attaques courantes.

Cependant, il est important de noter que l'utilisation de Kali Linux doit être effectuée dans le cadre d'une approche légale et éthique. L'auditeur doit obtenir l'autorisation appropriée et respecter les règles établies par l'organisation pour mener à bien l'audit du système d'information. De plus, les résultats des tests effectués avec Kali Linux doivent être analysés avec soin et communiqués de

manière appropriée pour prendre les mesures correctives nécessaires et améliorer la sécurité globale du système d'information.

En résumé, l'utilisation de Kali Linux dans l'audit du système d'information offre aux auditeurs une perspective puissante pour évaluer les vulnérabilités et renforcer la sécurité. Cependant, cela doit être fait de manière légale, éthique et avec une analyse judicieuse des résultats pour garantir une amélioration effective de la sécurité du système d'information

V.5. CONCLUSION

Nous voici au terme de notre travail de mémoire qui portait sur l'''Audit d'un système d'information avec Kali Linux ''

Le mémoire de recherche présenté se compose de quatre chapitres clés, à savoir l'introduction, la revue de la littérature, la méthodologie de la recherche et la présentation des résultats. Chacun de ces chapitres contribue à la compréhension et à l'analyse approfondie du sujet étudié.

Dans le premier chapitre, l'introduction, l'auteur expose le contexte général du sujet, met en évidence sa pertinence et énonce les objectifs de la recherche.

Le deuxième chapitre, la revue de la littérature. Dans ce chapitre nous avons présenté les travaux antérieurs et les études existantes sur le sujet de recherche.

Le troisième chapitre portait sur la méthodologie de la recherche. Ce chapitre décrit en détail les méthodes, les outils et les approches utilisés pour mener l'étude. Ici nous avons montré les méthodes qu'on a utilisé pour mener cette recherche.

Le quatrième chapitre portait sur la présentation des résultats. Ici on présente les résultats obtenus à partir de l'application de la méthodologie de recherche.

En résumé, l'audit du système d'information est essentiel pour assurer la sécurité et la conformité des infrastructures informatiques. Il permet de détecter les vulnérabilités, de prendre des mesures correctives et de renforcer la confiance des parties prenantes. Cependant, il doit être réalisé de manière continue et proactive pour s'adapter aux évolutions technologiques et aux nouvelles menaces. L'audit du système d'information joue un rôle clé dans la protection des données et la préservation de l'intégrité des systèmes. Les informations et les analyses présentées dans ce mémoire contribuent à l'enrichissement des connaissances dans le domaine de recherche et ouvrent des perspectives pour de futures études et recherches complémentaires.

BIBLIOGRAPHIE

1. Ouvrage

Amine, M. O. (2011). *Les techniques de sécurité des Réseaux* (éd. 2014-2015).

Khan, A. &. (s.d.). *Detection of Security Threat s in Wi-Fi Networks Using Kali Linux.*

KINDA, K. K. (2013). *Mise en place d'un portail captif sur le réseau de l'UPB.*

Kumwenda, M. (2023). Comment effectuer des audits de sécurité sur Linux avec Lynis.

O'Gorman, R. H. (s.d.). *Kali Linux Revealed: Mastering the Penetration Testing Distribution* (éd. 2017).

Praveena. (2017). *Penetration Testing of Network Security using Kali Linux",.*

Zahra, F. (2017). *Audit des systèmes d'information.*

Kazungu, J. (2022, Novembre). *Mise en place d'un serveur d'authentication avec un portail WI-FI captif.*

YENDE, PhD. (2018, Décembre). *Réseaux informatiques*

2. Webographie

Fondement de la sécurité informatique. (s.d.). Récupéré sur WOOXO: https://www.wooxo.fr/Conseils-Cybersecurite/Principes-securite-informatique#:~:text=Fondements%20de%20la%20s%C3%A9curit%C3%A9%20informatique&text=L'int%C3%A9grit%C3%A9%20%3A%20garantir%20que%20les,seuls%20acteurs%20d'une%20transaction.

(2023). Récupéré sur ANSSI: https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/

(s.d.). Récupéré sur wiki-ubuntu.fr: https://doc.ubuntu-fr.org/nikto

(2023). Récupéré sur SICOSFY: https://cisofy.com/lynis/

(2023). Récupéré sur tenable: https://fr.tenable.com/products/nessus/nessus-essentials

(2023). Récupéré sur Varonis: https://www.varonis.com/fr/blog/comment-utiliser-wireshark

(s.d.). Récupéré sur CNRS: https://www.dgdr.cnrs.fr/bo/2007/01-07/416-bo0107-pb0.html

(2015). Récupéré sur ComputerLand: https://www.computerland.fr/pourquoi-realiser-audit-informatique/#:~:text=L'audit%20informatique%20permet%20de,adapter%20les%20manipulations%20%C3%A0%20effectuer.

Goffinet, F. (s.d.). Consulté le 2023, sur Linux Administration : https://linux.goffinet.org/administration/audit/

IT-CONNECT. (2023). Récupéré sur https://www.it-connect.fr/cours/debuter-avec-kali-linux/

kali.org. (s.d.). Récupéré sur Kali.org: https://www.bing.com/search?q=audit+avec+kali+linux&qs=n&form=QBRE&sp=-1&ghc=2&lq=0&pq=audit+avec+kali+linux&sc=10-21&sk=&cvid=BFFC78480E694D77A84D55E85E494BC9&ghsh=0&ghacc=0&ghpl=

la sécurité. (s.d.). Récupéré sur Oracle: https://www.oracle.com/fr/security/qu-est-ce-que-la-cryptographie/#:~:text=En%20g%C3%A9n%C3%A9ral%2C%20la%20cryptographie%20est,un%20Nossage%20consid%C3%A9r%C3%A9%20comme%20confidentiel.

Le programmeur Marocain. (2023, June 7 Wednesday). Récupéré sur https://leprogrammeurmarocain.com/comment-utiliser-wireshark/

Microsoft Support. (2021). Récupéré sur https://support.microsoft.com/fr-fr/office/marge-libre-champ-de-t%C3%A2che-87145b2b-8d50-45a1-b89b-89aa73015d17#:~:text=Description%20Le%20champ%20Marge%20libre,de%20fin%20du%20projet%20entier.

NAVARRO, M. (2018, Décembre). *EBIOS Risk Manager*. Récupéré sur https://www.mauricenavarro.com/ressources/ebios-risk-manager/

OpenClassroom. (2023). Récupéré sur https://openclassrooms.com/fr/courses/2100086-decouvrez-le-monde-des-systeNos-dinformation/5195831-definissez-ce-quest-un-systeme-dinformation

Oracle. (2023). Récupéré sur Oracle: https://www.oracle.com/fr/security/qu-est-ce-que-la-cryptographie.html#:~:text=En%20g%C3%A9n%C3%A9ral%2C%20la%20cryptographie%20est,un%20Nossage%20consid%C3%A9r%C3%A9%20comme%20confidentiel

Rapid 7. (2022). Récupéré sur https://docs.rapid7.com/metasploit/msf-overview/

3. Journaux

O'Shaughnessy, W. (1992).

(2021.1). Récupéré sur Kali .

(s.d.). Récupéré sur nmap.org: nmap.org

Ponemon, I. (s.d.). Audit d'un système d'information.

Praveena. (2017). *Penetration Testing of Network Security using Kali Linux",*.

Red Hat. (2018, Mars 19). Récupéré sur Comprendre la sécurité informatique

Wooxo. (s.d.). Récupéré sur IT security for business continuity.