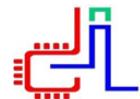




Faculté des Sciences de Bizerte

République Tunisienne
Ministère de l'Enseignement
Supérieur, de la Recherche
Scientifique et de la
Technologie
Université de Carthage



Département Informatique

Code.....

Mémoire de Projet de Fin d'Etudes

Pour l'obtention d'un Mastère Professionnel en Technologies des Réseaux de
Télécommunications
Option: Sécurité et Services dans les réseaux

Intitulé :

ETUDE ET MISE EN PLACE D'UNE SOLUTION DE GESTION DE LA SECURITE : CAS D'AFRIBONE MALI

Réalisé par :
Tidiane SYLLA

Au sein de
Afribone Mali



Encadré par :
Dr Rim HADDAD (FSB), Maître Assistante
Boubacar Sidiki DAGNOKO (Afribone Mali)

Dédicaces

Au Nom d'ALLAH, Le Tout Miséricordieux, Le Très Miséricordieux

Je dédie ce mémoire à mes parents, à femme et à mes enfants. Je leurs remercient pour les sacrifices et les efforts consentis durant cette formation et la réalisation de ce projet.

Remerciements

Je suis profondément reconnaissant envers mes deux encadreurs M. Boubacar Sidiki Dagnoko et Mme Rim Haddad pour m'avoir fait le grand honneur de diriger mon projet dans les meilleures conditions, ainsi que pour leurs encadrements, leurs conseils et leurs disponibilités.

Je témoigne ma reconnaissance à M. Oumar Maiga, Responsable Technique d'Afribone Mali pour m'avoir accordé ce stage. Je remercie M. Saidou Toure et M. Zoumana Coulibaly pour leurs aides précieuses, leurs conseils et les facilités qu'ils m'ont offerts. Je remercie également M. Mohamed Coulibaly, M. Alassane Niambélé, M. Fantiaga Samaké, M. Sitapha Diakité et Mlle Aissata Samaké, Youssouf Doumbia, Mohamed Keita pour l'accueil chaleureux et l'ambiance qu'ils m'ont offerte durant ce projet. Je remercie également tout le personnel d'Afribone Mali pour leur collaboration.

Je remercie tout le corps professoral de la Faculté des Sciences de Bizerte pour les efforts consentis dans notre formation. Je remercie particulièrement Mme Soumaya Hamouda et M. Tarek Ben Mena pour leurs écoutes, leurs disponibilités pour que ma formation soit possible malgré mes nombreuses contraintes.

Comme je n'y manquerai pas de remercier mes professeurs, membre du Jury pour l'honneur qu'ils ont fait en acceptant de faire partie de mon Jury.

Mes remerciements vont à l'endroit de tous ceux qui de près ou de loin ont contribué à l'élaboration de ce mémoire.

Résumé

Dans ce projet, on s'intéresse à la mise en place d'une solution de gestion de la sécurité du réseau d'Afribone Mali. Une telle solution est composée d'un tableau de bord de sécurité du réseau, d'une solution de gestion de logs centralisées et d'une équipe CIRT pour le pilotage de la solution.

De ce fait, notre travail porte sur les points suivants. On commence par la mise en place d'un tableau de bord de sécurité du réseau. Pour se faire, nous avons mis en place l'outil Security Onion associé à d'autres outils pour avoir une vue globale sur la sécurité du réseau. La seconde étape sera consacrée à la gestion des informations et événements de sécurité provenant des logs. Dernièrement, nous avons procédé à la mise en place d'une équipe CIRT pour le pilotage des différents outils mis en place afin d'assurer une meilleure gestion de sécurité au sein de l'entreprise.

Mots clés : Tableau de bord, Security Onion, NSM, log, IDS, CIRT, vulnérabilité, détection, intrusion.

Abstract

In this project, we are interested in setting up a security management solution for the Afribone Mali network. Such a solution is composed of a network security dashboard, a centralized log management solution and a CIRT team to manage the solution.

Our work therefore focuses on the following points. We begin by setting up a network security dashboard. To do so, we have implemented the Security Onion tool and other tools to get a global view of network security. The second step will be to manage log information and security events. Recently, we set up a CIRT team to leverage the various tools put in place to ensure better security management within the company.

Key words : Dashboard, Security Onion, NSM, log, IDS, CIRT, vulnerability, detection, intrusion.

Table des matières

| | |
|---|-----------|
| INTRODUCTION GÉNÉRALE..... | 1 |
| CHAPITRE 1. CONTEXTE GÉNÉRAL DU PROJET..... | 2 |
| 1.1. INTRODUCTION | 2 |
| 1.2. PRÉSENTATION DE L'ORGANISME D'ACCUEIL..... | 2 |
| 1.2.1. Création..... | 2 |
| 1.2.2. Domaine d'activité et services fournis..... | 2 |
| 1.3. MÉTHODOLOGIE DE TRAVAIL..... | 2 |
| 1.4. ARCHITECTURE DU RÉSEAU | 3 |
| 1.4.1. Le réseau d'accès | 3 |
| 1.4.2. Le réseau fédérateur..... | 4 |
| 1.5. L'AUDIT DE LA SÉCURITÉ ET DES SYSTÈMES..... | 4 |
| 1.6. CONCLUSION..... | 9 |
| CHAPITRE 2. SOLUTIONS DE GESTION DE LA SÉCURITÉ | 10 |
| 2.1. INTRODUCTION | 10 |
| 2.2. LA GESTION DE LA SÉCURITÉ DU RÉSEAU | 10 |
| 2.2.1. Généralités..... | 10 |
| 2.2.2. La supervision de la sécurité réseau | 12 |
| 2.2.3. La gestion de logs..... | 14 |
| 2.2.4. L'équipe CIRT | 16 |
| 2.3. LES SOLUTIONS DE SUPERVISIONS DE LA SECURITE RESEAU | 16 |
| 2.3.1. Security Onion..... | 17 |
| 2.3.2. OSSIM (Open Source Security Information Management) | 19 |
| 2.3.3. ArcSight | 20 |
| 2.3.4. Splunk..... | 20 |
| 2.3.5. Graylog2 : | 20 |
| 2.1. CHOIX DE LA SOLUTION..... | 20 |
| 2.2. CONCLUSION..... | 21 |
| CHAPITRE 3. DÉPLOIEMENT DE SECURITY ONION..... | 22 |
| 3.1. INTRODUCTION | 22 |
| 3.2. ARCHITECTURE DE SECURITY ONION ET DEPLOIEMENT | 22 |
| 3.2.1. Architecture de Security Onion..... | 22 |
| 3.2.2. Architecture du réseau cible | 23 |
| 3.2.3. Modes de déploiement de Security Onion | 23 |
| 3.2.4. Emplacements des sondes et du serveur | 24 |
| 3.3. INSTALLATION DU SERVEUR ET DES SONDES..... | 25 |
| 3.3.1. Configuration matérielle | 25 |
| 3.3.2. Installation du serveur | 26 |
| 3.3.3. Installation des sondes | 31 |
| 3.4. CONCLUSION..... | 35 |
| CHAPITRE 4. CONFIGURATIONS, MISE EN PLACE DE L'ÉQUIPE CIRT, TESTS..... | 36 |
| 4.1. INTRODUCTION | 36 |
| 4.2. CONFIGURATIONS DE SECURITY ONION | 36 |
| 4.2.1. Configuration du serveur..... | 36 |
| 4.2.2. Configuration des sondes | 36 |
| 4.2.3. Configuration des LIDS..... | 38 |
| 4.2.4. Maintenance de Security Onion | 39 |
| 4.3. MISE EN PLACE DE L'ÉQUIPE CIRT | 42 |
| 4.3.1. Généralités..... | 42 |
| 4.3.2. Constitution de l'équipe | 42 |
| 4.4. TESTS | 43 |
| 4.4.1. Cas de figure 1 : Scan d'une machine sur le réseau | 43 |

| | |
|---|-----------|
| 4.4.2. Cas de figure 2 : Tentative d'attaque par force brute..... | 43 |
| 4.5. CONCLUSION..... | 44 |
| CONCLUSION GÉNÉRALE | 45 |
| REFERENCES BIBLIOGRAPHIQUES..... | 46 |

Liste des figures

| | |
|--|----|
| Figure 1-1: Vue synoptique du Réseau d'accès d'Afribone Mali..... | 3 |
| Figure 1-2 : Vue synoptique du backbone d'Afribone Mali..... | 4 |
| Figure 1-3 : Interface de l'accueil d'OpenVAS | 7 |
| Figure 1-4 : Liste des vulnérabilités découvertes par OpenVAS sur une machine..... | 7 |
| Figure 1-5 : Détails d'une vulnérabilité, <i>http TRACE XSS attack</i> | 8 |
| Figure 2-1 : Cycles d'une attaque informatique..... | 11 |
| Figure 2-2 : Cycle de sécurité de l'entreprise, <i>source</i> [6] | 11 |
| Figure 2-3 : Couches d'une plateforme de SSR | 13 |
| Figure 2-4 : Architecture d'un système de gestion de logs | 16 |
| Figure 3-1 : Architecture de Security Onion, <i>source</i> [31]..... | 22 |
| Figure 3-2 : Vue synoptique du réseau d'Afribone Mali..... | 23 |
| Figure 3-3 : Les emplacements possibles pour les sondes | 24 |
| Figure 3-4 : Vue synoptique du réseau avec les sondes, les TAP et le serveur Security Onion..... | 25 |
| Figure 3-5 : Choix de l'interface réseau Management..... | 26 |
| Figure 3-6 : Résumé de la configuration réseau | 26 |
| Figure 3-7 : Lancement de la configuration de Security Onion..... | 26 |
| Figure 3-8 : Choix du cas d'utilisation..... | 27 |
| Figure 3-9 : Choix du mode de déploiement..... | 27 |
| Figure 3-10 : Choix du mode de configuration..... | 27 |
| Figure 3-11 : Nom d'utilisateur/mot de passe pour Sguil, Squert et ELSA | 28 |
| Figure 3-12 : Durée de garde des données | 28 |
| Figure 3-13 : Choix du NIDS | 28 |
| Figure 3-14 : Choix de la base de signature du NIDS Snort..... | 28 |
| Figure 3-15 : Saisie de l'Oinkcode..... | 29 |
| Figure 3-16 : Choix d'activation de Salt | 29 |
| Figure 3-17 : Choix d'activation d'ELSA | 29 |
| Figure 3-18 : Réservation d'espace disque pour les logs ELSA..... | 29 |
| Figure 3-19 : Résumé des paramètres d'installation du serveur..... | 30 |
| Figure 3-20 : Etat des services du serveur Security Onion..... | 30 |
| Figure 3-21 : Console Sguil avec une alerte OSSEC détaillée..... | 30 |
| Figure 3-22 : Interface d'ELSA | 31 |
| Figure 3-23 : Choix du mode de déploiement..... | 31 |
| Figure 3-24 : Demande de l'adresse IP du serveur..... | 31 |
| Figure 3-25 : Nom d'utilisateur possédant les droits SU sur le serveur..... | 32 |
| Figure 3-26 : Choix interface de sniffing | 32 |
| Figure 3-27 : Activation des IDS | 32 |
| Figure 3-28 : Activation de l'analyseur Bro | 32 |
| Figure 3-29 : Activation de l'extraction des exes par Bro..... | 33 |
| Figure 3-30 : Activation d'Argus | 33 |
| Figure 3-31 : Option Full packet capture..... | 33 |
| Figure 3-32 : Espace disque à réserver | 33 |
| Figure 3-33 : Activation de Salt sur une sonde | 34 |
| Figure 3-34 : Activation d'ELSA..... | 34 |
| Figure 3-35 : Mise à jour du nœud serveur..... | 34 |
| Figure 3-36 : Résumé des paramètres d'installation de la sonde | 34 |

| | |
|--|----|
| Figure 3-37 : Une partie des résultats de la sostat redacted | 35 |
| Figure 4-1 : Etat des services sur le serveur SO..... | 36 |
| Figure 4-2 : Configuration de la durée d'archivage de SO | 36 |
| Figure 4-3 : Configuration des réseaux Snort..... | 37 |
| Figure 4-4 : Configuration des réseaux Bro..... | 37 |
| Figure 4-5 : Statistique des règles Snort | 38 |
| Figure 4-6 : Un enregistrement dans un log d'une application non prise en charge | 39 |
| Figure 4-7 : Décodeur et règle personnalisé OSSEC pour le log de la figure 4-6..... | 39 |
| Figure 4-8 : Mise à jour de Security Onion avec soup..... | 40 |
| Figure 4-9 : Aperçu d'un dossier journalier | 41 |
| Figure 4-10 : Contenu du dossier des bases de données de MySQL..... | 41 |
| Figure 4-11 : Requête MySQL pour les espaces occupés <i>source</i> [6]. | 41 |
| Figure 4-12 : Résultats d'un scan vu les NIDS dans la console Sguil..... | 43 |
| Figure 4-13 : Attaque par force brute détectée et stoppée par OSSEC | 44 |

Liste des acronymes et abréviations

| | |
|---------|--|
| CERT | Computer Emergency Response Team |
| CIDR | Classless Inter-Domain Routing |
| CIRT | Computer Incident Response Team |
| DHCP | Dynamic Host Configuration Protocol |
| DMZ | DeMilitarized Zone |
| DNS | Domain Name Service |
| ELK | Elasticsearch Logstash Kibana |
| ELSA | Enterprise Log Search and Archive |
| FAI | Fournisseur d'Accès Internet |
| HIDS | Host-based Intrusion Detection System |
| HSRP | Hot Standby Routing Protocol |
| IDS | Intrusion Detection System |
| IoC | Indicator of Compromise |
| IoT | Internet of Things |
| ISO | International Organization for Standards |
| LAN | Local Area Network |
| LIDS | Log-based Intrusion Detection System |
| NAT | Network Address Translation |
| NIDS | Network Intrusion Detection System |
| NIPS | Network Intrusion Prevention System |
| NIST | National Institute of Standards and Technology |
| NSM | Network Security Monitoring |
| OCS | Open Computer and Software |
| OISF | Open Information Security Foundation |
| OpenVAS | Open Vulnerability Assessment System |
| OSPF | Open Shortest Path First |
| OSSEC | Open Source Security |
| OSSIM | Open Source Security Information Management |
| PCI-DSS | Payment Card Industry Data Security Standard |
| PEM | Petite et Moyenne Entreprise |
| RADIUS | Remote Authentication Dial In User System |
| RAID | Redundant Array of Independent Disk |
| SIEM | Security Information and Event Management |
| SIM | Security Information Management |

| | |
|-----------|--|
| SMS | Short Messaging Service |
| SNMP | Simple Network Management Protocol |
| SO | Security Onion |
| SSH | Secure Shell |
| SSR | Supervision de la Sécurité Réseau |
| TCP | Payment Card Industry Data Security Standard |
| ToIP/VoIP | Telephony over IP/Voice over IP |
| UDP | User Datagram Protocol |
| UFW | Uncomplicated FireWall) |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| VRRP | Virtual Router Redundancy Protocol |

Introduction Générale

Afribone Mali est un opérateur télécoms et fournisseur de services d'accès à Internet. Il dispose d'un grand nombre de clients et d'une infrastructure réseau conséquente.

Le souci premier d'Afribone Mali est de fournir des services Internet de qualité à ses clients tout en offrant une sécurité accrue des données de ses clients. Il doit également avoir une sécurité accrue de son infrastructure et de son système d'information.

Vu l'énorme quantité de données clients, de logs circulant sur son réseau et les événements de sécurité auquel il doit faire face, la mise en place d'une solution de gestion de la sécurité de son réseau s'impose.

Une solution de gestion de la sécurité du réseau est un ensemble d'outils, de méthodes et de techniques utilisés afin de gérer efficacement les événements de sécurité (alertes, incidents, attaques, etc...) et les logs (inhalérents à la sécurité ou non). Cette dernière doit être pilotée par une équipe nommée CIRT (Computer Incident Response Team).

Les outils utilisés peuvent être entre autres : un SIEM (Security Information and Event Management), un NSM (Network Security Monitoring). Parmi les méthodes, nous avons la mise en place d'une équipe CIRT et la mise en œuvre du cycle de gestion de la sécurité et des risques.

L'objectif de ce travail est de mettre en place une solution de gestion de la sécurité du réseau d'Afribone basée sur des outils **open source**, afin qu'elle soit mieux équipée pour protéger son réseau et ceux des clients.

Ce projet s'articule autour des points suivants :

- L'étude des outils open source de gestion de la sécurité des réseaux disponibles sur le marché ;
- La mise en place de ces outils et leurs intégrations dans les systèmes existants ;
- La constitution de l'équipe CIRT.

Ce présent mémoire est organisé comme suit :

- Le premier chapitre sera consacré à la présentation de l'entreprise et au contexte du projet.
- Le second chapitre présentera les concepts sur les solutions de gestion de la sécurité, et la solution choisie pour notre projet.
- Le troisième chapitre détaillera les préparatifs et les étapes du déploiement des outils de la solution choisie.
- Dans le quatrième et dernier chapitre, nous présenterons les configurations des outils, les tests.

1. Contexte général du projet

Chapitre 1. Contexte général du projet

1.1. Introduction

Dans ce chapitre, nous présenterons le contexte de notre travail. Ainsi, nous présenterons l'organisme d'accueil. Nous ferons également une étude approfondie de l'infrastructure du réseau existant et nous dégagerons la problématique de notre travail.

1.2. Présentation de l'organisme d'accueil

1.2.1. Création

Afribone Mali est l'un des premiers fournisseurs de services Internet au Mali. Elle a commencé ses activités en 1999. Elle est régie par la forme juridique de Société Anonyme (S.A).

Au fil des années, Afribone est devenue l'un des poids lourds de la fourniture d'accès Internet (FAI) à côté des plus gros (Orange Mali et Sotelma Malitel). Elle a su développer de très bonnes compétences dans l'ingénierie réseau, la conception web, la visioconférence et l'informatique évènementiel. En plus de la fourniture de l'accès Internet, Afribone offre également des services télécoms (interconnexion, installation de matériel de télécommunications, etc.).

1.2.2. Domaine d'activité et services fournis

Afribone propose une large gamme de connexions Internet haut débit, fiables et adaptées aux besoins des clients avec un service après-vente de qualité.

Elle s'est fortement développée dans le métier de l'ingénierie des réseaux et des télécommunications, mais également dans la production audiovisuelle. Ses atouts sont entre autres :

- Une forte culture technique, des compétences et une expertise en ingénierie informatique ;
- Des engagements de continuité de service, de qualité et de pérennité des solutions déployées ;
- Un savoir-faire reconnu ;
- Les offres de services en ingénierie recouvrent plusieurs domaines, dont : Audit (Audit de sécurité, de sauvegarde et d'infrastructure) ;
- Conception et câblage de réseaux (Cuirre, et fibre optique), réseaux sans fil, Hotspot, Routage et VPN ;
- Déploiement de services réseaux (DNS, DHCP, Bases de données, ToIP/VoIP, Visioconférence, etc.) ;
- Sécurité d'infrastructure (Solution antivirale, Firewall et proxy) ;
- Installation de serveurs (Messagerie, Microsoft, FreeRadius, ...) ;
- Solutions réseaux télécoms (installation de liaisons longue distance) ;
- Hébergement de sites web, de serveurs privés, etc.

Elle emploie plusieurs dizaines d'employés : des Ingénieurs, des Commerciaux, des Techniciens et des Chauffeurs. Elle dispose également d'une Hotline 24h/24 et 7j/7, ce qui fait d'elle le meilleur FAI aux yeux des clients.

1.3. Méthodologie de travail

Afin de réaliser toutes les phases du projet et atteindre les objectifs fixés, nous procéderons par les étapes suivantes :

- Etape 1 : Etude de l'existant et élaboration de la problématique ;
- Etape 2 : Etude des solutions de gestion de la sécurité, test et simulation ;
- Etape 3 : Déploiement de la solution choisie en grande nature et mise en place de l'équipe CIRT.

1. Contexte général du projet

1.4. Architecture du réseau

L'étude de l'infrastructure du réseau existant permet de mieux cerner le réseau et de définir l'étendue de la solution à déployer, ainsi que, de déceler d'éventuels problèmes ou non-conformités en termes de sécurité avant tout déploiement.

Le réseau d'Afribone est un réseau de type opérateur télécom, c'est-à-dire composé de deux grandes parties :

- Le réseau d'accès ;
- Et le réseau fédérateur ou backbone.

1.4.1. Le réseau d'accès

Le réseau d'accès est l'ensemble des équipements et des moyens de transmissions mis en œuvre par un opérateur de télécommunications pour la collecte des données et autres informations des abonnés vers le réseau de l'opérateur, et vice versa du réseau de l'opérateur vers les abonnés. Autrement dit, il s'agit de la manière dont l'opérateur dessert ses abonnés.

Le réseau d'accès d'Afribone est un réseau à base de Boucle locale radio de type point à multipoint. Cela permet de couvrir un grand territoire avec des bandes passantes élevées en utilisant les ondes hertziennes (non licenciées pour la plupart). Equipé des équipements RF (Radio Frequency) de dernière génération (Cambium, Radwin, RFLEX, 3 ROM), il (le réseau d'accès) lie plus de 1000 clients résidentiels et professionnels à travers la ville de Bamako, et cela sur des distances plus ou moins importantes (banlieue et villes périphériques comprises).

Les points d'accès sont installés dans les points géographiques stratégiques (relief, vue dégagée). Les antennes clientes (Subscriber Module Cambium) sont à leurs tours connectées aux points d'accès (Access Point Cambium).

Le trafic des points d'accès est alors envoyé vers le backbone en utilisant des antennes-relais et des faisceaux hertziens de grandes capacités.

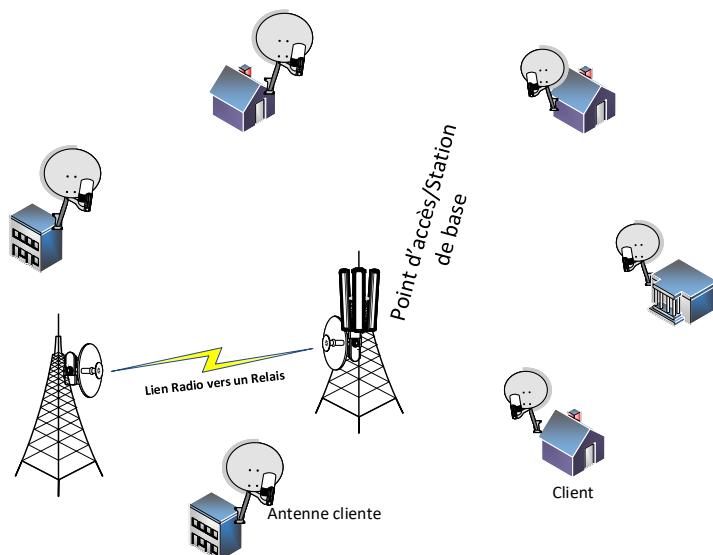


Figure 1-1: Vue synoptique du Réseau d'accès d'Afribone Mali

NB : Pour des raisons de confidentialité, plusieurs détails ont été masqués.

Avec un tel réseau, Afribone Mali offre à ses clients des accès hauts débits de très bonne qualité.

Ainsi, elle leur offre des services Internet, de visioconférence, de vidéo à la demande et de la téléphonie sur IP.

1. Contexte général du projet

1.4.2. Le réseau fédérateur

Le backbone, encore appelé réseau fédérateur est le cœur du réseau de l'opérateur. C'est par lui que passe toutes les communications. Il est chargé du routage des paquets IPv4/v6 à très grande vitesse.

Il est la partie du réseau qui supporte le gros du trafic. De ce fait, le backbone doit répondre à des mesures sécuritaires très strictes. Ces mesures concernent la sécurité de l'infrastructure (c'est une infrastructure critique) et la sécurité des informations qui y circulent.

Il est important de noter que pour des raisons de haute disponibilité dans l'accès et le backbone (point d'accès et relais), le backbone d'Afribone Mali est un réseau à architecture maillée. Chaque site comporte un lien principal et un lien de secours avec les autres sites. Les moyens de transmission mis en œuvre pour l'interconnexion sont les faisceaux hertziens à grande capacité (entre 50 et 300 Mbit/s).

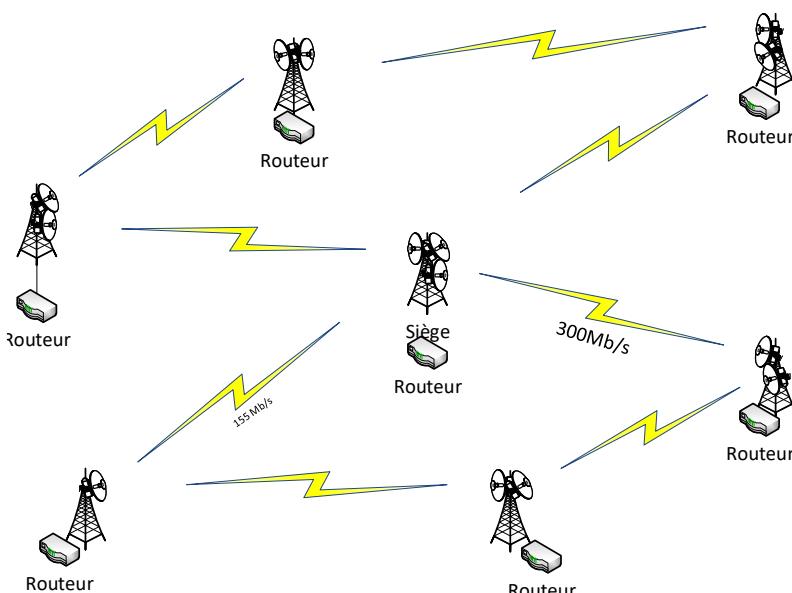


Figure 1-2 : Vue synoptique du backbone d'Afribone Mali.

NB : Pour des raisons de confidentialité, plusieurs détails ont été masqués.

Le protocole de routage mis en œuvre est le protocole Open Shortest Path First (OSPF). OSPF est un protocole de routage interne à une zone. Il est de la famille des protocoles de routage à état de liens. Un protocole de routage à état de lien se base sur l'état des différents liens (débits et connectivité) avec ses voisins pour établir sa table de routage. L'algorithme de Dijkstra où une de ses variantes est alors appliquée pour trouver le plus court chemin vers la destination.

L'ensemble du réseau est géré à partir du centre des opérations, situé au siège de l'organisation.

Le réseau local est organisé en plusieurs VLAN (Virtual Local Area Network) . Les postes sont interconnectés en utilisant du Fast Ethernet (100 Mbit/s). Le réseau local est protégé par un pare-feu. Le système de sécurité actuel du réseau local de l'organisation est donc un réseau avec un goulet d'étranglement unique. Cela accroît le niveau de sécurité en donnant la possibilité de contrôler l'ensemble du trafic. Un tel système n'a pas que des avantages, il présente aussi plusieurs inconvénients, que nous détaillerons à la partie recommandations.

1.5. L'audit de la sécurité et des systèmes

La mise en place une solution de sécurité sans diagnostiquer au préalable l'état et les actifs du réseau revient à un médecin qui prescrit des médicaments à un patient sans le consulter. Les solutions proposées et implémentées pourront temporairement marcher, mais peuvent ne rien servir à la longue. Une solution de gestion de la sécurité réseau coûte cher à une entreprise.

1. Contexte général du projet

L'audit de la sécurité du réseau consiste à observer tout ou partie du réseau (matériels, logiciels, etc.) selon un ou plusieurs aspects et à comparer les résultats obtenus à des référentiels dans le domaine de la sécurité.

Dans cette partie, nous allons rechercher et mettre en exergue les points forts et faibles du réseau et des systèmes. À partir de là, nous dégagerons des recommandations et des règles de bonnes pratiques à suivre. L'approche adoptée est de mener des tests d'intrusion et des scans de vulnérabilité [1].

Les résultats de cette phase nous permettront d'une part de déterminer les problèmes à résoudre pour que la solution soit efficace, mais aussi de délimiter les contours d'implémentation de la solution.

1.5.1. L'audit de l'architecture du réseau

L'audit de l'architecture du réseau permet de déceler d'éventuels problèmes de sécurité (physique et logique).

D'après les études menées sur les documents recueillis, le réseau¹ d'Afribone Mali est bien structuré. Les liens du backbone sont presque tous redondants. Les sources d'alimentations² sont également redondantes. L'infrastructure télécom peut fonctionner en mode dégradé.

Toutefois, au niveau LAN, nous avons noté un point de défaillance unique comme entrée et sortie du réseau. En effet, un seul firewall est utilisé et n'est pas dédoublé en permanence. Les ressources du réseau local sont correctement séparées par les VLAN.

Le Datacenter³ est également bien structuré. Il contient plusieurs DMZ⁴ de différents niveaux exposants des services sur Internet. En plus des serveurs d'Afribone, il y a des serveurs de divers clients qui sont également présent pour hébergement.

1.5.2. L'audit des switches et des routeurs

L'audit des équipements réseaux consiste à vérifier leur niveau de sécurité et la conformité de leurs configurations. Cela se fait en :

- Récupérant et en analysant les différents fichiers de configuration ;
- En s'assurant que les derniers patchs sont appliqués ;
- En s'assurant que tous les services non nécessaires sont désactivés ;
- Et s'assurer qu'un scan de vulnérabilité est réalisé périodiquement pour déceler les nouveaux risques et menaces et appliquer les mesures nécessaires.

L'analyse des fichiers de configuration nous a montrés que les différentes configurations des différents équipements sont bien faites et que les services non nécessaires sont désactivés.

Après les analyses menées, nous avons noté que les derniers patchs sont appliqués régulièrement. Les services non nécessaires sont désactivés sur tous les équipements réseaux que nous avons audités.

Le protocole utilisé pour la supervision des équipements est SNMP (Simple Network Management Protocol) version 2. La version 3 est la plus récente. Elle a apporté le chiffrement des messages et l'authentification des agents. Le problème avec cette version est la compatibilité avec le plus grand nombre d'équipements. C'est à cause de ce manque de compatibilité que la version 2 est utilisée. La version 2 assure la sécurité en offrant un mot de passe que les agents et le manager doivent

¹ Il s'agit de l'ensemble du réseau à savoir : le réseau local et le backbone.

² Les sources d'alimentations utilisées sur les sites : Le réseau électrique, l'énergie solaire et le groupe électrogène.

³ Un Datacenter est un centre ou une entreprise installe ses serveurs (DNS, Web, Mail, etc.).

⁴ DeMilitarized Zone

1. Contexte général du projet

savoir pour échanger des messages. Ce mot de passe est appelé le **community string**. À Afribone Mali, le community string utilisé est fort et presque impossible à craquer par brute force.

Jusqu'à notre arrivée, il n'y avait pas de scan de vulnérabilité. Cela s'explique principalement par le fait que l'entreprise était beaucoup plus préoccupée par la gestion des problèmes de ses clients et la continuité de son service (7j/7). Nous avons effectué un scan de vulnérabilité en utilisant le scanner de vulnérabilité open source OpenVAS⁵.

Les résultats des scans ont montré que les routeurs et switch scannés ne présentent pas de vulnérabilités majeures et connues à ce jour. Les scanneurs de vulnérabilités utilisent des bases actualisées de menaces et de failles pour évaluer, un service, une application ou un système.

1.5.3. L'audit des services et systèmes réseaux

Afribone Mali étant un fournisseur de services Internet, la fourniture de services de noms de domaines, d'hébergement web simple, d'applications web et de services de messageries, etc. font partie intégrante de ses prestations.

La sécurisation des serveurs des services cités ci-dessus est cruciale pour la continuité des services fournis. Pour mener à bien cette sécurisation, nous devons au préalable auditer les serveurs hébergeant ces services.

Pour ce faire, nous avons utilisé des outils open source pour l'audit et l'évaluation de la vulnérabilité d'un système. Pour rappel, une vulnérabilité est une faiblesse induite dans le système dû soit à une mauvaise configuration ou à un défaut depuis la conception. Les outils que nous avons utilisés à ce propos sont : Lynis et OpenVAS.

Lynis est un outil gratuit très utilisé dans le domaine de l'audit des systèmes et des services réseaux. Il est très léger, n'a pas besoin d'être installé pour fonctionner.

Après le lancement de Lynis, l'analyse se déroule rapidement sans affecter les services et le système même en production. Les différentes étapes de l'analyse sont [2]:

- Découverte du système d'exploitation
- Recherche des outils et utilitaires disponibles
- Recherche de mise à jour Lynis
- Test des plugins activés
- Test de sécurité par catégorie
- Rapport d'état du scan de sécurité.

Une fois l'analyse terminée, les résultats sont automatiquement disponibles. Parmi les résultats, nous avons l'état de sécurité des éléments scannés et testés, et les recommandations suivre pour éradiquer les menaces liées aux problèmes détectés.

Lynis fournit également des recommandations avec référence à l'appui pour permettre aux administrateurs de la sécurité d'éliminer les faiblesses de leurs services.

Comme cité plus haut, nous avons également utilisé OpenVAS. OpenVAS est un scanner de vulnérabilité, version gratuite de Nessus. Il est plus lourd que Lynis, et nécessite d'être installer sur un système. Un de ses inconvénients en plus de la lourdeur est qu'il peut causer l'interruption du service scanné. Il s'utilise via une interface web.

Après l'authentification, l'utilisateur est orienté vers la page d'accueil d'OpenVAS. Partant de là, il peut lancer des scans, explorer les résultats d'autres scans, configurer, etc. il faut noter cependant

⁵ OpenVAS: Open Vulnerability Assessment System.

1. Contexte général du projet

qu'un scan OpenVAS prend beaucoup plus de temps qu'un scan Lynis. Lorsque le scan est complété, nous pouvons explorer les résultats.

| Name | Status | Reports | Severity | Trend | Actions |
|---|--------|------------------|--------------|-------|---|
| Immediate scan of IP 196.200.55.90 | Done | 1 (1) Apr 5 2017 | 10.0 (High) | | View Edit Delete Download |
| Immediate scan of IP webdemo.afribonemali.net | Done | 1 (1) Apr 5 2017 | 5.8 (Medium) | | View Edit Delete Download |

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.
I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

Quick start: Immediately scan an IP address
IP address or hostname:
 Start Scan

For this short-cut I will do the following for you:
1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration

Figure 1-3 : Interface de l'accueil d'OpenVAS

Dans notre cas, nous disposons de deux machines, webdemo.afribonemali.net et 196.200.55.90. La colonne *severity* indique la criticité de la vulnérabilité de la machine. Pour découvrir la liste des vulnérabilités découvertes et leurs détails, l'utilisateur doit cliquer sur le nombre se trouvant dans la colonne *Report*.

La figure 1-4 montre les résultats du scan effectué sur une machine. On y trouve la liste des vulnérabilités découvertes, leur niveau de criticité et le service concerné par cette vulnérabilité. Pour découvrir plus de détails sur une vulnérabilité et voir les recommandations pour y remédier, l'utilisateur clique simplement sur la vulnérabilité en question. Cela donne comme résultat la figure 1-5. Dans les détails, on trouve les sections suivantes : Résumé, Résultats de détection de la vulnérabilité, la solution proposée pour y remédier, la méthode utilisée pour la détection de la vulnérabilité et les références relatives à cette vulnérabilité. Dans le résumé, on trouve une explication brève de la vulnérabilité et les possibilités qu'elle offre aux attaquants. La section solution propose la recommandation à suivre afin de corriger cette vulnérabilité pour que celle-ci ne soit pas exploitable par les attaquants.

| Vulnerability | Severity | QoD | Host | Location | Actions |
|--|--------------|-----|--|-------------|---|
| http TRACE XSS attack | 5.8 (Medium) | 99% | 196.200.59.134 (webdemo.afribonemali.net) | 80/tcp | View Edit |
| http TRACE XSS attack | 5.8 (Medium) | 99% | 196.200.59.134 (webdemo.afribonemali.net) | 443/tcp | View Edit |
| SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 5.0 (Medium) | 98% | 196.200.59.134 (webdemo.afribonemali.net) | 443/tcp | View Edit |
| SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 5.0 (Medium) | 98% | 196.200.59.134 (webdemo.afribonemali.net) | 2078/tcp | View Edit |
| SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 5.0 (Medium) | 98% | 196.200.59.134 (webdemo.afribonemali.net) | 2083/tcp | View Edit |
| SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 5.0 (Medium) | 98% | 196.200.59.134 (webdemo.afribonemali.net) | 2087/tcp | View Edit |
| SSL/TLS: Report Vulnerable Cipher Suites for HTTPS | 5.0 (Medium) | 98% | 196.200.59.134 (webdemo.afribonemali.net) | 2096/tcp | View Edit |
| SSH Weak Encryption Algorithms Supported | 4.3 (Medium) | 95% | 196.200.59.134 (webdemo.afribonemali.net) | 22/tcp | View Edit |
| SSL/TLS: Report Weak Cipher Suites | 4.3 (Medium) | 98% | 196.200.59.134 (webdemo.afribonemali.net) | 443/tcp | View Edit |
| TCP timestamps | 2.6 (Low) | 80% | 196.200.59.134 (webdemo.afribonemali.net) | general/tcp | View Edit |
| SSH Weak MAC Algorithms Supported | 2.6 (Low) | 95% | 196.200.59.134 (webdemo.afribonemali.net) | 22/tcp | View Edit |

Figure 1-4 : Liste des vulnérabilités découvertes par OpenVAS sur une machine

1. Contexte général du projet

The screenshot shows a 'Result Details' page from a network security tool. At the top, it says 'Task: Immediate scan of IP webdemo.afribonemali.net' and 'ID: d7df1807-4670-4f7b-93d9-0eaf25ac2026'. Below this is a table with columns: Vulnerability, Severity, QoD, Host, Location, and Actions. The 'Vulnerability' row shows 'http TRACE XSS attack' with a severity of '5.8 (Medium)', a QoD of '99%', the host '196.200.59.134', location '80/tcp', and icons for a file and a star.

| Vulnerability | Severity | QoD | Host | Location | Actions |
|-----------------------|--------------|-----|----------------|----------|---------|
| http TRACE XSS attack | 5.8 (Medium) | 99% | 196.200.59.134 | 80/tcp | |

Summary
Debugging functions are enabled on the remote HTTP server.
The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Vulnerability Detection Result

Solution:
Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on  
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)  
RewriteRule .* - [F]
```

See also <http://httpd.apache.org/docs/current/de/mod/core.html#traceenable>

Solution
Disable these methods.

Vulnerability Detection Method
Details: [http TRACE XSS attack \(OID: 1.3.6.1.4.1.25623.1.0.11213\)](#)

Figure 1-5 : Détails d'une vulnérabilité, *http TRACE XSS attack*

1.5.4. Recommandations

Les recommandations que nous avons effectuées portent essentiellement sur les services réseaux et les systèmes.

Les accès SSH aux principaux serveurs se font en utilisant les noms d'utilisateurs et mot de passe. Ce mode d'authentification SSH est déconseillé. Nous recommandons l'utilisation de certificat pour l'authentification SSH. En effet, les robots peuvent craquer le couple nom d'utilisateur/mot de passe. Or, en utilisant l'authentification avec certificat, le pirate aura nécessairement besoin d'une clé privée correspondante à la clé publique du serveur, chose qui lui est impossible à produire.

Nous recommandons également l'installation de bloqueur d'attaque brute force à destination des comptes email des clients et des comptes administrateurs des sites web hébergés.

Nous recommandons également la mise en haute disponibilité du pare-feu du réseau LAN de l'entreprise. En effet, ce pare-feu en plus du LAN gère plusieurs DMZ, qui hébergent plusieurs serveurs (Mail, Web, etc.).

La société possède à ce jour une seule connexion à Internet. À la moindre défaillance de cette connexion, c'est tout l'Internet de la société qui est coupé. Pour remédier à ce risque énorme, nous recommandons à l'entreprise de dédoubler sa connexion Internet en ajoutant une autre connexion avec un autre opérateur. Une fois cette recommandation appliquée, il lui sera facile d'implémenter l'une technique de redondance (VRRP : ¹ Virtual Router Redundancy Protocol, HSRP : Hot Standby Routing Protocol) de chemin au niveau de ses routeurs.

Nous recommandons la formation du personnel technique de l'entreprise. Afribone Mali doit former ces ingénieurs et techniciens sur les différents équipements et systèmes déployés, mais aussi sur la veille technologique.

Et enfin, nous déplorons le manque d'une politique de sécurité informatique. À cet effet, nous recommandons la rédaction et l'implémentation d'une politique de sécurité informatique incluant : la politique de sécurité physique, la politique de sécurité des mots de passe et la politique de sécurité du réseau informatique. L'élaboration de ces documents ne rentre pas dans le cadre de ce travail.

1. Contexte général du projet

1.6. Conclusion

Dans ce premier chapitre, nous avons présenté le contexte du projet. Par la suite, nous avons posé un diagnostic fiable de la situation sécuritaire d'Afribone Mali. Ce diagnostic nous a permis de ressortir les failles et les vulnérabilités. Partant de là, nous avons porté des recommandations.

Dans le prochain chapitre, nous ferons une étude des solutions de gestion de la sécurité des réseaux disponibles sur le marché.

Chapitre 2. Solutions de gestion de la sécurité

2.1. Introduction

Dans le chapitre précédent, nous avons présenté le contexte de travail. Nous avons effectué une étude de l'existant et dégagé la problématique de notre projet. Dans ce chapitre, nous effectuerons une étude détaillée des solutions de gestion de sécurité et de centralisation de logs open source existants puis nous choisirons, une solution en se fondant sur les critères définis dans la méthodologie.

2.2. La gestion de la sécurité du réseau

2.2.1. Généralités

La plupart des entreprises limitent la sécurité de leurs réseaux au déploiement de pare-feu, d'antivirus ou de système de détection d'intrusions. Ainsi, les responsables de la sécurité des dites entreprises créent toutes une batterie de règles de filtrage sur les pare-feu et croient qu'ils sont alors protégés. Les menaces auxquelles nous faisons face sont mondiales [3], car elles proviennent d'Internet, et Internet n'a pas de frontière. Internet est de nos jours comparable au far West des Etats Unis à l'époque du XXe Siècle. Les hackers sont organisés, les législateurs (gouvernements et organismes internationaux), les administrateurs de la sécurité des entreprises ne le sont pas ou sont mal organisés.

De nos jours, les attaques deviennent de plus en plus sophistiquées. Les hackers sont de sérieux adversaires, redoutables et implacables. Bien que le domaine de la sécurité informatique ait beaucoup évolué ces dernières années, outrepasser un firewall ou un IDS (Intrusion Detection System) est devenu une gymnastique pour les hackers expérimentés. Ainsi, les mesures (citées plus haut) que la plupart des administrateurs de la sécurité considèrent efficaces ne sont en fait que des étapes pour les pirates informatiques. En considérant l'anatomie d'une attaque informatique [4] (figure 2-1), l'on se rend compte que l'objectif principal d'un hacker (quel que soit le type) si l'on ne considère pas le déni de service, est, de pénétrer un réseau cible, maintenir son accès et voler ou modifier des informations, détruire le système ou les systèmes cibles.

Un pirate lorsqu'il pénètre un réseau, il fait tout ce qu'il faut pour rester inaperçu et dure le plus longtemps possible (Phase 5). S'il n'est pas détecté durant les premières phases de l'attaque, il peut causer d'importants dégâts. Parmi les dégâts qui peuvent être occasionnés, nous avons l'installation de ransomware⁶, la révélation d'email business (Business Email Compromise), le vol de données personnelles d'utilisateurs, etc.

Selon le site Help Net Security [5], le milieu de la finance est le plus visé, soit 23% des attaques. Suivant la même source, le secteur de l'e-commerce vient en deuxième position avec 19%, l'industrie de la fabrication avec 18%, la technologie avec 12% et l'assurance santé 11%. La part des opérateurs et des fournisseurs d'accès est que ce sont eux qui hébergent la plupart des services visés. Ainsi, protéger et surveiller constamment leurs réseaux permet de drastiquement réduire les attaques visant les services cités ci-dessus. La méthode la plus efficace d'y parvenir est l'utilisation une solution de gestion de la sécurité.

Une solution de gestion de la sécurité est l'ensemble des outils et des moyens utilisés pour superviser la sécurité du réseau, gérer les événements et incidents issus de la supervision. Elle doit

⁶ Rançongiciel : logiciel malveillant qui prend en otage les données personnelles en contre partie du paiement d'une rançon.

2. Solutions de gestion de la sécurité



Figure 2-1 : Cycles d'une attaque informatique

également permettre de répondre aux principes de la **träçabilité** et de **l'intégrité** de la sécurité informatique, autrement dit, permettre de garder intactes toutes traces d'activités normales ou suspectes dans le réseau et les systèmes. Le tout (supervision et gestion) est intégré dans le cycle de la sécurité au sein de l'entreprise [6].

Les tâches normales des responsables de la sécurité sont les deux premières phases du Cycle de Réponse d'un Incident de Bejtlich, c'est-à-dire **Planifier** et **Résister** [7]. Les deux autres revenants à l'équipe CIRT.

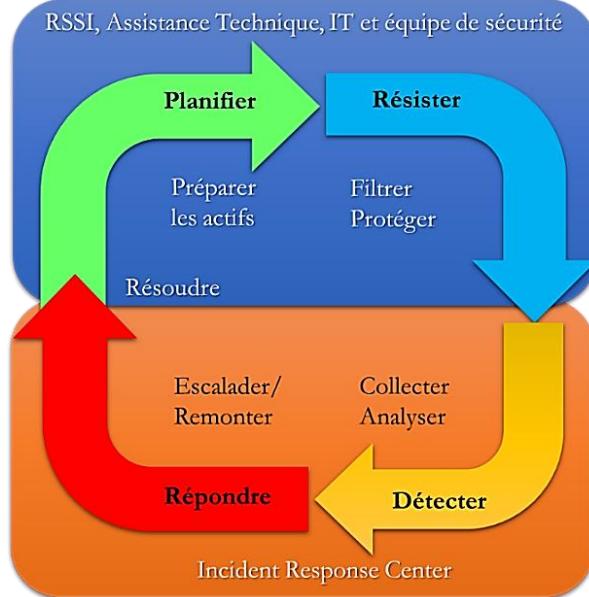


Figure 2-2 : Cycle de sécurité de l'entreprise, *source* [6]

La mise en place d'une solution de gestion de la sécurité répond au quatrième élément des cinq principes d'or de la sécurité : « Protection is key but detection is a must. » [8].

Ce principe met en avant les activités de surveillance des réseaux et des systèmes. Ces activités permettront de détecter des signes d'une intrusion en cours préparation ou en cours d'évolution. Ainsi, les responsables de la sécurité, l'équipe CIRT où les administrateurs du réseau pourront prendre des mesures adéquates afin d'arrêter la progression de l'attaque et de défaire l'attaquant, en ajoutant ou en modifiant des règles au niveau des pare-feu.

2. Solutions de gestion de la sécurité

2.2.2. La supervision de la sécurité réseau

La Supervision de la Sécurité du Réseau (SSR) ou Network Security Monitoring (NSM) en anglais, est : « la collecte, l'analyse et l'escalade des signes et des alertes pour détecter et répondre aux intrusions. » [6].

La supervision de la sécurité du réseau peut être vue comme une méthodologie, et non pas une simple action. Une fois correctement mis en place, elle permet aux responsables de la sécurité, notamment l'équipe CIRT, de détecter et de mettre fin à une attaque avant qu'elle ne cause de dégât. Pour y parvenir, la supervision de la sécurité du réseau est basée sur la corrélation intelligente des événements provenant de différentes sources mais liés à une même cause. Les sources sont entre autre : les IDS (NIDS : Network IDS, HIDS : Host-based IDS), les journaux d'événements (logs), les analyseurs de trafic, etc.

La supervision de la sécurité du réseau est née vers la fin des années 1990, aux Etats Unis d'Amérique [6]. Les entreprises et les gouvernements (la défense, en particulier) ont approché les chercheurs pour que ceux-ci développent des systèmes qui leur aideront à détecter les anomalies et les attaques. Dès le départ, la question juridique s'est posée. Les départements de la justice de différents pays se sont intéressés aux outils SSR, en qualifiant leurs usages d'espionnages et criminels. Ils ont fini par revoir leur position en considérant ces derniers et les données collectées par eux comme probants. A ce titre, plusieurs normes juridiques exigent un nombre au minimum d'années pour la rétention des données. On peut par exemple citer la norme PCI-DSS (Payment Card Industry Data Security Standard) [9].

La SSR n'est pas une solution magique aux problèmes de sécurité que rencontrent les entreprises. Ce sont des programmes. Pour qu'ils soient efficaces, les RSSI (Responsable de Sécurité des Systèmes d'Information) doivent comprendre les différents cycles d'une attaque, savoir les analyser. Chaque phase d'un cycle laisse des preuves au niveau de différentes sources de données⁷. Ces données sont mieux exploitées en utilisant différentes techniques d'analyse plus moins complexes. C'est cette capacité d'analyse qui permettra aux analystes de la sécurité de prendre le dessus sur les attaquants.

La SSR trouve mieux sa place dans une solution de gestion de la sécurité du réseau. En effet la SSR est requis pour fournir une solution de gestion de la sécurité du réseau et des systèmes, ce qui permet d'avoir un contrôle plus global sur le réseau et des analyses plus précises [10].

2.2.2.1. Architecture d'une plateforme de Supervision de la Sécurité Réseau

Une plateforme de supervision de la sécurité réseau est constituée des éléments suivants : outils de collecte de données, outils de distributions de données et d'outils de présentation de données.

Ces outils sont organisés en suivant une architecture en couches. La première couche est la couche des outils de collecte de données. La deuxième couche est celle des outils de distributions de données et la dernière, celle des outils de présentation de données.

Nous présenterons les détails de chaque couche dans les prochaines sections.

La couche outils de collecte de données

C'est l'ensemble des outils qui permettent de directement collecter les données à partir du réseau ou à travers les logs.

Ces données sont ensuite envoyées aux outils de présentation ou d'analyse de données via la couche de distribution. Parmi ces outils, on trouve : les systèmes de détection d'intrusion, les analyseurs de

⁷ Ici la source de données se réfère à un équipement réseau ou le log d'une application.

2. Solutions de gestion de la sécurité

Ces données sont ensuite envoyées aux outils de présentation ou d'analyse de données via la couche de distribution. Parmi ces outils, on trouve : les systèmes de détection d'intrusion, les analyseurs de trafic, les analyseurs de réseau et les sources de logs.



Figure 2-3 : Couches d'une plateforme de SSR

La couche outils de distribution de données

C'est la couche intermédiaire. Elle met en relation la couche de collecte et la couche de présentation des données. Autrement dit, elle est constituée d'outils qui permettent à la couche présentation de mieux exploiter les données collectées par la couche de collecte de données.

La couche outils de présentation de données

La couche outils de présentation de données permet d'exposer les données collectées aux analystes et aux experts du CIRT à des fins d'analyse et de prise de décision. Au niveau de cette couche, on trouve plusieurs catégories d'outils, certains avec des interfaces graphiques et d'autres en ligne de commande.

Les outils que la couche comprend sont entre autres : moteur de corrélation, gestion des alertes, investigation et escalade d'événements, etc.

2.2.2.2. Les types de données collectées

Un superviseur de la sécurité réseau collecte plusieurs types de données à différents niveaux et différents endroits. Selon [11], [6] et [3] les principaux types de données collectés par un superviseur de la sécurité réseau sont suivants : données à contenus intégrales, données statistiques, données de sessions, données d'alertes et les logs.

Les données à contenus intégrales

C'est lorsque l'intégralité du trafic est capturée et stockée à des fins d'analyse. Celles-ci (données capturées) comprennent les en-têtes (headers) et les contenus (payloads). Ainsi, quand l'analyste commence à investiguer avec ces données, il consulte d'abord les en-têtes des paquets en premier temps ensuite les payloads lorsqu'il doit pousser l'analyse.

Exemple : un analyste a remarqué un paquet suspect avec un en-tête http. Il a utilisé Wireshark pour voir le payload, et a pu extraire un fichier .exe qui a été téléchargé durant la session.

Les données statistiques

« Une donnée statistique est l'organisation, l'analyse, l'interprétation et la présentation d'autres types de données » [3]. Autrement dit, ces données permettent à un analyste de voir d'autres informations liées à une activité sur le réseau. Parmi les informations qui peuvent en sortir, on peut citer : nombre de paquets transmis et reçus, nombre de paquets par seconde, nombre de datagrammes UDP, pourcentage de segment TCP, statistiques relatives à un protocole, etc.

2. Solutions de gestion de la sécurité

Les données de sessions

Les données de sessions présentent un résumé des communications passées entre deux interlocuteurs, en occurrence deux machines. De petite taille, elles sont très faciles à exploiter et leur stockage long duré ne pose pas de problème. Par contre, elles n'offrent pas autant de détails que les données à contenus intégrales. Les informations par une donnée de session sont par exemple : adresse IP source/destination, port source/destination, la transaction effectuée, etc.

Les données d'alertes

Les données d'alertes sont générées par les consoles d'analyse et de corrélation de la plate-forme SSR. Les consoles de corrélation analysent en temps réel et en continu les données provenant de la couche distribution (cf. section précédente) et déclenchent une alerte dès qu'une donnée présente une anomalie par rapport aux règles, signatures ou toutes autres bases d'information.

L'alerte générée est une donnée de petite taille contenant la description de l'anomalie détectée et les pointeurs vers les données concernant cette anomalie. Il faut noter que la taille de la donnée d'alerte est très petite du fait qu'elle ne contient que des pointeurs vers les données qui sont en rapport avec l'alerte.

Les données de log

Ces données sont généralement des données brutes en provenance des équipements, des systèmes ou des applications. Ceux-ci peuvent être des données de journaux d'événements Windows, SYSLOG, données spécifiques à une application (ex. MySQL, apache, etc...), un pare-feu, un routeur, log d'authentification (RADIUS, VPN, etc..), etc.

2.2.3. La gestion de logs

Un log est un registre dans lequel est enregistré tout événement provenant du réseau ou des systèmes dans une entreprise. La gestion des logs est également partie intégrante d'une solution de gestion de la sécurité. La gestion des logs peut être définie comme toute activité liée à la collecte, la centralisation, l'analyse et l'archivage des logs générés par les différentes entités du réseau et des systèmes. Ces entités peuvent être : pare-feu, routeurs, switch, serveurs (applications et systèmes), ordinateurs PC, etc. autrement dit, un système de gestion de logs est constitué de logiciels, de matériels, de réseaux et de supports utilisés pour générer, transmettre, enregistrer et d'analyser les données desdits journaux [12].

Suivant le guide de gestion de log de la sécurité informatique du NIST⁸ [12] cf. [13], les éléments d'informations d'un incident peuvent être enregistrés à partir de plusieurs sources, tels que les routeurs, les pare-feu, les IDS, et les logs des applications et les services. Ainsi, il est possible d'avoir des indications d'incidents sans que les administrateurs s'en rendent compte. Pour que les incidents soient détectés et gérés, la solution de gestion de la sécurité met en place des outils qui permettent d'analyser en temps aussi réel que possible, les logs, le trafic et d'autres informations de manière automatique et de générer des alertes.

La gestion de log permet aux administrateurs de la sécurité des entreprises d'assurer le stockage des informations détaillées sur les événements des réseaux et des systèmes, notamment les événements de sécurité informatique.

2.2.3.1. Architecture d'un système de gestion de log

Le guide de gestion de log de la sécurité informatique du NIST [13] décrit un système de gestion de log comme étant l'ensemble du matériel, du réseau, des logiciels et supports utilisés pour générer,

⁸ National Institute of Standards and Technology

2. Solutions de gestion de la sécurité

transmettre, stocker, analyser et de disposer des données de log. Selon le même guide, un système de gestion de logs est constitué de trois (3) grandes parties qui sont :

- La génération de logs ;
- L'analyse de log et stockage ;
- Le monitoring de logs.

La partie génération de logs est constituée des équipements et des hôtes responsables de la génération des données de log. Les logs ainsi générés sont mis à disposition des serveurs de log selon divers moyens. Certains périphériques et systèmes disposent d'outils pour l'envoi des logs directement aux serveurs, c'est le cas de SYSLOG. D'autres comme, par exemple, des applications spécifiques écrivent leurs logs dans des fichiers spécifiques et les contenus de ces fichiers sont envoyés vers les serveurs via des outils tels que RSYSLOG ou Filebeat. Les logs sont souvent transférés aux nœuds de traitement en temps réel.

La partie analyse de log et stockage est composée des serveurs et des nœuds de traitements des logs. Selon [12] les éléments de cette partie sont appelés **collecteurs** et **agrégateurs**. Les logs proviennent de différentes sources et ont différents formats. Les logs reçus sont convertis dans des formats standards par des outils de conversion automatique ou *log parser*. Pour cela, le format SYSLOG est le plus utilisé. Une fois correctement converti, les données sont enregistrées dans les bases de données.

Le monitoring de logs, la troisième partie, contient les outils qui seront utilisés pour superviser, pour revoir les données de logs et les résultats des différentes analyses. Le monitoring de logs comprend un tableau de bord, des outils de génération de rapports, des outils de recherche dans les logs et surtout des outils de corrélation de logs.

La figure 2-4 représente un système de gestion de logs type.

2.2.3.2. Fonctions d'un système de gestion de logs

Les fonctions attendues d'un système de gestion de logs sont entre autres la collecte, l'analyse, le stockage et l'évacuation (supprimer). Ces fonctions doivent être réalisées sans altérer ou modifier de quel que ce soit les données des logs.

Selon [13] elles (fonctions) se divisent en quatre grands groupes. Ce sont les suivants :

- Général ;
- Stockage ;
- Analyse ;
- Disposition.

Les fonctions générales incluent la conversion de logs, le filtrage des événements, et l'agrégation des événements. La conversion de logs ou *log parsing* en anglais est le fait d'uniformiser tous les logs en un format unique et facilement compréhensible par les humains. Le filtrage des événements est la suppression des entrées de logs jugées inutiles parce qu'elles contiennent des informations qui ne nous intéressent pas. Les informations ainsi éliminées ne sont pas utiles pour l'analyse.

L'agrégation d'événements consiste à faire une consolidation d'un nombre d'entrées de logs similaires. Par exemple, dix (10) lignes concernant l'authentification échouée d'un compte utilisateur peuvent être résumées en une seule ligne « Tentative multiple d'authentification échouée pour le compte utilisateur admin sur le serveur mail. »

Les fonctions stockage regroupent les fonctions telles que la rotation de logs, la compression et l'archivage de logs, la normalisation de logs et la vérification de l'intégrité des logs.

2. Solutions de gestion de la sécurité

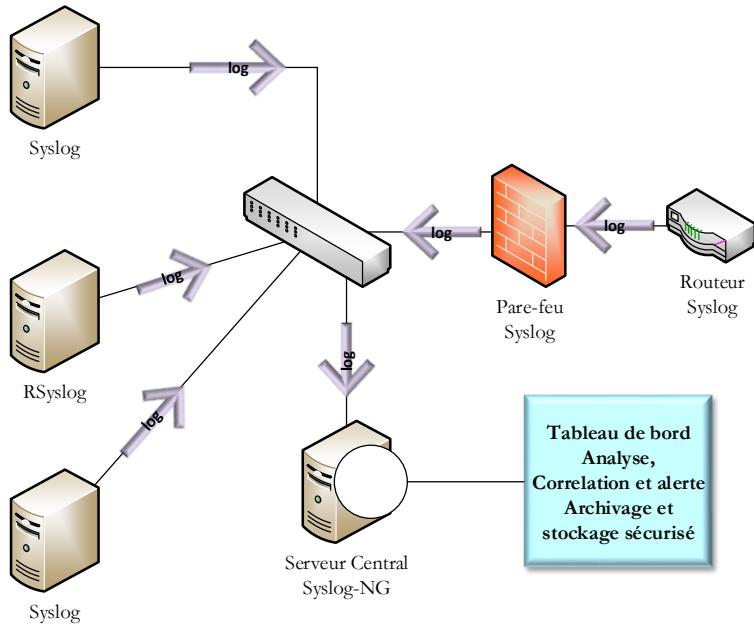


Figure 2-4 : Architecture d'un système de gestion de logs

La rotation de logs consiste à fermer des fichiers de logs existants et d'en créer de nouveaux, généralement suivant un planning bien spécifié (par heure, par jour, par mois, etc.). L'archivage de logs est le fait de garder les logs pour une période prolongée, généralement à des fins d'audit ou d'application des normes en vigueur. La vérification de l'intégrité des fichiers de log consiste à calculer des empreintes ou *message digest* et les stocker de manière sécurisée.

Les fonctions d'analyse rassemblent la corrélation d'événements, l'affichage et le reporting des logs. La fonction de corrélation d'événements recherche et trouve les relations entre les différentes entrées de logs. Cette corrélation est généralement basée sur les règles. Une autre méthode de corrélation est également utilisée telle que la méthode statistique. Ainsi, suivant la nature de l'information analysée, une alerte peut être générée pour attirer l'attention de l'analyste.

La fonction disposition est la partie chargée de supprimer des entrées de logs vieux d'un certain temps. Généralement, cette suppression a lieu lorsque les anciens ont été sauvegardés et archivés, ou ils n'ont pas assez d'importance pour être gardés.

2.2.4. L'équipe CIRT

Une CIRT (Computer Incident Response Team) encore appelée CERT (Computer Emergency Response Team) est une équipe ou département au sein d'une entreprise, chargé des questions relatives aux problèmes de sécurité de l'information, du réseau et des systèmes.

D'après [14] : « Une CERT est une organisation ou un département au sein d'une organisation chargé d'étudier la sécurité de l'Internet, découvrir les vulnérabilités et fournir l'assistance sécuritaire relative à une communauté identifiée. ». Ainsi, une CIRT surveille activement les activités du réseau et des systèmes, à la recherche d'éventuels intrusions ou signes d'intrusion. Pour ce faire, une CIRT doit être dotée d'outils lui permettant de collecter, d'analyser et de générer des alertes dès qu'il y'a une anomalie. Au sein d'une CIRT, on trouve : le responsable en chef, l'assistant au responsable en chef, des analystes, et des superviseurs.

2.3. Les solutions de supervisions de la sécurité réseau

Une solution de supervision de la sécurité réseau rentre dans la catégorie des SIEM (Security Information and Event Management). En effet, un SIEM encore appelé SIM (Security Information Management) est un outil qui permet d'avoir une vue unique sur tous les événements liés à la

2. Solutions de gestion de la sécurité

sécurité du réseau et des systèmes. Il comprend l'analyse et la corrélation de logs, de gestion des incidents et le reporting basé sur l'analyse d'événements. Un SIEM analyse d'autres données en plus des logs, mais la source de données primaire est le log [12].

Un SIEM agrège les données provenant des périphériques de sécurité, de réseau, des systèmes et des applications. Les données ainsi agrégées sont normalisées. Alors, un événement apparaissant plusieurs fois dans plusieurs sources différentes peut être corrélé. En plus des points cités plus haut, un SIEM fournit la capacité d'investigation (Forensic) à l'équipe CIRT. Cette dernière pourra entreprendre des mesures, escaladée l'incident ou simplement de le documenter. Quelques avantages d'un SIEM :

- Gestion de logs centralisée ;
- Corrélation de logs et mise en relation « cause à effet » ;
- Agrégation des événements de sécurité en une liste que l'on peut facilement gérer : classifié, catégorisé, etc.
- Permet de prévenir des dommages sur les ressources informatiques de l'entreprise ;
- Permet d'avoir un tableau de bord pour la gestion de la sécurité, l'assurance de conformité avec les politiques de sécurité, etc. ;

Il est important de savoir qu'il existe deux formes de supervision de la sécurité. La supervision de la sécurité de réseau proactive et la supervision de la sécurité de réseau réactive.

La supervision de la sécurité réseau proactive consiste à rechercher des vulnérabilités, des failles, des certificats invalides ou expirés, etc.

La supervision de la sécurité réseau réactive est la forme la plus utilisée. Elle consiste à la recherche d'incidents, à apporter une réponse aux incidents et à l'investigation de réseau.

2.3.1. Security Onion

Security Onion est une distribution Linux pour la détection d'intrusion, la supervision de la sécurité réseau et la gestion de logs [15]. Elle a été créée par Doug Burks. Sa dernière version est basée sur Ubuntu 14.04. Elle contient Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA (Enterprise Log Search and Archive), Xplico, NetworkMiner et plusieurs autres outils de sécurité [15]. Elle est totalement Open Source et est régulièrement maintenue à jour par Doug Burks et d'autres contributeurs.

Security Onion est une grande distribution qui facilite la mise en relation et l'intégration de plusieurs éléments. Ce qui fait d'elle, l'un des outils NSM les plus rapides à déployer à appréhender.

2.3.1.1. Snort

Snort est un système de détection et de prévention d'intrusion réseau (NIDS/NIPS) open source [16]. Il a été développé par Sourcefire, racheté par Cisco. Aujourd'hui, il est maintenu par Cisco [16]. C'est le NIDS/NIPS le plus déployé à nos jours [17].

Snort utilise la signature des règles, des protocoles et des anomalies comme techniques de détection d'intrusion. Il analyse le trafic en temps réel. En plus d'être un NIDS, il supporte d'autres modes de fonctionnement [18]. Ce sont le mode *Sniffer*, le mode *Packet Logger*.

Snort analyse en continu le trafic du réseau et génère des alertes d'intrusion à la moindre anomalie. Avec Security Onion, Snort est utilisé avec PF_RING pour avoir plus de capacité d'analyse [19]. Les règles sont régulièrement téléchargées à partir des bases de signatures de Snort. Il est également possible d'écrire ses propres règles.

2. Solutions de gestion de la sécurité

2.3.1.2. Suricata

A l'instar de Snort, Suricata est un également un système de détection et de prévention d'intrusion réseau basé sur les règles. Il est open source. Il est développé et maintenu depuis 2008 par Open Information Security Foundation (OISF), une organisation à but non lucratif [20]. Sa licence est distribuée sous GNU GPL.

Comme Snort, il peut fonctionner en d'autres modes (sniff et capture de paquets). Il télécharge les règles à partir des bases de signatures, mais il est également possible d'écrire ses propres règles pour la détection des menaces les plus complexes.

2.3.1.3. Bro

Bro IDS est un système de détection d'intrusion réseau à base d'analyse. C'est une plateforme d'analyse réseau puissante développée et maintenue par International Computer Science Institute à l'Université de Berkeley, en Californie [21]. La plateforme Bro est supportée (financièrement) par la National Science Foundation. Contrairement aux NIDS à base de règle, Bro effectue une analyse complète du trafic réseau, classe le trafic, et génère les alertes en cas d'anomalie.

Bro surveille le trafic, journalise toutes les connexions, tous les certificats SSL, toutes les requêtes DNS, http, ftp, ssh, etc., mais également les activités Syslog qu'il voit [15]. Ainsi, Bro arrive à détecter le trafic contenant un cheval de Troie, un fichier exécutable malicieux, etc., en temps réel. Il effectue également une corrélation temps réel des activités du réseau en utilisant les bases de renseignements sur les menaces [15]. Cela lui permet d'alerter l'utilisateur sur l'utilisation d'adresses IP malicieuses ou douteuses et des domaines douteux.

2.3.1.4. OSSEC

OSSEC (Open Source Security) est un HIDS (Host Intrusion Detection System) créé par Daniel Cid. OSSEC possède un puissant moteur de corrélation et d'analyse, qui intègre la vérification de l'intégrité des fichiers, la vérification du registre Windows, une politique de sécurité centralisée [22]. Il permet également la détection de Rootkit, l'alerte temps réel et un système de réponse active [23]. OSSEC est classé dans la catégorie des LIDS (Log-based Intrusion Detection System) [24] .

OSSEC supporte plusieurs modes de fonctionnement : local, serveur, agent et hybride. En mode serveur, les agents OSSEC remontent de manière sûre les résultats d'analyses vers le serveur, qui effectuera la corrélation. Ils vérifient l'intégrité des fichiers système en plus des fichiers spécifiés par l'utilisateur. Ils surveillent les logs de plusieurs applications, en comparant leurs contenus à des règles (prédéfinies ou personnalisées) et en faisant une corrélation par rapport à d'autres événements. A la moindre anomalie, OSSEC génère alors une alerte (SMS, email). Chaque alerte possède un niveau. Les niveaux varient de 0 à 15. Une alerte de niveau 0 est ignorée, tandis qu'une alerte de niveau 14 nécessite un traitement, car elle indique une compromission.

OSSEC convertit les logs suivant des décodeurs et fait l'analyse et la corrélation des événements en utilisant des règles. La plupart des règles sont préinstallées à l'installation d'OSSEC. Ces règles sont très souvent basées sur les indicateurs de compromissions [25] (IOC : Indicators of Compromise) et sur les bases de renseignements des menaces et des vulnérabilités actualisées.

2.3.1.5. Sguil

Sguil est une application de type desktop spécialement conçue pour la réception et l'affichage des alertes. Pour cela, elle est connectée à une base de données centrale hébergée sur MySQL. Elle a été créée par Bamm Visscher. Elle est maintenue comme open source, et sa dernière version à l'édition de ce document est 0.9.0.

2. Solutions de gestion de la sécurité

2.3.1.6. Squert

Squert est l'équivalent web de Sguil. Autrement dit, Squert permet de visualiser et d'effectuer des recherches sur les alertes enregistrées dans la base de données de Sguil. L'interface de Squert permet d'effectuer la chasse aux événements, en plus, elle permet d'effectuer des actions supplémentaires, comme vérifier la signature d'une alerte par rapport à base à jour de menaces.

2.3.1.7. ELSA

On ne peut pas présenter un SSR sans parler de gestionnaire de log. Enterprise Log Search and Archive (ELSA) est une plateforme de gestion de log centralisée à base de syslog. Elle est basée sur Syslog-NG, MySQL et Sphinx. Elle supporte des recherches de type *full text* sur un grand nombre de données. Son intégration avec Security Onion permet aux analystes de recherche dans les logs les événements liés par exemple aux alertes générées par les IDS ou les analyseurs réseaux, etc.

2.3.1.8. ELK

ELK (Elasticsearch Logstash Kibana) est une plateforme de gestion centralisée de log qui intègre plusieurs technologies ensemble dans le but de faciliter encore plus la recherche de log, la classification et bien d'autres choses. Son intégration dans Security Onion est en cours de test et devra à terme remplacer ELSA. C'est également une plateforme disponible en mode haute disponibilité et en mode distribué pour permettre une gestion ultra performante de très grandes quantités de logs.

2.3.2. OSSIM (Open Source Security Information Management)

OSSIM est un outil de supervision de la sécurité réseau également très populaire. C'est une solution pleinement fonctionnelle. Il a été créé en 2003 par AlienVault. Il est Open Source et continue à être maintenu par AlienVault. AlienVault développe une version payante de ce superviseur, c'est AlienVault USM (Unified Security Management) et elle coûte très chère.

OSSIM est basé sur la distribution Debian (une distribution Linux). Elle comporte beaucoup d'outils : OSSEC, OpenVAS, OCS Inventory, Evaluation de risque (Risk Assesment), Nagios Availability Monitor, Nmap, etc.

2.3.2.1. OSSEC

Nous avons décrit OSSEC dans une section précédente. Comme Security Onion, OSSIM déploie OSSEC comme HIDS à cause de ses qualités et son architecture agent/serveur.

2.3.2.2. Snort, Suricata

Les NDIS Snort et Suricata ont été décrits dans des sections précédentes. Ils sont présents dans OSSIM à l'instar de Security Onion.

2.3.2.3. OpenVAS

OpenVAS (Open Vulnerability Assesment System) est une plateforme qui intègre plusieurs outils et services qui permettent d'avoir un puissant scanneur de vulnérabilité [26]. En effet, OpenVAS permet d'analyser la vulnérabilité d'un quelconque système en effectuant toute une batterie de test. La plateforme OpenVAS est la version open source (libre) de Greenbone Networks (payante).

OSSIM intègre OpenVAS dans le but de fournir une plateforme d'évaluation de la vulnérabilité couplée à un SIEM.

2.3.2.4. Risk Assesment :

La fonctionnalité Risk Assesment ou évaluation du risque en français, permet d'évaluer le risque lié à un événement. Cette évaluation se base la priorité affecter à l'hôte concerné, la menace détectée et la probabilité d'occurrence de l'événement [27].

2. Solutions de gestion de la sécurité

2.3.2.5. OCS Inventory

OCS Inventory (Open Computer and Software) est une plateforme qui permet de réaliser l'inventaire du parc informatique (matériel et logiciel) de manière automatique [28]. Elle est très puissante et elle utilise une faible bande passante. Elle existe en deux versions, une version open source et une version payante. Sa dernière version est OCS Inventory NG 2.3.1. Elle supporte toutes les plateformes informatiques connues : Windows, MAC OS, Linux, Android, IOS.

OSSIM intègre OCS Inventory pour lui permettre de découvrir automatiquement toutes les machines et services activés sur le réseau. Ainsi, dès l'installation d'OSSIM, vous avez la possibilité de découvrir tous les ordinateurs et composants informatiques disponibles sur votre réseau, ce qui est très avantageux quand on est en face d'un réseau de plus de 1000 ordinateurs par exemple.

2.3.2.6. Nagios

Nagios est l'outil de supervision de réseau à ne plus décrire, tant qu'il a fait ses preuves. C'est un outil de supervision de réseau open source. Sa première version date de 1996 [29].

Il est intégré à OSSIM afin de permettre de gérer la disponibilité de machines configurées sur celle-ci (plateforme OSSIM).

2.3.3. ArcSight

ArcSight est une solution entreprise payante développée par Hewlett-Packard (HP), dans le but de fournir une solution de gestion de sécurité aux entreprises. Elle possède toutes les fonctionnalités d'un SSR. Sa licence coûte très chère.

ArcSight est disponible en plusieurs versions, toutes payantes. ArcSight Enterprise Security Manager (ESM) a été conçu pour des sociétés de grandes étendues (plusieurs milliers d'actifs à gérer) [30], tandis qu'ArcSight Express a été conçu pour les PME.

2.3.4. Splunk

Splunk à l'instar des autres SIEM et SSR monitore et gère les logs [30]. Splunk existe en deux versions. Une version gratuite limitée à 500 Mo de données à traiter et version payante au-delà des 500 Mo. Le prix devient rapidement exorbitant en fonction de la quantité de données à traiter.

Splunk propose plusieurs produits selon le budget des entreprises. Parmi ceux-ci, on trouve Splunk Enterprise, Splunk Cloud, etc.

2.3.5. Graylog2 :

Graylog2 est une solution open source de gestion log développée en java et basée sur Elasticsearch. Grâce à son système de plugin, on peut y ajouter beaucoup de plugins. Cela permet de l'exécuter comme un NSM, mais aussi en un SIEM.

2.1. Choix de la solution

Comme nous l'avons évoqué dans notre méthodologie, nous travaillerons dans ce projet avec des outils open source. Cela s'intègre également dans la vision de l'entreprise qui a une culture de l'open source fortement ancrée. De ce fait, nous avons étudié et testé trois solutions open source, à savoir : Security Onion, OSSIM et Graylog2. Les résultats des tests effectués sont répertoriés dans le tableau ci-dessous.

2. Solutions de gestion de la sécurité

Tableau 1 : Tableau comparatif des différentes solutions testées.

| Rubrique | AlienVault OSSIM | Graylog 2 | Security Onion |
|-------------------------------|------------------|-----------|----------------|
| Totalement Open source | ✗ | ✓ | ✓ |
| NSM | | ✓ | ✓ |
| SIEM | ✓ | ✓ | ✓ |
| Gestion et intégrité des logs | ✗ | ✓ | ✓ |
| Intégration avec l'existant | ✓ | ✗ | ✓ |
| Très bien documenté | ✓ | ✗ | ✓ |
| Mise à jour régulière | ✓ | | ✓ |
| Configuration matérielle | ✗ | ✗ | ✓ |
| Règles de corrélation | ✓ | ✗ | ✓ |
| NIDS Snort/Suricata | ✓ | ✗ | ✓ |
| HIDS OSSEC | ✓ | ✗ | ✓ |
| Tableau de bord | ✓ | ✗ | ✓ |
| Network Miner | | | ✓ |
| CapMe | | | ✓ |
| Wireshark | ✗ | | ✓ |
| Argus | | | ✓ |
| OpenVAS | ✓ | | |
| Nagios | ✓ | | |
| Support de Elasticsearch | | ✗ | |
| Logstash Kibana | | | ✓ |

Légende : ✓ : Caractéristique disponible à part entière, ✗ : Caractéristique disponible en partie

Les résultats nous démontrent la richesse de Security Onion par rapport aux autres solutions. En plus d'être un NSM puissant, il est totalement open source et présentent plusieurs outils pour l'investigation et les enquêtes poussées dont une équipe CIRT a besoin. Cela répond parfaitement au besoin et à la politique de l'entreprise.

Security Onion est très bien documenté. Il possède une grande communauté d'utilisateurs et un support même étant gratuit. Il nous permet aussi, si l'on veut utiliser un autre gestionnaire de log qu'ELSA, par exemple ELK, de le désactiver. Avec le responsable technique, nous avons choisi Security Onion.

2.2. Conclusion

Dans ce chapitre, nous avons effectué une étude détaillée des solutions de gestion de sécurité. Nous avons également choisi les composants de la solution à déployer.

Le prochain chapitre sera consacré au choix de la solution, à son déploiement et aux différentes configurations.

Chapitre 3. Déploiement de Security Onion

3.1. Introduction

Cette partie sera consacrée à l'architecture et au déploiement de la solution que nous avons choisie, c'est-à-dire Security Onion. Security Onion permettra de répondre aux questions que nous nous sommes posées au début de ce travail.

3.2. Architecture de Security Onion et déploiement

3.2.1. Architecture de Security Onion

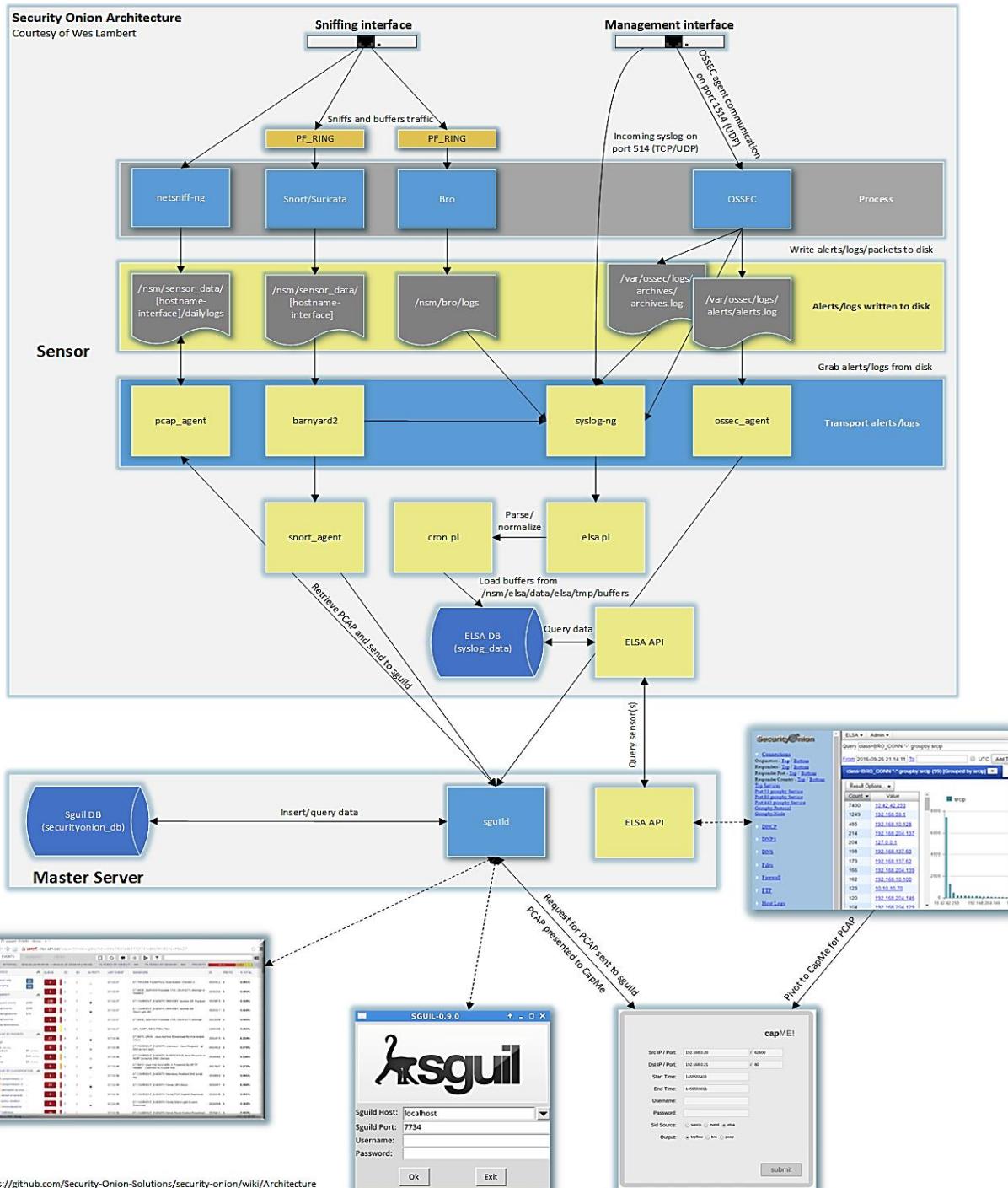


Figure 3-1 : Architecture de Security Onion, source [31]

3. Déploiement de Security Onion

Nous avons décrit les principaux composants de Security Onion dans le chapitre précédent. L'interaction entre ces différents composants est présentée dans la figure 3-1. Les composants sont repartis en collecteur, distributeurs et en consoles de visualisation. Ces différentes couches ont été décrites dans la section 2.1.2.1 du chapitre 2. Nous remarquons également que les composants sont regroupés à deux niveaux distincts : Sensor (sonde) et Master server (serveur).

Security Onion est une solution fondée sur le modèle distribuée client/serveur. Une sonde Security Onion est une machine sur laquelle sont installés plusieurs outils pour la collecte et l'analyse du trafic, c'est la machine cliente. Parmi ces outils, nous avons principalement : NIDS (Snort ou Suricata), l'analyseur de réseau Bro et OSSEC. Ces éléments ont été décrits dans le chapitre précédent. Les sondes remonteront leurs informations vers le serveur de Security Onion.

Un serveur Security Onion est une machine sur laquelle sont installées les consoles d'administration et de supervision de la sécurité du réseau. C'est à partir du serveur que l'équipe CIRT pourra mener les différentes opérations voir et gérer les incidents.

3.2.2. Architecture du réseau cible

La figure 3-2 présente une vue synoptique de l'architecture du réseau dans lequel nous allons installer Security Onion. Pour des raisons de confidentialité, certains détails ont été volontairement masqués, afin de ne pas divulguer des informations qui pourront compromettre la sécurité de l'entreprise.

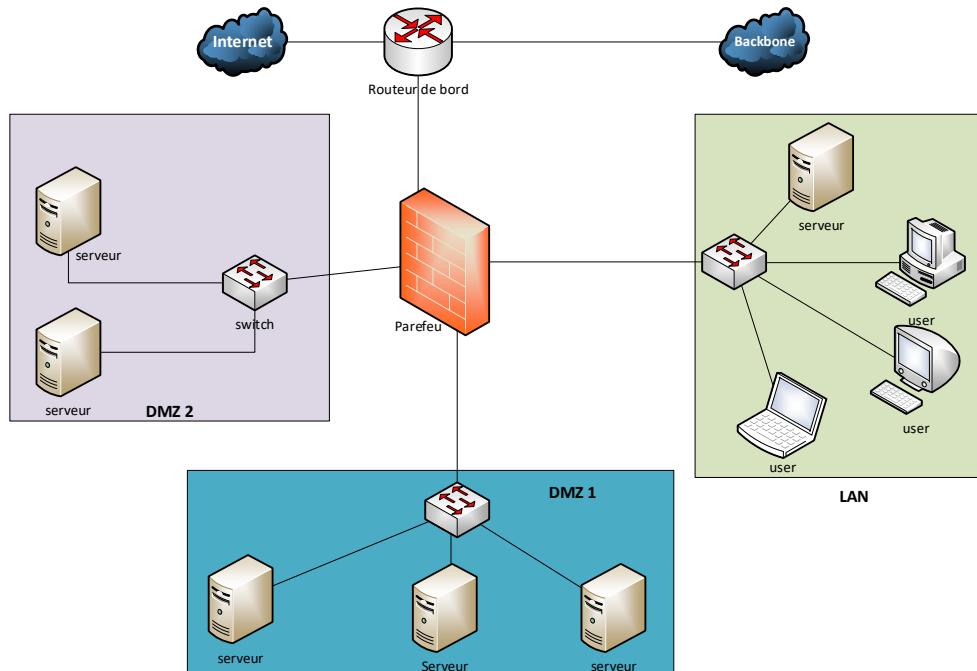


Figure 3-2 : Vue synoptique du réseau d'Afribone Mali

3.2.3. Modes de déploiement de Security Onion

Security Onion dispose de trois (3) modes de déploiement. Il s'agit du mode standalone ou intégré, du mode distribué et du mode hybride [15].

3.2.3.1. Mode serveur/sonde intégré (Standalone)

Dans ce mode de déploiement, une seule machine physique ou virtuelle est utilisée pour l'exécution du serveur et des composants de la sonde. Ladite machine peut avoir plusieurs interfaces, pour superviser plusieurs LAN. Ce mode de déploiement est utilisé pour les réseaux de petite taille.

3. Déploiement de Security Onion

3.2.3.2. Mode distribué

Ce mode déploiement consiste à utiliser une seule machine comme serveur, et plusieurs autres comme sondes. Il est recommandé en milieu fortement distribué, au niveau des réseaux de grande taille. Les analystes se connectent sur les consoles présentent sur le serveur.

3.2.3.3. Mode hybride

Le mode hybride permet d'avoir une machine standalone et des sondes remontant des informations vers le composant serveur de la machine standalone.

3.2.3.4. Mode de déploiement choisi

Dans ce projet, nous avons choisi le mode distribué. En effet, le réseau d'Afribone Mali a une taille conséquente, et supporte un grand trafic.

3.2.4. Emplacements des sondes et du serveur

À partir de l'architecture du réseau (figure 3-2), nous remarquons qu'il faut plusieurs sondes pour avoir une vue globale sur tout le trafic qui entre et sort du réseau. Partant de là, il faut alors choisir les emplacements des différentes sondes.

Le choix des emplacements des différentes sondes est crucial pour la réussite du déploiement. En effet, l'analyse continue du trafic réseau, représente l'un des nerfs de la solution à mettre en place. Les NIDS, analyseurs de réseau et de comportement, fonctionnent en capturant et en analysant le trafic en temps réel. La question qui se pose à ce moment est la suivante : comment capturer le trafic en continu sans influer sur celui-ci ? La réponse est la suivante : Il existe deux principaux moyens pour accomplir cette tâche, c'est à dire, la recopie des ports au niveau des switchs et l'utilisation d'enregistreur de trafic réseau *Network TAP*.

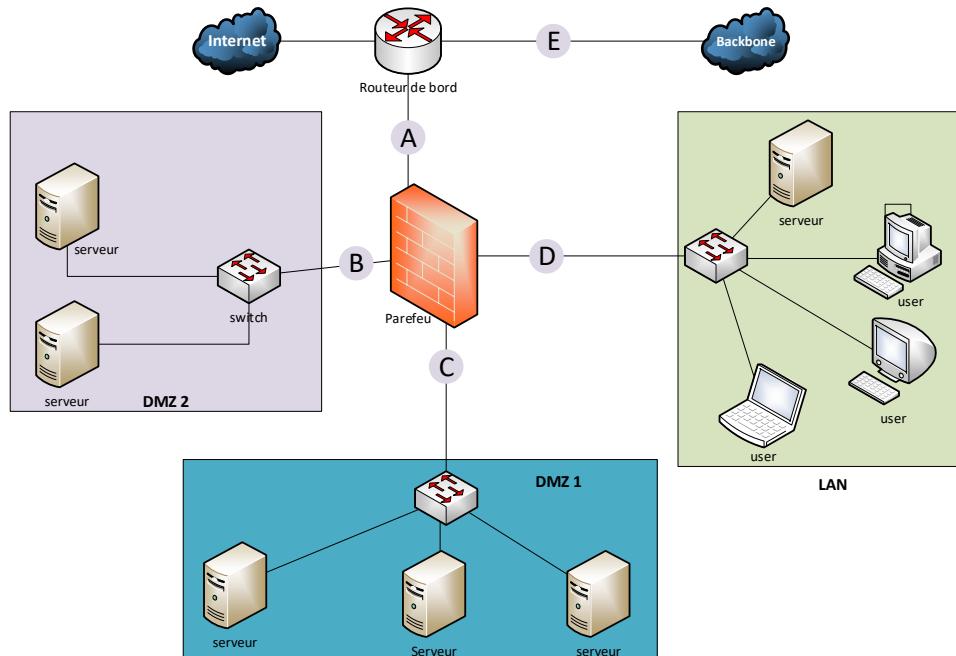


Figure 3-3 : Les emplacements possibles pour les sondes

La recopie des ports a plusieurs noms dans le jargon, selon les fabricants. Pour certains, c'est le *port spanning* (Cisco) pour d'autres c'est le *port mirroring* (dell). Cela consiste à recopier tout le trafic des ports indiqués vers un port spécifique du switch. C'est une fonction qui est disponible seulement sur les switchs de classes entreprises.

Un enregistreur de trafic réseau plus connu sous Network Tap est un équipement spécialement conçu pour recopier tout le trafic qu'il reçoit vers un port. Il est généralement placé sur le lien

3. Déploiement de Security Onion

agrégé (entre switch et routeur ou pare-feu). Son emplacement ne cause pas de problème en cas de panne, le trafic continuera à fluer, seul l'enregistrement sera arrêté. Dans notre projet, nous avons choisi d'utiliser le TAP.

Sur la figure 3-3, nous avons les emplacements suivants à partir desquels on peut positionner les différentes sondes. L'emplacement A situé entre le routeur de bord et le pare-feu nous permet de voir l'intégralité du trafic provenant du réseau local et des DMZ, mais le NAT (Network Address Translation) masque les adresses provenant des réseaux situés derrière le pare-feu. Donc, l'emplacement A ne sera pas utilisé. Les emplacements B, C et D sont parfaits pour nos sondes, car on peut voir passer tous les trafics provenant des différents sous réseaux. L'emplacement E nous permettra de voir le trafic à destination des clients, là aussi c'est un emplacement parfait pour voir le trafic des clients. Pour des raisons juridiques, nous n'avons pas été autorisés à placer de sonde à ce niveau. Pour finir, la configuration matérielle des sondes a également jouée sur l'emplacement des différentes sondes. Une sonde doit avoir une configuration matérielle proportionnelle au trafic supervisé.

Le serveur sera mis dans le LAN afin de le protéger contre les agressions venant de l'extérieur du réseau.

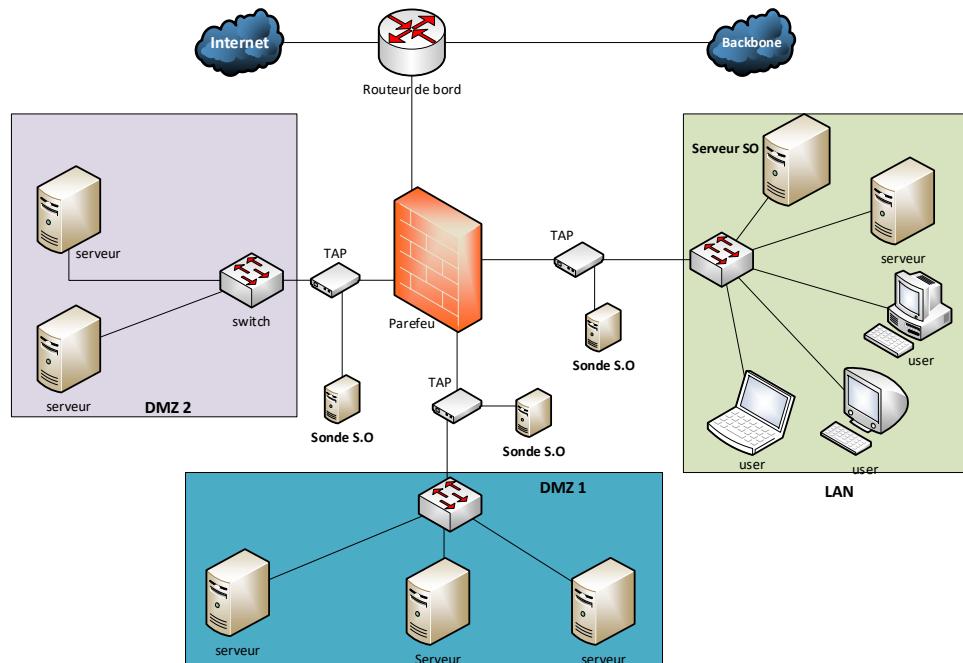


Figure 3-4 : Vue synoptique du réseau avec les sondes, les TAP et le serveur Security Onion

3.3. Installation du serveur et des sondes

3.3.1. Configuration matérielle

Les caractéristiques typiques des machines qui seront utilisées pour bien mener à terme les tâches de NSM sont les suivantes [32] :

- Processeur : 1 cœur de processeur par interface de monitoring.
- Mémoire RAM : Au minimum 4Go, avec 1 Go supplémentaire pour chaque interface monitorée connecté à un port SPAN ou un TAP pour par exemple un trafic de 200 Mb/s. Si le volume de trafic est très important, alors il faut augmenter en mémoire RAM, jusqu'à 256 Go ou plus, et cela en fonction de la taille de l'organisation.

3. Déploiement de Security Onion

- Disque dur : Grande capacité de stockage, avec comme système de stockage le RAID⁹. Il faut noter que les données de supervision et les trafics associés sont sauvegardés sur le disque.
- Carte réseau : au moins deux cartes réseaux par sonde.

3.3.2. Installation du serveur

La procédure d'installation de la distribution Security Onion est la même selon que la machine est en mode standalone, serveur ou sonde. Une fois cette installation terminée, il faut configurer la distribution. Cela se fait en cliquant sur le bouton *Setup*, à partir du bureau.

Une fois le Setup lancé, un menu se présente à nous pour la configuration des cartes réseaux, c'est-à-dire la carte de gestion *Management* et la carte *Sniffing*. On fixe alors l'adresse IP de la carte *Management*, la carte *Sniffing* sera sans adresse IP (figure 3-5).

Nous avons alors suivi toutes les étapes, en fournissant les informations comme l'adresse IP, le

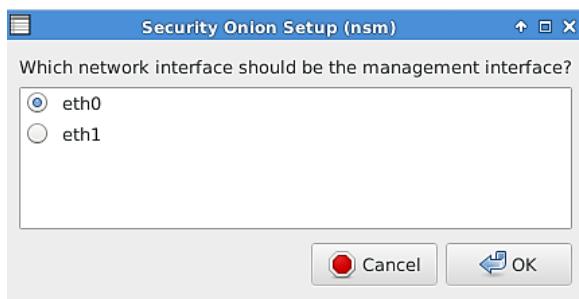


Figure 3-5 : Choix de l'interface réseau Management

masque de sous réseau, la passerelle par défaut et les serveurs DNS. Une fois ces étapes effectuées, nous obtenons cela (figure 3-6).

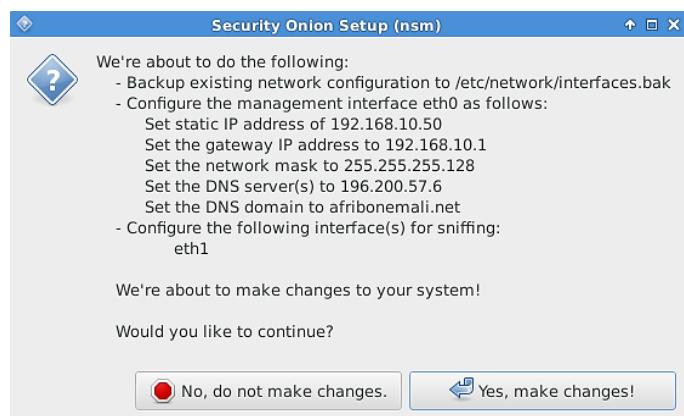


Figure 3-6 : Résumé de la configuration réseau

Après avoir validé cette configuration, la machine redémarre et nous lançons Setup encore une fois pour la configuration (figure 3-7).

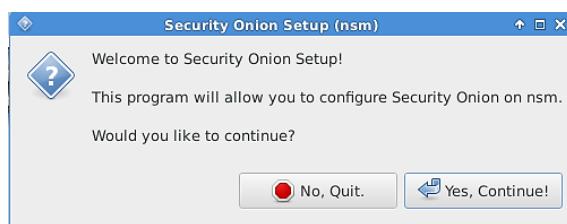


Figure 3-7 : Lancement de la configuration de Security Onion

⁹ Redundant Array of Independent Disk

3. Déploiement de Security Onion

Lorsque nous avons cliqué sur « Yes, Continue ! », le choix du cas d'utilisation se présente dans la fenêtre qui s'affiche. Nous choisissons Production Mode (figure 3-8).

Après avoir validé le choix sur Production Mode, la fenêtre suivante nous affiche le choix du mode du déploiement, c'est-à-dire Standalone, Serveur ou Sonde. Nous sommes en train d'installer le serveur, nous choisissons alors Serveur (figure 3-9).

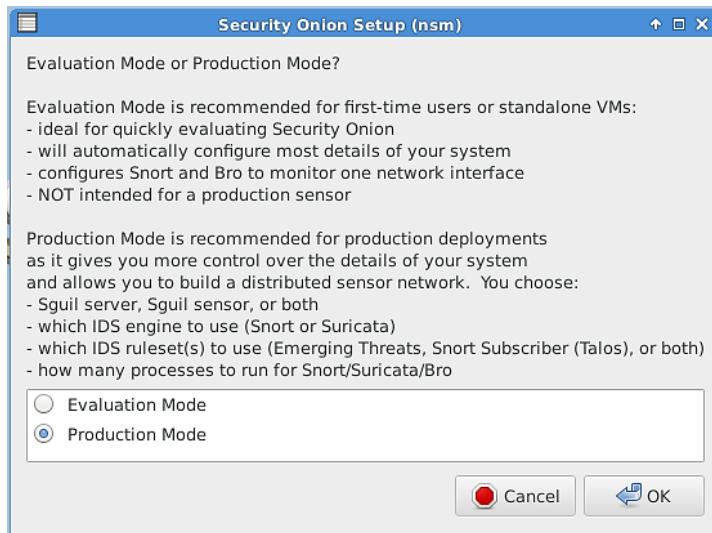


Figure 3-8 : Choix du cas d'utilisation

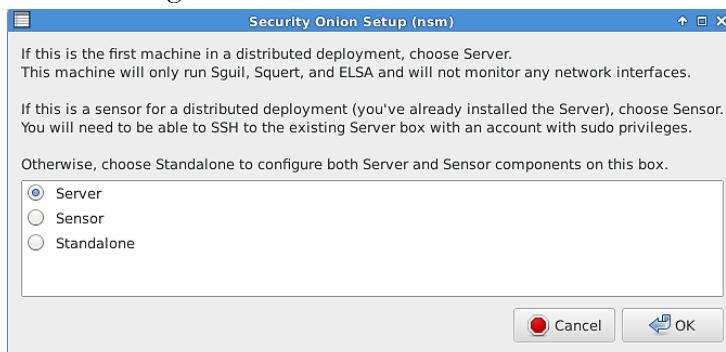


Figure 3-9 : Choix du mode de déploiement

Une fois le choix du mode de déploiement effectué, Security Onion nous demande de choisir le mode configuration (figure 3-10). Nous avons le choix entre « Best pratiques » et Custom. Nous choisissons « Custom » afin de complètement personnaliser notre installation.



Figure 3-10 : Choix du mode de configuration

Puisque nous sommes en train d'installer le serveur, nous devons configurer Sguil, Squert et ELSA. Pour cela, Security Onion nous demande de fournir un nom d'utilisateur et un mot de passe qui permet d'accéder à ses éléments (figure 3-11).

3. Déploiement de Security Onion

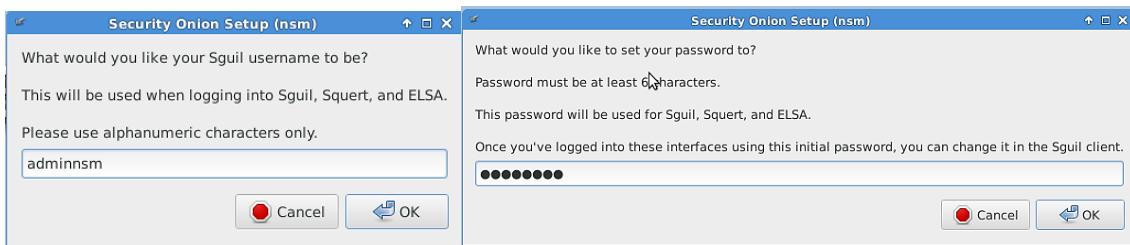


Figure 3-11 : Nom d'utilisateur/mot de passe pour Sguil, Squert et ELSA

Après le nom d'utilisateur/mot de passe, vient la configuration de la durée de sauvegarde des données d'alertes d'IDS, des événements et des données de session (figure 3-12).

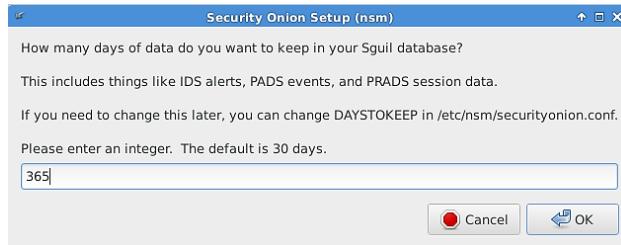


Figure 3-12 : Durée de garde des données

La fenêtre suivante nous propose deux NIDS parmi lesquels il faut choisir. Les NIDS proposés sont ceux de la distribution de Security Onion, c'est-à-dire Snort et Suricata. Nous avons choisi d'utiliser Snort (figure 3-13). Snort est le NIDS open source le plus utilisé, de plus il est très bien documenté.



Figure 3-13 : Choix du NIDS

Une fois le NIDS choisi, nous devons choisir la base de signature de ce dernier. Nous avons choisi la dernière option « Snort Subscriber (Talos) ruleset only and set a Snort Subscriber policy ». En effet, cette option permet à Snort d'aller chercher les signatures (ruleset) tous les jours au niveau des bases Snort couvrant la majeure partie des nouvelles menaces, et il nécessite d'avoir un Oinkcode. Un Oinkcode est un code unique associé à un compte utilisateur Snort (figure 3-14).

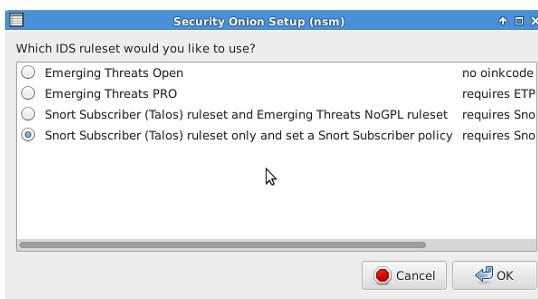


Figure 3-14 : Choix de la base de signature du NIDS Snort

Il faut à présent saisir l'Oinkcode que nous avons obtenu après notre enregistrement auprès de Snort (figure 3-15). Il faut noter que cet enregistrement se fait gratuitement.

3. Déploiement de Security Onion

Ensuite, il nous ait proposé de choisir d'activer Salt ou non. Salt permettra à notre serveur de plus facilement gérer les comptes d'utilisateurs des machines sondes, les clés SSH, etc. autrement dit, Salt permet au serveur de communiquer en sécurité avec les sondes. Nous choisissons de l'activer (figure 3-16).



Figure 3-15 : Saisie de l'Oinkcode

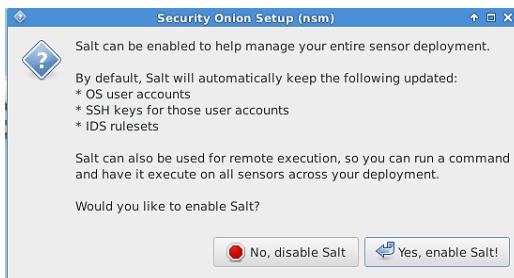


Figure 3-16 : Choix d'activation de Salt

L'étape suivante nous demande si l'on veut activer ELSA ou non. ELSA a été décrite dans le chapitre précédent. Si nous souhaitons utiliser une autre plateforme de gestion de logs autre qu'ELSA, nous le désactivons. Dans ce cas, nous avons d'utilisé ELSA (figure 3-17).

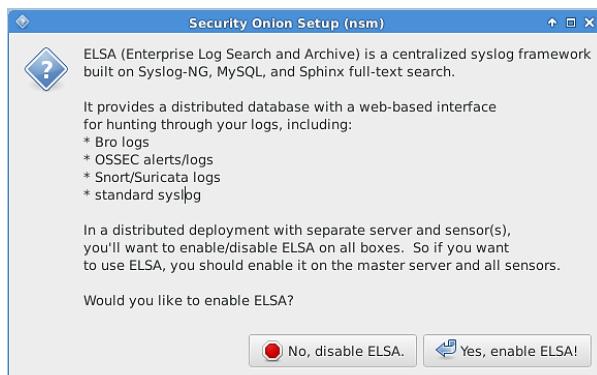


Figure 3-17 : Choix d'activation d'ELSA

Lorsqu'on choisit d'utiliser ELSA comme plateforme de gestion de logs, Security Onion demande de réserver de l'espace disque pour les logs (figure 3-18). Nous avons choisi 10Go pour un départ.

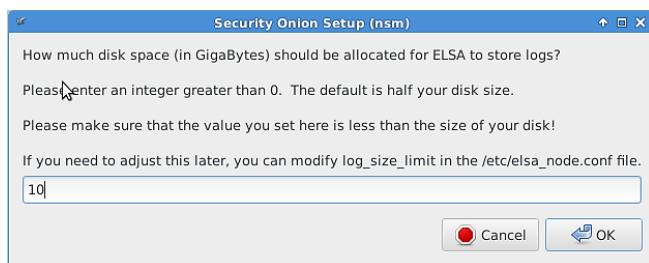


Figure 3-18 : Réservation d'espace disque pour les logs ELSA

Le résumé de l'installation à effectuer s'affiche et il faut cliquer sur valider pour démarrer l'installation et appliquer les réglages que nous avons choisi.

3. Déploiement de Security Onion

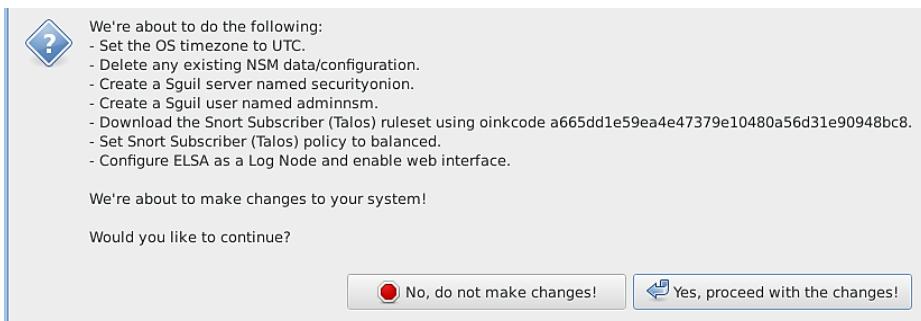


Figure 3-19 : Résumé des paramètres d'installation du serveur

Une fois l'installation terminée, nous avons exécuté la commande **sudo service nsm restart** pour redémarrer les services et avoir leurs statuts (figure 3-20).

```
admin-nsm@nsm:~$ sudo service nsm restart
Restarting: securityonion
  * stopping: sguil server
  * starting: sguil server
[ OK ]
Restarting: HIDS
  * stopping: ossec_agent (sguil)
  * starting: ossec_agent (sguil)
[ OK ]
admin-nsm@nsm:~$
```

Figure 3-20 : Etat des services du serveur Security Onion

On peut tester la console Sguil (figure 3-21) et l'interface d'ELSA (figure 3-22).

The SGUIL-0.9.0 interface shows a list of events:

| ST | CNT | Sensor | Alert ID | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|----|-----|-----------|----------|---------------------|---------|-------|---------|-------|----|-----------------------------|
| RT | 37 | nsm-ossec | 1.1 | 2017-05-02 16:18:55 | 0.0.0.0 | | 0.0.0.0 | | 0 | [OSSEC] Integrity checks... |
| RT | 1 | nsm-ossec | 1.6 | 2017-05-02 16:20:24 | 0.0.0.0 | | 0.0.0.0 | | 0 | [OSSEC] New group add... |
| RT | 5 | nsm-ossec | 1.36 | 2017-05-02 23:34:22 | 0.0.0.0 | | 0.0.0.0 | | 0 | [OSSEC] Integrity checks... |

Details of the last event (Alert ID 1.36):

Display Detail

Integrity checksum changed for: '/etc/gshadow'
 Size changed from '836' to '854'
 Old md5sum was: '8ea43b5bbbcf4e2f752ea9084ef20f68'
 New md5sum is : '0bbf9d247699c406ec35950bef9791b0'
 Old sha1sum was: '02539506331a1a749d7ba4b69c8b41504a5a97bb'
 New sha1sum is : '45385628d3be53f330c883ea66aef2015718678d'

Bottom panel:

- IP Resolution, Agent Status, Snort Statistics, System Ms
- Reverse DNS, Enable External DNS (checked)
- Src IP: []
- Src Name: []
- Dst IP: []
- Dst Name: []
- Whois Query: None Src IP Dst IP

Figure 3-21 : Console Sguil avec une alerte OSSEC détaillée

3. Déploiement de Security Onion

The screenshot shows the ELSA interface with a search bar at the top containing the query: 'class=none program="ossec" "alert" "Integrity checksum" "-ossec: Agent" "-ossec: Ossec" "-packets_received"'. Below the search bar, there are filters for 'From' (2017-05-01 09:01:09) and 'To' (2017-05-01 09:01:09), 'UTC', 'Add Term', 'Report On', 'Index', 'Reuse current tab', and 'Grid display'. The results table has 'Result Options...' and 'Field Summary' buttons. The table shows 100 records over 433 ms, with pages 1 through 15. The 'Fields' column displays the raw log data, which includes timestamp, alert level (Info), and alert details such as rule numbers (5501, 5502, 5503, 5504, 5505, 5506, 5507, 5508) and session information.

Figure 3-22 : Interface d'ELSA

3.3.3. Installation des sondes

La procédure d'installation d'une sonde Security Onion est presque la même que celle d'un serveur. Une fois l'installation de la distribution terminée, on procède par le lancement du Setup. Les premières étapes consistent à configurer les paramètres réseaux de la machine.

Quand les paramètres réseaux de la machine sont correctement configurés, on passe à l'étape d'installation des éléments de la distribution (figure 3-23).

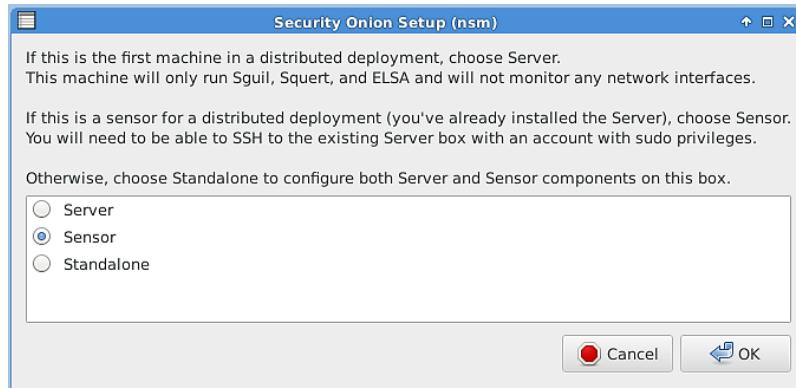


Figure 3-23 : Choix du mode de déploiement

Comme nous sommes en train d'installer une sonde, nous optons pour deuxième choix. Une fois le monde sonde choisi, Security Onion nous demande de fournir l'adresse IP du serveur maître. Dans notre cas, l'adresse IP du serveur est le 192.168.10.50 (figure 3-24).

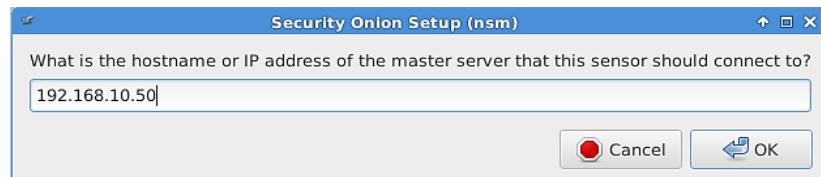


Figure 3-24 : Demande de l'adresse IP du serveur

Après avoir choisi l'adresse IP du serveur, nous devons indiquer un compte utilisateur qui possède les priviléges super utilisateur sur le serveur et qui peut y accéder en SSH (figure 3-25).

3. Déploiement de Security Onion

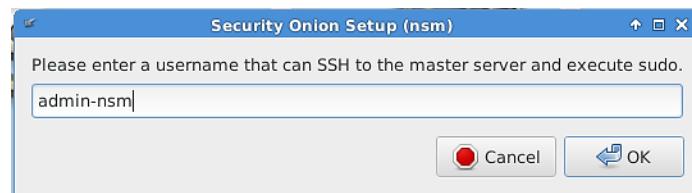


Figure 3-25 : Nom d'utilisateur possédant les droits SU sur le serveur

Une fois ces informations fournies, nous devons également configurer l'interface de *sniffing*. Nous avons configuré en amont l'interface eth0 comme interface de management. Nous choisirons l'interface eth1 comme interface de *sniffing* (figure 3-26).

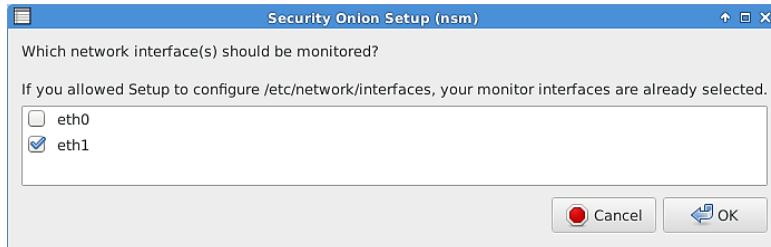


Figure 3-26 : Choix interface de sniffing

A présent nous devons choisir les modules que nous souhaitons activer. Security Onion nous propose d'activer ou non les NIDS. Nous choisissons Oui (figure 3-27).



Figure 3-27 : Activation des IDS

Lorsque nous avons activé les IDS, Security Onion nous a demandé de choisir un paramètre concernant les homes networks, c'est-à-dire les réseaux locaux. Nous laissons les valeurs par défauts à ce niveau (Classes d'adresses IP privées RFC 1918) : 192.168.0.0/24, 10.0.0.0/8, 172.16.0.0/16.

Ensuite SO nous demande si l'on souhaite, d'activer l'analyseur Bro. Nous choisissons d'activer Bro, car il sera l'œil de notre réseau en plus des NDIS et HIDS (figure 3-28).



Figure 3-28 : Activation de l'analyseur Bro

L'analyseur Bro possède la capacité d'extraire tous les fichiers exécutables, et peut les stocker dans un emplacement à partir duquel on peut y accéder. Cette fonctionnalité est très intéressante dans le cadre d'une investigation en cas de présence d'un fichier malicieux ou suspect sur le réseau (figure 3-29).

3. Déploiement de Security Onion

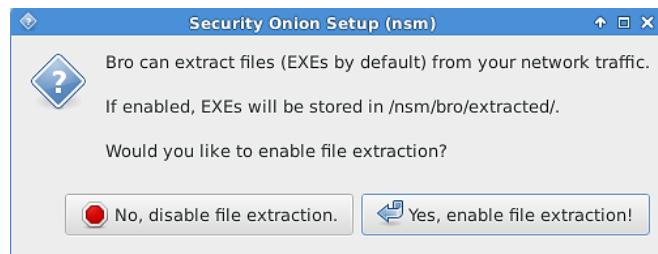


Figure 3-29 : Activation de l'extraction des exes par Bro

Security Onion embarque Argus. Argus surveille le trafic réseau et log toutes les données de session vers le serveur. Ceci est particulièrement intéressant lorsqu'un analyste souhaite voir toutes les activités en rapport avec une session [33] (figure 3-30).

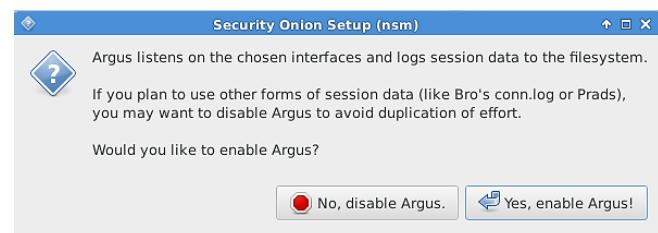


Figure 3-30 : Activation d'Argus

Après avoir effectué toutes ces étapes, la configuration de notre sonde n'est pas encore terminée. Nous devons choisir le mode de surveillance du trafic du réseau. Pour cela, Security Onion nous offre deux possibilités : Sauvegarde complète du trafic ou sauvegarde simple des trafics relatifs aux différents événements d'alertes (figure 3-31).

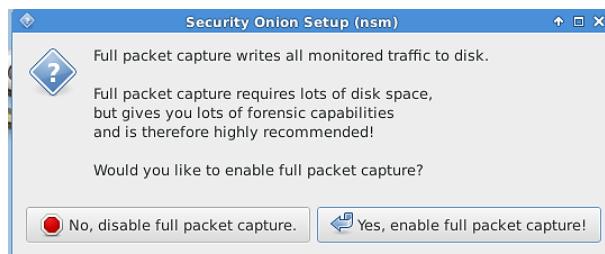


Figure 3-31 : Option Full packet capture

L'option full packet capture est très intéressante dans la mesure où elle va permettre la revue de l'entièreté des données capturées à partir du réseau. Son inconvénient est qu'il prend beaucoup d'espace disque.

Ensuite Security Onion nous demande de fournir l'espace disque à remplir pour déclencher une purge des logs. Par défaut nous laissons cette à 90 pourcent (figure 3-32).

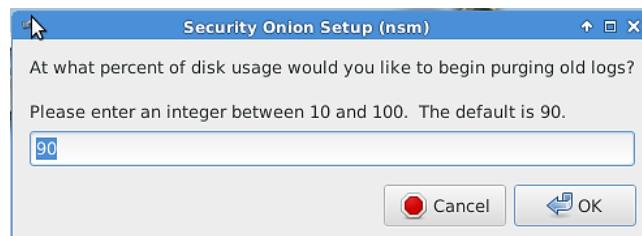


Figure 3-32 : Espace disque à réserver

Une fois effectué, SO nous demande si l'on souhaite activer Salt. Nous choisissons l'option activer Salt. Nous avons déjà activé Salt sur le serveur (figure 3-33).

3. Déploiement de Security Onion

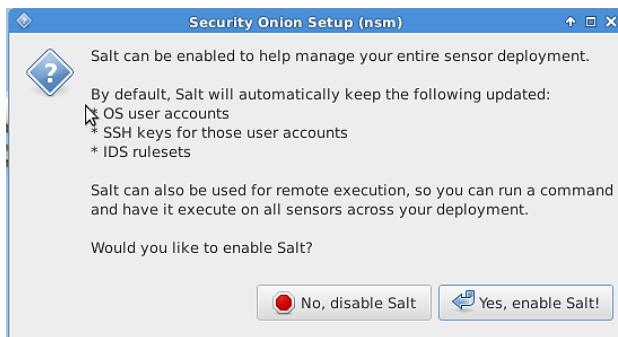


Figure 3-33 : Activation de Salt sur une sonde

Dans l'étape suivante nous devons activer ELSA (figure 3-34).

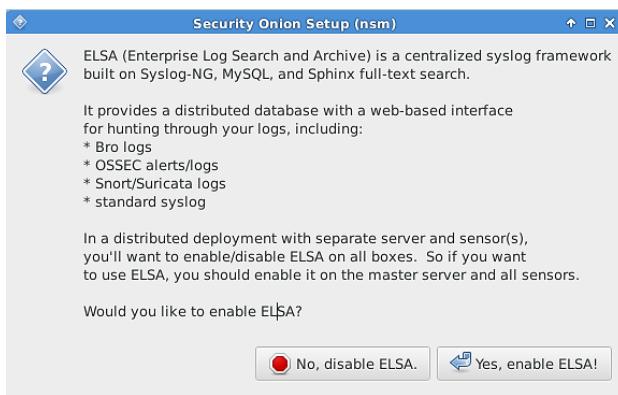


Figure 3-34 : Activation d'ELSA

Après avoir activé ELSA comme un nœud sur la sonde, l'étape suivante demande de mettre à jour ELSA sur le serveur (figure 3-35).

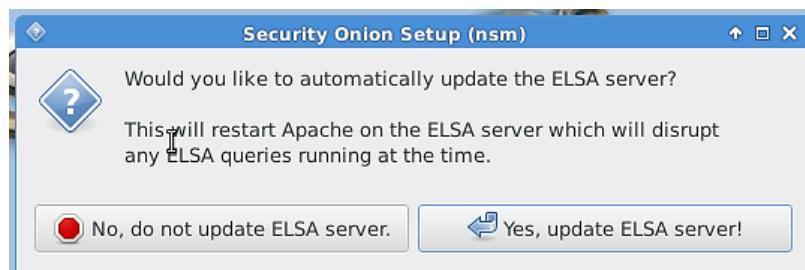


Figure 3-35 : Mise à jour du nœud serveur

Pour procéder à l'installation et appliquer les choix que nous avons faits, nous cliquons sur le bouton « Yes, proceed with the changes ! » (figure 3-36).

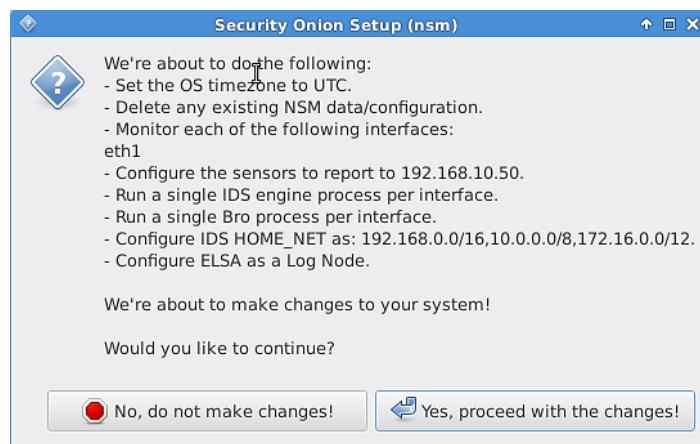


Figure 3-36 : Résumé des paramètres d'installation de la sonde

3. Déploiement de Security Onion

Après l'installation, nous avons exécuté la commande **sostat redacted** pour vérifier l'état des services.

```
root@nsm:/home/admin-nsm# sostat redacted
=====
Service Status
=====
Status: HIDS
  * ossec_agent (sguil)[ OK ]
Status: Bro
Name      Type    Host        Status   Pid  Started
manager   manager localhost  running  9802  03 May 11:58:09
proxy     proxy   localhost  running  9845  03 May 11:58:10
nsm-eth1-1 worker  localhost  running  9890  03 May 11:58:12
Status: nsm-eth1
  * netsniff-ng (full packet data)[ OK ]
  * pcap_agent (sguil)[ OK ]
  * snort_agent-1 (sguil)[ OK ]
  * snort-1 (alert data)[ OK ]
  * barnyard2-1 (spooler, unified2 format)[ OK ]
  * argus[ OK ]
```

Figure 3-37 : Une partie des résultats de la **sostat redacted**

3.4. Conclusion

Dans cette partie, nous avons réalisé le gros du travail, c'est-à-dire, le choix de l'emplacement des sondes et le déploiement de la solution de supervision de la sécurité du réseau. Nous avons également effectué les configurations initiales.

Le prochain chapitre est consacré aux configurations avancées, aux personnalisations, la mise en place de l'équipe CIRT et les tests.

Chapitre 4. Configurations, Mise en place de l'équipe CIRT, Tests

4.1. Introduction

Ce chapitre sera consacré à la configuration des nœuds de Security Onion, c'est-à-dire le serveur et les sondes. Nous avons précédemment décrit l'architecture du déploiement et nous avons effectué l'installation et les configurations initiales du serveur et des sondes. Dans cette partie, nous allons nous appesantir sur les configurations avancées, les tests et la mise en place de l'équipe CIRT.

4.2. Configurations de Security Onion

Les fichiers relatifs à la configuration de SO sont localisés dans le répertoire /etc/nsm, et cela quel que soit la machine sur laquelle on se trouve (serveur/sonde). Dans ce répertoire, on trouve les configurations de tous les outils.

4.2.1. Configuration du serveur

Pour vérifier que tous les services activés sur le serveur fonctionnent normalement, nous exécutons la commande **service nsm status**. Le résultat de cette commande devra afficher cela (figure 4-1).

```
root@nsm:/etc/nsm# service nsm status
Status: securityonion
  * sguil server                                     [  OK  ]
Status: HIDS
  * ossec_agent (sguil)                             [  OK  ]
root@nsm:/etc/nsm#
```

Figure 4-1 : Etat des services sur le serveur SO

Sur le serveur, il est possible de configurer la durée de sauvegarde des archives avant leurs suppressions. Cette configuration se fait dans le fichier /etc/nsm/securityonion.conf. Dans ce fichier, on fixe la valeur de la variable DAYSTOKEEP. Par défaut, cette valeur est fixée à 30, mais nous avons choisi 365 jours.

```
# Which IDS engine would you like to run?
ENGINE=snort

# How many days would you like to keep in the Sguil database archive?
DAYSTOKEEP=365

# How many days worth of tables would you like to repair every day?
DAYSTOREPAIR=7
```

Figure 4-2 : Configuration de la durée d'archivage de SO

4.2.2. Configuration des sondes

4.2.2.1. Généralités

L'une des tâches les plus importantes d'une sonde est la fonction d'IDS. Ainsi, après l'installation, il est possible configurer les réseaux surveillés par l'IDS installé, s'ils sont différents des réseaux du RFC 1918. Les configurations relatives à une sonde se font dans le répertoire /etc/nsm/\$HOSTNAME-INTERFACE/. \$HOSTNAME correspond au nom d'hôte de la sonde et INTERFACE correspond à l'interface monitorée.

Une fois dans ce répertoire, on modifie soit **snort.conf** ou **suricata.yaml**, dépendant de l'IDS installé.

Sur la figure 4-3, la variable HOME_NET permet de configurer les réseaux internes à surveiller.

HOME_NET est configurée avec les réseaux de classe privée du RFC 1918. On remarque que la variable EXTERNAL_NET, avec comme valeur **any**, cela permet de s'intéresser à tous les réseaux provenant de l'extérieur.

4. Configurations, Mise en place de l'équipe CIRT, Tests

```
# Setup the network addresses you are protecting
ipvar HOME_NET [192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
```

Figure 4-3 : Configuration des réseaux Snort

La configuration des réseaux à surveiller par l'analyseur Bro se fait dans le fichier `/opt/bro/etc/networks.cfg`.

```
[# List of local networks in CIDR notation, optionally followed by a
# descriptive tag.
# For example, "10.0.0.0/8" or "fe80::/64" are valid prefixes.

192.168.0.0/16
10.0.0.0/8
172.16.0.0/12
```

Figure 4-4 : Configuration des réseaux Bro

Comme avec Snort, les réseaux configurés par défaut sont les réseaux de classes privées du RFC 1918.

En plus des règles prédéfinies, des règles téléchargées, Snort nous permet d'écrire nos propres règles. L'ensemble de ces règles se trouve dans le répertoire `/etc/nsm/rules`. Des règles spécifiques à une sonde se trouvent dans le fichier `/etc/nsm/$HOSTNAME-INTERFACE/rules/local.rules`.

Les alertes de Snort sont configurées pour être envoyées au format **baynard2**. « baynard2 » est configuré pour transcrire les sorties de Snort vers la base de Sguil.

4.2.2.2. Règles personnalisés

L'une des puissances de Snort est qu'il nous donne la possibilité d'écrire nos propres règles. Une règle Snort se découpe en deux parties : l'entête de la règle, et les options de la règle.

L'entête de la règle contient les actions à entreprendre, le protocole auquel la règle s'applique, et les ports sources et de destinations. Les options de la règle nous permettent de spécifier un message descriptif à associer à la règle, mais les vérifications d'autres champs des paquets. Elles correspondent au corps de la règle.

La syntaxe d'une règle Snort est la suivante : **action proto src_ip src_port direction dst_ip dst_port (options)** [34].

action correspond à l'action à entreprendre au cas où un paquet correspond à la règle. Snort comporte plusieurs actions intégrées. On peut citer par exemple **log**, **alert**, **activate**, **pass**. Il est possible d'écrire sa propre action à entreprendre.

proto correspond au protocole à analyser. Ils sont au nombre de quatre (4) : tcp, udp, ip, et icmp.

src_ip et **dst_ip** correspondent aux adresses IP source et de destination à regarder. En général, pour une règle dont la direction est de l'extérieur vers intérieur, le champ **src_ip** est mis à la chaîne **any**. Il est possible d'utiliser la notation CIDR pour définir un réseau de destination au lieu d'une seule adresse de destination.

4. Configurations, Mise en place de l'équipe CIRT, Tests

Les champs **src_port** et **src_dst** sont pour les ports sources et destinations. Ils peuvent prendre la valeur **any**.

Etant donné le nombre très important de règles disponibles et téléchargées par Snort, il est très rare de voir un analyste écrire ses propres règles. La figure 4-5 montre le nombre de règles disponibles pour notre IDS Snort dans SO. La commande **sostat | less** nous permet d'avoir cette information.

```
Rule Stats...
New:-----20
Deleted:---0
Enabled Rules:----9336
Dropped Rules:----0
Disabled Rules:---23173
Total Rules:-----32509
No IP Blacklist Changes
Done
Please review /var/log/nsm/sid_changes.log for additional details
Fly Piggy Fly!
```

Figure 4-5 : Statistique des règles Snort

Nous remarquons qu'à partir de ces statistiques, qu'il y'a 32 509 règles au total dont 9336 règles sont actifs.

Exemple : alert tcp any any -> any any (flags : SF, 12 ; msg : "Scan possible en cours";)

Cette règle demande à Snort d'inspecter tous les paquets entrant et sortant, n'importe quelle adresse source et destination, n'importe quel port source et destination. Il va chercher si les drapeaux SYN et FIN sont activés, cela permet de savoir s'il s'agit d'un type de scan de port. S'il trouve des paquets avec les FLAGS TCP fixé à SF, il génère une alerte avec le message « Scan possible en cours ».

4.2.3. Configuration des LIDS

4.2.3.1. Généralités

D'autres configurations sont disponibles, notamment celles des HIDS/LIDS. Les agents/serveurs OSSEC prennent en charge cette fonction.

La configuration d'OSSEC se fait dans le fichier **/var/ossec/etc/ossec.conf**. Ce fichier contient beaucoup de sections de configuration [24].

OSSEC surveille les logs en se basant sur des règles bien définies. S'il détecte une anomalie par rapport aux règles, OSSEC envoie des alertes dans le fichier **/var/ossec/logs/alerts/alerts.log**. L'agent OSSEC intégré au serveur SO lit les alertes, les retranscrit puis les envoient à la base de Sguil. Ainsi, on peut se référer à [35] pour les éléments à surveiller lors d'écriture des règles de corrélation.

OSSEC peut être configuré pour envoyer les alertes d'un certain niveau par email.

4.2.3.2. Règles personnalisés

OSSEC possède ses propres parseurs de logs et règles de corrélation. Il comporte des règles pour la plupart des applications et systèmes connus. Si on dispose d'une application qui n'est pas supportée par OSSEC, par exemple une application développée en interne, on peut écrire ses propres règles et parseurs pour la prise en charge de cette application.

Les fichiers de log à surveiller sont configurés dans la section **localfile** du fichier de configuration d'OSSEC.

Les règles et les décodeurs d'OSSEC sont écrits au format xml. Les décodeurs sont localisés dans les fichiers **/var/ossec/etc/decoders.xml** et **/var/ossec/rules/*.xml**.

4. Configurations, Mise en place de l'équipe CIRT, Tests

Exemple : Décodage et règle pour un log spécifique à une application non prise en charge par ossec.

```
2017-05-05 10:09:35 "Tentative d'accès avec un compte d'utilisateur inexistant"  
login:manger [192.168.10.18]
```

Figure 4-6 : Un enregistrement dans un log d'une application non prise en charge

Décodeur :

```
<decoder name="diagokelan-access">  
    <type>diagokelan-log</type>  
    <prematch>^[\S+]</prematch>  
    <regex offset="after_prematch">^\w+ user\S\S+ [\d+\.\d+\.\d+\.\d+]</regex>  
    <order>user, srcip</order>  
</decoder>
```

Règle :

```
<rule id="1112" level="8">  
    <if_sid>1111</if_sid>  
    <decoded_as>diagokelan</decoded_as>  
    <match>^Tentative d'accès echoué</match>  
    <srcip>\d+\.\d+\.\d+\.\d+</srcip>  
    <description>Accès non autorisé</description>  
</rule>
```

Figure 4-7 : Décodeur et règle personnalisé OSSEC pour le log de la figure 4-6

4.2.4. Maintenance de Security Onion

L'installation et les configurations initiales du serveur et des sondes Security Onion ne sont que les débuts de l'aventure. Les composants installés ont besoin d'être régulièrement mis à jour. Les espaces de stockage que demandent ces différents services sont grands et doivent être régulièrement surveillés.

4.2.4.1. Mises à jour

La plateforme NSM de Security Onion s'exécute sur une distribution Linux, et a besoin d'être régulièrement mise à jour. Un système qui n'est pas régulièrement mis à jour tournera certainement avec beaucoup de failles et de vulnérabilités.

SO tourne sur Ubuntu, donc, nous permet alors d'effectuer des mises à jour à travers le gestionnaire de paquets **apt**. Cela peut se faire soit en mode graphique ou en mode ligne de commande.

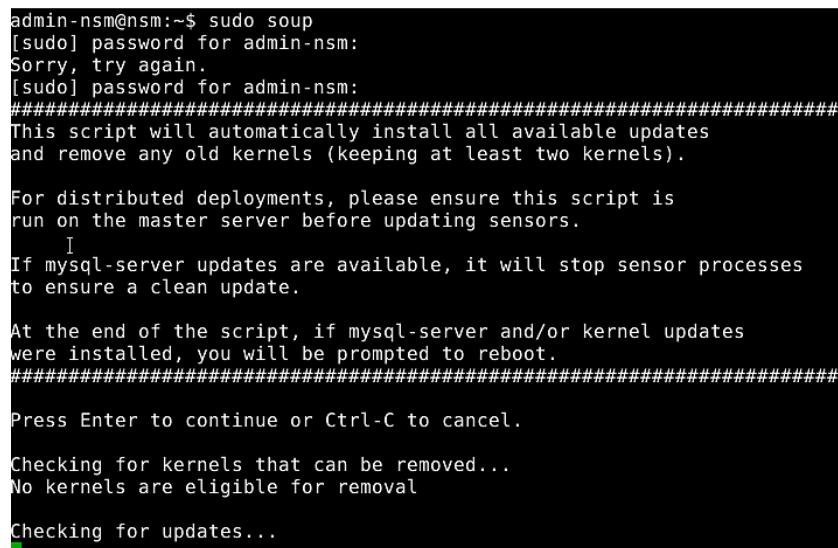
En cliquant sur le bouton « Install Now », le système télécharge et installe les mises à jour directement en mode graphique. Il faut également noter que les mises à jour en mode graphique (sont recherchées et proposées automatiquement).

En mode console, on utilise la commande **apt-get update** et **apt-upgrade**. La première commande permet rechercher les mises à jour génériques pour la plupart des applications et des packages installés sur le système. La deuxième commande vérifie les applications out daté, et propose de leur mettre à jour. L'upgrade concerne les applications ou les paquets de version inférieure par rapport à la version à jour.

4. Configurations, Mise en place de l'équipe CIRT, Tests

Les mises à jour mentionnées ci-dessus sont pour le système, les packages et les applications installées. SO dispose d'un outil pour les mises à jour qui lui est spécifiques. À travers cette plateforme, SO met à jour les différents composants et outils qu'il intègre. Il s'agit de l'outil **soup**.

Comme notre déploiement est distribué, **soup** est combiné à **salt** pour la mise à jour des sondes [36]. La procédure à suivre est d'abord de mettre à jour le serveur. Pour cela, on exécute la commande **soup** sur le serveur (figure 4-8).



```
admin-nsm@nsm:~$ sudo soup
[sudo] password for admin-nsm:
Sorry, try again.
[sudo] password for admin-nsm:
#####
This script will automatically install all available updates
and remove any old kernels (keeping at least two kernels).

For distributed deployments, please ensure this script is
run on the master server before updating sensors.
    I
If mysql-server updates are available, it will stop sensor processes
to ensure a clean update.

At the end of the script, if mysql-server and/or kernel updates
were installed, you will be prompted to reboot.
#####

Press Enter to continue or Ctrl-C to cancel.

Checking for kernels that can be removed...
No kernels are eligible for removal

Checking for updates...
```

Figure 4-8 : Mise à jour de Security Onion avec soup.

4.2.4.2. Limiter les accès

Le serveur doit être protégé contre les accès non autorisé. Pour cela, nous ouvrons seulement les ports autorisés à savoir : 514 pour Syslog, 22 pour SSH, 1514 pour OSSEC et 443 pour l'accès HTTPS.

UFW (Uncomplicated FireWall) est l'utilitaire qui sert de pare-feu pour la distribution SO. Pour contrôler l'état des ports ouverts au niveau du pare-feu, on utilise la commande **ufw status**.

4.2.4.3. Gérer les espaces disques

Aussitôt bien installé et configuré, les outils Security Onion commencent à sniffer le trafic du réseau en direct. Si la fonction **full packet capture** est activée, alors les sondes et le serveur sauvegarde tout le trafic sniffer. Cela demande une disponibilité de grands espaces de stockage pour le court et le moyen terme. Cette fonction est réalisée par l'outil **netsniff-ng**. Netsniff-ng est capable de sniffer un lien jusqu'à 10 Gb/s.

Les outils NSM qu'embarque SO commencent alors à collecter, à interpréter et à analyser les données en live du réseau. Les données collectées par ces outils sont de divers types (cf. chapitre 2). Ces données sont ensuite enregistrées dans divers emplacements au niveau du disque. Selon [6], parmi ces emplacements, deux sont les plus importants :

- **/nsm** répertoire dans lequel sont stockés tous les logs et les données capturées ;
- **/var/lib/mysql** répertoire de stockage des bases de données MySQL.

Le répertoire **/var/lib/mysql** utilise moins d'espace que **/nsm**. Les données de SO sont stockées dans le répertoire **/nsm/sensor_data/nomsonde-interface/dailylogs/YYYY-MM-DD**. Nomsonde correspond au nom d'hôte de la machine sonde. Le nom du fichier que ce dossier contient est snort suivi du timestamp (au format Unix) auquel le fichier a été modifié. Le contenu du fichier est au format pcap.

4. Configurations, Mise en place de l'équipe CIRT, Tests

```
root@nsm:/nsm/sensor_data/nsm-eth1/dailylogs/2017-05-09# ls -l
total 684
-rw-r--r-- 1 sguil sguil 12587009 May  9 12:04 snort.log.1494328773
root@nsm:/nsm/sensor_data/nsm-eth1/dailylogs/2017-05-09#
```

Figure 4-9 : Aperçu d'un dossier journalier

```
root@nsm:/var/lib/mysql# ls -l
total 28696
-rw-r--r-- 1 mysql mysql      0 Sep  3 2016 debian-5.5.flag
drwx----- 2 mysql mysql    4096 May  4 09:40 elsa_web
-rw-rw---- 1 mysql mysql 18874368 May  9 12:24 ibdata1
-rw-rw---- 1 mysql mysql 5242880 May  9 12:24 ib_logfile0
-rw-rw---- 1 mysql mysql 5242880 May  8 11:05 ib_logfile1
drwx----- 2 mysql mysql    4096 Sep  3 2016 mysql
-rw-rw---- 1 mysql mysql      6 Sep  3 2016 mysql_upgrade_info
drwx----- 2 mysql mysql    4096 Sep  3 2016 performance_schema
drwx----- 2 mysql mysql    4096 May  4 09:39 syslog
drwx----- 2 mysql mysql    4096 May  9 11:18 syslog_data
```

Figure 4-10 : Contenu du dossier des bases de données de MySQL

La figure 4-10 nous montre le contenu du dossier des bases de données de MySQL. On y remarque que les bases de données créées sont : elsa_web, syslog, syslog_data. Les autres sont les bases spécifiques à MySQL.

L'un des principaux avantages de SO est le fait qu'il dispose de plusieurs scripts qui vérifient régulièrement l'utilisation de l'espace disque. Si l'espace disque utilisé atteint le seuil fixé¹⁰, les scripts effacent automatiquement les anciennes données capturées (pcap). Par défaut, ce seuil est fixé à 90% de l'espace disque.

Les bases de données Sguil, Syslog et ELSA enregistrées sur MySQL occupent beaucoup d'espace disque. Pour vérifier l'espace disque occupé par ces différentes bases, l'utilisateur doit simplement se connecter au serveur MySQL et exécuter la requête suivante :

```
SELECT DBName, CONCAT(LPAD(FORMAT(SDSize/POWER(1024,pw),3),17,''),',
-> SUBSTR(' KMGTP',pw+1,1),'B') "Data Size",CONCAT(LPAD(
-> FORMAT(SXSize/POWER(1024,pw),3),17,''),',',SUBSTR(' KMGTP',pw+1,1),'B') "Index Size",
-> CONCAT(LPAD(FORMAT(STSize/POWER(1024,pw),3),17,''),',
-> SUBSTR(' KMGTP',pw+1,1),'B') "Total Size" FROM
-> (SELECT IFNULL(DB,'All Databases') DBName,SUM(DSize) SDSize,SUM(XSize) SXSize,
-> SUM(TSize) STSize FROM (SELECT table_schema DB,data_length DSize,
-> index_length XSize,data_length+index_length TSize FROM information_schema.tables
-> WHERE table_schema NOT IN ('mysql','information_schema','performance_schema')) AAA
-> GROUP BY DB WITH ROLLUP AA,(SELECT 3 pw) BB ORDER BY (SDSize+SXSize);
```

Figure 4-11 : Requête MySQL pour les espaces occupés *source [6]*.

Security Onion embarque également un script pour le nettoyage de la base de données de Sguil. Lors de l'installation du serveur, nous avons configuré une variable **DAYSTOKEEP**. Cette variable se trouve dans le fichier **/etc/nsm/securityonion.conf**. Le script **sguil-db-purge** vérifie les données enregistrées dans la base de données de Sguil. Il supprime les données dont l'âge a dépassé la valeur de la variable DAYSTOKEEP. Si par exemple la valeur de DAYSTOKEEP est de 365, **sguil-purge-db** supprimera toutes les données datant de 366 jours ou plus.

¹⁰ Ce seuil a été fixé lors de l'installation des composants de SO

4. Configurations, Mise en place de l'équipe CIRT, Tests

La surveillance de l'espace disque occupé par les logs est aussi nécessaire. Ainsi, si les logs sont stockés plus d'un an par exemple, l'administrateur de la sécurité devra alors les exporter vers un autre stockage.

En plus de la surveillance des espaces occupés par les outils individuels, nous pouvons surveiller l'espace disque globale disponible et utilisé. La commande **df -h** permet de voir l'espace libre et occupé sur les partitions du système.

4.3. Mise en place de l'équipe CIRT

4.3.1. Généralités

Le déploiement d'une solution de gestion de la sécurité n'est pas complet s'il n'y a pas au sein de l'entreprise, de l'organisation une équipe CIRT. L'équipe CIRT est chargée de piloter et de mener les opérations de supervision de la sécurité de réseau. Travailler avec un SSR permet à une équipe CIRT de prendre de meilleures décisions et d'agir beaucoup plus rapidement.

4.3.2. Constitution de l'équipe

Selon [6], une équipe CIRT devra composée de trois sections, dirigée par un responsable. Toujours selon la même source, les sections devront être réparties comme suit :

- Détection et réponse aux incidents ;
- Renseignement appliqué sur les menaces (Threat Intelligence) ;
- Infrastructure et développement.

Responsable de l'équipe

Le rôle du responsable de l'équipe CIRT est chargé d'organiser, de former et mener l'équipe à bien réussir ses opérations. La décision finale à appliquer, lui revient. Il se repose sur les informations remontées par les différents responsables de section, notamment la section Détection et Réponse aux incidents et Renseignement sur les menaces. Le responsable Technique de l'entreprise aura cette tâche.

Détection et réponse aux incidents

Cette section devra être constituée d'un Analyste principal et un technicien chargé de la surveillance des événements. [6] décrit cette section comme étant responsable du suivi journalier et de l'escalade des incidents de sécurité.

L'analyste principal devra un expérimenté de la sécurité informatique. Il devra également avoir les facultés de chasseur d'événements. Il forme le technicien de la surveillance des événements, et ce dernier lui remonte les événements suspects. Le technicien lui est chargé de surveiller la sécurité du réseau 24h/24, et cela même étant en dehors des locaux de l'entreprise.

L'analyste principal sera un ingénieur expérimenté du service technique. Le technicien sera un technicien en réseau, formé pour utiliser un NSM.

Renseignement sur les menaces

Cette section est la plus difficile à former. En effet, elle est chargée de suivre et de se renseigner sur les menaces inhérentes aux activités numériques. Elle est également chargée de suivre l'audit du réseau interne. Selon [6], cette section devra être chargée de faire des tests de simulation d'adversaires et des tests de pénétrations. La section renseignement sur les menaces est constituée d'un ingénieur chargé du renseignement, et d'ingénieurs chargés de simuler les équipes bleues¹¹ et

¹¹ Blue team : équipe chargée d'agir en interne comme des consultants. Elle est chargée de mettre en place les mesures pour sécuriser l'entreprise de l'intérieur.

4. Configurations, Mise en place de l'équipe CIRT, Tests

rouges¹² (Red Team et Blue Team). L'ingénieur chargé du renseignement informe régulièrement la section détection et réponse aux incidents sur les menaces actuelles et les actions à entreprendre pour les contrer.

Infrastructure et développement

La section infrastructure et développement fournie aux deux autres sections des outils pour leurs permettre de bien mener leurs opérations. Elle veille également à la mise en place de nouveaux outils et techniques de détection.

Elle devra être constituée d'un développeur et d'un administrateur système.

4.4. Tests

Pour tester que la solution mise en place fonctionne très bien, nous procéderons à plusieurs tests, selon plusieurs cas de figure.

4.4.1. Cas de figure 1 : Scan d'une machine sur le réseau

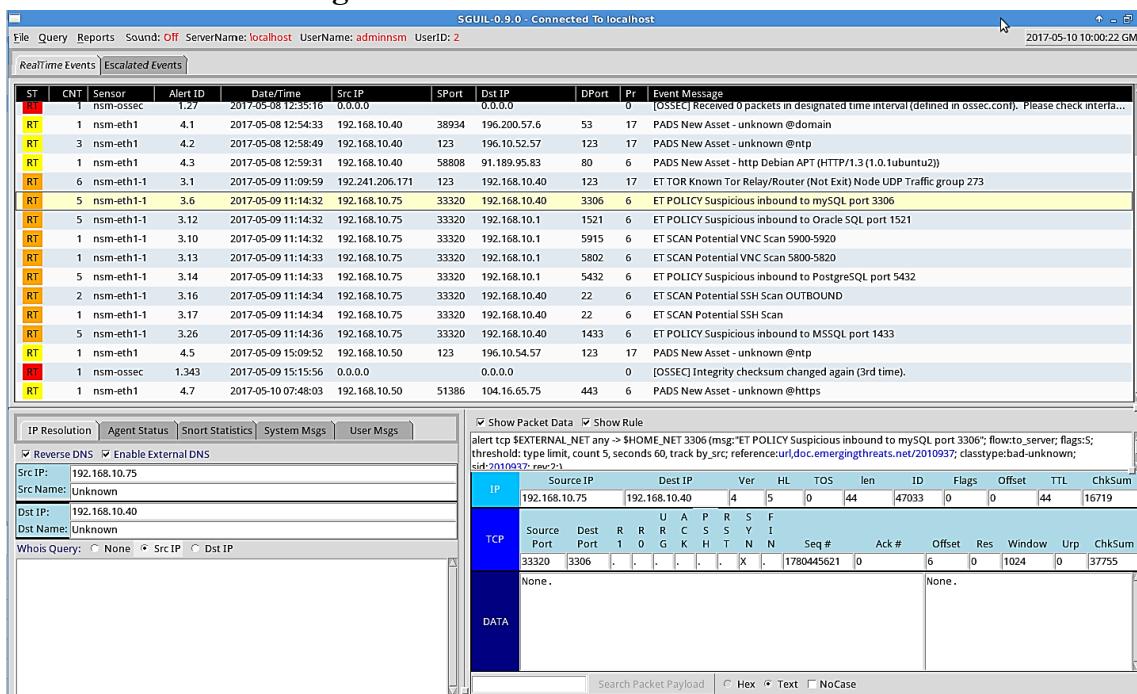


Figure 4-12 : Résultats d'un scan vu les NIDS dans la console Sguil

La méthode la simple pour vérifier le bon fonctionnement d'un NDIS est de procéder par un scan. L'outil le plus utilisé pour les scans est **nmap**. Nmap étant installé sur Kali Linux, nous l'avons utilisé pour scanner le réseau. Le résultat ne s'est pas fait attendre. Instantanément, les alertes ont été envoyées vers Sguil, qui les affiche aussitôt (figure 4-12). Lorsque nous cochons l'option « Show Packet Data », nous remarquons que seul le drapeau **SYN** est positionné. Cela renseigne sur le type de scan effectué, dans ce cas c'est le scan SYN.

4.4.2. Cas de figure 2 : Tentative d'attaque par force brute

Pour tester le HIDS OSSEC installé sur les hôtes, nous avons essayé de faire une authentification SSH par force brute. Pour ce faire, nous avons utilisé l'outil **medusa** disponible dans la distribution KALI Linux.

Durant nos configurations, nous avons activé l'option réponse active d'OSSEC pour qu'il bloque

¹² Red team : équipe chargée d'agir comme des pirates informatiques. Elle est chargée de simuler les attaques et les menaces à la recherche constante de failles dans la protection mise en place par la Blue Team.

4. Configurations, Mise en place de l'équipe CIRT, Tests

les tentatives multiples. Sur la figure 4-13, Sguil affiche les alertes d'OSSEC concernant une authentification échouée. Il précise que c'est une authentication SSH échoué, ensuite indique qu'il y'a plusieurs tentatives avec un mot de passe erroné. En analysant les détails de la dernière alerte, l'on voit qu'OSSEC a bloqué la machine responsable de ces tentatives multiples. Nous également examiné le temps d'entre chaque tentative. Il y'a eu 9 tentatives en 15 secondes, ce qui laisse voir qu'il y'a eu une attaque par force brute mais elle a échoué.

The screenshot shows the Sguil interface with several OSSEC alerts listed in a table. The alerts are:

| RT | User | Count | Date | Source IP | Destination IP | Details |
|----|-----------|-------|---------------------|---------------|----------------|---|
| 5 | nsm-ossec | 1.344 | 2017-05-10 12:07:30 | 192.168.10.75 | 0.0.0.0 | [OSSEC] User login failed. |
| 8 | nsm-ossec | 1.345 | 2017-05-10 12:07:32 | 192.168.10.75 | 0.0.0.0 | [OSSEC] SSHD authentication failed. |
| 4 | nsm-ossec | 1.348 | 2017-05-10 12:07:36 | 0.0.0.0 | 0.0.0.0 | [OSSEC] User authentication failure. |
| 4 | nsm-ossec | 1.349 | 2017-05-10 12:07:36 | 0.0.0.0 | 0.0.0.0 | [OSSEC] User missed the password more than one time |
| 1 | nsm-ossec | 1.364 | 2017-05-10 12:07:46 | 192.168.10.75 | 0.0.0.0 | [OSSEC] Multiple SSHD authentication failures. |

Below the table, there is a search interface for IP Resolution, Agent Status, Snort Statistics, System Msgs (selected), and User Msgs. The System Msgs tab shows a list of failed password attempts for user 'admin-nsm' from source IP 192.168.10.75 over port 48178 ssh2. The details pane on the right shows the full log entries for these attempts.

Figure 4-13 : Attaque par force brute détectée et stoppée par OSSEC

4.5. Conclusion

Dans ce chapitre, nous avons effectué des configurations plus poussées sur Security Onion. Nous avons vu comment maintenir SO. Nous avons également procédé à la mise en place de l'équipe CIRT au sein de l'entreprise. Pour finir, nous avons procédé à des tests.

Conclusion Générale

Au terme de ce projet, et compte tenu de tout ce qui précède, il est de toute évidence que les problèmes qui ont été soulevés au départ à savoir entre autres l'étude et la mise en place d'une solution de gestion de la sécurité ont été résolus. À travers cette solution, Afribone Mali fera une gestion efficace de la sécurité de son réseau. Cette solution lui permettra aussi de protéger ses clients de la plupart des menaces en provenance d'Internet et contribuera à la sécurité du réseau national.

En effet, dans ce projet, nous avons pu mettre en place une solution composée d'un Network Security Monitoring en l'occurrence Security Onion composée d'un gestionnaire centralisé de logs, en l'occurrence ELSA. Nous avons également mis en place l'équipe CIRT qui pourra valablement s'appuyer sur la solution déployée pour mener à bien ses missions. Avec cette solution, les équipes d'Afribone verront les intrusions et pourront prendre les mesures nécessaires pour les arrêter (Snort, OSSEC, Sguil, Squert). Ces outils (CapMe, Network Miner, Xplico, Wireshark) leurs permettront de mener des investigations poussées pour tirer des conclusions plus adaptées après des événements de sécurité. Les traces ainsi obtenues pourront être utilisées comme preuve contre un attaquant.

Il nous a aussi permis de conforter les connaissances déjà assimilée et d'acquérir de nouvelles compétences dans le domaine professionnel. Ce projet nous a également permis la maîtrise de techniques d'audit de la sécurité des réseaux et des systèmes. Partant de là, nous avons cerné les différents points critiques et les failles de sécurité du réseau et des systèmes. Nous avons proposé des recommandations afin d'avoir un réseau et des systèmes sécurisés avant le déploiement de toute solution de gestion de la sécurité.

Ce projet a été l'occasion pour en tant que professionnel des réseaux et des télécommunications de mettre en pratique les connaissances théoriques de la sécurité des réseaux. Cette formation théorique s'est révélée particulièrement adaptée aux compétences souhaitées et m'a permis de relever le défi posé. En outre, elle m'a permis de me diversifier et d'aborder le monde très prisé des professionnels de la sécurité informatique.

Ce travail pourra être complété par l'intégration d'un SIEM open source avec Security Onion. Cela renforcera le dispositif de supervision et enrichira le tableau de bord.

Dans l'avenir, nous souhaiterons apporter notre contribution à la sécurité dans l'Internet des Objets (IoT). En effet, les résultats de ce travail sont limités au périmètre du réseau d'Afribone Mali et de son datacenter. Cela est dû à la non adéquation de la solution de gestion déployé. Pour pallier à cette limitation, nous proposerons des outils pour la gestion de la sécurité des objets connectés, afin d'aboutir à une évolution beaucoup plus sûre des réseaux IoT à grande échelle, et permettrons de résoudre une partie du problème de la sécurité de la vie privée des utilisateurs dans l'IoT.

Références bibliographiques

- [1] ACISSI, Sécurité informatique - Ethical Hacking, Apprendre l'attaque pour mieux se défendre, Herblain, France: Editions ENI, 2013, pp. 12-14.
- [2] CISOfy, «Lynis - Security auditing tool for UNIX/Linux systems,» 2017. [En ligne]. Available: <https://ciscofy.com/lynis/>. [Accès le 18 Avril 2017].
- [3] J. S. Chris Sanders, Applied Network Security Monitoring, Collection, Detection, and Analysis, Waltham: Syngress, 2014.
- [4] RSA EMC Corporation, «Hacker Tactics, Techniques and Procedures,» 2015.
- [5] Help Net Security, «Hackers changing tactics, techniques and procedures,» 24 Octobre 2016. [En ligne]. Available: <https://www.helpnetsecurity.com/2016/10/24/hackers-changing-tactics/>. [Accès le 06 04 2017].
- [6] R. Bejtlich, The Practice of Network Security Monitoring, San Francisco: No starch press, 2013.
- [7] Cymbel, «The Big Picture of the Security Incident Cycle,» 01 Octobre 2010. [En ligne]. Available: <https://www.cymbel.com/security-compliance/the-big-picture-of-the-security-incident-cycle/>. [Accès le 12 Avril 2017].
- [8] G. Smith, «Log Analysis with the ELK Stack (Elasticsearch, Logstash and Kibana),» 2016.
- [9] Sysdream IT Security Services, «Certification PCI DSS,» 2017. [En ligne]. Available: <https://sysdream.com/pci-dss/certification/>. [Accès le 12 Avril 2017].
- [10] R. Heenan et M. Naghmeh, «Introduction to Security Onion,» *The First Post Graduate Cyber Security Symposium*, pp. 1-4, 10 Mai 2016.
- [11] L. C.S, *The principle of Network Security Monitoring [NSM]*, 2015, p. 60.
- [12] S. Gupta et L. D. Kees, «Logging and Monitoring to Detect Network Intrusion and Compliance Violations in the Environment,» *SANS Institute InfoSec Reading Room*, p. 44, 2012.
- [13] K. Kent et M. Souppaya, Guide to Computer Security Log Management, Gaithersburg: National Institute of Standards and Technology, 2006.
- [14] M. K. K. A. R. O. M. N. Peter MUJA, «Building a Cyber Security Emergency Response Team (CERT) for the NREN Community – The case of KENET CERT,» *UbuntuNet Alliance annual conference*, n° %18, pp. 158-167, 2015.
- [15] D. Burks, «Introduction To Security Onion,» 16 Mars 2017. [En ligne]. Available: <https://github.com/security-onion-solutions/security-onion/wiki/IntroductionToSecurityOnion>. [Accès le 21 Avril 2017].
- [16] Cisco, «Snort official documentation,» 2017. [En ligne]. Available: <https://www.snort.org/documents#OfficialDocumentation>. [Accès le 21 Avril 2017].

4. Configurations, Mise en place de l'équipe CIRT, Tests

- [17] Cisco, «Snort: The World's Most Widely Deployed IPS Technology,» 11 Novembre 2014. [En ligne]. Available: http://www.cisco.com/c/en/us/products/collateral/security/brief_c17-733286.html. [Accès le 21 Avril 2017].
- [18] Cisco, «Snort | Getting Started,» [En ligne]. Available: <http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node3.html>. [Accès le 21 04 2017].
- [19] D. Burks, «Snort,» 18 Février 2017. [En ligne]. Available: <https://github.com/security-onion-solutions/security-onion/wiki/Snort>. [Accès le 21 Avril 2017].
- [20] Suricata, «Suricata, Open source IDS/IPS/NSM engine,» [En ligne]. Available: <https://suricata-ids.org/>. [Accès le 21 Avril 2017].
- [21] Bro, «The Bro Network Security Monitor,» 2017. [En ligne]. Available: <https://www.bro.org/>. [Accès le 21 Avril 2017].
- [22] OSSEC, «About OSSEC,» OSSEC Project Team, 2017. [En ligne]. Available: <http://ossec.github.io/about.html>. [Accès le 21 Avril 2017].
- [23] A. Hay, D. Cid et B. Rory, OSSEC Host-Based Intrusion Detection, Burlington: Syngress Publishing, Inc., 2008.
- [24] D. Cid, *Log Analysis using OSSEC*, 2007, p. 46.
- [25] D. Cid, «Server Security: Indicators of Compromised Behavior with OSSEC,» 17 Mars 2016. [En ligne]. Available: <https://blog.sucuri.net/2016/03/server-security-anomaly-behaviour-with-ossec.html>. [Accès le 21 Avril 2017].
- [26] OpenVAS, «OpenVAS - Open Vulnerability Assesment System,» 2017. [En ligne]. Available: <http://www.openvas.org/>. [Accès le 25 Avril 2017].
- [27] D. Karg, J. D. Munoz, D. Gil, F. Ospitia, S. Gonzales et J. Casal, Open Source Security Information Management, 2003.
- [28] OCS INVENTORY NG, «Projet OCS Inventory,» 2017. [En ligne]. Available: <https://www.ocsinventory-ng.org/fr/>. [Accès le 25 Avril 2017].
- [29] Nagios, «History of Nagios,» [En ligne]. Available: <https://www.nagios.org/about/history/>. [Accès le 25 Avril 2017].
- [30] S. Lawton, «A Guide to Security Information and Event Management,» 16 Février 2015. [En ligne]. Available: <http://www.tomsitpro.com/articles/siem-solutions-guide,2-864-2.html>. [Accès le 25 Avril 2017].
- [31] L. Wes et D. Burks, «Architecture - Security Onion Solution,» 29 Septembre 2017. [En ligne]. Available: <https://github.com/Security-Onion-Solutions/security-onion/wiki/Architecture>. [Accès le 27 Avril 2017].
- [32] D. Burks, «Hardware requirements,» 15 Février 2017. [En ligne]. Available: <https://github.com/Security-Onion-Solutions/security-onion/wiki/Hardware>. [Accès le 27 Avril 2017].

4. Configurations, Mise en place de l'équipe CIRT, Tests

- [33] QoSient, LLC, «Argus - Auditing Network Activity - Getting Started,» 17 Avril 2012. [En ligne]. Available: <https://qosient.com/argus/gettingstarted.shtml>. [Accès le 03 Mai 2017].
- [34] O'Reilly, «Write Your Own Snort Rules,» [En ligne]. Available: <http://archive.oreilly.com/pub/h/1393>. [Accès le 05 Mai 2017].
- [35] A. Chuvakin et L. Zelster, «Critical Log Review Checklist for Security Incidents,» 2017. [En ligne]. Available: <https://zeltserv.com/security-incident-log-review-checklist/>. [Accès le 04 Mai 2017].
- [36] D. Burks, «Upgrade,» 14 Mars 2017. [En ligne]. Available: <https://github.com/Security-Onion-Solutions/security-onion/wiki/Upgrade>. [Accès le 08 Mai 2017].