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

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

01 BP 526 Cotonou - Bénin Tel : +229 55 028 070 / 53 973 060
https://www.ifri-uac.bj Courriel : contact@ifri.uac.bj

MÉMOIRE

pour l'obtention du

Diplôme de Licence en Informatique

Option : Sécurité Informatique

Présenté par :
Lizette Onésia Majoie **ABOUE**

Mise en place du système de détection et de prévention d'intrusions SURICATA dans un système d'informations : Cas de JENY SAS

Sous la supervision :
Dr Pierre Jerôme **ZOHOU**

Membres du jury :

AHOUANDJINOU Arnaud	Docteur	IFRI	Président
AKAKPO Hervé	Ingenieur	IFRI	Examinateur
ZOHOU Jerôme	Docteur	IFRI	Rapporteur

Année Académique : **2020-2021**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Table des figures vi

Liste des tableaux vii

Liste des acronymes viii

Glossaire 1

Introduction 2

1 Revue de littérature 4

2 Analyse et choix technique 12

3 Présentation de la solution, conception et résultats des tests 19

Conclusion 31

Bibliographie 32

Webographie 33

Table des matières 34

Dédicace

À
mon père **Mr Antoine ABOUE**, ma mère **Véronique SEWADE**, mes sœurs **Bernice**, **Rebecca**, **Précieuse** et **Géniale**.

Remerciements

Ce projet est le résultat de multiples efforts et contributions conjugués de personnes ressources et expérimentées qu'il serait judicieux de remercier.

Il s'agit de :

- Professeur Eugène C. EZIN, le Directeur de l'Institut de Formation et de Recherche en Informatique (IFRI) pour ses conseils ;
- Docteur (MC) Gaston EDAH, le Directeur Adjoint de l'Institut de Formation et de Recherche en Informatique (IFRI) pour l'accompagnement le long de la formation ;
- Monsieur Pierre Jérôme ZOHOU , notre encadreur, pour sa disponibilité et sa bonne foi à répondre à nos préoccupations durant la réalisation de ce projet ;
- Mademoiselle Udalride TOGNIDE, notre maître de stage, pour son aide dans l'élaboration de ce projet par ses conseils et son soutien durant toute la période de stage ;
- Monsieur Sylvain KIKI , pour son aide au cours de notre stage ;
- Président et aux membres du jury pour l'honneur qu'ils nous ont fait en acceptant d'examiner ce travail ;
- L'administration de l'IFRI pour le précieux travail effectué afin que nous, étudiants, puissions travailler dans les meilleures conditions ;
- Monsieur Regis SINKPOTA et Mademoiselle AHOUANYE Marielle, pour leur assistance lors de la rédaction de ce document ;
- Tous nos enseignants , nos camarades , pour avoir partagé leurs connaissances avec nous et favorisé l'acquisition de celles-ci par la pratique.

  Nos remerciements vont également à l'endroit de toute personne ayant contribué de quelque manière, de près ou de loin, à la réalisation de ce projet et dont le nom ne figure pas sur cette liste.

Résumé

Dans un contexte où les cybermenaces sont de plus en plus sophistiquées, la protection du système d'information (SI) représente un enjeu crucial pour toute organisation. JENY SAS, fournisseur d'accès à Internet et gestionnaire du registre .bj, fait face à de nombreuses intrusions, particulièrement les week-ends, ainsi qu'à une forte utilisation inexpliquée de la bande passante. Face à ces menaces croissantes, l'entreprise décide d'adopter une solution de détection et de prévention des intrusions (IDS/IPS). Ce travail a pour objectif de mettre en place et d'évaluer SURICATA afin d'améliorer la protection du SI. L'installation et la configuration de SURICATA s'intègrent dans l'infrastructure existante, accompagnées de la plateforme SNORBY pour faciliter l'analyse et la gestion des alertes de sécurité. Pour évaluer l'efficacité de la solution, des tests d'intrusion sont réalisés afin de mesurer la capacité de détection de SURICATA, ainsi que sa capacité de prévention. L'ensemble des tests montre que la solution identifie et bloque efficacement les attaques simulées. Les résultats obtenus mettent en évidence une amélioration significative de la sécurité du SI de JENY SAS, en offrant une meilleure visibilité sur les tentatives d'intrusion et une réponse proactive aux menaces.

Mots clés : système d'information, intrusion, détection, prévention des intrusions, fournisseur d'accès à Internet, bande passante, réponse proactive.

Abstract

In a context where cyber threats are becoming increasingly sophisticated, protecting the information system (IS) is a critical issue for any organization. JENY SAS, an Internet service provider and manager of the .bj registry, faces numerous intrusions, particularly on weekends, as well as unexplained high bandwidth usage. In response to these growing threats, the company has decided to adopt an intrusion detection and prevention solution (IDS/IPS). This work aims to deploy and evaluate SURICATA to enhance IS security. The installation and configuration of SURICATA are integrated into the existing infrastructure, along with the SNORBY platform to facilitate security alert analysis and management. To assess the effectiveness of the solution, intrusion tests are conducted to evaluate SURICATA's detection capabilities as well as its prevention capabilities. The results demonstrate that the solution effectively identifies and blocks simulated attacks. The findings highlight a significant improvement in JENY SAS's IS security, providing better visibility into intrusion attempts and a proactive response to threats.

Keywords: information system, intrusion, detection, intrusion prevention, Internet service provider, bandwidth, proactive response.

Table des figures

1.1 Historique des systèmes de détection d'intrusions 5

2.1 Logo de Suricata 17

3.1 Architecture réseau de JENY SAS 21
3.2 Vérification du statut de Suricata 22
3.3 Récupération des règles 23
3.4 Statut de suricata après les configurations 23
3.5 Architecture réseau de JENY SAS après l'installation de Suricata 24
3.6 Interface d'authentification de Snorby 25
3.7 Interface graphique de Snorby 25
3.8 Détection des attaques reçues 26
3.9 Détails sur les attaques détectées 26
3.10 Courbe des capteurs 26
3.11 Courbe des sévérités 27
3.12 Vue d'ensemble des attaques 27
3.13 Fonctionnement de Barnyard2 28
3.14 Capture des pings externes 28
3.15 Capture du tableau de bord pendant l'attaque ping flood 29
3.16 Capture du téléchargement du site compromis 29
3.17 Capture de l'enregistrement du blocage 30

Liste des tableaux

1.1 Fonctions principales d'un Système de Détection d'Intrusion (IDS) 6

2.1 Tableau de l'analyse qualitative des outils de détection et de prévention d'intrusions . 16

3.1 Configuration de la machine virtuelle 21

Liste des acronymes

HIDS :

Host Intrusion Detection System viii, 8, 34

HIPS :

Host Intrusion Prevention System 10, 35

IDS :

Intrusion Detection System viii, 4–11, 14, 34

IPS :

Intrusion Protection System viii, 4, 8–11, 14, 35

KIPS :

Kernel Intrusion Prevention System 11, 35

LAN :

Local Area Network viii, 11

NIDS :

Network Intrusion Detection System viii, 8, 34

NIPS :

Network Intrusion Prevention System 10, 35

WIPS :

Wireless Intrusion Prevention System 11, 35

Glossaire

DoS (Denial of Service) : Une attaque visant à rendre un service ou une ressource d'un système informatique inaccessible en saturant ses ressources ou son réseau. 11

MAC (Message Authentication Code) : Un code utilisé pour garantir l'intégrité et l'authenticité d'un message transmis sur un réseau, en utilisant une clé secrète partagée. 11

MITM (Man in the Middle) : Une attaque où un attaquant intercepte et manipule les communications entre deux parties sans qu'elles en soient conscientes. 11

Introduction Générale

L'évolution constante de la technologie souligne l'importance pour les entreprises d'adopter une politique efficace de gestion des grandes quantités d'informations. Elles s'appuient souvent sur des ressources telles que les serveurs pour optimiser cette gestion.

Contexte

Les entreprises qu'elles soient petites ou grandes sont souvent cibles de nombreuses attaques informatiques qui commencent par de petites intrusions pour mener à des actes malveillants. Avec la crise sanitaire ayant favorisé le télétravail, on remarque une augmentation des attaques informatiques. Les attaquants à la recherche d'informations s'introduisent clandestinement dans les réseaux informatiques. La divulgation, le vol et l'altération des informations peuvent entraîner de lourdes pertes sur plusieurs domaines au sein de l'entreprise. La sécurité des informations est donc devenue une question de plus en plus prisée dans certaines entreprises, comme c'est le cas de JENY SAS.

Problématique

JENY SAS, fournisseur d'accès à Internet et gestionnaire du registre du .bj, héberge des données essentielles utilisées en permanence par ses employés pour fournir des services à ses clients. Cependant, l'entreprise rencontre régulièrement des problèmes d'indisponibilité des informations dans son système, souvent causés par des tiers malveillants. Afin de remédier à cette situation, le Responsable Technique a décidé de mettre en place un système fiable de détection et de prévention des intrusions. Ce projet vise principalement à détecter et prévenir les attaques informatiques, à enregistrer toutes les activités et à surveiller le réseau. C'est dans cette optique que notre projet a été conçu.

Objectifs

L'objectif principal de ce projet est de mettre en place une solution informatique permettant la détection et la prévention des intrusions. Cet objectif est décliné dans les points suivants :

- Installer et configurer une solution efficace dans la détection et la prévention des intrusions ;

- Appliquer les règles adéquates pour avoir une plateforme sécurisée ;
- Adapter une interface graphique à notre solution pour la consultation des intrusions.

Ainsi cette solution permet à l'entreprise JENY SAS de détecter toutes les intrusions, de les prévenir et de surveiller le trafic du réseau. Cette solution prend aussi en compte les besoins de journalisation des activités dans le réseau.

Présentation de la Direction Technique de JENY SAS

La Direction Technique est l'une des directions centrales de JENY SAS. Elle est composée du service de monitoring, du Service Après-Vente (SAV), du service de l'administration et de la sécurité des serveurs, du service de la programmation et du service de la technique. Elle a pour rôle de diriger et de coordonner les orientations techniques et technologiques de JENY SAS. Elle veille à leur bonne mise en œuvre et exploitation pour atteindre les objectifs liés à la Technique.

Organisation du mémoire

Le document est structuré en trois chapitres. Le premier chapitre, intitulé **Revue de littérature**, traite des généralités liées aux systèmes de détection et de prévention des intrusions, en détaillant leurs caractéristiques et les concepts fondamentaux associés. Le second chapitre, ayant pour titre **Analyse et choix technique**, présente une étude approfondie de la solution sélectionnée, en exposant les raisons motivant ce choix et en analysant les différentes options techniques disponibles. Enfin, le troisième chapitre,portant le titre de **Présentation de la solution, conception et résultats des tests**, décrit les techniques de conception mises en œuvre et présente les résultats des tests effectués pour vérifier le bon fonctionnement de la solution proposée.

Chapitre 1

Revue de littérature

Introduction

L'apparition de la pandémie de coronavirus a contraint de nombreuses entreprises et organisations à adopter le travail à distance. Cette situation a entraîné une augmentation considérable du volume de paquets transitant dans le réseau, tout en réduisant significativement le niveau global de sécurité. Face à ces nouveaux défis, diverses solutions ont été mises en place afin de restreindre les accès aux réseaux informatiques et d'atténuer les risques liés aux cyberattaques. Cependant, certains attaquants parviennent à contourner ces mesures de sécurité et à s'introduire clandestinement dans les systèmes d'information, compromettant ainsi leur intégrité et leur confidentialité.

En informatique, une intrusion désigne tout accès non autorisé à un système informatique, un réseau ou une application, généralement dans le but d'altérer, de voler ou de détruire des données, d'exploiter des vulnérabilités ou de perturber le fonctionnement normal d'un système.

Pour faire face à ces menaces grandissantes, des systèmes de détection IDS et de prévention IPS ont été élaborés. Ces acronymes désignent un ensemble de mécanismes avancés dédiés à l'identification et à la neutralisation des activités anormales ou suspectes au sein des infrastructures réseau, contribuant ainsi à renforcer la cybersécurité des organisations.

1.1 Les systèmes de détection d'intrusions IDS

1.1.1 Historique et définition des systèmes de détection d'intrusion

1.1.1.1 Historique des systèmes de détection d'intrusions

Le premier système de détection d'intrusion (IDS) a été créé en 1984 par Dorothy Denning et Peter Neuman pour sécuriser Arpanet, l'ancêtre d'Internet. Appelé IDES, il reposait sur une approche comportementale pour identifier les activités suspectes. En 1993, il a évolué en NIDES, intégrant de nouvelles techniques d'analyse pour améliorer la détection. Parallèlement, le projet Haystack de Crosby Marks a abouti en 1988 à un IDS basé sur des signatures plutôt que des règles comportementales. Ces avancées ont mené à l'émergence des systèmes HIDS (Host Intrusion Detection Systems) et NIDS (Network Intrusion Detection Systems) dans les années 1990.

En 1990, Todd Heberlein introduit le NIDS, et le Centre de cryptologie de l'armée de l'air américaine développe ASIM, combinant matériel et logiciels pour détecter les intrusions. En 1994, la société Wheel Group lance NetRanger, la première solution IDS commercialisable, et ISS crée RealSecure pour l'environnement Windows NT4. En 1998, Cisco Systems acquiert Wheel Group, consolidant sa position dans la cybersécurité.

Les années suivantes ont vu de nombreuses fusions et acquisitions dans le domaine des IDS, renforçant les capacités technologiques et l'innovation face aux nouvelles menaces. Ce phénomène continue aujourd'hui, les entreprises cherchant à s'adapter aux cyberattaques en constante évolution.

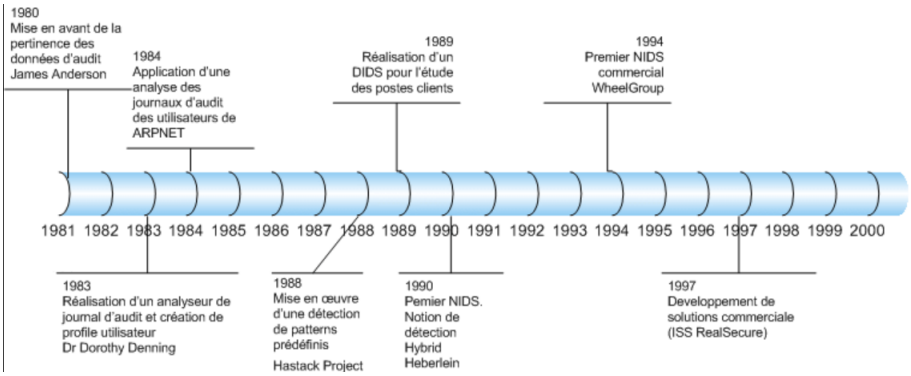


FIGURE 1.1 : Historique des systèmes de détection d'intrusions
[6]

1.1.1.2 Définition des systèmes de détection d'intrusions

Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). C'est un mécanisme permettant ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.C'est aussi un appareil ou une application qui alerte l'administrateur en cas de faille de sécurité, de violation de règles ou d'autres problèmes susceptibles de compromettre son réseau informatique.

1.1.2 Fonctionnement des systèmes de détection d'intrusions IDS

Un Système de Détection d'Intrusion (IDS) surveille et analyse les activités d'un réseau ou d'un système pour détecter des comportements suspects. Il collecte des données provenant de différentes sources, comme les journaux système et le trafic réseau, via des capteurs en temps réel. Ces données sont ensuite comparées à des politiques de sécurité et des signatures d'attaques connues par un analyseur. Si une activité suspecte est détectée, une alerte est générée. Un gestionnaire centralise ces alertes et aide les administrateurs à prendre des mesures appropriées, comme ajuster les règles de sécurité ou isoler des segments du réseau, garantissant ainsi une réaction rapide aux menaces et la sécurité du système.[2]

Pour surveiller le trafic à la recherche d'activités malveillantes, les IDS utilisent trois méthodes de détection à savoir :

- Détection basée sur les signatures ou basée sur les connaissances ;
- Détection basée sur les anomalies ou basée sur le comportement ;
- Détection basée sur la réputation.

1.1.2.1 Détection basée sur les signatures ou basée sur les connaissances

La détection basée sur les signatures surveille des modèles spécifiques, comme les signatures de cyberattaques ou les séquences d'octets dans le trafic réseau, similaire à un logiciel antivirus. Elle permet d'identifier facilement les menaces connues, mais peut être inefficace face aux nouvelles attaques, car elle repose uniquement sur des signatures ou des modèles d'attaque précédents.

1.1.2.2 Détection basée sur les anomalies ou basée sur le comportement

La détection basée sur les anomalies surveille les violations en analysant les journaux du système pour identifier des activités anormales par rapport au comportement normal d'un appareil ou d'un réseau. Cette méthode peut détecter des cyberattaques inconnues et utilise parfois l'apprentissage automatique pour établir un modèle comportemental normal afin de comparer de nouvelles activités. Bien que pouvant générer des faux positifs, les IDS basés sur la détection d'anomalies offrent une meilleure sécurité que ceux basés sur les signatures. Ils réagissent différemment selon le type d'anomalie détectée.

1.1.2.3 Détection basée sur la réputation

Les IDS basés sur la réputation détectent les menaces en fonction de la réputation des entités impliquées, comme les hôtes tentant d'accéder au réseau. Ils analysent des attributs de fichiers (source, signature, âge, utilisation) et utilisent des moteurs de réputation avec des algorithmes pour évaluer si les données sont menaçantes. Ce type d'IDS est souvent utilisé dans les logiciels anti-malware et antivirus pour analyser des fichiers exécutables ou batch susceptibles de contenir du code malveillant.

1.1.3 Fonction des systèmes de détection d'intrusions IDS

Un Système de Détection d'Intrusion (IDS) remplit quatre fonctions essentielles : l'analyse, la journalisation, la gestion et l'action.

Les descriptions de ces fonctions sont consignées dans le tableau qui suit :

Fonction	Description
Analyse	Surveillance et examen du trafic réseau et des activités système pour détecter des comportements anormaux ou suspects.
Journalisation	Enregistrement détaillé des événements et des alertes pour analyses ultérieures et audits de sécurité.
Gestion	Configuration, déploiement et maintenance de l'IDS, y compris la définition des politiques de sécurité et la mise à jour des signatures d'attaque.
Action	Réponse aux menaces détectées, telles que la génération d'alertes, le blocage de communications ou la mise en quarantaine de segments du réseau.

TABLE 1.1 : Fonctions principales d'un Système de Détection d'Intrusion (IDS)

1.1.4 Composition des systèmes de détection d'intrusions IDS

Les IDS ont trois composants nécessaires, qui sont :

- le composant de surveillance du système d'information (Probing), qui surveille le (ou les) système d'information (SI) ;
- le composant de monitoring, qui fait la synthèse des données récoltés par le composant de surveillance du système d'information ;
- le composant de décision.

On ne considère pas l'interface utilisateur, qui ne constitue pas une fonctionnalité nécessaire au bon fonctionnement d'un IDS.

1.1.4.1 La couche surveillance du système d'information

La couche de surveillance du système d'information est responsable de l'enregistrement exhaustif de toutes les actions effectuées au sein du réseau. Ces actions proviennent principalement de deux sources distinctes :

- **Le trafic réseau**, qui est surveillé par les **Systèmes de Détection d'Intrusion Réseau (NIDS)**.
- **Le système d'exploitation**, qui est supervisé par les **Systèmes de Détection d'Intrusion Hôte (HIDS)**.

Les actions enregistrées peuvent inclure une variété d'opérations, telles que la lecture et l'écriture de fichiers, les tentatives d'authentification, les modifications de configurations système, et bien d'autres. Toutes ces activités sont consignées sous forme de **journaux (logs)**, qui sont ensuite transmises à la couche de surveillance pour une analyse approfondie. Cette analyse permet :

- d'identifier des anomalies ;
- de détecter des intrusions potentielles ;
- de garantir la sécurité globale du système d'information.

1.1.4.2 La couche de monitoring

La couche de monitoring est chargée d'analyser les logs. Son objectif principal est d'évaluer les menaces pesant sur le système d'information en identifiant des événements notables. Pour ce faire, les logs sont regroupés afin de détecter des motifs permettant de reconnaître une action connue, qui est ensuite évaluée. Ces événements sont alors classés en deux catégories : événements notables ou non.

Dans le cas où des événements notables sont détectés, l'IDS évalue la menace pesant sur le système d'information.

Après avoir identifié la menace pesant sur le système d'information, l'IDS émet une évaluation sur la sécurité du réseau ou des systèmes et transmet sa décision à la couche de décision.

1.1.4.3 La couche de décision

Si la couche de surveillance juge que le système a été compromis, l'IDS peut prendre plusieurs décisions :

- **Premièrement**, il peut **prévenir l'administrateur du système d'information** afin que celui-ci puisse prendre les mesures nécessaires.
- **Deuxièmement**, il peut **effectuer une action prédéfinie par l'administrateur système** afin d'empêcher l'intrusion ou, à défaut, de la ralentir.

1.1.5 Types des systèmes de détection d'intrusions

Les différents IDS se caractérisent par leur domaine de surveillance. Il existe trois grandes familles distinctes d'IDS.

1.1.5.1 Les Host Intrusion Detection System (HIDS)

Les systèmes de détection d'intrusion basés sur l'hôte (HIDS) sont des solutions qui s'exécutent directement sur des appareils ou des hôtes distincts au sein d'un réseau. Ils surveillent uniquement les paquets de données entrants et sortants des appareils connectés et alertent l'administrateur ou les utilisateurs en cas de détection d'une activité suspecte. Ces systèmes analysent divers éléments tels que les appels système, les modifications de fichiers et les journaux d'application.

1.1.5.2 Les Network Intrusion Detection System (NIDS)

Les NIDS sont des IDS utilisés pour protéger un réseau. Ils comportent généralement une sonde (par exemple, une machine) qui écoute et surveille en temps réel l'ensemble du trafic réseau. Cette sonde analyse les paquets de données et génère des alertes lorsqu'elle détecte des intrusions ou des paquets suspects pouvant représenter une menace.

Le NIDS fait partie intégrante de l'infrastructure réseau et surveille les paquets qui la traversent. Il coexiste avec des équipements tels que les commutateurs, qui possèdent des capacités de mise en miroir, de capture et de répartition du trafic réseau.

1.1.5.3 Les IDS hybrides

Les IDS hybrides combinent les caractéristiques des NIDS et des HIDS, offrant ainsi une surveillance à la fois du réseau et des terminaux. Les sondes sont positionnées à des points stratégiques et peuvent fonctionner comme des NIDS et/ou des HIDS, en fonction de leur emplacement.

1.2 Les systèmes de prévention d'intrusions IPS

1.2.1 Définition d'un système de prévention d'intrusion

Un système de prévention d'intrusion (ou IPS, Intrusion Prevention System) est un outil de sécurité des systèmes d'information, similaire aux IDS, qui permet de prendre des mesures afin de limiter les impacts d'une attaque. Contrairement aux IDS, qui se contentent de détecter les menaces, un IPS agit de manière proactive en bloquant automatiquement les activités suspectes.

1.2.2 Fonctionnement des systèmes de prévention d'intrusion

Les Systèmes de Prévention des Intrusions (IPS) incluent plusieurs techniques, notamment :

- **Protection de la mémoire et des processus des systèmes**
- **Interception de session**
- **Solutions de pare-feu et routeurs**

Pour protéger le trafic contre les activités malveillantes, les IPS utilisent trois principales méthodes de détection :

- **Détection basée sur les signatures** : Identification des attaques connues grâce à une base de signatures préétablies.
- **Détection basée sur les anomalies ou le comportement** : Détection d'écarts par rapport au comportement normal du réseau ou du système.
- **Détection par analyse de protocole avec état** : Surveillance approfondie des protocoles de communication en tenant compte du contexte et de l'état des connexions.

1.2.2.1 Détection basée sur les signatures

Les IPS qui reposent sur la détection basée sur les signatures analysent le trafic réseau entrant et sortant en le comparant à une base de données de signatures d'attaques connues. Cette méthode permet d'identifier rapidement des menaces en se référant à des modèles préalablement enregistrés.

Les IPS basés sur les signatures se divisent en deux catégories principales :

- **Signatures orientées vers l'exploitation**
- **Signatures de vulnérabilité**

Bien que la détection basée sur les signatures soit efficace pour identifier des menaces connues, elle peut être limitée face à des attaques nouvelles ou inconnues.

1.2.2.2 Détection statistique basée sur les anomalies ou basée sur le comportement

Les IDS utilisant la détection statistique basée sur les anomalies surveillent le trafic réseau afin d'identifier des incohérences ou des comportements inhabituels. Ils établissent une ligne de base représentant le comportement normal du réseau ou du système. Sur cette base, l'IPS analyse le trafic en temps réel et signale toute activité suspecte s'écartant de ce comportement normal.

Par exemple, la ligne de base peut être définie par une bande passante spécifique ou par un protocole particulier utilisé au sein du réseau. Si l'IPS détecte une augmentation soudaine de la bande passante ou l'utilisation d'un protocole inhabituel, il déclenchera une alarme et pourra bloquer le trafic suspect.

1.2.2.3 Détection basée par l'analyse de protocole avec état

Un IPS, en utilisant une analyse de protocole avec état, détecte les écarts dans l'état d'un protocole de manière similaire à la détection basée sur les anomalies. Il s'appuie sur des profils universels prédéfinis, conformes aux bonnes pratiques établies par les leaders de l'industrie et les fournisseurs.

Par exemple, l'IPS peut surveiller les requêtes et leurs réponses correspondantes. Chaque requête doit engendrer une réponse prévisible. Si une réponse ne correspond pas aux attentes, l'IPS la signale comme suspecte et l'analyse plus en détail.

1.2.3 Composition des systèmes de prévention d'intrusion

Un IPS (Système de Prévention des Intrusions) désigne tout produit ou dispositif conçu pour empêcher des attaquants d'accéder à votre réseau, tels qu'un pare-feu ou un logiciel antivirus.

Les mécanismes de prévention incluent :

- **Correspondance d'adresses** : vérification des adresses IP pour détecter les sources suspectes ;
- **Correspondance de chaîne et de sous-chaîne HTTP** : identification de motifs malveillants ;
- **Correspondance de schémas génériques** : analyse des modèles récurrents utilisés ;
- **Analyse de connexion TCP** : surveillance des sessions TCP pour repérer des anomalies ;
- **Détection d'anomalies dans les paquets** : identification de paquets non conformes ;
- **Détection d'anomalies du trafic** : observation des variations inhabituelles du volume ;
- **Correspondance de ports TCP/UDP** : surveillance des connexions établies .

1.2.4 Types des systèmes de prévention d'intrusion

1.2.4.1 Les Host-based Intrusion Prevention System (HIPS)

Les solutions HIPS (Host-based Intrusion Prevention Systems) peuvent surveiller les systèmes critiques afin de détecter et de prévenir les activités malveillantes en analysant le comportement du code exécuté.

L'un de leurs principaux avantages est leur capacité à détecter les attaques chiffrées, en plus de protéger les données sensibles, notamment celles liées à l'identité personnelle et à l'intégrité des systèmes hôtes.

Les HIPS fonctionnent directement sur un seul appareil et sont souvent déployés en complément d'un IDS ou d'un IPS basé sur le réseau afin d'améliorer la sécurité globale.

1.2.4.2 Les Network Intrusion Prevention System (NIPS)

Les NIPS (Network-based Intrusion Prevention Systems) analysent les paquets de données et surveillent l'activité des protocoles pour identifier et prévenir les activités suspectes ou malveillantes. Ils collectent des données provenant du réseau et des hôtes pour détecter les appareils, systèmes d'exploitation et applications autorisés.

Ils enregistrent également le trafic normal pour repérer les anomalies. Les NIPS (Network-based Intrusion Prevention Systems) atténuent les attaques en limitant l'utilisation de la bande passante,

interrompant les connexions TCP ou rejetant certains paquets. Cependant, ils ont des limites, notamment pour l'analyse du trafic chiffré, la gestion des attaques ciblées et la prise en charge de charges de trafic élevées.

1.2.4.3 Les Wireless Intrusion Prevention System (WIPS)

Un WIPS (Wireless Intrusion Prevention System) peut surveiller un réseau sans fil afin de détecter le trafic ou les activités suspectes en analysant les protocoles de communication et en prenant des mesures pour les bloquer ou les neutraliser.

Un WIPS est généralement implémenté en superposition à l'infrastructure de réseau LAN sans fil existante. Toutefois, il peut également être déployé de manière autonome et appliqué comme une politique de sécurité sans fil au sein des systèmes d'information.

Cette solution IPS permet de prévenir diverses menaces, notamment les points d'accès mal configurés, les attaques par déni de service (DoS (Denial of Service)), les pots de miel, l'usurpation d'adresse MAC (Message Authentication Code), les attaques de l'homme du milieu (MITM (Man in the Middle)), et bien d'autres.

1.2.4.4 Les Kernel Intrusion Prevention System (KIPS)

Les KIPS (Kernel Intrusion Prevention System) sont des systèmes de prévention des intrusions qui fonctionnent directement au niveau du noyau du système d'exploitation. Contrairement aux autres solutions de sécurité qui se concentrent sur la surveillance du réseau ou des applications, les KIPS analysent les appels système, les modifications de mémoire et les interactions entre les processus pour détecter toute activité suspecte ou malveillante.

Ces solutions sont particulièrement efficaces pour identifier des attaques sophistiquées visant l'intégrité du noyau, telles que les rootkits, les escalades de privilèges et les injections de code malveillant.

Conclusion

En analysant les éléments précédents, nous constatons l'importance capitale de la sécurisation des systèmes d'information. Les solutions de détection et de prévention des intrusions sont indispensables pour garantir l'intégrité, la disponibilité et la confidentialité des ressources réseau [1]. En leur absence, un réseau devient vulnérable aux attaques, ce qui peut entraîner sa paralysie et des pertes de données critiques.

Pour assurer une protection efficace, il est essentiel de bien comprendre les différents types d'IDS et d'IPS, ainsi que leurs modes de fonctionnement et leurs domaines d'application respectifs. Dans le chapitre suivant, nous explorerons en détail les diverses solutions existantes, analyserons leurs caractéristiques et procéderons à une sélection adaptée à nos besoins spécifiques.

Chapitre 2

Analyse et choix technique

Introduction

Dans ce chapitre, nous présenterons les différentes solutions de détection et de prévention des intrusions disponibles, en les comparant afin de sélectionner celle qui répond le mieux aux besoins de notre système d'informations. L'objectif principal est d'assurer les principes fondamentaux de la sécurité, notamment la confidentialité, l'intégrité et la disponibilité des données sur les différents serveurs du réseau.

Pour cela, nous nous baserons sur des critères d'évaluation rigoureux afin de transformer notre infrastructure actuelle en un système hautement sécurisé, capable de détecter, prévenir et neutraliser efficacement les menaces potentielles.

2.1 Justifications de la mise en place d'une solution de détection et de prévention des intrusions

Avant de sélectionner une solution adaptée, il est essentiel de se poser certaines questions stratégiques afin de garantir un choix optimal. Parmi les interrogations clés à considérer :

- L'activité de notre structure repose-t-elle en grande partie sur la disponibilité et la sécurité de nos réseaux ?
- Le volume des requêtes sur notre réseau devient-il si important qu'il impacte les performances des serveurs informatiques ?
- Observons-nous une augmentation du trafic réseau, avec l'apparition d'adresses IP inconnues lors de l'analyse des captures de trafic ?

Ces éléments permettent d'évaluer la nécessité d'une solution de détection et de prévention des intrusions, en vue d'optimiser la résilience et la sécurité du système d'information.

2.2 Avantages d'une solution de détection et de prévention des intrusions en entreprise

Les entreprises, quelle que soit leur taille, sont de plus en plus exposées aux cybermenaces. L'intégration d'un système de détection et de prévention des intrusions (IDS/IPS) présente plusieurs avantages stratégiques pour la sécurité des infrastructures informatiques. Parmi les principaux bénéfices, nous pouvons citer :

1. **Détection en temps réel des tentatives d'intrusion**
2. **Journalisation et traçabilité des incidents de sécurité**
3. **Protection proactive du réseau et des services critiques**

2.3 Présentation de quelques solutions de détection et de prévention d'intrusions

2.3.1 Solutions de détection des intrusions (IDS)

Les systèmes de détection d'intrusions (IDS) permettent d'analyser le trafic réseau et les activités suspectes afin de détecter des menaces potentielles. Voici quelques solutions populaires utilisées en entreprise [3] :

- **Snort**

  Snort est l'un des IDS les plus utilisés en entreprise. Il fonctionne en analysant le trafic réseau en temps réel et en appliquant des règles de détection basées sur des signatures d'attaques connues. Il est apprécié pour sa flexibilité et sa large communauté, facilitant son adoption dans des environnements d'entreprise.

- **Suricata**

  Suricata est un IDS/IPS avancé qui offre des performances optimisées grâce à l'inspection approfondie des paquets (DPI) et la prise en charge native des protocoles courants. Il permet de détecter et prévenir les menaces en s'appuyant sur des signatures et des règles de corrélation.

- **Prelude IDS**

  Prelude IDS est une solution modulaire qui centralise la détection des intrusions en intégrant plusieurs sources d'informations, y compris des logs, des pare-feux et des sondes réseau.

- **OSSIM (Open Source Security Information Management)**

  Développé par AlienVault, OSSIM est une plateforme de gestion des événements de sécurité (SIEM) qui intègre plusieurs outils IDS, notamment Snort et Suricata. Il permet d'unifier la détection, la corrélation et la gestion des incidents de cybersécurité dans un environnement d'entreprise. OSSIM est souvent utilisé par les entreprises cherchant à centraliser la surveillance de leur infrastructure IT.

- **Zeek (anciennement Bro IDS)**

  Zeek est un IDS réseau qui se distingue par son approche analytique. Plutôt que de fonctionner uniquement sur des signatures de menaces, il permet une analyse comportementale des flux réseau afin de détecter des anomalies en comparant le trafic réel à un modèle de référence.

- **Sagan**

  Contrairement aux autres IDS qui se concentrent sur l'analyse du trafic réseau, Sagan est un moteur d'analyse de journaux conçu pour les centres d'opérations de sécurité (SOC).

2.3.2 Présentation de quelques solutions de prévention d'intrusions

- **Fail2ban**

  Fail2ban est un logiciel de sécurité open source conçu pour protéger les serveurs contre les attaques par force brute et autres comportements malveillants. Il surveille les fichiers de journalisation des services installés sur la machine, détecte les tentatives de connexion échouées répétées ou les activités suspectes, puis bannit automatiquement les adresses IP incriminées en configurant des règles de pare-feu via des outils tels qu'`iptables`.

- **Suricata**

  Suricata est un moteur de détection et de prévention des intrusions (IDS/IPS) open source développé par l'Open Information Security Foundation (OISF). En mode IPS, Suricata peut non seulement détecter les activités malveillantes, mais aussi les prévenir en bloquant le trafic suspect conformément aux règles définies. [9]

2.4 Étude comparative des systèmes de détection et de prévention d'intrusions

Dans le tableau ci-dessous, nous avons opté pour une analyse qualitative des différentes solutions IDS et IPS. Les caractéristiques de chaque solution sont évaluées selon une échelle qualitative comprenant les niveaux suivants : Très faible, Faible, Moyen, Élevé et Très élevé. Dans cette échelle, "Très faible" représente le niveau le plus bas, tandis que "Très élevé" indique le niveau le plus élevé. Cette approche permet de comparer les solutions de manière intuitive et compréhensible, facilitant ainsi la prise de décision en fonction des besoins spécifiques.

Solution IDS	Type de détection	Performance	Efficacité	Facilité d'utilisation	Coût	Cas d'utilisation	Faux positifs
Snort	Basée sur des signatures	Moyen	Moyen	Élevée	Faible	Détection simple	Élevé
Suricata	Basée sur des signatures et analyse approfondie	Très élevée	Élevée	Moyenne	Moyen	Réseaux à haut débit nécessitant une analyse en temps réel	Moyen
Zeek	Analyse comportementale et journalisation détaillée	Élevée	Très élevée	Faible	Élevé	Analyse détaillée et post-incident	Faible
Prelude IDS	Hybride (signatures et anomalies)	Moyen	Élevée	Moyenne	Élevé	Environnements hétérogènes nécessitant une corrélation d'événements	Moyen

Solution IDS	Type de détection	Performance	Efficacité	Facilité d'utilisation	Coût	Cas d'utilisation	Faux positifs
OSSIM	Intégration de multiples outils IDS	Variable selon les outils intégrés	Variable selon les outils intégrés	Moyenne	Très élevé	Gestion unifiée des événements de sécurité	Variable selon les outils intégrés
Sagan	Basée sur des signatures (analyse de logs)	Élevée	Moyenne	Élevée	Faible	Analyse en temps réel des journaux système	Élevé
Fail2ban	Basée sur des signatures (analyse de logs)	Élevée	Moyenne	Très élevée	Faible	Protection contre les attaques par force brute	Moyen

TABLE 2.1 : Tableau de l'analyse qualitative des outils de détection et de prévention d'intrusions

Sur la base de cette comparaison, notre choix se porte sur **Suricata** en raison de ses performances élevées, de sa capacité à analyser le trafic en profondeur (DPI) et de son architecture multi-thread optimisée. Contrairement à d'autres solutions, Suricata offre une détection des intrusions en temps réel avec un support natif des formats modernes comme JSON, facilitant ainsi l'intégration avec des outils de surveillance et de gestion des incidents. De plus, sa compatibilité avec les règles Snort et son mode IPS permettent d'assurer une protection proactive et efficace du réseau.

2.5 Paramètres à prendre en compte pour le choix de notre solution

Le processus d'analyse d'une solution de détection et de prévention est complexe, et faire des erreurs de choix peut entraîner une perte de temps, d'argent et compliquer votre infrastructure. Pour cette raison, voici une liste de contrôle des principaux éléments à prendre en compte pour effectuer une analyse correcte :

- Prendre connaissance des applications que l'outil de supervision réseau prend en charge afin de vérifier sa compatibilité avec les fabricants de votre solution ;
- Se renseigner sur le système de licence avant de choisir un outil ;
- S'informer sur la configuration de la solution et sa gestion ;
- Vérifier si la solution prend en compte la création de rapports et la journalisation ;
- Vérifier si la solution affiche et fournit les informations nécessaires de façon lisible sur toutes les intrusions.

Il est à noter que les critères de choix ci-dessus dépendent des fonctions de l'organisation et de ses objectifs.

2.6 Choix de la solution SURICATA



FIGURE 2.1 : Logo de Suricata

Le choix d'un outil de détection et de prévention des intrusions dépend essentiellement des objectifs et des attentes de l'entreprise. Après une analyse approfondie des différentes solutions présentées dans le tableau comparatif, nous avons décidé d'opter pour Suricata. Ce choix s'explique par plusieurs facteurs clés.

Nous avons souhaité expérimenter une solution différente de celle utilisée par l'entreprise JENY SAS, où nous avons effectué notre stage académique. Ce choix stratégique nous permet de diversifier nos compétences et d'explorer une alternative plus flexible et plus moderne.

Suricata s'est révélé être une solution adaptée à notre projet, notamment en raison de ses fonctionnalités avancées et de sa nature open source, qui le rend accessible et évolutif. Il se distingue par sa capacité à remplir trois rôles essentiels en cybersécurité : détection d'intrusions (IDS), prévention d'intrusions (IPS) et supervision de la sécurité réseau (NSM).

Contrairement à Snort, qui fonctionne sur un seul thread, Suricata est conçu pour tirer parti des processeurs multi-cœurs grâce à son architecture multi-threadée. Cette caractéristique lui permet de gérer efficacement des environnements à haut trafic, offrant ainsi de meilleures performances sur du matériel moderne. [8]

Conclusion

Le choix d'un outil de détection et de prévention des intrusions est une étape cruciale pour assurer la sécurité d'un réseau. Pour ce faire, les entreprises doivent se poser un certain nombre de questions essentielles afin d'évaluer la solution la mieux adaptée à leurs besoins. Ce chapitre a permis de mettre en lumière les principaux critères de sélection qui facilitent ce processus décisionnel.

Il est important de souligner que le choix d'un tel outil dépend non seulement des fonctionnalités offertes par la solution, mais également de la taille et de la complexité du réseau à protéger. Une infrastructure de grande envergure nécessitera une solution plus robuste et évolutive, tandis qu'un réseau plus modeste pourra s'appuyer sur une solution plus légère mais tout aussi efficace.

Ainsi, une analyse approfondie des besoins, des contraintes techniques et des objectifs de l'organisation est indispensable avant toute prise de décision. Ce travail préparatoire garantit une protection optimale contre les menaces et permet d'intégrer une solution de sécurité performante et adaptée à l'environnement réseau concerné.

Chapitre 3

Présentation de la solution, conception et résultats des tests

Introduction

Un système d'information (SI) est un ensemble organisé de ressources permettant de collecter, stocker, traiter et distribuer de l'information. La protection de ces informations est souvent assurée par des solutions de détection et de prévention d'intrusions.

Dans ce chapitre, nous allons tout d'abord présenter notre solution **SURICATA**. Ensuite, nous détaillerons sa conception en précisant l'environnement de travail mis en place. Enfin, nous réaliserons une série de tests afin de vérifier le bon fonctionnement de notre solution.

3.1 Présentation de SURICATA

Suricata est le principal moteur de détection de menaces open source indépendant. En combinant la détection d'intrusion (**IDS**), la prévention d'intrusion (**IPS**), la surveillance de la sécurité du réseau (**NSM**) et le traitement **PCAP**, Suricata peut rapidement identifier, arrêter et évaluer même les attaques les plus sophistiquées.

3.1.1 Modes de fonctionnement de SURICATA

L'un des principaux atouts de Suricata réside dans son architecture multithread, qui optimise ses performances. Ses threads fonctionnent selon trois modes principaux, dont l'un se divise en deux sous-modes. [5]

3.1.1.1 Mode Workers

Le mode d'exécution Workers est le plus performant. Dans ce mode, la carte réseau ou le pilote répartit efficacement les paquets entre les différents threads de traitement de Suricata. Chaque thread prend en charge l'intégralité du pipeline de traitement des paquets, garantissant ainsi une analyse complète et optimisée. [5]

3.1.1.2 Mode Autofp

Le mode Autofp est utilisé pour le traitement des fichiers PCAP ainsi que dans certaines configurations IPS, comme NFQ. Il fonctionne avec un ou plusieurs threads de capture, chargés d'intercepter les paquets et d'en effectuer le décodage avant de les transmettre aux threads de traitement du flux. [5]

3.1.1.3 Mode single

Le mode d'exécution Single fonctionne de manière similaire au mode Workers, à la différence qu'il ne repose que sur un seul thread pour le traitement des paquets. Cette configuration limite les performances globales du système, mais elle est particulièrement utile dans un environnement de développement ou de test, où l'analyse des processus internes et le débogage du moteur de détection sont prioritaires par rapport à l'efficacité du traitement des paquets en parallèle. [5]

3.2 Conception de la solution

3.2.1 Présentation de l'architecture réseau de JENY SAS

L'architecture réseau désigne l'infrastructure informatique mise en place pour assurer la connectivité entre les utilisateurs, les équipements et les applications.

À **JENY SAS**, cette architecture repose sur plusieurs composants essentiels, notamment :

- Des **serveurs Web** pour l'hébergement des applications et des services en ligne.
- Un **serveur de messagerie** pour la gestion des courriels internes et externes.
- Un **serveur DNS** pour la résolution des noms de domaine.
- Un **serveur NAS** (Network Attached Storage) pour le stockage et le partage des fichiers.
- Un **serveur d'authentification** garantissant un accès sécurisé aux ressources du réseau.
- Deux **pare-feu** assurant la protection du réseau contre les menaces extérieures.
- Un **routeur** pour la gestion et l'acheminement du trafic réseau.
- Une infrastructure **cloud** pour le stockage et le traitement des données dématérialisées.
- Des **imprimantes** connectées pour les besoins bureautiques.
- Un parc informatique composé de **ordinateurs portables (laptops)** et **ordinateurs de bureau (desktops)**.

À **JENY SAS**, l'architecture réseau est représentée dans le schéma ci-dessous (fig 3.1) :

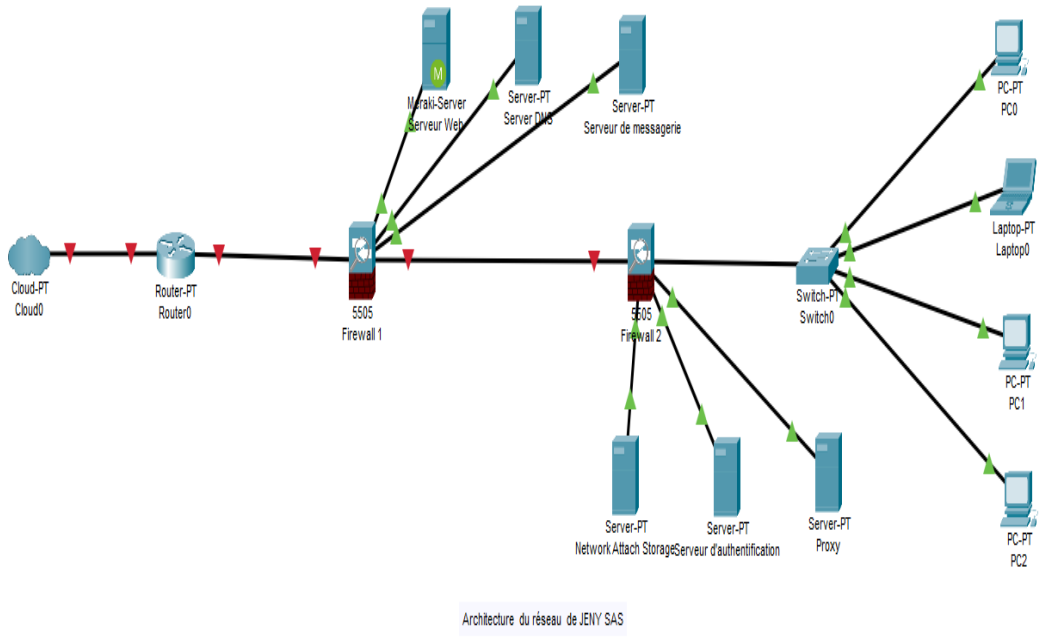


FIGURE 3.1 : Architecture réseau de JENY SAS

3.2.2 Présentation de l'espace de travail

La réalisation de ce projet de stage demande l'utilisation de la solution de virtualisation **VirtualBox**, sur laquelle nous installons une machine virtuelle fonctionnant sous **Debian 10.7**.

Caractéristique	Valeur
Nom de la machine	LizVdebVm1
Nom d'hôte	debianliz
RAM	2024 Mo
Disque dur	28 Go
Carte réseau	Accès pont

TABLE 3.1 : Configuration de la machine virtuelle

3.2.3 Installation et configuration de Suricata

Nous configurons Suricata de manière à ce qu'il génère des alertes à chaque tentative d'intrusion détectée sur le réseau. Pour ce faire, il est essentiel de s'assurer que tous les paquets requis sont correctement installés afin de garantir un fonctionnement optimal du système de détection d'intrusion. [7]

3.2.3.1 Mise à jour et installation des prérequis

Avant de procéder à la configuration de Suricata, il est primordial d'effectuer une mise à jour du système et d'installer l'ensemble des paquets nécessaires à son bon fonctionnement. Ces dépendances sont essentielles pour garantir une installation optimale et une exécution efficace de l'outil.

3.2.3.2 Configuration de Suricata

Après la configuration de l'ensemble des dépendances requises, l'installation de Suricata s'effectue à l'aide de la commande suivante :

```
sudo apt-get install suricata
```

Une fois l'installation terminée, il est nécessaire de configurer Suricata en modifiant le fichier de configuration principal, **suricata.yaml**. Ce fichier contient l'ensemble des paramètres essentiels pour le bon fonctionnement de l'outil.[4]

Nous procédons à la personnalisation de cette configuration en renseignant plusieurs informations clés, notamment **l'adresse du réseau à surveiller**, **l'interface réseau de la machine utilisée**, **la taille maximale des fichiers analysés** et **l'activation des fonctionnalités essentielles en fonction des besoins spécifiques du système**.

Ayant apporté ces modifications, il convient de vérifier l'état du service Suricata afin de s'assurer qu'il est bien en cours d'exécution. Pour cela, on utilise la commande suivante :

```
systemctl status suricata
```

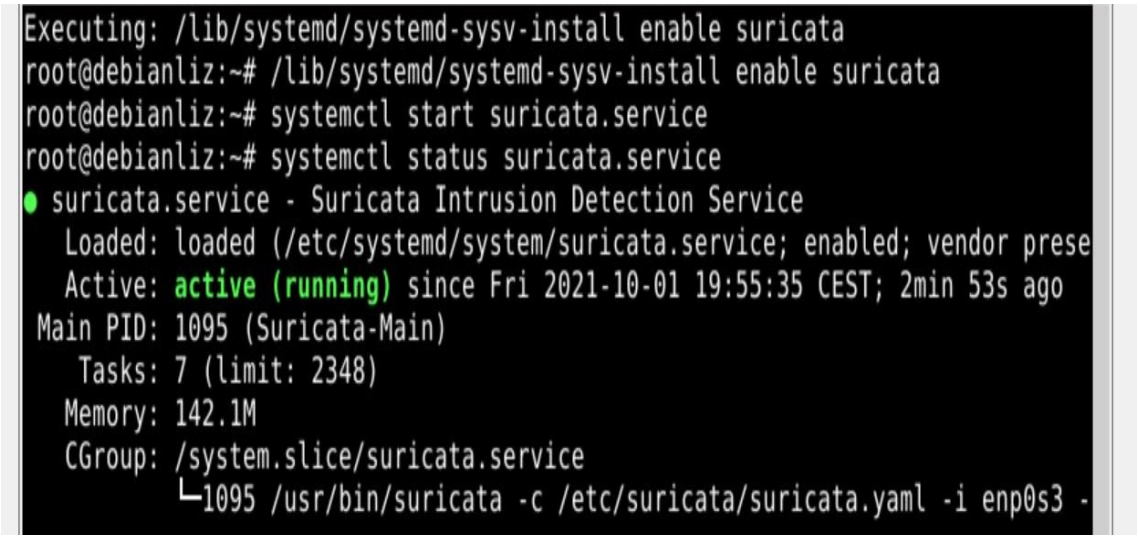


FIGURE 3.2 : Vérification du statut de Suricata

Après exécution de la commande précédente, nous observons que le statut du service est affiché comme **active** (fig 3.2). Cela signifie que **Suricata est en cours d'exécution et pleinement opérationnel**. Il est désormais prêt à analyser le trafic réseau et à générer des alertes en cas d'intrusion .

Mise à jour des règles de Suricata

Pour assurer une protection efficace, il est essentiel de maintenir les règles de détection à jour. Les règles sont stockées dans le répertoire suivant :

```
/etc/suricata/rules
```

Nous appliquons les règles mises à jour en nous basant sur les configurations définies dans le fichier **/etc/oinkmaster.conf**.

```
sudo oinkmaster -C /etc/oinkmaster.conf -o /etc/suricata/rules
```

Cette commande permet de télécharger les nouvelles règles, de les comparer aux anciennes et de les appliquer automatiquement à notre configuration.

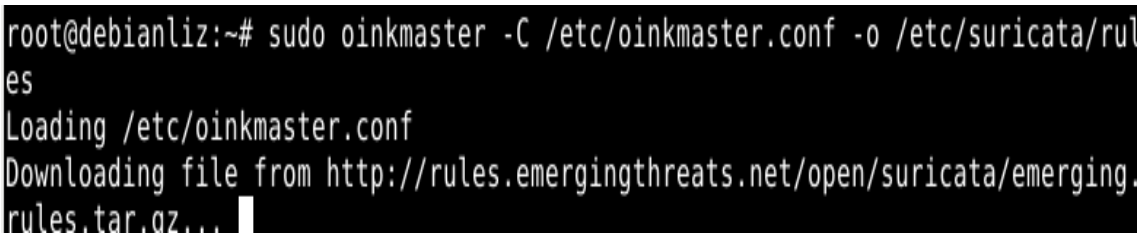


FIGURE 3.3 : Récupération des règles

Après la récupération des nouvelles règles (fig 3.3), **Suricata bénéficie d'une base de signatures plus étendue**, renforçant ainsi ses capacités de détection des intrusions et d'analyse du trafic réseau.

Vérification du bon fonctionnement de Suricata :

Pour s'assurer que les modifications ont bien été prises en compte, nous redémarrons le service Suricata et vérifions son statut.

```
sudo systemctl restart suricata
```

Une fois le redémarrage effectué, nous vérifions si le service est toujours actif et en cours d'exécution :

```
sudo systemctl status suricata
```

Si le service est indiqué comme **active (running)**, cela signifie que Suricata fonctionne correctement avec les nouvelles règles appliquées (fig 3.4).

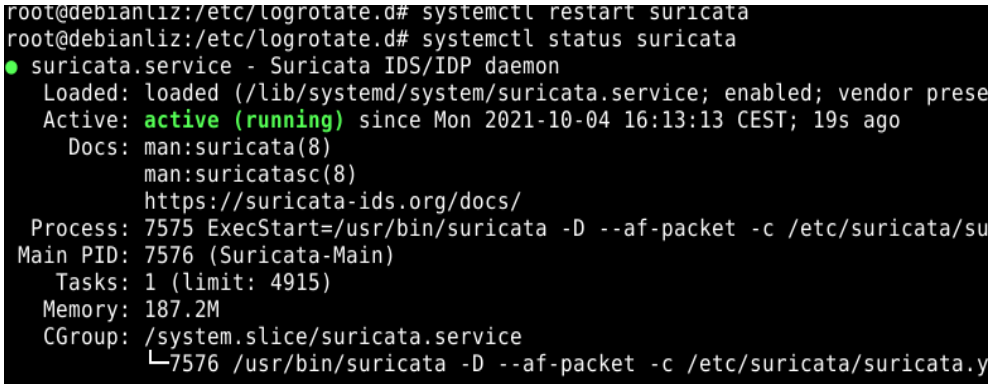


FIGURE 3.4 : Statut de suricata après les configurations

Après avoir vérifié que **Suricata fonctionne parfaitement**, nous pouvons poursuivre la mise en

place de notre solution.

3.2.3.3 Positionnement de Suricata dans le réseau

Dans une architecture réseau où Suricata est utilisé comme un système de détection et prévention des intrusions principalement (**IPS**), il est recommandé de le positionner entre le **routeur** et le **premier pare-feu** (fig 3.5). Ce placement stratégique permet à Suricata d'analyser et de bloquer les menaces avant qu'elles n'atteignent les pare-feux, réduisant ainsi leur charge de travail et optimisant les performances globales du réseau. En filtrant le trafic en amont, Suricata empêche les attaques de pénétrer plus profondément dans l'infrastructure, garantissant une protection proactive et une meilleure visibilité sur les tentatives d'intrusion. Cette approche renforce la sécurité globale du réseau en stoppant les menaces à la source, avant qu'elles n'affectent les équipements critiques.

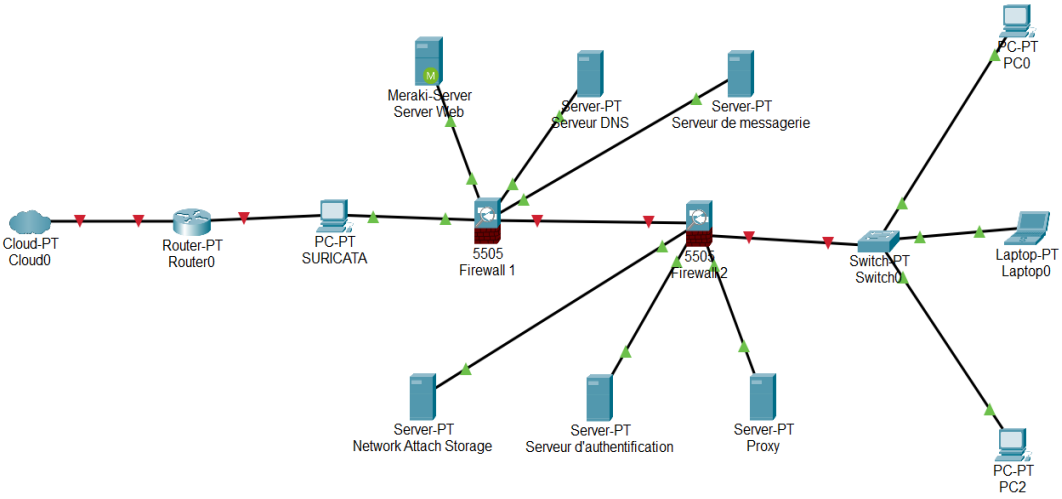


FIGURE 3.5 : Architecture réseau de JENY SAS après l'installation de Suricata

Suricata ne propose ni une interface de visualisation ergonomique ni une gestion simplifiée des alertes. De ce fait, il est nécessaire d'intégrer des outils complémentaires afin de construire une solution complète et performante.

3.2.4 Choix d'une interface web et d'un analyseur de journaux

Afin de visualiser efficacement les événements réseau, nous choisissons :

- **Snorby** : interface graphique pour afficher et analyser les alertes ;
- **Barnyard2** : outil pour analyser et convertir les journaux de Suricata afin de les intégrer à Snorby.

Ces outils assurent une **surveillance avancée et une visualisation des menaces**. Nous procédons à leur installation et configuration.

3.2.5 Présentation et configuration de Snorby

Snorby est une interface web open-source pour l'analyse et la visualisation des logs générés par les systèmes IDS, comme Snort et Suricata. Développé en Ruby on Rails, il offre une interface intuitive pour surveiller les événements de sécurité réseau.

Les objectifs principaux de Snorby sont :

- **Simplicité** : interface ergonomique ;
- **Organisation** : structuration des alertes ;
- **Puissance** : outils d'analyse performants.

3.2.5.1 Installation des dépendances

L'installation de Snorby nécessite l'installation de MySQL pour le stockage des données et la configuration de l'utilisateur dédié. Après la configuration, l'outil `bundler` est installé pour gérer les dépendances Ruby.

```
gem install bundler
```

Puis, les dépendances de Snorby sont installées avec :

```
bundle install
```

Pour accéder à l'interface, nous ouvrons un navigateur à l'URL suivante : `http://localhost:3000`



FIGURE 3.6 : Interface d'authentification de Snorby

Une fois authentifié, le tableau de bord offre une vue claire des alertes de sécurité et des statistiques en temps réel pour faciliter l'analyse des événements réseau.

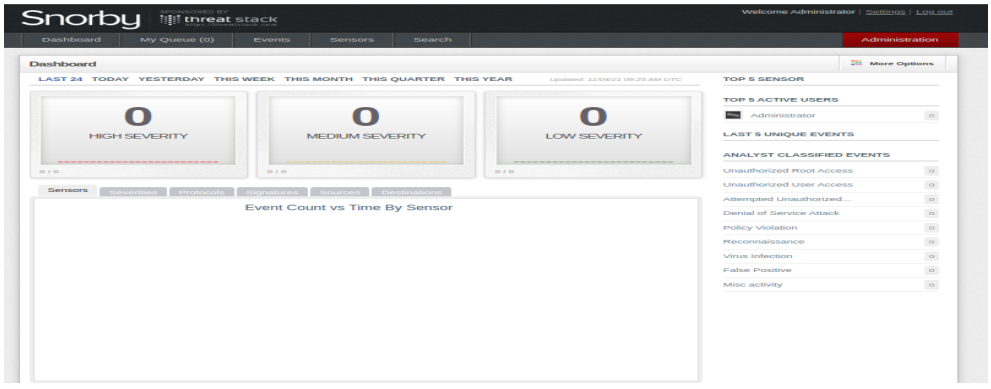


FIGURE 3.7 : Interface graphique de Snorby

Nous constatons que des intrusions ont été détectées par Snorby et sont affichées sur son interface graphique.

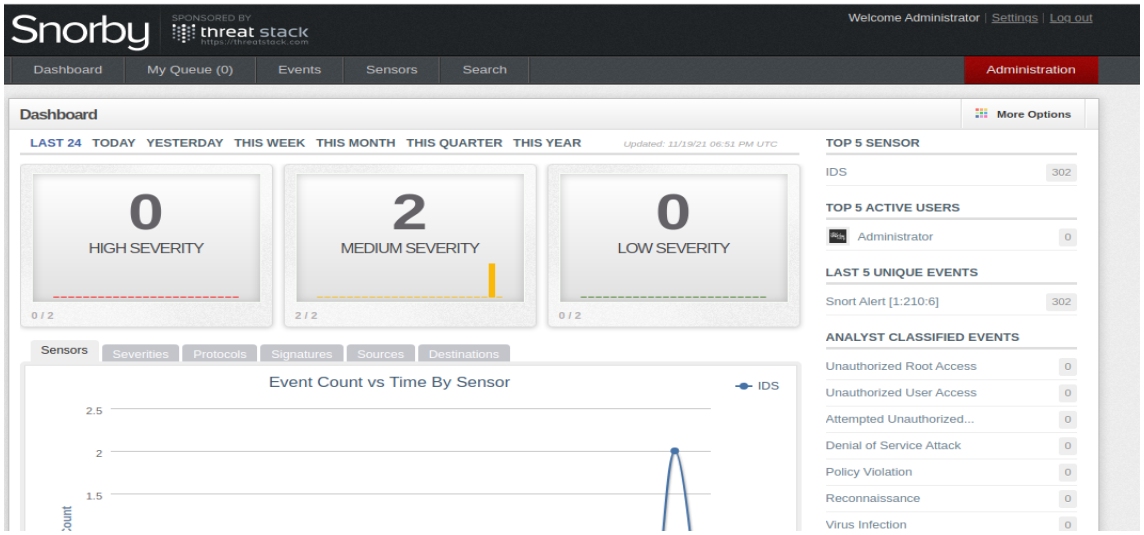


FIGURE 3.8 : Détection des attaques reçues

Voici quelques détails sur chaque intrusion détectée :

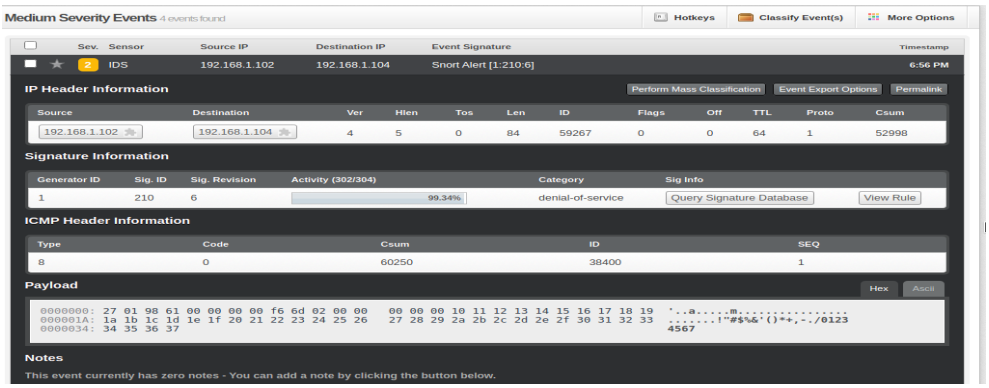


FIGURE 3.9 : Détails sur les attaques détectées

Snorby propose des représentations graphiques permettant d'obtenir des informations détaillées sur les capteurs et d'évaluer la gravité des attaques détectées.

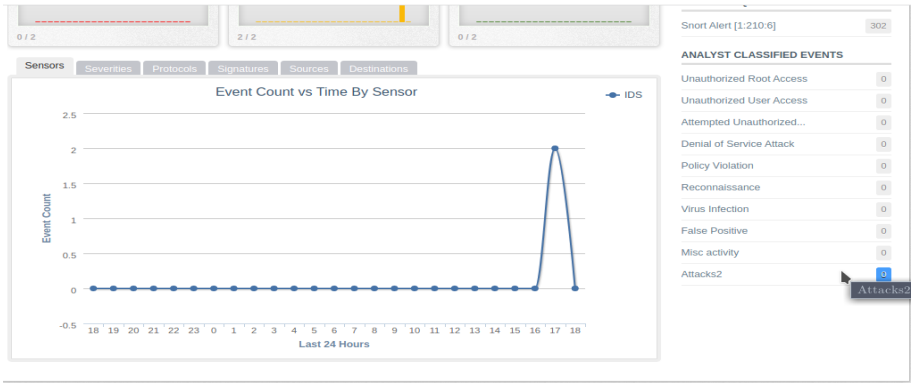


FIGURE 3.10 : Courbe des capteurs

Une intrusion peut être classée en fonction de son niveau de sévérité, qui peut être faible, modérée ou élevée. La sévérité représente l'ampleur de l'impact qu'une intrusion peut avoir sur le réseau et l'ensemble des ressources du système d'information. Une intrusion de faible sévérité peut ne causer que des perturbations mineures, tandis qu'une intrusion de sévérité modérée peut compromettre certaines fonctionnalités du système. En revanche, une intrusion de grande sévérité peut entraîner des conséquences critiques, telles qu'une interruption complète des services, une exfiltration de données sensibles ou une compromission totale de l'infrastructure informatique.

L'évaluation précise de la sévérité d'une attaque est donc essentielle pour prioriser les actions de remédiation et renforcer la sécurité du système.

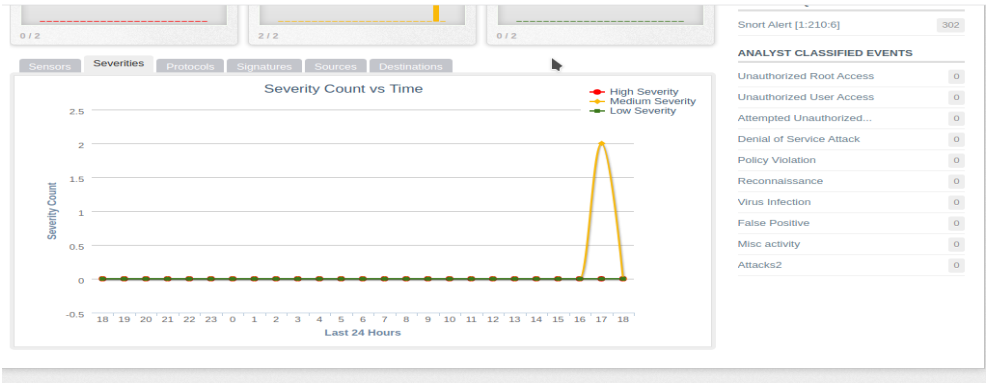


FIGURE 3.11 : Courbe des sévérités

La courbe a un sens de variation qui suit exactement les sévérités des intrusions détectées.
Une vue d'ensemble des intrusions détectées par Snorby :

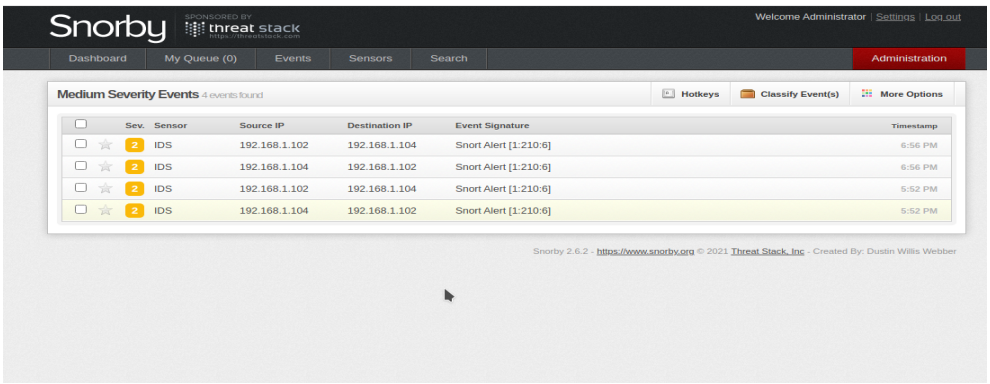


FIGURE 3.12 : Vue d'ensemble des attaques

Nous avons ici la liste des événements détectés depuis l'installation de Snorby et enregistrés dans la base.

3.2.6 Présentation et configuration de Barnyard2

Barnyard2 est un interpréteur open-source permettant de traiter les fichiers binaires `unified2` générés par Suricata. Il permet à Suricata d'écrire sur le disque tout en déléguant l'analyse des données, afin de ne pas affecter les performances du système.

Nous utilisons le mode continu avec mise en signet, en spécifiant le fichier `suricata.waldo`

dans le fichier de configuration `barnyard2.conf` pour garantir une surveillance continue sans perte de données. Après l'installation, nous vérifions le bon fonctionnement de Barnyard2.



FIGURE 3.13 : Fonctionnement de Barnyard2

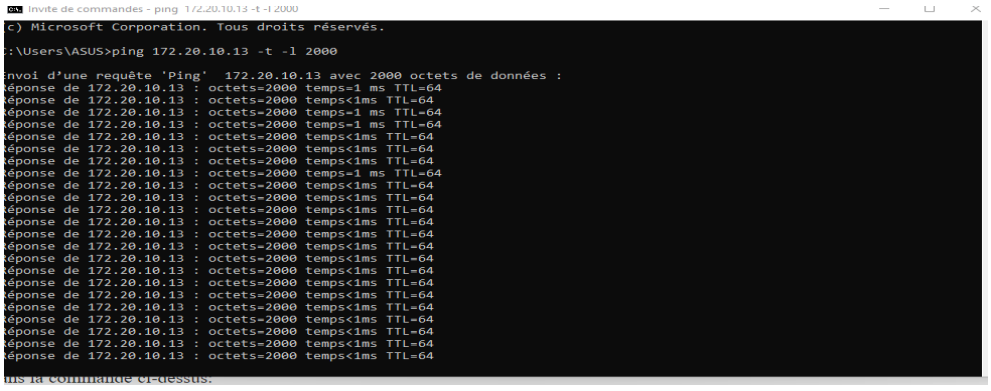
La vérification montre que Barnyard2 fonctionne correctement (fig 3.13).

3.2.7 Tests et vérifications

Étant donné que SURICATA est à la fois un IDS et un IPS, nous testons ses fonctions de détection et de prévention séparément.

3.2.7.1 Test de SURICATA dans sa fonction d'IDS

Nous testons une attaque par déni de service (`ping flood`) en envoyant un grand nombre de requêtes ICMP à une machine cible. Nous ajoutons une règle Suricata dans `lizette.rules` pour détecter cette attaque.


Invite de commandes - ping 172.20.10.13 -t -l 2000
(c) Microsoft Corporation. Tous droits réservés.
C:\Users\ASUS>ping 172.20.10.13 -t -l 2000
Envoi d'une requête 'Ping' 172.20.10.13 avec 2000 octets de données :
Réponse de 172.20.10.13 : octets=2000 temps=1 ms TTL=64
Réponse de 172.20.10.13 : octets=2000 temps<1ms TTL=64
Réponse de 172.20.10.13 : octets=2000 temps=1 ms TTL=64
Réponse de 172.20.10.13 : octets=2000 temps=1 ms TTL=64
Réponse de 172.20.10.13 : octets=2000 temps<1ms TTL=64
Réponse de 172.20.10.13 : octets=2000 temps<1ms TTL=64
Réponse de 172.20.10.13 : octets=2000 temps<1ms TTL=64
Réponse de 172.20.10.13 : octets=2000 temps=1 ms TTL=64
Réponse de 172.20.10.13 : octets=2000 temps<1

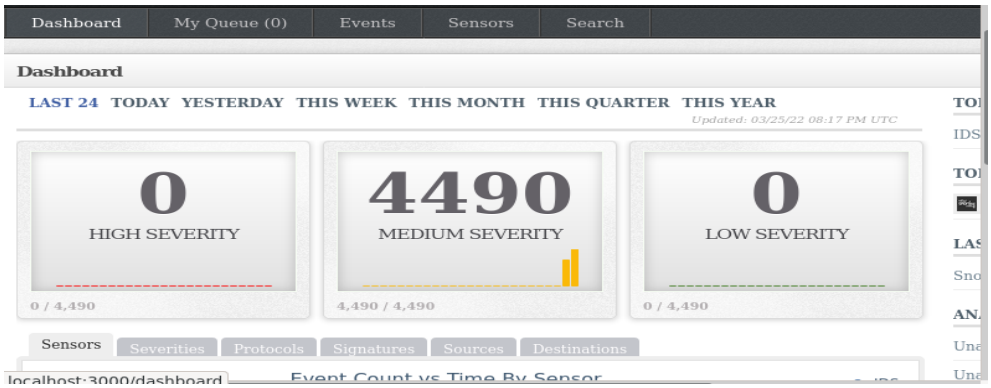


FIGURE 3.15 : Capture du tableau de bord pendant l'attaque ping flood

Nous observons que Suricata a détecté une intrusion de type attaque par déni de service (Denial-of-Service). Ces intrusions ont été identifiées et classées dans la catégorie de sévérité moyenne.

La réponse à cette intrusion relève des capacités de détection d'intrusion (IPS) de Suricata.

3.2.7.2 Test de Suricata dans sa fonction d'IPS

Il s'agit de configurer Suricata dans sa fonction de Prévention d'Intrusion (IPS) et de lui spécifier ensuite l'action à entreprendre dès qu'il détecte une anomalie. Dans ce cas, nous travaillons sur une intrusion interne : le téléchargement de fichiers malveillants, pouvant entraîner de graves conséquences. Nous rédigeons donc une nouvelle règle, en précisant que l'action à prendre est de bloquer (drop) tout téléchargement suspect dans le réseau.

Pour ce faire, nous utilisons le site **testmyids** et tentons de télécharger son fichier `index.html` depuis notre machine.

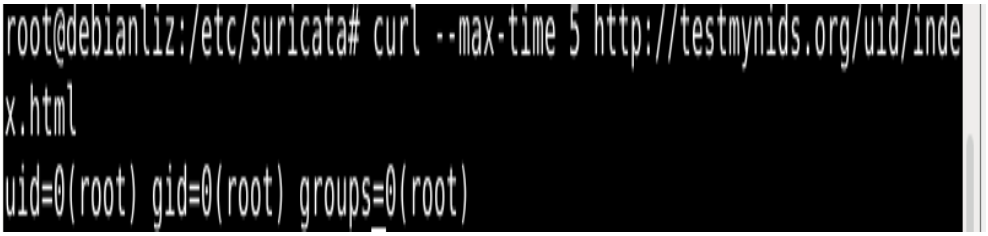


FIGURE 3.16 : Capture du téléchargement du site compromis

En sortie, nous obtenons une réponse indiquant un échec du téléchargement, ce qui confirme que l'opération n'a pas été menée à bien.

Nous procédons également à la vérification du fichier `fast.log` de Suricata pour nous assurer que l'événement a bien été enregistré.

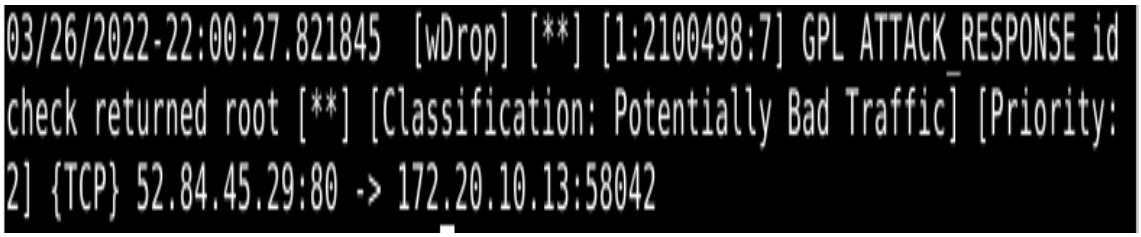


FIGURE 3.17 : Capture de l'enregistrement du blocage

L'intrusion est correctement bloquée et journalisée dans les logs de Suricata (fig 3.17). L'interface Snorby montre également une augmentation des intrusions répertoriées, confirmant que l'incident a été détecté et signalé efficacement.

3.2.8 Évolution de la sécurité du réseau de JENY SAS après l'intégration de Suricata

L'installation de Suricata a renforcé la sécurité du réseau de JENY SAS, apportant des améliorations notables :

- **Surveillance en temps réel :** Détection proactive des anomalies et intrusions.
- **Détection et blocage des attaques :** Fonctionnement en mode IPS pour bloquer automatiquement les attaques.
- **Réduction du risque d'intrusion :** Mise en place de règles de filtrage rigoureuses pour couvrir les vulnérabilités spécifiques.
- **Amélioration de la gestion des alertes :** Utilisation de l'interface Snorby pour une gestion plus efficace des alertes.
- **Consolidation de la sécurité du système d'information :** Renforcement de la confiance des employés, partenaires et clients.

En résumé, Suricata améliore significativement la sécurité du réseau de JENY SAS, avec une détection rapide, un blocage des attaques et une gestion centralisée des alertes.

Conclusion

L'utilisation d'un outil de détection et de prévention des intrusions présente des avantages considérables pour les entreprises et les organisations. En effet, cela leur permet d'obtenir une vue d'ensemble précise de l'état de leurs systèmes et réseaux, ce qui est essentiel pour une gestion proactive de la sécurité. De plus, l'implémentation de telles solutions contribue non seulement à la sécurisation des infrastructures, mais aussi à l'augmentation du chiffre d'affaires en renforçant la confiance des clients grâce à la garantie d'une protection optimale.

La mise en place de la solution Suricata, accompagnée des outils nécessaires pour en faciliter l'utilisation, a été réalisée avec succès. Les tests effectués ont démontré que la solution fonctionne efficacement, détectant et bloquant les menaces de manière fiable, conformément aux attentes définies lors de l'implémentation.

Conclusion Générale et Perspectives

3.3 Conclusion

Ce travail s'inscrit dans le cadre de la mise en place d'un système de détection et de prévention des intrusions au sein de l'infrastructure de JENY SAS, fournisseur d'accès à Internet et gestionnaire du domaine national `.bj`. Pour répondre aux besoins croissants en matière de sécurité du système d'information, nous installons et configurons Suricata, une solution open source légère et performante, capable de détecter les intrusions, prévenir les attaques et surveiller le trafic réseau.

L'installation s'accompagne d'un ensemble de configurations adaptées au contexte de l'entreprise, notamment le choix de l'interface réseau, les paramètres d'analyse des paquets, et la gestion des alertes. Pour faciliter la lecture et l'analyse des événements de sécurité générés par Suricata, nous intégrons également la plateforme Snorby. Cette interface web intuitive permet de visualiser en temps réel les données collectées, de filtrer les événements par catégories, et d'effectuer un suivi précis des incidents.

Des tests d'attaque simulée sont réalisés à partir d'une machine externe afin de vérifier l'efficacité de la solution en place. Les résultats obtenus permettent de détecter plusieurs types de comportements suspects, attestant de la capacité du système à renforcer la sécurité de l'environnement informatique de l'entreprise.

À l'issue de cette implémentation, quelques pistes d'amélioration sont identifiées. Il serait utile de développer des règles personnalisées afin de réduire le taux de fausses alertes. Par ailleurs, la création d'une application dédiée pourrait offrir aux administrateurs un moyen plus ergonomique de gérer Suricata, en dehors de la ligne de commande.

Ainsi, ce projet démontre l'intérêt et la faisabilité d'un système de détection et de prévention des intrusions accessible, adaptable et efficace pour renforcer la protection des données stratégiques d'une entreprise comme JENY SAS.

Bibliographie

[1] L. Bloch and C. Wolfhugel. *Sécurité Informatique : Principes et Méthodes*. Éditions Eyrolles, 2007.

[2] I. Poulmanogo. Rapport de recherche pour le cours ift6271- sécurité informatique. *Les systemes de detection d'intrusion*, 2018.

Webographie

[3] Dementium. meilleurs outils de systemes de detection. https://dementium2.com/administrateur-net/9-meilleurs-outils-de-systemes-de-detection-d/, consulté le 08 Aout 2021.

[4] Blog eldernode. setup and configure suricata on debian. https://blog.eldernode.com/setup-and-configure-suricata-on-debian/, consulté le 25 Juin 2021.

[5] Readthedocs. runmodes suricata. https://suricata.readthedocs.io/en/suricata-6.0.0/performance/runmodes.html, consulté le 08 Aout 2021.

[6] Researchgate. Evolution des systemes de detection d'intrusions. https://www.researchgate.net/figure/Evolution-des-Systemes-de-Detection-dIntrusion_fig4_383200555, consulté le 20 Mai 2022.

[7] Net security. installation-dun-nids-suricata. https://net-security.fr/security/installation-dun-nids-suricata/, consulté le 25 Mars 2021.

[8] stamus. Suricata vs snort. https://www.stamus-networks.com/suricata-vs-snort, consulté le 20 Mai 2022.

[9] Forum suricata. use suricata ids as ips on centos. https://forum.suricata.io/t/use-suricata-ids-as-ips-on-centos-8/584/9, consulté le 20 Mars 2021.

Table des matières

Dédicace ii

Remerciements iii

Résumé iv

. iv

Abstract v

. v

Table des figures vi

Liste des tableaux vii

Liste des acronymes viii

Glossaire 1

Introduction 2

1 Revue de littérature 4

Introduction 4

1.1 Les systèmes de détection d'intrusions IDS 4

1.1.1 Historique et définition des systèmes de détection d'intrusion 4

1.1.1.1 Historique des systèmes de détection d'intrusions 4

1.1.1.2 Définition des systèmes de détection d'intrusions 5

1.1.2 Fonctionnement des systèmes de détection d'intrusions IDS 5

1.1.2.1 Détection basée sur les signatures ou basée sur les connaissances . . . 6

1.1.2.2 Détection basée sur les anomalies ou basée sur le comportement . . . 6

1.1.2.3 Détection basée sur la réputation 6

1.1.3 Fonction des systèmes de détection d'intrusions IDS 6

1.1.4 Composition des systèmes de détection d'intrusions IDS 7

1.1.4.1 La couche surveillance du système d'information 7

1.1.4.2 La couche de monitoring 7

1.1.4.3 La couche de décision 8

1.1.5 Types des systèmes de détection d'intrusions 8

1.1.5.1 Les Host Intrusion Detection System (HIDS) 8

1.1.5.2 Les Network Intrusion Detection System (NIDS) 8

1.1.5.3 Les IDS hybrides 8

1.2 Les systèmes de prévention d'intrusions IPS . . . 8
1.2.1 Définition d'un système de prévention d'intrusion . . . 8
1.2.2 Fonctionnement des systèmes de prévention d'intrusion . . . 9
1.2.2.1 Détection basée sur les signatures . . . 9
1.2.2.2 Détection statistique basée sur les anomalies ou basée sur le comportement . . . 9
1.2.2.3 Détection basée par l'analyse de protocole avec état . . . 10
1.2.3 Composition des systèmes de prévention d'intrusion . . . 10
1.2.4 Types des systèmes de prévention d'intrusion . . . 10
1.2.4.1 Les Host-based Intrusion Prevention System (HIPS) . . . 10
1.2.4.2 Les Network Intrusion Prevention System (NIPS) . . . 10
1.2.4.3 Les Wireless Intrusion Prevention System (WIPS) . . . 11
1.2.4.4 Les Kernel Intrusion Prevention System (KIPS) . . . 11
Conclusion . . . 11

2 Analyse et choix technique **12**
Introduction . . . 12
2.1 Justifications de la mise en place d'une solution de détection et de prévention des intrusions . . . 12
2.2 Avantages d'une solution de détection et de prévention des intrusions en entreprise . 13
2.3 Présentation de quelques solutions de détection et de prévention d'intrusions . . . 13
2.3.1 Solutions de détection des intrusions (IDS) . . . 13
2.3.2 Présentation de quelques solutions de prévention d'intrusions . . . 14
2.4 Étude comparative des systèmes de détection et de prévention d'intrusions . . . 14
2.5 Paramètres à prendre en compte pour le choix de notre solution . . . 17
2.6 Choix de la solution SURICATA . . . 17
Conclusion . . . 18

3 Présentation de la solution, conception et résultats des tests **19**
Introduction . . . 19
3.1 Présentation de SURICATA . . . 19
3.1.1 Modes de fonctionnement de SURICATA . . . 19
3.1.1.1 Mode Workers . . . 19
3.1.1.2 Mode Autofp . . . 20
3.1.1.3 Mode single . . . 20
3.2 Conception de la solution . . . 20
3.2.1 Présentation de l'architecture réseau de JENY SAS . . . 20
3.2.2 Présentation de l'espace de travail . . . 21
3.2.3 Installation et configuration de Suricata . . . 21
3.2.3.1 Mise à jour et installation des prérequis . . . 21
3.2.3.2 Configuration de Suricata . . . 22
3.2.3.3 Positionnement de Suricata dans le réseau . . . 24
3.2.4 Choix d'une interface web et d'un analyseur de journaux . . . 24
3.2.5 Présentation et configuration de Snorby . . . 24
3.2.5.1 Installation des dépendances . . . 25

3.2.6 Présentation et configuration de Barnyard2 27
3.2.7 Tests et vérifications 28
3.2.7.1 Test de SURICATA dans sa fonction d'IDS 28
3.2.7.2 Test de Suricata dans sa fonction d'IPS 29
3.2.8 Évolution de la sécurité du réseau de JENY SAS après l'intégration de Suricata 30
Conclusion 30

Conclusion **31**
3.3 Conclusion 31

Bibliographie **32**

Webographie **33**

Table des matières **34**