MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
RÉPUBLIQUE DU BÉNIN

LES COURS SONOU

REPUBLIQUE DE BENIN

****

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE (MESRS)

****

INSTITUT UNIVERSITAIRE ''LES COURS SONOU'' (LCS)

****

MEMOIRE DE FIN DE FORMATION DE LICENCE

****

Mention : Sciences de l'Ingénieur

Option : Sécurité des Systèmes et Réseaux Informatiques (SSRI)

THEME : Mise en place d'un système de détection d'intrusion (IDS) avec SNORT : cas de la DBAU

Réalisé et présenté par :

BELLO Fayçal et TOUDOGUIN Francis

Sous la supervision de :

Maître de Stage :

M. Narcisse AKPLOGAN

Maître de Mémoire :

Mme Ida TCHIBOZO

Année académique :2023-2024

AVANT-PROPOS

Ce mémoire est réalisé dans le cadre de l'obtention du diplôme de Licence professionnelle. Il a été réalisé au sein de la Direction des Bourses et Aides-Universitaires (DBAU) du Bénin durant la période du 04 Mars 2024 au 07 Juin 2024, soutenu en Juin et supervisé par Madame Ida TCHIBOZO.

SOMMAIRE

DEDICACE

C'est avec profonde gratitude et sincères mots, que nous dédions ce modeste travail de fin d'étude à nos chers parents ; qui ont sacrifie leur vie pour notre réussite et nous ont éclaire le chemin par leurs conseils judicieux.

Nous espérons qu'un jour, nous pourrons leurs rendre un peu de ce qu'ils ont fait pour nous, que dieu leur prête bonheur et longue vie. Nous dédions aussi ce travail à nos frères et sœurs, nos familles, nos amis, tous nos professeurs qui nous ont enseigne et a tous ceux qui nous sont chers.

REMERCIEMENTS

Nous remercions en premier lieu notre Dieu qui nous a éclairé le chemin du savoir et qui nous a donné la volonté et la patience d'achever ce travail de mémoire, notre grand salut sur le premier éducateur notre prophète Mohamed (satisfaction et salut de dieu soit sur lui).

Nous adressons nos vifs remerciements et nos sincères gratitudes à tous ceux qui nous ont aidés de près ou de loin à élaborer ce travail.

Nous remercions en particulier nos encadreurs Mme Ida TCHIBOZO , Mr Narcisse AKPLOGAN et Mr KEKIN Ley qui nous ont fait l'honneur d'avoir la charge d'encadrer notre travail de mémoire avec grande patience, pour la confiance qu'ils ont eu en notre projet et surtout pour leurs orientations, ainsi que leurs aides précieuses et leurs conseils pour réaliser ce mémoire.

Ainsi que tous nos professeurs qui nous ont enseigné durant nos études à ''LCS'' et les membres de l'administration de la DBAU pour leurs accueils.

Nous tenons à remercier tous nos collègues d'étude, particulièrement notre promotion.

A la fin nos profonds remerciements pour les membres de jury qui ont accepté d'évaluer ce Travail.

LISTES DES TABLEAUX

LISTES DES FIGURES

SIGLES ET ABREVIATIONS

DBAU : Direction des Bourses et Aides Universitaires

DBSU : Direction des Bourses et Secours Universitaires

MESRS : Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

IDS : Intrusion Detection System

IPS : Intrusion Prevention System

DNS : Domain Name System

DoS : Denial of Service

DDoS : Distributed Denial of Service

ID : Identification

MITM : Man In The Middle

VPN : Virtual Private Network

NIDS : Network-based Intrusion Detection System

HIDS : Host-based Intrusion Detection System

GLOSSAIRE

1. **IDS (Intrusion Detection System) :** Un système de détection d'intrusion est un outil de sécurité informatique conçu pour détecter et signaler les activités suspectes ou malveillantes sur un réseau ou un système informatique.
2. **IPS (Intrusion Prevention System) :** Un système de prévention d'intrusion est un dispositif de sécurité informatique qui surveille et analyse le trafic réseau afin de prévenir les attaques en temps réel, en bloquant ou en neutralisant les menaces détectées.
3. **Capteur :** Un capteur est un composant d'un IDS qui surveille le trafic réseau ou les activités des hôtes pour détecter les intrusions ou les comportements suspects.
4. **Agent :** Un agent est un logiciel installé sur un hôte informatique pour surveiller son activité et détecter les intrusions ou les violations de sécurité.
5. **Politique de surveillance** : Une politique de surveillance définit les règles et les critères selon lesquels un IDS surveille le réseau ou les systèmes informatiques pour détecter les activités suspectes.
6. **Règles de détection :** Les règles de détection sont des instructions programmées dans un IDS pour identifier les signes d'intrusion ou de comportement anormal.
7. **Seuil d'alerte :** Un seuil d'alerte est un niveau préconfiguré de trafic ou d'activité qui déclenche une alerte lorsqu'il est dépassé, indiquant une possible intrusion ou un comportement suspect.
8. **Faux positif :** Un faux positif est une alerte générée par un IDS qui identifie incorrectement une activité normale comme étant une intrusion ou une menace.

9. **Faux négatif :** Un faux négatif est une situation où un IDS ne détecte pas une véritable intrusion ou menace, laissant le réseau ou le système vulnérable.
10. **Corrélation des événements** : La corrélation des événements est le processus d'analyse des données provenant de multiples sources pour identifier les schémas et les relations qui pourraient indiquer une activité malveillante ou une attaque coordonnée.

11. **SIEM (Security Information and Event Management) :** Le SIEM est une solution logicielle qui combine la gestion des informations de sécurité (SIM) et la gestion des événements de sécurité (SEM) pour fournir une visibilité et une analyse approfondies des données de sécurité.

12. **Incident de sécurité :** Un incident de sécurité est tout événement qui compromet l'intégrité, la confidentialité ou la disponibilité des informations ou des systèmes d'une organisation, souvent détecté et géré par un IDS.

13. **Gestion des incidents :** La gestion des incidents est le processus de détection, de réponse, de récupération et d'analyse des incidents de sécurité pour minimiser les dommages potentiels et assurer la continuité des opérations.

14. **Politique de sécurité :** Une politique de sécurité est un ensemble de règles, de procédures et de directives définissant les objectifs, les responsabilités et les mesures de sécurité à mettre en œuvre pour protéger les actifs informatiques d'une organisation.

15. **Conformité réglementaire :** La conformité réglementaire fait référence au respect des lois, des réglementations et des normes de l'industrie en matière de sécurité informatique, souvent nécessitant la mise en œuvre d'IDS pour surveiller et maintenir la conformité.

RESUME

Notre projet d'étude immerge dans le domaine de la sécurité informatique. Aujourd'hui l'information est la sève de l'entreprise et de toute organisation, sa protection contre toute menace est par ailleurs plus que nécessaire, d'où l'intérêt de notre travail qui, en partant de quelques connaissances de base sur la sécurité informatique et la détection d'intrusions, consiste à mettre en place un système de détection d'intrusions (le SNORT).

ABSTRACT

Our study project immerses itself in the field of computer security. Today information is the lifeblood of the company and of any organization, its protection against any threat is more than necessary, hence the interest of our work which, starting from some basic knowledge on the computer security and intrusion detection, consists of setting up an intrusion detection system (SNORT).

INTRODUCTION

La Direction des Bourses et Aides Universitaires (DBAU ex DBSU) est l'une des directions techniques du Ministère de l'Enseignement Supérieur et de la Recherche Scientifique (MESRS) qui a pour mission la conception, la coordination de la mise en œuvre et le suivi-évaluation de la politique de l'Etat en matière de bourses et aides universitaires.

L'essor fulgurant d'Internet et la généralisation des réseaux ouverts ont engendré une multiplication des attaques informatiques. Les vulnérabilités en matière de sécurité se multiplient, que ce soit au niveau de la conception des protocoles de communication ou de leur implémentation. Parallèlement, la disponibilité et l'accessibilité croissantes des connaissances, outils et scripts utilisés pour mener des attaques accentuent ce phénomène. Ainsi, la mise en place d'un système de détection d'intrusions (IDS) devient impérative.

Cette technologie repose sur la recherche de motifs spécifiques caractéristiques d'une attaque au sein d'un flux de données. Les IDS sont devenus un élément essentiel et critique au sein de toute architecture de sécurité informatique. Ils doivent être intégrés dans une politique de sécurité globale. L'objectif principal d'un IDS est de détecter toute violation des politiques de sécurité établies, permettant ainsi de signaler les attaques potentielles.

Pour concrétiser la mise en place d'un IDS, nous envisageons d'utiliser un logiciel open source appelé SNORTS. Ce système se base sur le principe d'analyse de chaînes de caractères présentes dans les paquets de données. Afin de détecter une attaque, il est nécessaire de décrire celle-ci par une signature spécifique. C'est à partir de cette signature que seront formulées les règles que l'IDS utilisera pour la détection des intrusions.

CHAPITRE I : REVUE LITTERAIRE

Ce chapitre porte sur la sécurité informatique.

I.1 Introduction

La sécurité informatique joue un rôle majeur dans les technologies numériques modernes, avec l'augmentation de la demande d'internet dans différents domaines (sanitaire, social, éducatif, militaire…), les besoins en sécurité sont de plus en plus importants, le développement des applications et des sites tel que : le commerce électronique, le paiement en ligne ou la vidéoconférence, implique de nouveaux besoins comme l'identification des entités communicantes, l'intégrité des messages échangés, la confidentialité de la transaction, l'authentification des entités, l'anonymat du propriétaire du certificat, l'habilitation des droits, la procuration, …etc.

I.2 Objectifs de sécurité

La notion de sécurité fait référence à la propriété d'un système, d'un service ou d'une entité. Elle s'exprime par les objectifs (services) de sécurité suivante :

 Disponibilité : est la propriété qui permet de garantir l'accès aux ressources. Exemples de ressources : serveur, réseau, donnée …

Il ne suffit pas qu'une ressource soit disponible. Elle doit être utilisable avec des temps de réponse acceptables. Un service doit être assuré avec un minimum d'interruption (continuité de service). La disponibilité est obtenue, par exemple, par une certaine redondance ou duplication des ressources.

 Intégrité : est lié au fait que des ressources ou services n'ont pas été altérés (détruits ou modifiés) tant de façon intentionnelle qu'accidentelle. Il est indispensable de se protéger contre la modification des données lors de leur stockage, de leur traitement ou de leur transfert. En télécommunication, **le contrôle d'intégrité** consiste à vérifier que les données n'ont pas été modifiées tant de façon intentionnelle (attaques informatiques) qu'accidentelle durant la transmission.

 Confidentialité : c'est la propriété qui garantit que les informations transmises ne sont compréhensibles que par les entités autorisées. Deux actions complémentaires permettent d'assurer la confidentialité des données :

-Limiter et contrôler l'accès aux données afin que seules les personnes autorisées puissent les lire.

-Transformer les données par des techniques de chiffrement pour qu'elles deviennent inintelligibles aux personnes qui n'ont pas les moyens de les déchiffrer. Le chiffrement des données (ou cryptographie) contribue à en assurer la confidentialité des données et à en augmenter la sécurité des données lors de leur transmission ou de leur stockage.

 Authentification : c'est la propriété qui consiste à vérifier l'identité d'une entité avant de lui donner l'accès à une ressource. L'entité devra prouver son identité : Exemples : mot de passe, empreinte biométrique. Tous les mécanismes de contrôle d'accès logique aux ressources informatiques nécessitent de gérer l'identification et l'authentification (pas d'accès anonyme aux ressources).

 Non répudiation : est le fait de ne pourvoir nier qu'un évènement (action transaction) a eu lieu. Par exemple, la non répudiation permet d'avoir une preuve comme quoi un utilisateur a envoyé (ou reçu) un message particulier. Ainsi, l'utilisateur ne peut nier cet envoi (ou réception).

I.3 Attaques

I.3.1 Définition

Une attaque peut être définie par : n'importe quelle action qui tente d'exploiter une (ou plusieurs) vulnérabilité(s) dans un système pour violer un ou plusieurs besoins de sécurité et est généralement préjudiciable.

I.3.2 Objectifs des attaques

Les objectifs des attaques visent :

 Interception : Une tierce partie non autorisée obtient un accès à un actif. C'est une attaque portée à la confidentialité. Il peut s'agir d'une personne, d'un programme ou

d'un ordinateur. Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichiers ou de programmes en sont des exemples.

 Modification : Une tierce partie non autorisée obtient accès à un actif et le modifie. Il s'agit d'une attaque portée à l'intégrité. Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau sont des exemples de telles attaques.

 Fabrication : Une tierce partie non autorisée insère des faux objets dans un système. C'est une attaque portée à l'authenticité. Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrement à un fichier.

 Interruption : Un actif du système est détruit ou devient indisponible ou inutilisable. C'est une attaque portée à la disponibilité. La destruction d'une pièce matérielle, la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichiers en sont des exemples.

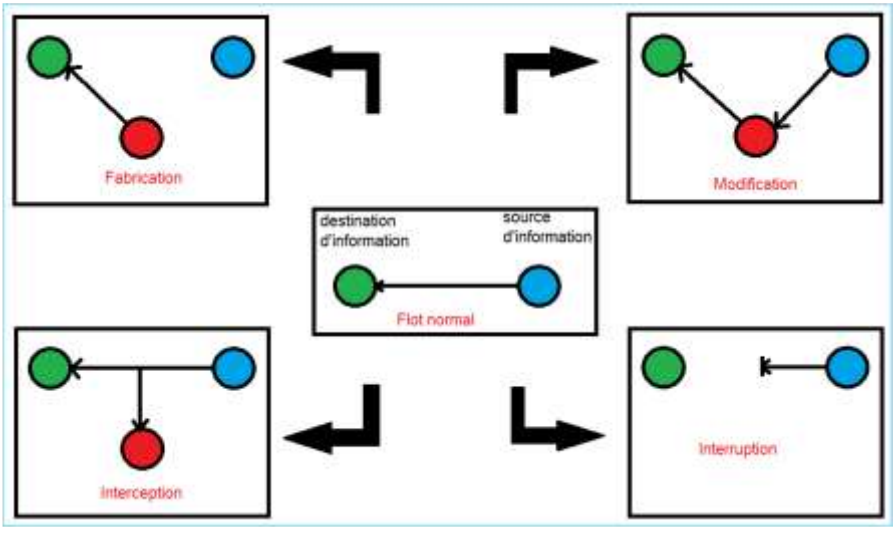

Figure 1 : Les objectifs des attaques

I.3.3 La reconnaissance passive

Il s'agit d'une phase d'attaques où l'intrus n'effectue pas une action pour collecter les informations. Il se restreint à observer passivement les événements afin d'en tirer les conclusions. Une des attaques les plus répandues est l'écoute du trafic (sniffing).

Le principe consiste à installer une sonde sur le réseau pour capter le trafic et le sauvegarder dans des fichiers journaux. L'analyse de ces fichiers permet de connaître les machines installées sur le réseau et de déterminer les ports ouverts et les systèmes d'exploitation utilisés. L'attaque est considérée lente si l'attaquant cherche une information précise sur une machine particulière du réseau. En revanche elle est si discrète qu'il est difficile de la détecter.

I.3.4 La reconnaissance active

L'objectif de la reconnaissance active est similaire à celui de la reconnaissance passive. Il s'agit d'acquérir des informations utiles sur le réseau cible. La reconnaissance active parait néanmoins plus fructueuse puisque l'attaquant ne se restreint pas à inspecter les données échangées entre les différents hôtes. Cependant, il initie lui-même des connections réseaux pour tester le comportement des machines. Il cherche des informations précises concernant les hôtes accessibles, l'emplacement des routeurs et des pare feux, les systèmes d'exploitation, les ports ouverts, les services fournis et les versions des applications exécutées. Parmi les techniques les plus utilisées pour acquérir ces informations nous évoquons les utilitaires **PING**, **NsLookup**, **DIG**, **Traceroute.**

I.4 Les techniques d'attaque

I.4.1 Spoofing

Nous trouvons 3 attaques **Spoofing** principales :

 Spoofing IP : Le spoofing IP est une technique permettant à un pirate d'envoyer à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate. Le spoofing IP n'est pas pour autant un changement d'adresse IP. Plus exactement, il s'agit d'une mascarade de l'adresse IP au niveau des paquets émis, c'est-à-dire une modification des paquets envoyés afin de faire croire au destinataire qu'ils proviennent d'une autre machine.

 Spoofing ARP : Le spoofing ARP est une technique qui modifie le cache ARP. Le cache ARP contient une association entre les adresses matérielles des machines et les

adresses IP, l'objectif du pirate est de conserver son adresse matérielle, mais d'utiliser l'adresse IP d'un hôte approuvé. Ces informations sont simultanément envoyées vers la cible et vers le cache. A partir de cet instant, les paquets de la cible seront routés vers l'adresse matérielle du pirate.

 Spoofing DNS : Le système DNS a pour rôle de convertir un nom de domaine en son adresse IP et réciproquement, à savoir : convertir une adresse IP en un nom de domaine. Cette attaque consiste à faire parvenir de fausses réponses aux requêtes DNS émises par une victime. Il existe deux types de méthode : **DNS ID spoofing** L'attaquant essaie de répondre à un client en attente d'une réponse d'un serveur DNS, avec une fausse réponse et avant que le serveur DNS ne réponde. **DNS Cache Poisoning** L'attaquant essaie d'empoisonner le cache (table de correspondance IP-NomMachine) du serveur DNS avec d'autres informations.

I.4.2 Attaque l'homme du milieu (Man In The Middle)

L'attaque de l'homme du milieu ou MITM, est une attaque utilisant au moins trois ordinateurs. Deux ordinateurs communiquent ensemble, un troisième au milieu casse la liaison entre les deux ordinateurs, et se fait passer pour l'autre entité, il intercepte et envoie les communications et peut de plus les modifier.

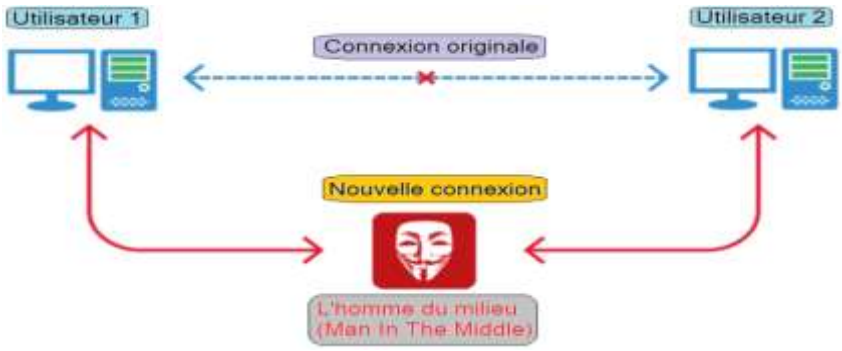

Figure 2 : Simuler le scénario de l'attaque MITM

La plupart des attaques de type ***man in the middle*** consistent à écouter le réseau à l'aide d'outils d'écoute du réseau comme ***wireshark*** (un analyseur de paquets. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques).

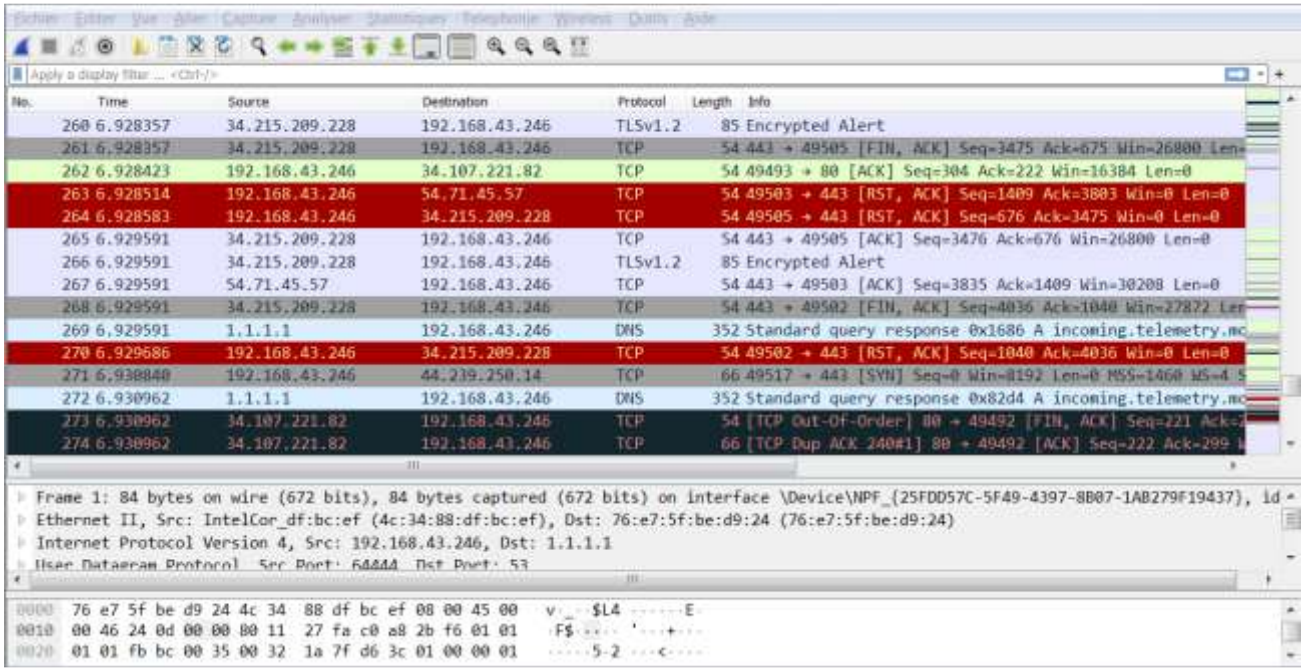

Figure 3 : Capture de l'outil Wireshark

I.4.3 Sniffing

Consiste à configurer la carte réseau pour récupérer l'ensemble des données transmises par le biais d'un réseau de la couche 2 à la couche 7 du modèle OSI, et utiliser ces données pour d'autres attaques.

I.4.4 DoS et DDoS

 DoS: Un DoS (Denial of Service) est une attaque de déni de service. Le but d'un déni de service est de faire tomber un serveur. L'attaque par **Synflood** (consiste à envoyer une grande quantité de requête de type Syn.) est l'une des attaques les plus répandues, elle consiste à demander des connexions et ne pas y répondre. Lors d'une demande de connexion, le serveur est en attente et bloque pendant un certain temps une partie de ses ressources pour cette nouvelle connexion. Le but est l'envoyer plus de demandes de connexion qu'il ne peut en traiter dans un temps donné. Le serveur ne pourra plus subvenir au besoin des vrais clients.

 DDoS : Le DDoS est similaire au DoS, mais l'attaque se fait à partir de plusieurs machines. Une attaque DoS est simple à contrôler, il suffit d'établir une règle dans le pare-feu afin de bloquer l'adresse IP attaquante. Dans le cas d'un DDoS cela se complique énormément.

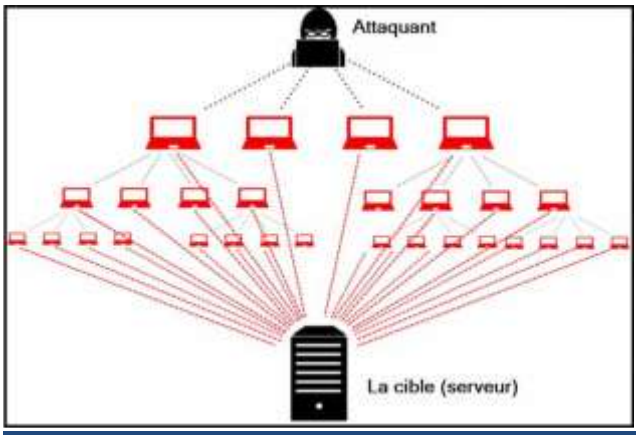

Figure 4 : Architecture attaque DDoS

I.5 Mécanismes de sécurité

Aujourd'hui, la sécurité est un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent. Et nous trouvons plusieurs mécanismes de sécurité :

I.5.1 Pare-feu (firewall)

Le pare-feu ou **Firewall** en anglais, c'est un mécanisme indispensable dans la sécurité informatique des entreprises et même dans des simples ordinateurs. Le Pare-feu propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau. Et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec les activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données. Il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseaux.

I.5.1.1 Fonctionnement du Pare-feu

Un système Pare-feu ou Firewall contient un ensemble de règles prédéfinies permettant, d'autoriser la connexion (Allow), de bloquer la connexion (Deny), de rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politique de sécurité permettant :

 Soit d'autoriser uniquement les communications ayant été explicitement autorisées (tout ce qui n'est pas explicitement autorisé est interdit).

 Soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

Un système Firewall fonctionne sur le principe du filtrage simple de paquets. Il analyse les en-têtes de chaque paquet de données échangé entre une machine du réseau interne et une machine extérieure. Les en-têtes systématiquement analysés par le firewall sont :

Adresse IP de machine émettrice

Adresse IP de machine réceptrice

Type de paquet (TCP, UDP, etc…)

Numéro de **port** (un numéro associé à un service ou une application réseau.).

I.5.1.2 Les Firewalls BRIDGE

Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de Firewall. Leurs interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence d'adresse IP est particulièrement utile, car cela signifie que le Firewall est indétectable pour un pirate. En effet, quand une requête ARP est émise sur le câble réseau, le Firewall ne répondra jamais. Ses adresses **Mac** (12 chiffres hexadécimaux « 48bits » identifiant une interface réseau) ne circuleront jamais sur le réseau, et comme il ne fait que transmettre les paquets, il sera totalement invisible sur le réseau. Et ces Firewalls se trouvent typiquement sur les **switchs** (Un commutateur réseau « en anglais switch », est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels).

 Inconvénients :

Possibilité de le contourner (il suffit de passer outre ses règles).

Configuration souvent contraignante.

Les fonctionnalités présentes sont très basiques (filtrages sur adresse IP, port).

 Avantage :

Impossible de l'éviter (les paquets passeront par ses interfaces).

I.5.2 Antivirus

Les antivirus sont des programmes capables de détecter la présence de virus sur un ordinateur, ainsi que de nettoyer celui-ci dans la mesure du possible si jamais un ou des virus sont trouvés. Nettoyer signifie supprimer le virus du fichier sans l'endommager. Mais parfois, ce nettoyage simple n'est pas possible.

I.5.3 Systèmes de détection d'intrusions IDS

Un système de détection d'intrusion **(ou IDS)** est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

I.5.4 Système de prévention d'intrusion IPS

Un système de prévention d'intrusion **(ou IPS)** est un outil similaire aux IDS, sauf que ce système peut prendre des mesures afin de diminuer les risques d'impact d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement.

I.5.5 Cryptographie

La cryptographie est une science basée sur les mathématiques, et aussi une des disciplines de la cryptologie s'attachant à protéger des messages (assurant la confidentialité, l'authenticité et l'intégrité) avec un algorithme de chiffrement, Chiffrer un message consiste de le rendre inintelligible, sauf pour celui qui possède le moyen (une clé) de le déchiffrer.

 La cryptographie Symétrique : Aussi appelé chiffrement à clé secrète, il consiste à utiliser la même clé pour le chiffrement et le déchiffrement.

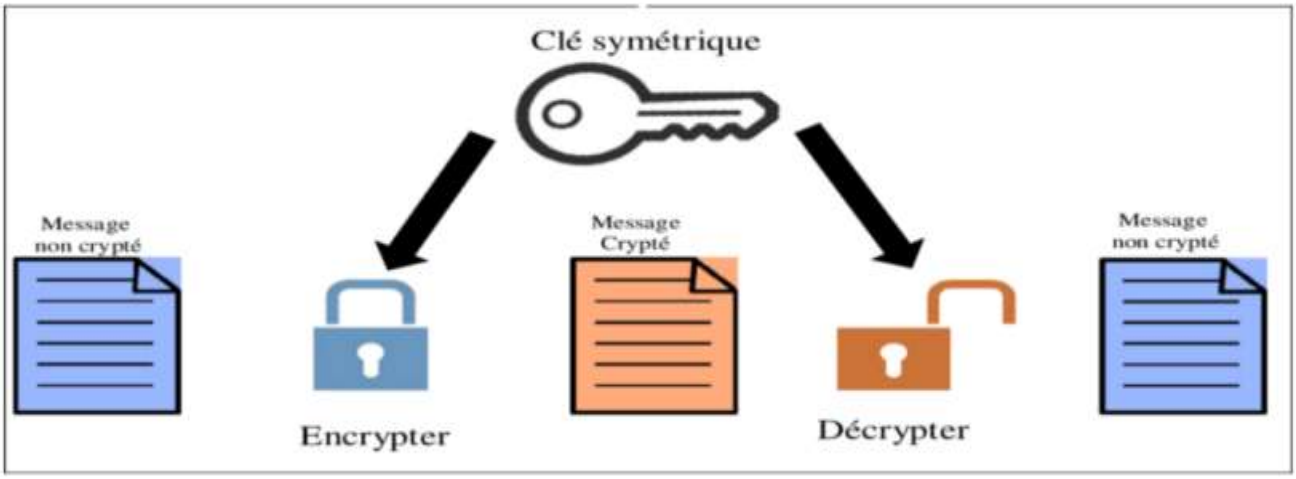

Figure 5 : Cryptage Décryptage Symétrique

 La cryptographie Asymétrique : Ce chiffrement est aussi appelé chiffrement à clés publiques. Le principe de l'algorithme de ce chiffrement est qu'il s'agit d'une fonction unidirectionnelle à trappe. Une telle fonction a la particularité d'être facile à calculer dans un sens, mais difficile voire quasi impossible dans le sens inverse. La seule manière de pouvoir réaliser le calcul inverse est de connaître une trappe. Une trappe pourrait par exemple être une faille dans e générateur de clés. Cette faille peut être soit intentionnelle de la part du concepteur ou accidentelle.

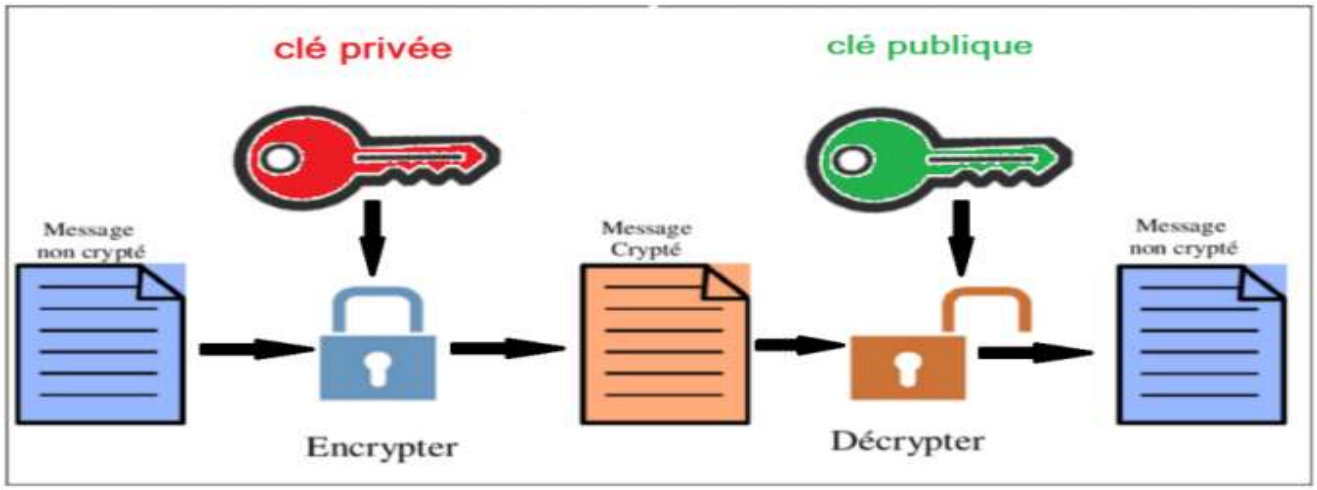

Figure 6 : Cryptage Décryptage Asymétrique

 Signature électronique : Signature électronique ou numérique est un code digital permet à la personne qui reçoit une information de contrôler l'authenticité de son

origine. Et également de vérifier que l'information en question est intacte. Aussi, les signatures électroniques permettent l'authentification et le contrôle de l'intégrité et également la non répudiation.

 Certificat : Certificat est Document électronique, carte d'identité émis par une autorité de certification. Il valide l'identité des interlocuteurs d'une transaction électronique, associe une identité à une clé publique l'encryptions et fournit des informations de gestion sur le certificat et le détenteur.

Figure 7 : Certificat de Facebook.com

I.5.6 VPN

De nos jours, les cyber-attaques se sont multipliées, y compris envers les particuliers. Ces derniers ont décidé de s'armer d'une protection efficace comme le VPN pour faire face aux hackers. Un VPN ou Réseau Privé Virtuel en français est une connexion inter-réseau permettant de relier 2 réseaux locaux différents de façon sécurisé par un protocole de **tunnelisation**. La tunnelisation est un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.

CHAPITRE II :
METHODOLOGIE UTILISEE

Malgré les grands intérêts de la sécurité informatique, l'évolution des techniques utilisées par les hackers ne cessent d'accroitre, dues aux failles de la sécurité des systèmes d'information. Plusieurs contre-mesures ont été développées, dont les systèmes de détection et de prévention d'intrusions.

Cette solution fera l'objet de notre étude. Dans ce chapitre nous allons étudier les systèmes de détection d'intrusion et les systèmes de prévention d'intrusion, ainsi que leur fonctionnement. Et pour clôturer ce chapitre, nous allons présenter l'architecture de notre structure d'accueil et nous allons faire une étude comparative des différents IDS.

II.2.1 Définition des systèmes de détection et de prévention d'intrusion

• **IDS :** est un ensemble de composants logiciels et/ou matériels dont la fonction principale est de détecter et analyser des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

Certains termes sont souvent employés quand on parle d'IDS :

Faux positif : une alerte provenant d'un IDS, mais qui ne correspond pas à une attaque réelle.

Faux négatif : une intrusion réelle qui n'a pas été détectée par l'IDS.

• **IPS :** est un outil des spécialistes en sécurité des systèmes d'information, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque.

II.2.2 Différence entre les systèmes de détection et de prévention d'intrusion

Les IDS et les IPS lisent tous deux les paquets réseau et en comparent le contenu à une base de menaces connues. La principale différence entre les deux tient à ce qui se passe ensuite. Les IDS sont des outils de détection et de surveillance qui n'engagent pas d'action de leur propre fait. Les IPS constituent un système de contrôle qui accepte ou rejette un paquet en fonction d'un ensemble de règles.

II.2.3 Comparaison entre les différents types de Systèmes de Détection d'Intrusion

II.2.3.1 Les différents types de système de détection d'intrusion

À cause de la diversité des attaques que mettent en oeuvre les pirates, l'installation des systèmes de détection d'intrusion doit se faire à plusieurs niveaux. Il existe donc différents types d'IDS :

1. **Les NIDS :**

Les NIDS sont des IDS dédiés aux réseaux. Ils comportent généralement une machine qui écoute sur le segment de réseau à surveiller, un capteur et un moteur qui réalise l'analyse du trafic afin de détecter les intrusions en temps réel. Un NIDS écoute donc tout le trafic réseau, puis l'analyse et génère des alertes si des paquets semblent dangereux.

Exemples :

• Suricata [https://suricata.io/]

• Snort [https://www.snort.org/]

• Bro (renommé Zeek depuis 2018) [https://zeek.org/]

• Enterasys [https://www.extremenetworks.com/]

• Check Point [https://www.checkpoint.com/]

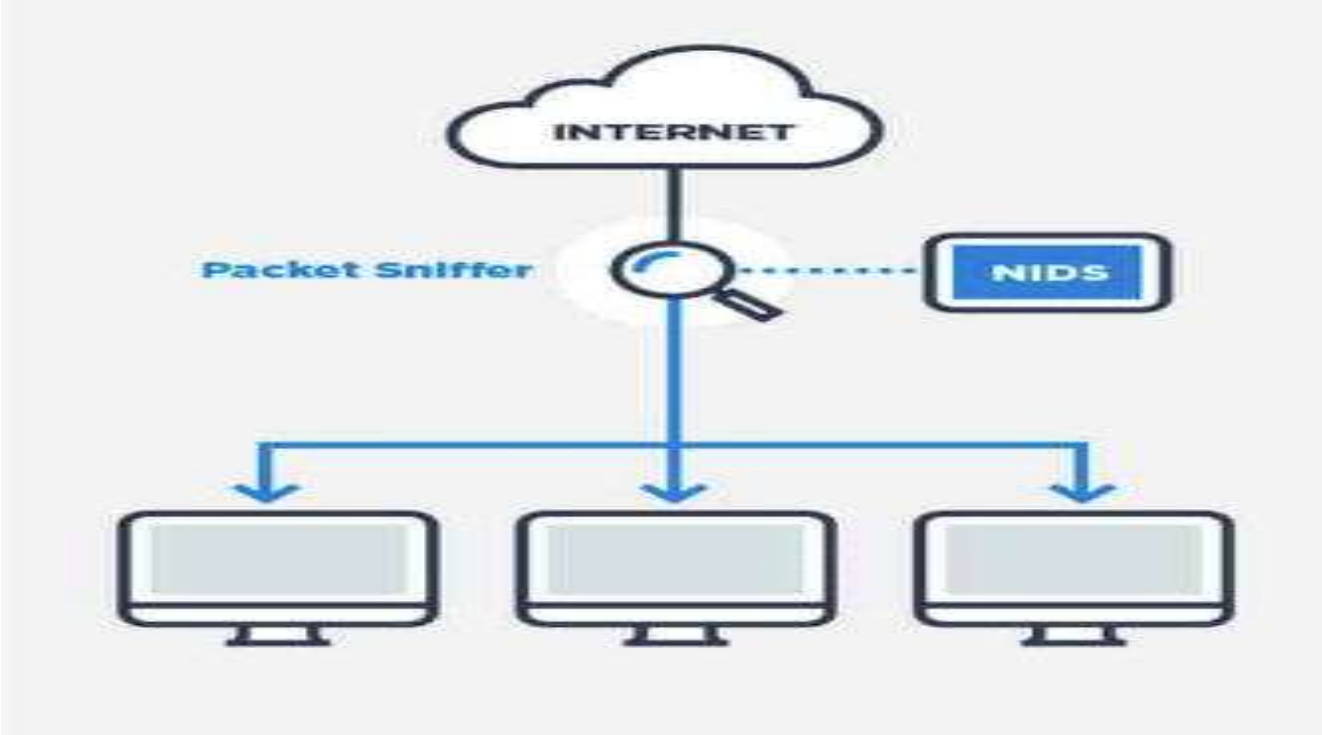

Figure 8 : Système de détection d'intrusion réseau.

2. **Les HIDS :** Les systèmes de détection d'intrusion basés sur l'hôte, analysent l'information concernant cet hôte. Le but de ce type de système de détection d'intrusion est d'assurer l'intégrité des données d'un système et analyser le flux relatif à une machine ainsi que ces journaux.

Exemples :

• DarkSpy

• IceSword

• AIDE [https://aide.github.io/]

• Fail2ban [https://http://www.fail2ban.org/]

• OSSEC [https://www.ossec.net/]

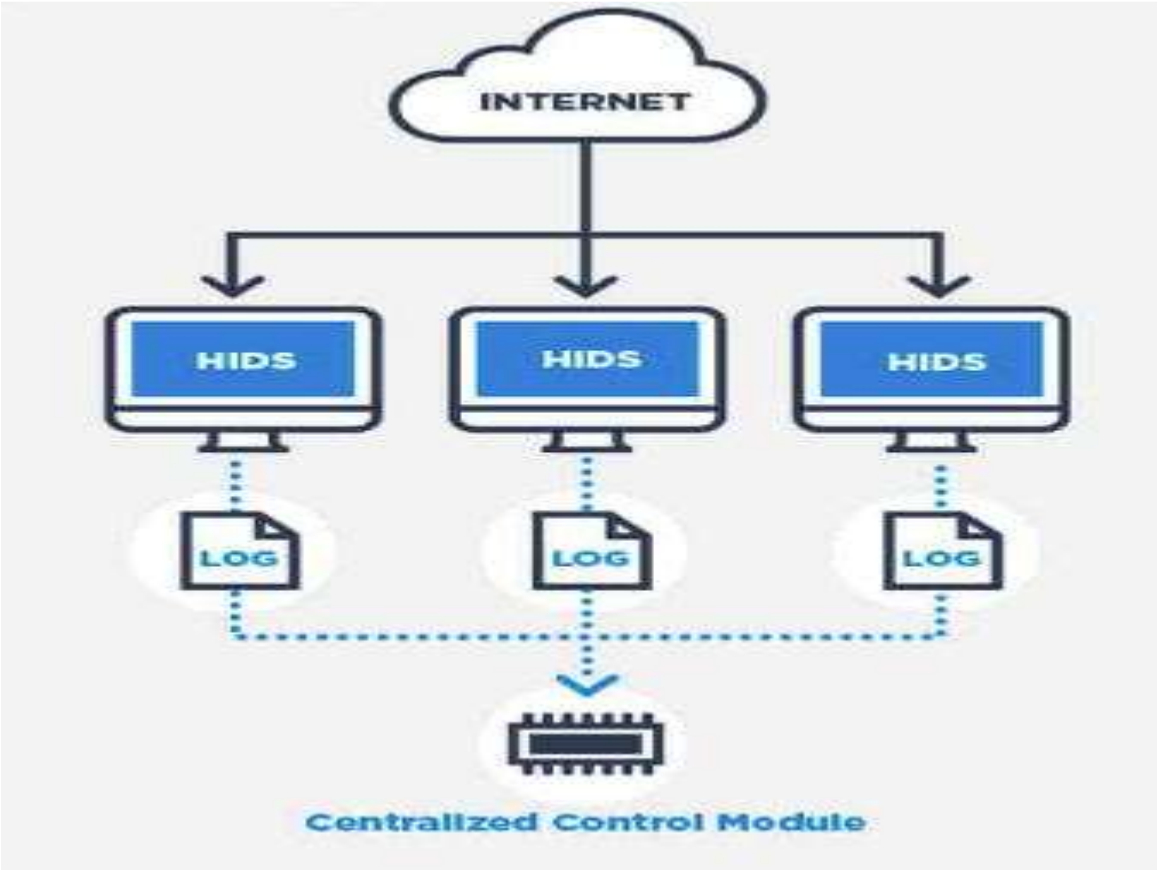

Figure 9 : Système de détection d'intrusion hôte

Les IDS hybrides : Les systèmes de détection d'intrusion hybrides sont généralement utilisés dans un environnement décentralisé, ils permettent de réunir les informations de diverses sondes placées sur le réseau. Leur appellation « hybride » provient du fait qu'ils sont capables de réunir aussi bien des informations provenant d'un système de détection d'intrusion basée sur l'hôte qu'un système de détection d'intrusion basée sur le réseau.

Exemples :

- Prelude [https://www.prelude-siem.com/]
- OSSIM [https://cybersecurity.att.com/products/ossim]

Types d'IDS	Avantages	Inconvénients

HIDS	- Contrôler les activités locales des utilisateurs avec précision ; - Capable de déterminer si une tentative d'attaque est couronnée de succès ; - Capable de fonctionner dans des environnements cryptés ; - Détecter des attaques qui ne sont pas vues par NIDS	-la difficulté de déploiement et de gestion, surtout lorsque le nombre d'hôtes qui ont besoin de protection est large.
NIDS	- Couverture de l'ensemble du réseau ; - Support pour la détection d'un nombre d'attaques conséquent ; - assure la sécurité contre les attaques puisqu'il est invisible.	- Impossible d'analyser les données cryptées ; - Le choix de règles trop génériques pourra conduire à une quantité de faux positifs beaucoup trop importante; - Ne permet pas d'assurer si une tentative d'attaque est couronnée de succès ; - Difficile à traiter tous les paquets circulant sur un grand réseau.
IDS hybrides	- Bénéficiant du support des HIDS, ils sont insensibles aux problèmes rencontrés par les	- Récent et difficile de s'interfacer avec les hyperviseurs ;

	NIDS; - Meilleure corrélation; - Diminution des faux positifs.	- gestion et interprétation des alarmes plus difficiles

TABLEAU 1 : Tableau comparatif des différents types de systèmes de détection d'intrusion

II.2.3.1.1 Caractéristiques d'un système de détection d'intrusion

Parmi les caractéristiques souhaitables trouvées dans un système de détection d'intrusion, nous pouvons citer :

- Résister aux tentatives de corruption, c'est-à-dire, il doit pouvoir détecter s'il a subi lui-même une modification indésirable ;
- S'adapter au cours du temps aux changements du système surveillé et du comportement des utilisateurs ;
- Etre facilement configurable pour implémenter une politique de sécurité spécifique d'un réseau.

II.2.3.1.2 Fonctionnement d'un système de détection d'intrusion

Il faut distinguer deux aspects dans le fonctionnement d'un IDS : le mode de détection utilisé et la réponse apportée par l'IDS lors de la détection d'une intrusion. Il existe deux modes de détection, la détection d'anomalies et la reconnaissance de signatures. De même, deux types de réponses existent, la réponse passive et la réponse active.

- Les Méthodes de détections

- **La détection d'anomalies :** La détection d'anomalie consiste à détecter des anomalies par rapport à un trafic habituel. La mise en place comprend toujours

une phase d'apprentissage au cours de laquelle les systèmes de détection d'intrusion vont découvrir le fonctionnement normal des éléments surveillés. Ils sont en mesure de signaler les divergences par rapport au fonctionnement normal. De plus, des ajustements sont nécessaires pour faire évoluer le modèle de référence de sorte qu'il reflète l'activité normale des utilisateurs et réduire le nombre de fausses alertes générées. Dans le cas d'un HIDS, ce type de détection peut être basé sur des informations telles que l'activité sur le disque, les horaires de connexion ou d'utilisation de certains fichiers.

- **La reconnaissance de signature :** Il faut noter que la reconnaissance de signature est le mode de fonctionnement le plus implémenté par les IDS du marché.

  Elle consiste à rechercher dans l'activité de l'élément surveillé les empreintes d'attaques connues. L'IDS par nature est réactif, il ne peut détecter que les attaques dont il possède la signature. Pour cela, il nécessite des mises à jour fréquentes. L'efficacité de ce système de détection réside dans la précision de sa base de signature. C'est la raison pour laquelle ces systèmes sont contournés par les pirates. Il est possible d'établir des signatures génériques, qui permettent de détecter les variantes d'une attaque. Cela demande une bonne connaissance des attaques et du réseau, de façon à stopper les variantes d'une attaque, au niveau des paquets ou au niveau Protocol.

- Les réponses "Active" et "Passive"

Il existe deux types de réponses, suivant les IDS utilisés. La réponse passive est disponible pour tous les IDS alors que la réponse active est plus ou moins implémentée.

- **Réponse active :** La réponse active a pour but de stopper une attaque au moment de sa détection. Elle implique des actions automatisées prises par un IDS qui

permet de couper rapidement une connexion suspecte quand le système détecte une intrusion. Pour cela, on dispose de deux techniques : la reconfiguration du pare-feu et l'interruption de la connexion TCP.

- **Réponse passive :** La réponse passive d'un IDS consiste à enregistrer les intrusions détectées dans un fichier de log qui sera analysé par le responsable de sécurité. Certains IDS permettent de logger l'ensemble d'une connexion identifiée comme malveillante. Ceci permet de remédier aux failles de sécurité pour empêcher les attaques enregistrées de se reproduire, mais elle n'empêche pas directement une attaque de se produire.

II.2.3.1.3 Étude comparative des principaux systèmes de détection d'intrusion informatique existants

Dans cette section, nous présentons plusieurs IDS existants.

- **SURICATA :** NIDS / NIPS open source, rapide et robuste, il effectue la détection en temps réel. Il se compose de quelques modules tels que capture, collection, décodage et détection. Il configure les flux distincts après avoir capturé et spécifié comment le flux sera séparé entre les processeurs.
- **SNORT :** NIDS / NIPS provenant du monde Open Source. Sa version commerciale, plus complète en fonction du monitoring, lui a donné une bonne réputation auprès des entreprises. Il est capable d'effectuer en temps réel des analyses de trafic et de logger les paquets sur un réseau IP. Il peut effectuer des analyses de protocole et peut être utilisé pour détecter une grande variété d'attaques et de sondes comme des dépassements de buffers, scans, attaques et bien plus.
- **BRO (Zeek) :** NIDS / NIPS et open source. Il n'existe aucun plug-in ni interface graphique pour paramétrer l'outil. Le système étant produit par des chercheurs, les mises à jour et les communautés d'utilisateurs sont parfois insuffisantes. Le gros avantage de BRO est son analyse réseau en temps réel qui permet de garantir une durabilité du réseau.

IDS Existants	Avantages	Inconvénients
SURICATA	- Gratuit à télécharger et est open source ; -Les fonctionnalités avancées comprennent le multi-threading et l'utilisation des GPU (accélération graphique);	-Moins de support par rapport aux autres IDS ; - Compliqué à installer
SNORT	- Facilité d'écriture des règles pour la détection d'intrusion; - Très flexible et dynamique en termes de déploiement ; - Gratuit à télécharger et est open source ; -Les fonctionnalités avancées comprennent le multi-threading et l'utilisation des GPU (accélération graphique);	- Pas d'interface graphique pour la manipulation des règles ; - Compliqué à installer
BRO (Zeek)	- Fonctionne efficacement dans les réseaux à fort trafic et gère les grands projets de réseau ; - Architecture très extensible	- Compliqué à mettre en place ;

TABLEAU 2 : Comparaison des différents outils de détection existants

II.2.3.1.4 Limites des systèmes de Détection d'Intrusion

Ces limites s'appliquent aux techniques de détection comme par exemple, celles de détection d'anomalie. Nous avons :

- **Consommation de ressources :** outre la taille des fichiers de logs (de l'ordre du gigaoctet (Go), la détection d'intrusion est excessivement gourmande en ressources. En effet un système NIDS doit générer des journaux de comptes-rendus d'activité anormale ou douteuse sur le réseau.
- **Perte de paquets (limitation des performances) :** les vitesses de transmission sont parfois telles qu'elles dépassent largement la vitesse d'écriture des disques durs, ou même la vitesse de traitement des processeurs. Il n'est donc pas rare que des paquets ne soient pas traités par l'IDS, et que certains d'entre eux soient néanmoins reçus par la machine destinataire.
- **Vulnérabilité aux dénis de service :** un attaquant peut essayer de provoquer un déni de service au niveau du système de détection d'intrusion, ou pire au niveau du système d'exploitation de la machine supportant l'IDS. Une fois l'IDS désactivé (« hors service »), l'attaquant peut tenter tout ce qui lui convient.
- **Placement de l'IDS :** au niveau du placement de l'IDS (implémentation et design), il est intéressant de faire de la détection d'intrusion dans la zone démilitarisée (attaques contre les systèmes publics), dans le (ou les) réseau(x) privé(s) (intrusions vers ou depuis l'intérieur) et derrière le pare-feu (détection des signes parmi tout le trafic entrant et sortant). Chacun de ces positionnements a ses avantages et inconvénients. L'important est de bien identifier les ressources à protéger (risques d'affaires majeurs) et ce qui est le plus susceptible d'être attaqué. Il convient alors d'implémenter précautionneusement l'IDS (paramétrage, etc.) en fonction du placement choisi.
- **Pollution/Surcharge :** Il est aussi possible d'envoyer une quantité importante d'attaques inoffensives afin de surcharger les alertes de l'IDS, et ainsi glisser une

attaque plus furtive qui aura du mal à être identifiée, si le flot d'informations généré est suffisant.

- **Contournement/Évasion :** Les IDS peuvent également être contournés ou outrepassés. Dans le cas d'une attaque par évasion, le système de détection d'intrusion rejette un paquet qui sera pourtant accepté par la destination. Il se peut, par exemple, qu'une différence de systèmes d'exploitation entre la machine supportant l'IDS et la machine surveillée fasse que certains paquets rejetés par le système de détection d'intrusion soient acceptés par la destination (comme des paquets UDP avec une somme de contrôle erronée, rejetés par la plupart des systèmes d'exploitation sauf les plus anciens).
- **Temps de détection :** Le temps de détection est un élément capital pour un IDS : la détection des intrusions se fait-elle en temps réel ou nécessite-t-elle un délai? Quel délai (quelques jours... ?). L'expérience montre qu'il faut habituellement un certain laps de temps afin de déceler ou de reconstituer une attaque (temps d'analyse, de réaction...).

II.2.3.2 Les différents types de Système de Prévention d'Intrusion

Les IPS ont pour fonction principale d'empêcher toute activité suspecte détectée au sein d'un système, ils sont capables de prévenir une attaque avant qu'elle atteigne sa destination. Il existe trois (03) types d'IPS. On distingue :

- **HIPS (*Host-based Intrusion Prevention System*) :** ce sont des IPS permettant de surveiller le poste de travail à travers différentes techniques, ils surveillent les processus, les drivers, les fichiers *dll* etc. En cas de détection de processus suspect, le HIPS peut le tuer pour mettre fin à ses agissements. Les HIPS peuvent donc protéger des attaques de buffer overflow.
- **NIPS (*Network Intrusion Prevention System*) :** ce sont des IPS permettant de surveiller le trafic réseau, ils peuvent prendre des mesures telles que terminer une

session TCP. Une déclinaison en WIPS (wireless intrusion prevention system) est parfois utilisée pour évoquer la protection des réseaux sans-fil.

- **KIPS (*Kernel Intrusion Prevention System*) :** ils permettent de détecter toutes tentatives d'intrusion au niveau du noyau, mais ils sont moins utilisés.

Types d'IPS	Avantages	Inconvénients
HIPS	- Protège les systèmes des comportements dangereux et pas seulement du trafic.	- Coût d'exploitation ; - Problèmes d'interopérabilité (Capacité de plusieurs systèmes) ; - Problèmes lors de mise à jour de système.
NIPS	- Protection active.	- Point sensible du réseau ; - Faux positifs (risque de blocage de trafic légitime).
KIPS	- détecter toute tentative d'intrusion au niveau du noyau	- interdire l'OS d'exécuter un appel système qui ouvrirait un Shell de commandes.

TABLEAU 3 : Avantages et inconvénients des différents IPS

II.2.3.2.1 Avantages, Inconvénients et Limites des IPS

- **Avantages :**

Les IPS ont la capacité de bloquer immédiatement les attaques et comportent plusieurs outils pour empêcher les attaquants d'accéder au réseau.

- **Inconvénients :**

Les IPS peuvent bloquer tout ce qui parait infectieux et arrête malencontreusement des applications ou des trafics légitimes. Ils laissent parfois passer certaines attaques sans les repérer.

- **Limites :**

  Les principales limites et contraintes des IPS à ce jour semblent être leur mise en place délicate, leur administration rebutante, la possibilité de bloquer tout le réseau en cas de fausse alerte, ainsi que l'inexistence d'un standard actuel.

II.2.4 Domaines d'applications des IDS

- **Systèmes distribués :**

  Les systèmes de détection et de prévention d'intrusions dans les Systèmes distribués permettent de repérer et d'empêcher l'intrusion d'un utilisateur malveillant dans un système distribué comme une grille informatique ou un réseau en nuage.

- **Internet des objets :**

  Avec la constante augmentation des Réseaux de capteurs, leur nombre devrait approcher les 26 milliards en 2020, l'Internet des Objets représente de nombreux enjeux de sécurité, notamment dus à leur faible puissance de calcul, leur hétérogénéité, le nombre de capteurs dans le réseau ainsi que la Topologie du réseau. De ce fait, les systèmes de détection d'intrusion traditionnels ne peuvent pas directement être appliqués aux réseaux de capteurs. Néanmoins, de nombreuses avancées ont été présentées au cours des années 2000-2010 pour pallier à cette problématique.

II.2.5 Description du système informatique de la DBAU

II.2.5.1 Description des ressources du système informatique

Toute révision ou modification d'un système informatique doit être faite suite à une connaissance globale de l'architecture du réseau informatique. L'architecture de la

DBAU est située sur un bâtiment en concubinage avec la DCUS. Nous allons nous focaliser sur l'architecture réseau de la DBAU.

II.2.5.1.1 Les ressources matérielles

Le siège de la DBAU dispose d'environ 25 ordinateurs, de 01 routeurs, 04 Switch, 01 serveur, des câbles RJ-45, des points d'accès Internet, des imprimantes réseaux et des téléphones VoIP qui sont interconnectés par Ethernet et une sortie vers un réseau WIFI pour les utilisateurs du réseau sans fil.

II.2.5.1.2 Les ressources logicielles

Concernant les ressources logicielles, les postes des utilisateurs fonctionnent avec le système d'exploitation Windows 11 et Windows 10. Les serveurs quant à eux tournent sur Debian. Une suite bureautique de la société Microsoft installée sur les postes bureautiques pour faire du traitement d'informations (texte, calcul, courriel, etc…)

II.2.5.2 Architecture du système informatique de la DBAU

Le réseau intranet de la DBAU est constitué des équipements d'interconnexion (routeur, switch, point d'accès et des imprimantes réseaux), d'un serveur Proxmox (Proxmox VE Enterprise) , de GRANDSTREAM Networks Inc pour la téléphonie par Voix IP. Le réseau interne caractérisé par une topologie étoilée.

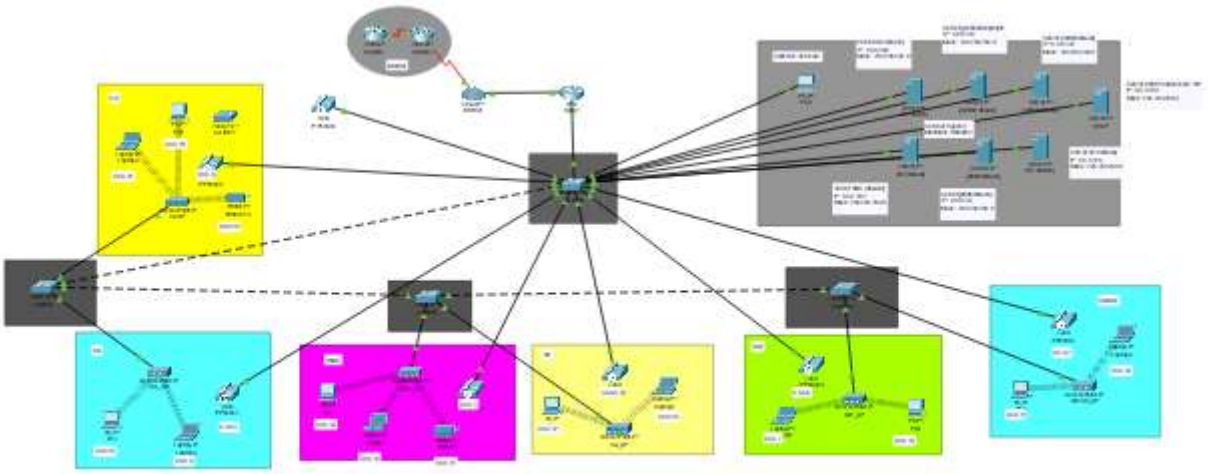

Figure 10 : Architecture du réseau de la DBAU

II.2.6 Critères et Efficacité du choix de SNORT pour la mise en place de l'IDS

Les critères et efficacités qui on aboutit au choix de SNORT sont entre autres :

II.2.6.1Critères

Nous avons choisi d'utiliser SNORT, car étant libre et gratuit, SNORT offre la capacité théorique de traiter plus de règles sur des réseaux, avec des volumes de trafic plus importants, sur le même matériel. De plus, il est très flexible en termes de création de règles pour détecter une intrusion.

II.2.6.2Efficacités

L'efficacité de SNORT se détermine par :

- **Rapidité :** un système de détection d'intrusion comme SNORT exécute et propage son analyse d'une manière prompte pour une réaction rapide dans le cas d'existence d'une attaque afin de permettre à l'agent de sécurité de réagir.
- **Complétude :** SNORT a la capacité de détecter toutes sortes d'attaques.
- **Ergonomie :** SNORT dispose d'une interface graphique et une interface web sous licence GPLv3 écrite avec Django destinée à l'édition des règles SNORT.
- Il est disponible pour la plupart des systèmes d'exploitation (Windows et Linux comme Ubuntu, Debian, CentOS).

II.2.7 Matériel et méthode utilisés

II.2.7.1 Matériel utilisé

Pour notre environnement de test, nous avons utilisé deux (02) machines virtuelles l'une comportant l'IDS fonctionnant sur Ubuntu et l'autre attaquante fonctionnant aussi sur Ubuntu.

II.2.7.2 Méthode utilisée

Compte tenu de l'architecture déjà en place dans l'organisation nous avons été contraints d'installer notre système de détection d'intrusion sur une autre machine. Ainsi pour la réalisation de ce projet, nous avons décidé de virtualiser l'architecture

afin de déployer pleinement notre système et de le tester dans un environnement sans risque afin de ne pas exposer le système de **la DBAU.**

CHAPITRE III : REALISATION ET CONCEPTION

Ce chapitre montre des interfaces de notre projet.

Installation de SNORT

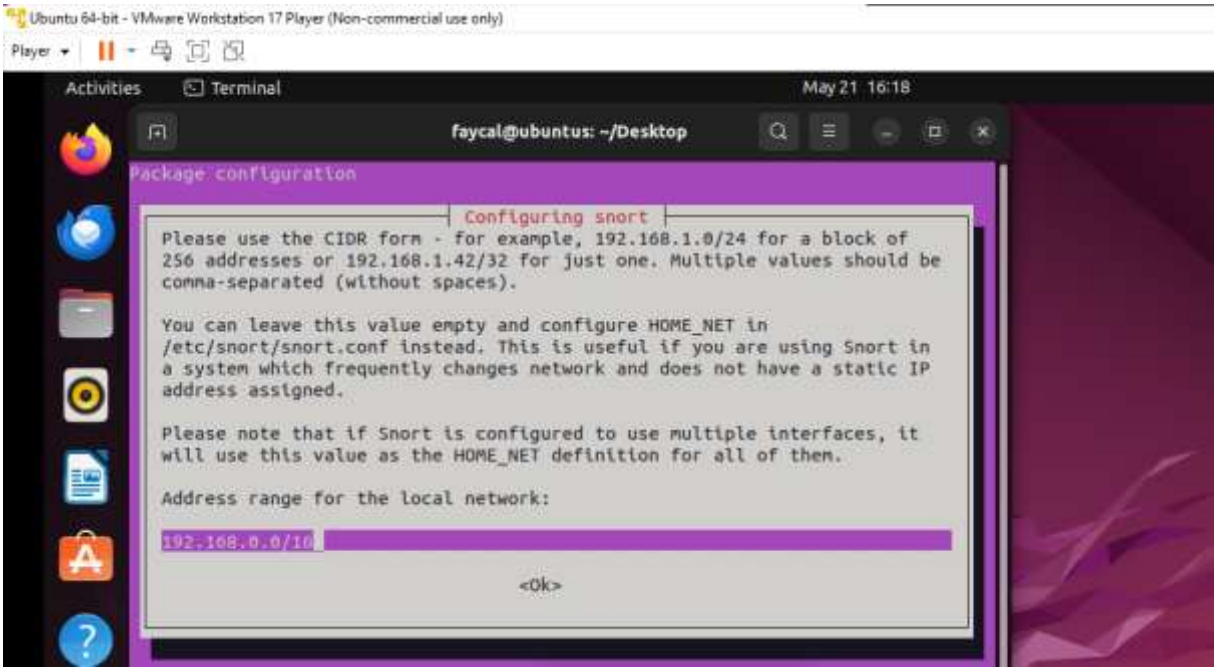

Figure 11 : Interface d'installation de SNORT

Une fois le système mis à jour, nous allons installer SNORT. Pour cela tapez la commande *sudo apt-get install snort* dans le terminal. Après l'interface ci-dessus s'affiche en tant qu'assistant de configuration de **SNORT**, a ce niveau i faut choisir une plage d'adresse sur laquelle l'outil écoutera le réseau afin de répondre ans attention.

Enregistrement des règles de SNORT

Une fois SNORT installer, pour définir les règles, il faut éditer le fichier << local.rules >> avec la commande : *sudo nano /etc/snort/rules/local.rules*. Après

l'interface du fichier s'affiche et il faut saisir la ligne suivante *alert icmp any any -> $HOME_NET any (msg:"Tentative connexion ICMP"; sid:00001; rev:1;).*

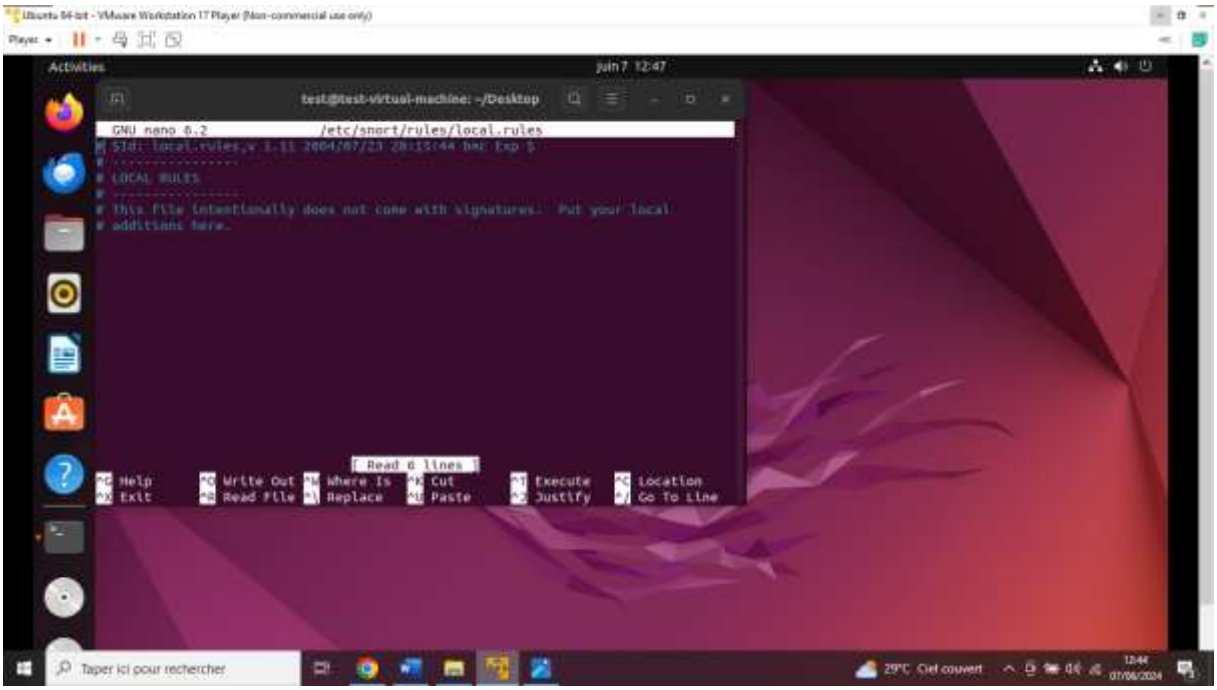

Figure 12 : Interface d'enregistrement des règles SNORT

ELK

Elastic Stack - anciennement connue sous le nom de *ELK Stack* - est une collection de logiciels open-source produite par Elastic qui vous permet de rechercher, d'analyser et de visualiser des journaux générés à partir de n'importe quelle source dans n'importe quel format, une pratique connue sous le nom de *journalisation centralisée*. La journalisation centralisée peut être utile lorsque vous tentez d'identifier des problèmes avec vos serveurs ou vos applications, car elle vous permet de consulter tous vos journaux en un seul endroit. Elle est également utile car elle vous permet d'identifier les problèmes qui concernent plusieurs serveurs, en corrélant leurs journaux pendant une période spécifique.

Pour son installation, il faut taper la commande *sudo apt install elasticsearch*,il faut passer ensuite à sa configuration en passant par la commande *sudo nano /etc/elasticsearch/elasticsearch.yml* dans son interface de configuration. Après configuration il faut le démarrer en tapant *sudo systemctl start elasticsearch* et en suite le rendre opérationnel à chaque démarrage de notre serveur avec la commande *sudo systemctl enable elasticsearch.*

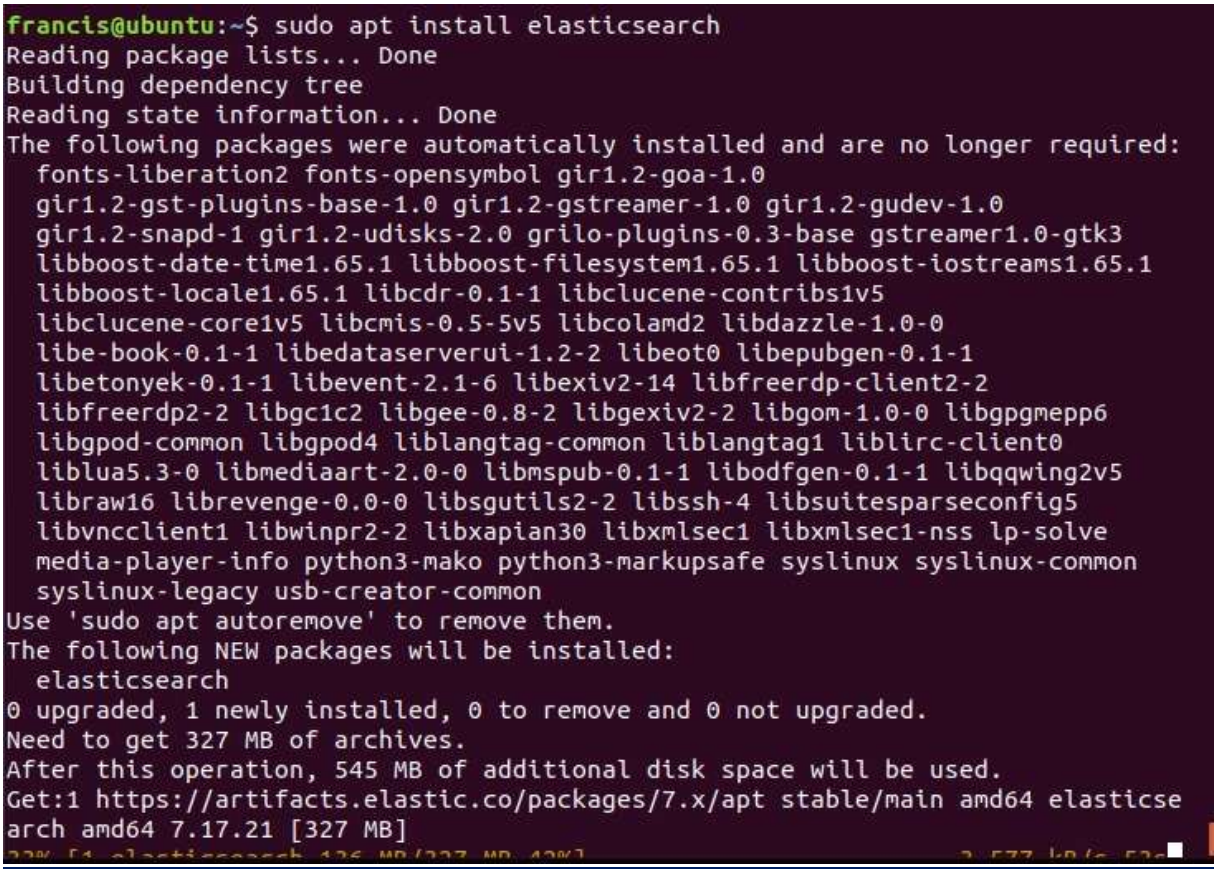

Figure 13 : Interface d'installation ELK

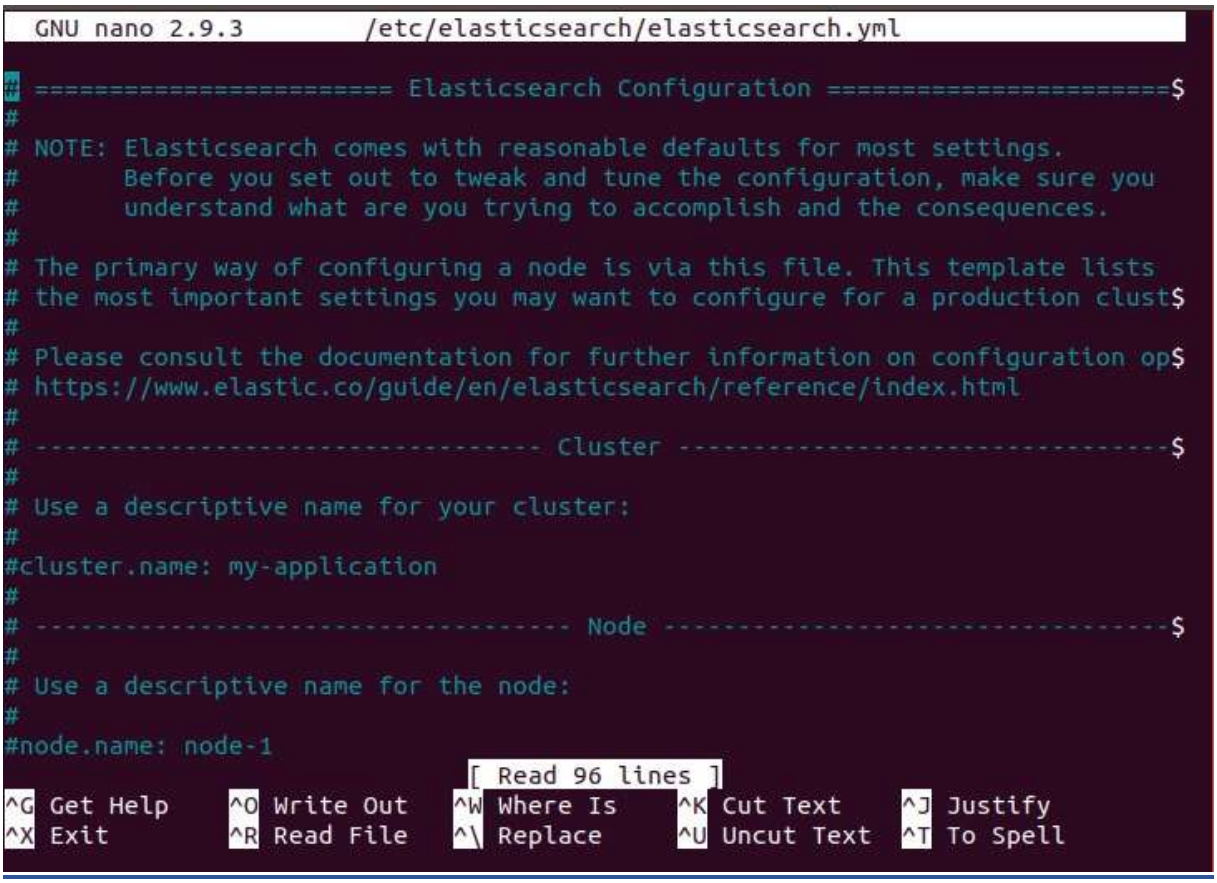

Figure 14 : Interface de configuration ELK

KIBANA

KIBANA est un outil de visualisation et d'exploration de données utilisé pour les cas d'utilisation de l'analyse des journaux et des séries chronologiques, de la surveillance des applications et de l'intelligence opérationnelle. Il offre des fonctionnalités puissantes et faciles à utiliser telles que des histogrammes, des graphiques linéaires, des diagrammes circulaires, des cartes thermiques et une prise en charge géospatiale intégrée.

Pour son installation il faut taper la commande *sudo apt install kibana* ensuite passez à la configuration, au démarrage et à son activation avec les commande *sudo systemctl enable kibana* *sudo systemctl start kibana* .

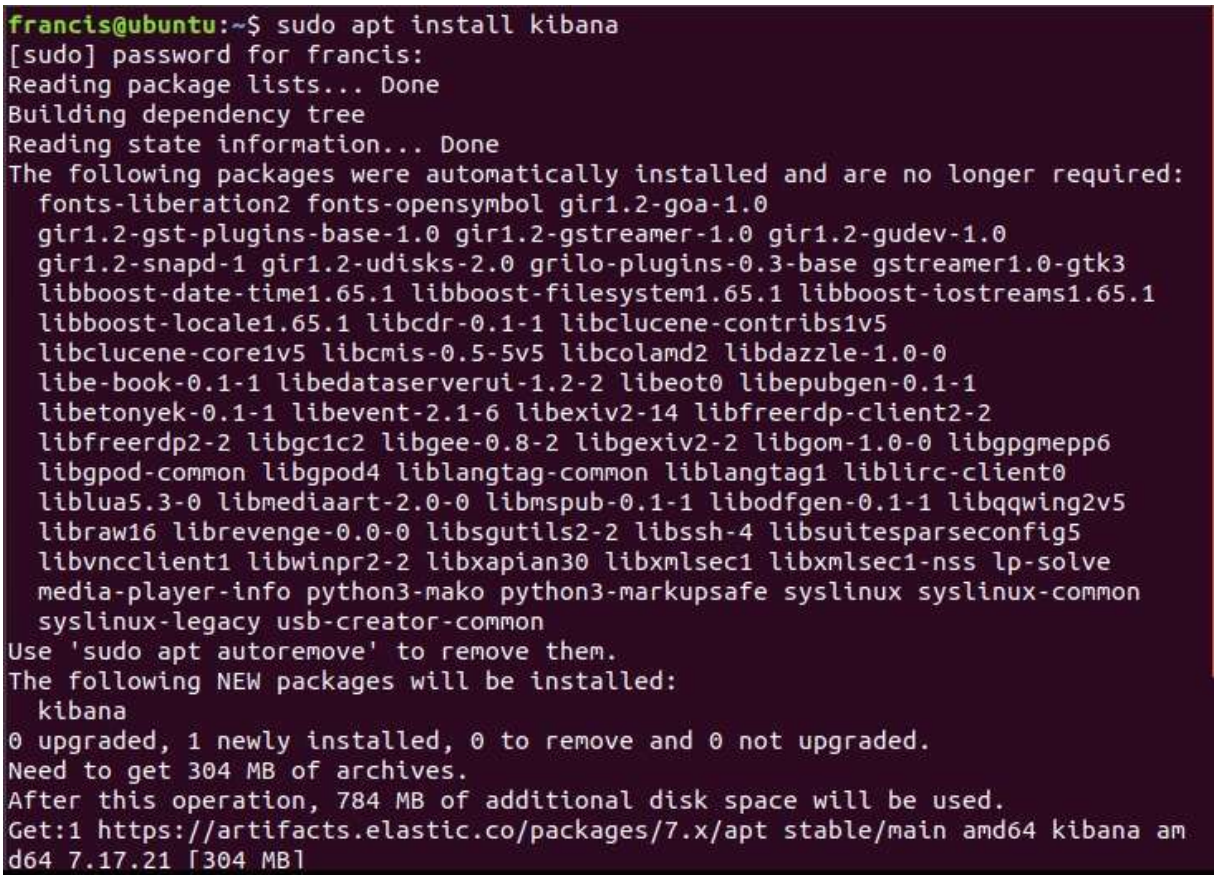

Figure 15 : Interface d'installation KIBANA

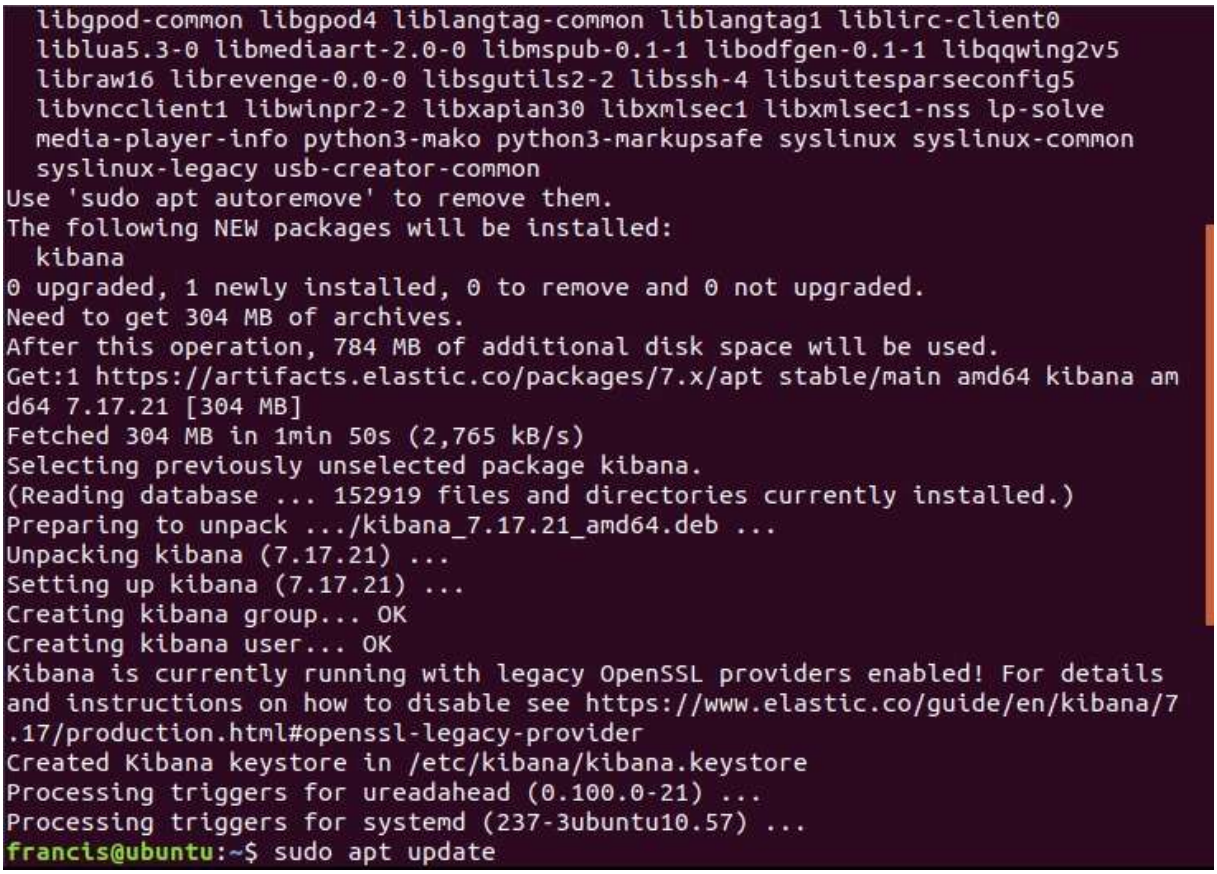

Figure 16 : Interface de démarrage de KIBANA

CONCLUSION

SNORT est un logiciel open source de détection d'intrusion (IDS) et de prévention d'intrusion (IPS), permettant l'inspection des Paquets en Profondeur. SNORT est un outil très intéressant dans la mise en place d'une sécurité réseau. De plus SNORT placé dans l'enceinte d'un réseau permet de détecter les failles les plus répandues qui proviennent généralement de l'intérieur de l'entreprise, et non de l'extérieur. Ce système de détection multiplateforme est en perpétuelle évolution et semble être un des meilleurs outils dans la connaissance des vulnérabilités auxquelles les entreprises sont exposées.

WEBOGRAPHIE

- ✓ Plate-forme de SNORT https://all-it-network.com/snort/
- ✓ Plate-forme de Monitoring de Ubuntu https://wiki.monitoring-fr.org/securite/snort/snort-ubuntu-install.html
- ✓ Plate-forme de elasticsearch et kibana pour la gestion de journal de logstachs et de tableau de bord https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elastic-stack-on-ubuntu-20-04-fr
- ✓ Vidéo Youtube d'installation de elk et kibana https://www.youtube.com/watch?v=PsLepTFhbeI
- ✓ IA Chat gpt pour l'amélioration des textes https://chatgpt.com/?model=text-davinci-002-render-sha
- ✓ Plate-forme de mémoire en ligne https://www.memoireonline.com/

BIBLIOGRAPHIE

- ✓ Mémoire 2010-2011 de Hamzata GUEYE sur la mise en place de IDS avec SURICATA
- ✓ Mémoire 2020-2021de Hervé MESSANH sur la mise en place d'un IDS avec SURICATA : Cas de BOLLORE
- ✓ Mémoire 2021-2022 de ALASSANI Alassane et AWALI Rachidou sur la conception et réalisation d'un centre d'écoute clients : Cas su Trésor
- ✓ Mémoire de ACAKPO Salomon et DJOGBE Hermès sur la gestion des demandes de frais de rédaction de rapport des stage, de mémoire et de thèse à la DBAU

TABLE DES MATIERES