République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin d'étude
pour l'obtention du diplôme de Master en Informatique
Option : Administration et sécurité des réseaux

Thème

Mise en place d'un systéme de détection et de prévention d'intusion

Réaliser par:

Mlle BELKHATMI Keltouma
Mlle BENAMARA Ouarda

Président: Mr MIR
Encadreur : Mr MEHAOUED
Examinateur : Mr AKILAL

2015/2016

Table des Matières

Liste des figures

Liste des tableaux

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin d'étude
pour l'obtention du diplôme de Master en Informatique
Option : Administration et sécurité des réseaux

Thème

Mise en place d'un systéme de détection et de prévention d'intusion

---

Réaliser par:

Mlle BELKHATMI Keltouma
Mlle BENAMARA Ouarda

Président: Mr MIR
Encadreur : Mr MEHAOUED
Examinateur : Mr AKILAL

2015/2016

Remerciements

En préambule à ce mémoire nous remercions ALLAH qui nous aide et nous donne la patience et le courage durant ces années d'étude.

Nous souhaitons adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire.

Nos remerciements vont tout d'abord au corps professoral et administratif de département d'informatique de l'université ABDERAHAMENE MIRA de BEJAIA pour la richesse et la qualité de ses enseignements et qui déploie des grands efforts pour assurer à leurs étudiants une formation de qualité.

Ensuite nous tenons à remercier nos familles, surtout nos parents qui nous ont épaulés, soutenues et suivies tout au long de ce projet.

Nous tenons aussi à remercier Mr MEHAOUED Kamal et surtout Mr. KESSOUM, Laaziz pour le temps qu'ils nous ont consacré et leurs précieux conseils.

Nos remerciements vont également à tout le personnel de l'entreprise générale emballage pour son hospitalité et un particulièrement à celui qui nous à guidés tout au long du stage.

Enfin, nous adressons nos plus sincères remerciements à tous nos proches et amis, qui nous ont toujours soutenues et encouragées au cours de la réalisation de ce mémoire.

Merci à toutes et à tous.

Dédicaces

Je dédie ce présent mémoire :

À ma très chère mère Affable, honorable, aimable : Tu représentes pour moi le symbole de la bonté par excellence, la source de tendresse et l'exemple du dévouement qui n'a pas cessé de m'encourager et de prier pour moi. Ta prière et ta bénédiction m'ont étés d'un grand secours pour mener à bien mes études.

À mon père qui m'a toujours encouragé et soutenu moralement, auquel je dois ma réussite et auquel je ne rendrai jamais assez.

À mes très chères soeurs Anais, Rania, mes très chers frères Mouhand et Shakir et à ma cousine Vanissa, qui m'ont énormément aidé et à qui j'éprouve mon affection.

À ma grande mère Fatima Je la souhaite une longue vie.

À celle qui m'a toujours aidé, écouté, soutenu et encouragé tout au long de mon Parcours, celle qui était toujours à mes côtés, ma très chère copine Sonia.

À mes ancles, mes tantes, mes cousins et cousines.

À celui qui a su me supporter, m'aider et m'encourager, mon très cher Massi, en témoignage de sa gentillesse et de son affection.

À ma très chère copine Naima, ma binôme Dida et mes copines de chambre Ahlam, Sihem.

À tous mes professeurs et surtout mon encadreur Mr MEHAOUED Kamal ainsi Mr KESSOUM Laaziz.

À toutes les personnes qui me connaissent.

Ouarda

Dédicaces

Je dédie ce présent mémoire :

A celle qui s'est toujours dévouée et s'est sacrifiée pour moi, celle qui m'a aidée du mieux qu'elle pouvait pour réussir, celle qui a toujours été là dans mes moments de détresse, ma très chère mère.

À celui qui m'a toujours aidé, écouté, soutenu et encouragé tout au long de mon parcours, celui qui est toujours à mes côtés et qui a su me supporter, mon très chér père.

À ma trè chère soeur Sarah, mon très cher frère Ghilas qui m'ont énormément aidé et à qui je témoigne mon affection.

À mon trés cher Farid qui m'a toujours encouragé et soutenu moralement.

À mon binôme Warda.

À mes très chères copines Thilali, Mouma, Nawel, Ouzna et à tous Mes amies.

À tous mes professeurs et surtout mes encadreurs Mr MEHAOUED Kamal et Mr KESSOUM Laaziz.

En un mot à tous les gens qui contribués de près ou de loin a ma réussite .

Keltouma

Introduction générale

Introduction générale

Les systèmes et réseaux informatiques contiennent diverses formes de vulnérabilité, donc la sécurité est, de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet.

Pour faire face à ces problèmes de sécurité informatique, différents mécanismes ont été mis en place pour prévenir toute sort d'attaque comme les pare-feux, antivirus, qui s'avèrent limités face au développement rapide des techniques de piratage, d'où la nécessité de mettre en place un système de détection et de prévention d'intrusion.

Le système de détection et de prévention d'intrusion, est une technique permettant de détecter les intrusions de les prévenir, ce système nous aide à prévoir ,surveiller ou à identifier toute activité non autorisée dans un réseau.

Objectif

Notre projet a pour but la configuration d'un système détection et prévention d'intrusion, et sa mis en place sous le pare-feu pfsense au niveau de l'architecture réseau de générale emballage.

Ce mémoire sera organisé comme suite :

Dans le premier chapitre, nous allons détailler des généralités sur la sécurité informatique, et en suite nous présentons l'organisme d'accueil qui nous a pris en charge durant toute la période de notre stage pratique.

Dans le second chapitre, nous allons donner une description bien détaillée des systèmes de détection et de prévention d'intrusion (leurs différents types, leurs principes de fonctionnement, une comparaison entre IDS et IPS).

Enfin, dans le dernier chapitre, nous expliquerons le fonctionnement de l'outil de détection et de prévention d'intrusion snort sous pfsense.

1

La sécurité informatique et l'organisme d'accueil

introduction

Un réseau informatique est un ensemble d'équipements interconnectés en vue de transmettre un signal porteur des informations. Il permet aussi de partager des ressources comme par exemple des fichiers, imprimantes, ...etc. Il Offre des services comme http, ftp, dns, ...etc. Dés lors un problème se pose par rapport à l'accès aux ressources et services : les droits d'accès des utilisateurs, des machines internes ou externes (du réseau).

N'importe qui ne doit pas faire n'importe quoi quand il est dans le réseau, surtout quand il n'est pas autorisé à y accéder.

D'ou la nécessité de sécuriser le réseau, contre tout ce qui constitue une menace.

1.1 Les réseaux

1.1.1 La norme OSI:

1.1.1.1 Définition

Le modèle OSI (Open Systems Interconnection) est un modèle générique et standard d'architecture d'un réseau en 7 couches, élaboré par l'organisme ISO (Organisation Internationale de normalisation) en 1984. La mise en évidence de ces différentes couches se base sur les caractéristiques suivantes qui étaient recherchées par l'ISO :

- Création d'une couche lorsqu'un niveau d'abstraction est nécessaire.
- Définition précise des services et opérations de chaque couche.
- Définition des opérations de chaque couche en s'appuyant sur des protocoles normalisés.
- Choix des frontières entre couches de manière à minimiser le flux d'information aux interfaces.
- Définition d'une couche supplémentaire lorsque des opérations d'ordre différent doivent être réalisées.[16]

1.1.1.2 Les différentes couches du modèle OSI:

Dans le découpage en 7 couches, on distingue :[17]

- Les couches basses (1-4) : transfert de l'information par les différents services de transport.

- Les couches hautes (5-7) : traitement de l'information par les différents services applicatifs.

7	Application
6	Présentation
5	Session
4	Transport
3	Réseau
2	Liaison
1	Physique

Table 1.1: architecture du modèle OSI.

✓ **Couche physique** : La couche physique (physical (eng)) gère la communication avec l'interface physique afin de faire transiter ou de récupérer les données sur le support de transmission, qui peut être électrique, mécanique. Ce sont les contraintes matérielles du support utilisé qui décident des objectifs à atteindre pour cette couche : conversion en signaux électriques, taille et forme des connecteurs, dimensions et position des antennes,...etc.

✓ **Couche liaison** : La couche liaison (liaison de données : datalink (eng)) s'occupe de la bonne transmission de l'information entre les noeuds via le support, en assurant la gestion des erreurs de transmission et la synchronisation des données. Là aussi, le support de transmission conditionne les protocoles à mettre en oeuvre.

✓ **Couche réseau** : La couche réseau (network (eng)) a en charge de déterminer le choix de la route entre les noeuds afin de transmettre de manière indépendante l'information ou les différents paquets la constituant en prenant en compte en temps réel le trafic. Cette couche assure aussi un certain nombre de contrôles de congestion qui ne sont pas gérés par la couche liaison.

✓ **Couche transport** : La couche transport (transport (eng)) supervise le découpage et le réassemblage de l'information en paquets, contrôlant ainsi la cohérence de la transmission de l'information de l'émetteur vers le destinataire.

✓ **Couche session** : La couche session (session (eng)) gère une communication complète entre plusieurs noeuds, permettant, ainsi d'établir et de maintenir un réel dialogue suivi (une session), pouvant être constitué de temps morts pendant lesquels aucune donnée n'est physiquement transmise.

✓ **Couche présentation** : La couche présentation (présentation (eng)) a en charge la représentation des données, c'est-à-dire de structurer et convertir les données échangées ainsi que leur syntaxe afin d'assurer la communication entre des noeuds disparates (différences hardware et/ou software).

✓ **Couche application** : La couche application (application (eng)) est le point d'accès des applications aux services réseaux. On y retrouve toutes les applications de communication via le réseau communément utilisées sur un LAN ou sur Internet : applications de transfert de fichier, courrier électronique,...etc.

1.1.2 Le TCP/IP

1.1.2.1 Définition :

Le protocole TCP/IP, développé originellement par le ministère de la défense américain en 1981, propose l'évolution des concepts déjà utilisés en partie pour le réseau historique ARPAnet (1972), et est employé en très forte proportion sur le réseau Internet. Au-delà de son aspect historique, TCP/IP doit aussi son succès à son indépendance vis-à-vis de tout constructeur informatique.

En réalité, TCP/IP définit une suite de divers protocoles probabilistes, appelé aussi modèle DOD (Department of Defense), pour la communication sur un réseau informatique, notamment le protocole TCP et le protocole IP qui sont parmi les principaux protocoles de ce modèle.[4]

1.1.2.2 Découpage en couches:

<table>
<tr><th colspan="2">Modèle OSI</th><th colspan="2">Modèle TCP/IP</th></tr>
<tr><td>7</td><td>Application</td><td rowspan="3">4</td><td rowspan="3">Application</td></tr>
<tr><td>6</td><td>Présentation</td></tr>
<tr><td>5</td><td>Session</td></tr>
<tr><td>4</td><td>Transport</td><td>3</td><td>Transport (TCP)</td></tr>
<tr><td>3</td><td>Réseaux</td><td>2</td><td>Internet(IP)</td></tr>
<tr><td>2</td><td>Liaison de donnée</td><td rowspan="2">1</td><td rowspan="2">Accès au réseau</td></tr>
<tr><td>1</td><td>Physique</td></tr>
</table>

Table 1.2: le modèle OSI et le modèle TCP/IP.

Le protocole TCP/IP étant antérieur au modèle OSI, il ne respecte pas réellement celui-ci. Cependant, on peut faire grossièrement correspondre les différents services utilisés et proposés par TCP/IP avec le modèle OSI, et obtenir ainsi un modèle en 4 couches.

Les services des couches 1 et 2 (physique et liaison) du modèle OSI sont intégrés dans une seule couche (hôte-réseau), les couches 5 et 6 (session et présentation) n'existent pas réellement dans le modèle TCP/IP et leurs services sont réalisés par la couche application si besoin est :[4]

✓ **Hôte-réseau** : La couche hôte-réseau, intégrant les services des couches physique et liaison du modèle OSI, a en charge la communication avec l'interface physique afin de transmettre ou de récupérer les paquets de données qui lui sont transmis de la couche supérieure. Le protocole utilisé pour assurer cet interfaçage n'est pas explicitement défini puisqu'il dépend du réseau utilisé ainsi que du noeud (Ethernet en LAN, X25 en WAN, ...etc.).

✓ **Internet** : La couche Internet, correspondant à la couche réseau du modèle OSI, s'occupe de l'acheminement, à bonne destination, des paquets de données indépendamment les uns des autres, soit donc de leur routage à travers les différents noeuds par rapport au trafic et à la congestion du réseau. Il n'est en revanche pas du ressort de cette couche de vérifier le bon acheminement.

Le protocole IP (Internet Protocol) assure intégralement les services de cette couche, et constitue donc l'un des points-clefs du modèle TCP/IP. Le format et la structure des paquets IP sont précisément définis.

✓ **Transport** : La couche transport, pendant de la couche homonyme du modèle OSI, gère le fractionnement et le réassemblage en paquets du flux de données à transmettre. Le routage ayant pour conséquence un arrivage des paquets dans un ordre incertain, cette couche s'occupe aussi du réagencement ordonné de tous les paquets d'un même message. Les deux principaux protocoles pouvant assurer les services de cette couche sont les suivants :

- **TCP (Transmission Control Protocol)** : protocole fiable, assurant une communication sans erreur par un mécanisme question/réponse/confirmation/synchronisation (orienté connexion).
- **UDP (User Datagram Protocol)** : protocole non-fiable, assurant une communication rapide mais pouvant contenir des erreurs en utilisant un mécanisme question/réponse (sans connexion).

✓ **Application** : La couche application, similaire à la couche homonyme du modèle OSI, correspond aux différentes applications utilisant les services réseaux pour communiquer à travers un réseau. Un grand nombre de protocole divers de haut niveau permettent d'assurer les services de cette couche :

- Telnet : ouverture de session à distance.
- FTP (File Transfer Protocol) : protocole de transfert de fichiers.
- HTTP (HyperText Transfer Protocol) : protocole de transfert de l'hypertexte.
- SMTP (Simple Mail Transfer Protocol) : protocole simple de transfert de courrier.
- DNS (Domain Name System) : système de nom de domaine.

1.2 La sécurité informatique

La sécurité informatique est un terme large qui réunit les moyens humains, technologiques, organisationnels qui tentent de garantir certaines propriétés d'un système d'information.[18]

1.3 Objectif de la sécurité informatique

On peut définir les objectifs de la sécurité informatique comme suit :[19]

✓ **L'intégrité** : l'information ne sera modifiée que par les personnes autorisées.

✓ **La confidentialité** : demande l'information qui se trouve dans le système soit lue que par les personnes autorisées.

✓ **La disponibilité** : demande que l'information qui se trouve dans le système soit disponible aux personnes autorisées.

✓ **Le non répudiation** : permet de garantir qu'une transaction ne puisse être niée.

✓ **L'authentification** : consiste à assurer que seules les personnes autorisées aient accès aux ressources.

1.4 Terminologie de la sécurité informatique

La sécurité informatique utilise vocabulaire bien spécifique, que nous énumérons comme suit :

1.4.1 Vulnérabilité

Est une faiblesse d'un système de sécurité se traduisant par une incapacité partielle de celui-ci à faire face aux menaces informatiques qui le guettent. Par exemple, une erreur d'implémentation dans le développement d'une application, est exploitée pour nuire à l'application (pénétration, refus de service, ...etc.). Elle peut être également provenir d'une mauvaise configuration.[20]

1.4.2 Menace

La menace désigne l'exploitation d'une faiblesse de sécurité par un attaquant, que ce soit interne ou externe a l'entreprise.

La probabilité qu'elle soit une faille de sécurité, est évaluée par des études statistiques même si elle est difficile à réaliser.[5]

1.4.3 Risque

Les menaces engendrent des risques et des couts humains et financiers : perte de confidentialité des données sensibles, indisponibilité des infrastructures et des données, dommages pour le patrimoine intellectuel et la notoriété.[18]

Les risques peuvent survenir si les systèmes menacés présentent des vulnérabilités.

1.4.4 Une attaque

Une attaque est le résultat de l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel, erreur de configuration,...etc.) à des fins non connues par l'exploitant du système et il est généralement préjudiciables.[21]

1.4.5 Intrusion

C'est réaliser une attaque ou une menace pour un système d'informatique, pour que ce dernier ne soit plus en sécurité.[22]

1.4.6 Contre-mesure

Contre-mesure donne les capacités et les mesures pour se défendre contre les intrusions.[23]

1.4.7 Cryptographie et cryptanalyse

1.4.7.1 Cryptage (chiffrement)

Transformation d'un message clair en un message chiffré.[24]

1.4.7.2 Décryptage (déchiffrement)

C'est de retrouver, à partir d'un message chiffré, le message clair lui correspondant.[24]

1.4.7.3 Clé

Est un paramètre partagé entre l'émetteur et le récepteur, et implémenté dans les opérations de chiffrement et déchiffrement.[24]

1.5 Éléments d'une politique de sécurité

Il ne faut pas perdre de vue que la sécurité est comme une chaîne, guère plus solide que son maillon le plus faible. En plus de la formation et de la sensibilisation permanente des utilisateurs.[24]
La politique de sécurité peut être découpée en plusieurs parties :[9]

✓ **Défaillance matérielle** : Tout équipement physique est sujet à défaillance (usure, vieillissement, défaut,...etc.). Et l'achat d'équipements de qualité et standard accompagnés d'une bonne garantie avec support technique est essentiel pour minimiser les délais de remise en fonction. Seule une forme de sauvegarde peut cependant protéger les données.

✓ **Défaillance logicielle** : Tout programme informatique contient des bugs. La seule façon de se protéger efficacement contre ceux-ci est de faire des copies de l'information à risque. Une mise à jour régulière des logiciels et la visite des sites consacrés à ce type de problème peuvent contribuer à en diminuer la fréquence des bugs.

✓ **Accidents (pannes, incendies, inondations,...etc.)** : Pour protéger les donnés et les fichiers face à des problèmes, il est indispensable de faire une sauvegarde. Cette procédure de sauvegarde peut combiner plusieurs moyens fonctionnant à des échelles de temps différentes :

- disques RAID[1] pour maintenir la disponibilité des serveurs.
- copie de sécurité via le réseau (quotidienne).
- copie de sécurité dans un autre bâtiment.

La disposition et l'infrastructure des locaux peuvent aussi fournir une protection intéressante. Pour des sites particulièrement importants (site informatique, central d'une banque...etc.) il sera nécessaire de prévoir la possibilité de basculer totalement et rapidement vers un site de secours (éventuellement assuré par un sous-traitant spécialisé).

Ce site devra donc contenir une copie de tous les logiciels et matériels spécifiques à l'activité de la société.

✓ **Erreur humaine** : Outre les copies de sécurité, seule une formation adéquate du personnel peut limiter ce problème.

[1]Redundant Array of Independent Diske : est un ensemble de technique de virtulisation du stockage, permettant de répartier des données sur plusiers disques dure.

✓ **Vol via des dispositifs physique (disques et bandes)** : Contrôler l'accès à ces équipements : ne mettre des unités de disquette, bandes...etc. Que sur les ordinateurs où c'est essentiel. Mettre en place des dispositifs de surveillance.

✓ **Virus provenant de disquettes** : Il faut minimiser l'utillisation des disques puisque ont plus de risque. L'installation de programme antivirus peut s'avérer une protection efficace mais coûteuse. Le diminue la productivité et nécessite de fréquente mise à jour.

✓ **Piratage et virus réseau** : Cette problématique est plus complexe et l'omniprésence des réseaux, notamment l'Internet, lui confère une importance particulière. Les problèmes de sécurité de cette catégorie sont particulièrement dommageables et font l'objet de l'étude qui suit.

1.6 Les défauts de la sécurité informatique

Les défauts de sécurité d'un système d'information les plus souvent constatés sont :

- Installation des logiciels et matériels par défaut.
- Mises à jour non effectuées.
- Mots de passe inexistants ou par défaut.
- Services inutiles conservés (Netbios...etc.).
- Traces inexploitées.
- Procédures de sécurité obsolètes.
- Eléments et outils de test laissés en place dans les configurations en production.
- Authentification faible.
- Télémaintenance sans contrôle fort.

1.7 Menace sur les réseaux

1.7.1 Vulnérabilité

Internet est une mine d'informations pour les entreprises et pour les utilisateurs. En naviguant sur Internet, on peut accéder à des millions de page Web.

A l'aide de moteur de recherche, on peut obtenir des informations qui sont nécessaires pour le travail, au moment où on en a besoin.

Le Web est une ressource indispensable pour la productivité des entreprises, mais il y a aussi des dangers (les virus, les vers, les cookies...etc.), alors le Web montre une faiblesse.[5]

1.7.2 Attaques informatiques

Tout ordinateur connecté à un réseau informatique, est potentiellement vulnérable à une attaque.[23]

1.7.2.1 Anatomie d'une attaque

Fréquemment appelés " les 5 P " dans la littérature, ces cinq verbes anglophones constituent le squelette de toute attaque informatique :

✓ **Probe (Analyser)** : Dans un premier temps, une personne mal intentionnée va chercher les failles pour pénétrer le réseau.

✓ **Penetrate (Pénétrer)** : Une fois plusieurs failles identifiées, le pirate va chercher à les exploiter afin de pénétrer au sein du SI.

✓ **Persist (Persister)** : une fois le réseau infiltré, le pirate cherchera à y revenir facilement. Pour cela, il installera par exemple des back doors. Cependant, en général, il corrigera la faille par laquelle il s'est introduit afin de s'assurer qu'aucun autre pirate n'exploitera sa cible.

✓ **Propagate (Propager)** : Le réseau est infiltré, l'accès est facile. Le pirate pourra alors explorer le réseau et trouver des nouvelles cibles qui l'intéresseraient.

✓ **Paralyze (Paralyser)** : Les cibles identifiées, le pirate va agir et nuire au SI.

1.7.2.2 Cyber-attaques

Longtemps, les organismes étatiques se sont cantonnés à un rôle de veille, d'alerte, de recueil et de renseignements. Aujourd'hui, un rôle défensif leur est officiellement assigné. Cela signifie qu'ils doivent coordonner l'action des services de l'Etat pour la mise en oeuvre de leur cyber-défense.

On peut cependant imaginer qu'en cas d'attaque contre des infrastructures vitales avec des conséquences humaines, un État pourrait considérer cela comme un acte de guerre, et agir en conséquence : c'est-à-dire riposter.

Cependant aucun Etat n'a, pour le moment, révélé l'existence officielle d'un programme de cyber contre-attaque.[22]

1.7.3 Types d'attaque

Il existe trois types d'attaque:

1.7.3.1 Les attaques directes

Les attaques directes se produisent uniquement lorsqu'un ordinateur est connecté à Internet ou à un réseau local et le hacker utilise des logiciels pour envoyer les paquets directement à partir de son ordinateur à la victime [1].

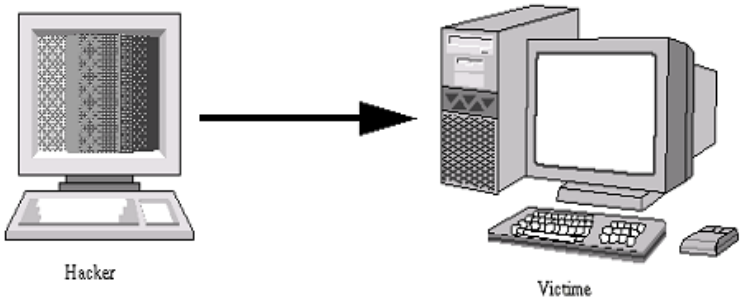

Figure 1.1: attaque directe [1].

1.7.3.2 Les attaques indirectes par rebond

Les attaques par rebond constituent un ensemble d'attaque a envoyés à l'ordinateur intermédiaire qui répercute l'attaque vers la victime. Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

- Masquer l'identité (l'adresse IP) du hacker.
- Eventuellement, utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante...etc.) pour attaquer [2].

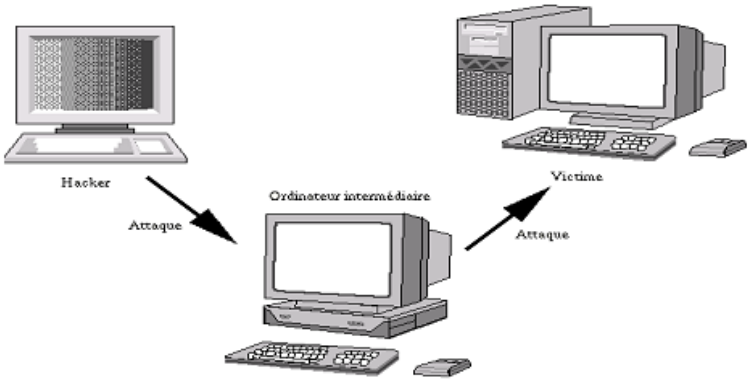

Figure 1.2: attaque indirecte par rebond [2].

1.7.3.3 Les attaques indirectes par réponse

Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages que les attaques par rebond. Le principe de cette attaque est d'envoyer une requête à l'ordinateur intermédiaire pour qu'il transmette la réponse de cette requête vers l'ordinateur victime [3].

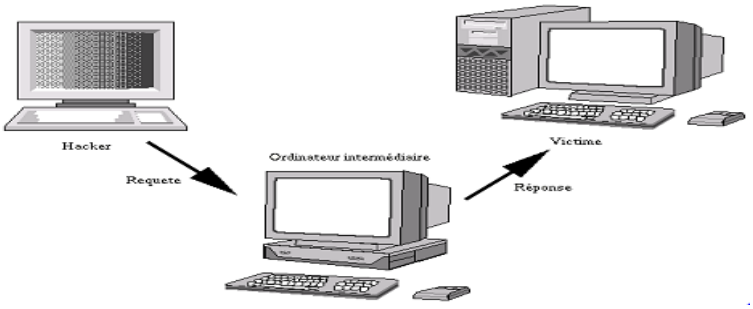

Figure 1.3: attaques indirectes par réponse [3].

1.7.4 Quelques attaques courantes

Il existe plusieurs attaques pour cella on peut citer:

1.7.4.1 Le balayage de port

✓ Attaque par balayage ICMP : Elle consiste à ce que le client envoie un paquet avec le protocole ICMP qui utilise la fonction request connue sous le nom " ping ", vers le serveur qui lui répond avec un paquet ICMP echo-reply, comme l'illustre la figure 1.4.

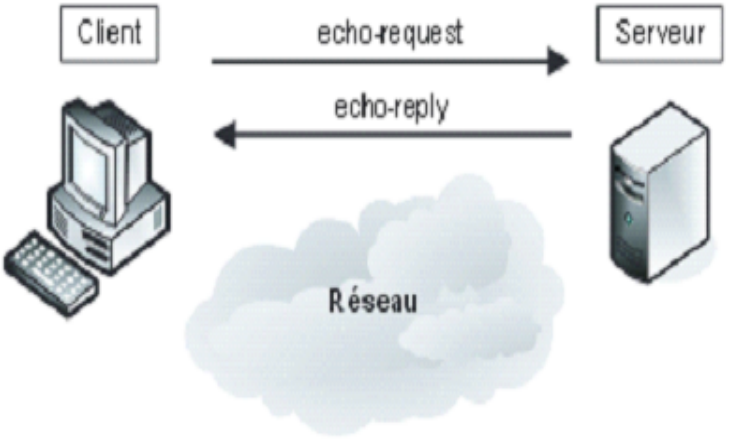

Figure 1.4: attaque par balayage ICMP [4].

Il existe deux méthodes pour cartographier le réseau par cette technique :

- En balayant (scanning) le réseau et en interrogeant chaque adresse IP possible, ce qui n'est pas très discret.
- En visant une seule fois l'adresse de broadcaste du réseau, ce qui fait répondre toutes les machines présentes. Une seule demande permet ainsi d'engendrer l'envoi de toutes les réponses.

Cependant, du fait de l'accroissement constant de l'insécurité, nombre d'administrateurs de pare-feu ont pris l'initiative de ne pas laisser passer les réponses à de telles demandes [5].

✓ **Attaque par balayage TCP** : C'est en partant du principe que le flux réseau toujours accessible au pirate est celui qui est destiné à être accessible au public que la technique du balayage TCP a été inventée. Similaire au balayage ICMP, sa spécificité est de s'appuyer sur le protocole TCP. Le client envoie un paquet SYN vers un port réseau particulier de l'adresse IP du serveur. Si le port est en écoute, un paquet SYN/ACK est reçu en retour. Sinon, la réception d'un paquet RST signifie qu'il n'y a pas de service en écoute sur le port. Le client envoie en réponse un paquet RST pour terminer la connexion, comme l'illustre la figure 1.5 [5].

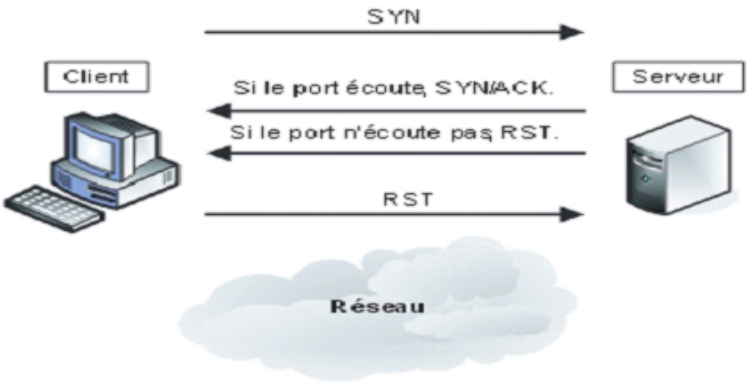

Figure 1.5: attaque par balayage TCP [5].

Si aucune réponse n'est reçue en retour, c'est qu'il existe un équipement filtrant entre le serveur et le client ou qu'il n'y a aucune machine derrière l'adresse IP visée.

Cette technique est cependant si peu discrète, que des variantes ont été élaborées pour améliorer le balayage en jouant sur le principe de fonctionnement de la pile TCP/IP [5].

✓ **Attaque par balayage semi-ouvert TCP** : Les variantes à cette technique du balayage TCP reposent sur le non-respect de la définition du protocole TCP/IP. Nous venons de voir qu'il existait une séquence lors de l'établissement d'une session TCP. Lorsque cette séquence n'est pas respectée, le serveur TCP se comporte différemment, ainsi que les équipements filtrants présents sur le chemin.

La variante dite de balayage semi-ouvert consiste en un balayage dans lequel le client envoie son paquet SYN et reçoit les paquets prévus en retour, comme l'illustre la figure 1.5. Contrairement au balayage TCP normal, le client n'envoie pas de paquet RST pour rompre la session. Il note simplement la réponse et passe au port suivant. Par ce procédé, la session TCP n'est pas ouverte, puisque le handshake ne s'est pas terminé, et le serveur ne trace pas cet échange de données.[4]

✓ **IP spoofing** : Le pirate commence par choisir le système qu'il veut attaquer pour qu'il se fasse passer pour un autre système en falsifiant son adresse IP pour obtenir le maximum de détails sur le système cible, et il détermine les systèmes ou adresses IP autorisés à se connecter au système cible. Le pirate ensuite attaque le serveur cible en utilisant l'adresse IP falsifiée.

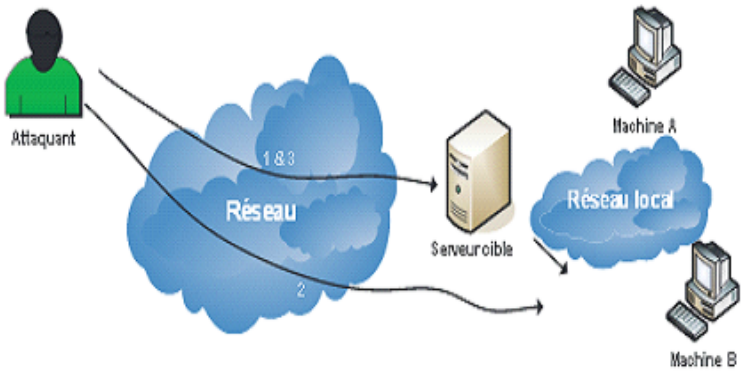

Figure 1.6: attaque IP spoofing [3].

✓ **Virus** : C'est un petit programme qui a la faculté de se reproduire automatiquement. Il va recopier son propre code tel quel, ou en le modifiant, dans des éléments qui sont déjà dans l'ordinateur. Le plus souvent son but est de nuire [3].

✓ **Denis de service** : Cette attaque n'est pas pour rattraper les informations sur une machine à distance mais de paralyser un service ou un réseau complet, et l'utilisateur ne peut plus accéder au ressources, Les deux exemples principaux, sont le " ping flood " ou l'envoi massif de courrier électroniques pour saturer une boîte aux lettre (mailbombing) [3].

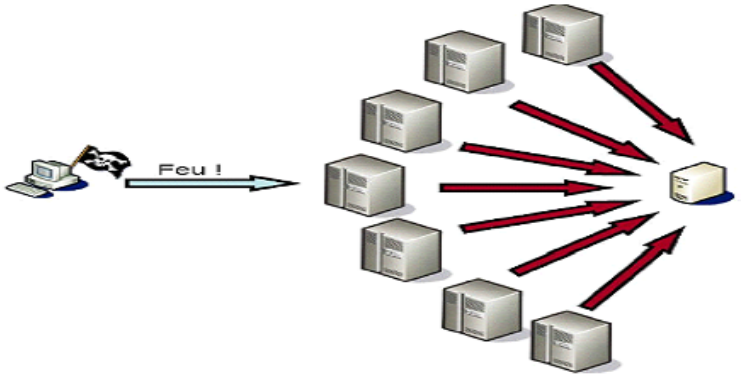

Figure 1.7: principe de DDOS [6].

1.8 Les dispositifs de protection

La variété et la disponibilité des outils d'attaques augmentent le risque des intrusions. Par conséquent les administrateurs s'appuient sur diverses solutions dans le but de maintenir la protection du réseau informatique.

Voici quelques solutions proposées :

1.8.1 Un antivirus :

Logiciel censé protéger un ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire.[6]

1.8.2 Un pare-feu :

Un pare-feu est logiciel et/ou matériel qui filtre et protège un système en bloquant les connexions venant de l'extérieur (entrées) ou de l'intérieur (sorties) pour empêcher ou autoriser l'accès à des services Web [7].

Il permet aussi de faire de la translation d'adresse pour servir de routeur.

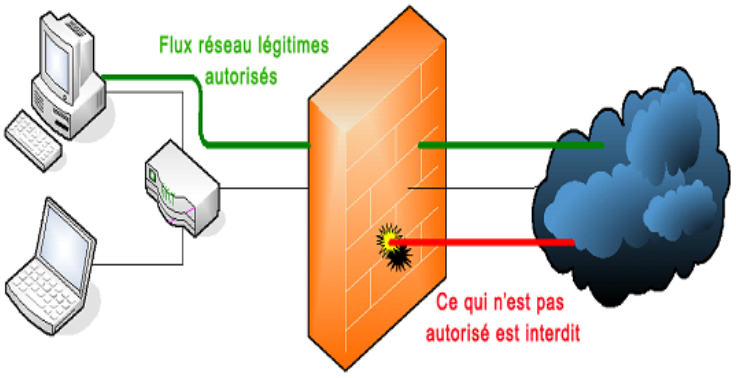

Figure 1.8: l'emplacement d'un pare-feu dans un réseau [7].

1.8.3 Serveur proxy :

Un serveur proxy appelé aussi serveur mandataire, est un composant logiciel informatique qui joue le rôle de l'intermédiaire entre deux machines pour surveiller leurs échanges.

La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, ...etc.) [8].

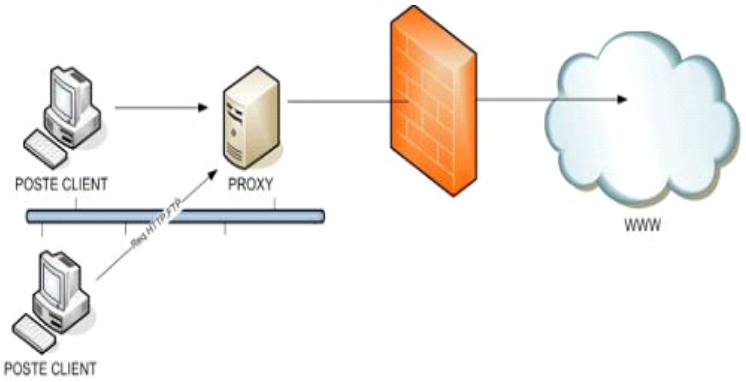

Figure 1.9: l'emplacement d'un proxy dans un réseau [8].

1.8.4 Un système détection d'intrusion :

La détection d'intrusions consiste à analyser les informations collectées par les mécanismes d'audit de sécurité, à la recherche d'éventuelles attaques. Bien qu'il soit possible d'étendre le principe, nous concentrerons sur les systèmes informatiques. Les méthodes de détection d'intrusion diffèrent sur la manière d'analyser le journal d'audits [23].

1.8.5 La DMZ :

Une DMZ (Demilitarized zone) est une zone tampon 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 publics (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 [9].

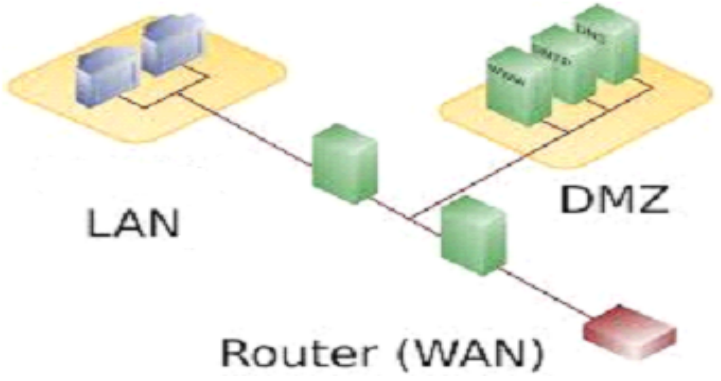

Figure 1.10: la DMZ entre LAN et WAN [9].

1.8.6 VPN :

Virtual Private Network, est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant les infrastructures publiques. Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites, et ce de façon simple et économique. Jusqu'à l'avènement des VPN, les sociétés devaient utiliser des liaisons Transpac, ou des lignes louées. Les VPN ont permis de démocratiser ce type de liaison.[25]

1.9 Général Emballage Spa

Général Emballage est leader en Algérie de l'industrie du carton ondulé. Il fabrique, à la commande, des plaques double- face (cannelures B, C, E et F) et double-double (BC et BE), des emballages et des displays.

Et réalise des post-impressions en Haute résolution jusqu'à 6 couleurs avec vernis intégral ou sélectif.

Les équipes maîtrisent l'ensemble des tâches de production : études, prototypage, réalisations de formes de découpe et de films d'impression, fabrication des emballages et des displays, livraison.

Entré en exploitation en 2002, Général Emballage est une Société de capitaux avec un capital social de 2.000.000.000 DZD opérant sur 3 sites industriels (Akbou, Oran et Sétif) avec près d'un millier d'employés et un Chiffre d'affaire de 6 milliards DZD. Général Emballage est une entreprise certifiée ISO 9001:2008.

1.10 Historique

2000 : 1er Août Création de la SARL Général Emballage avec un capital de 32 millions de dinars dans la Zone d'activités de Taharacht (Akbou. W de Béjaia) (décision APSI N°13051 du 06 juin 1998).

2002 : Entrée en production de l'usine d'Akbou avec un effectif de 83 employés.

2006 : Le capital est porté à 150 millions de dinars.

2007 :
- Le capital est porté à 1,23 milliards de dinars.
- Entrée en production de l'usine de Sétif.
- Trophée de la Production (Euro-Développement PME).

2008 :
- Début d'exportation vers la Tunisie.

- Entrée en exploitation de l'unité d'Oran.

2009 :
- 03 Juin : Augmentation du capital à 2 milliards de DA et entrée de MAGHREB PRIVATE EQUITY FUND II « Cyprus II» (MPEF II) avec une participation de 40
- Effectif : 597 employés.

2010 :
- Effectif : 630 employés.

2011 :
- Effectif : 699 employés.
- Novembre: Cotation COFACE « @@@ ».

2012 :
- Juin : L'usine d'Oran est transférée à la ZI Hassi-Ameur.
- Juin : Production des premiers ouvrages en Haute résolution.
- Juillet 02 : Signature d'une Convention cadre de partenariat avec l'Université de Béjaia.
- Décembre 17 : Notation COFACE « @@@ ».

2013 :
- Janvier 23 : Certification ISO 9001:2008.
- Octobre 8: Démarrage de la 1ére promotion de Licence en Emballage et Qualité à l'Université de Béjaia « L'Université de Béjaia et Général Emballage lancent, à partir de la rentrée universitaire de septembre 2013 une licence professionnelle en Emballage et qualité L'inscription est ouverte, à partir du 04 septembre 2013, aux étudiants de l'Université de Béjaia ayant accompli avec succès une 1ère année de Tronc commun (ST, SM ou SNV) Durée des études: 02 années avec de fréquents séjours en entreprise un Master pro sera ouvert au profit des licenciés ayant accompli 03 années d'expérience professionnelle » .

2014 : Février 22 : Signature d'un protocole d'accord de recrutement avec l'Agence Nationale de l'Emploi (ANEM).

2015 :
- Janvier : Démarrage d'unité de production à Sétif.
- Juin 02 : Prix d'encouragement du Trophée Export 2014 (World Trade Center (WTCA).

1.11 Situation géographique

le siège social est à ZAC Taharacht , Akbou, dans la wilaya de Béjaia.
RC N° : 00 B 0183268 du 05/08/2009
NIF : 000006018326879
Article d'imposition : 06256000300
NIS : 099806250344426

1.12 Organigramme de Général Emballage

Voici le schéma de Général Emballage, dont chaque direction a pour but d'assurer le bon fonctionnement de chaque partie comme le montre cette figure :

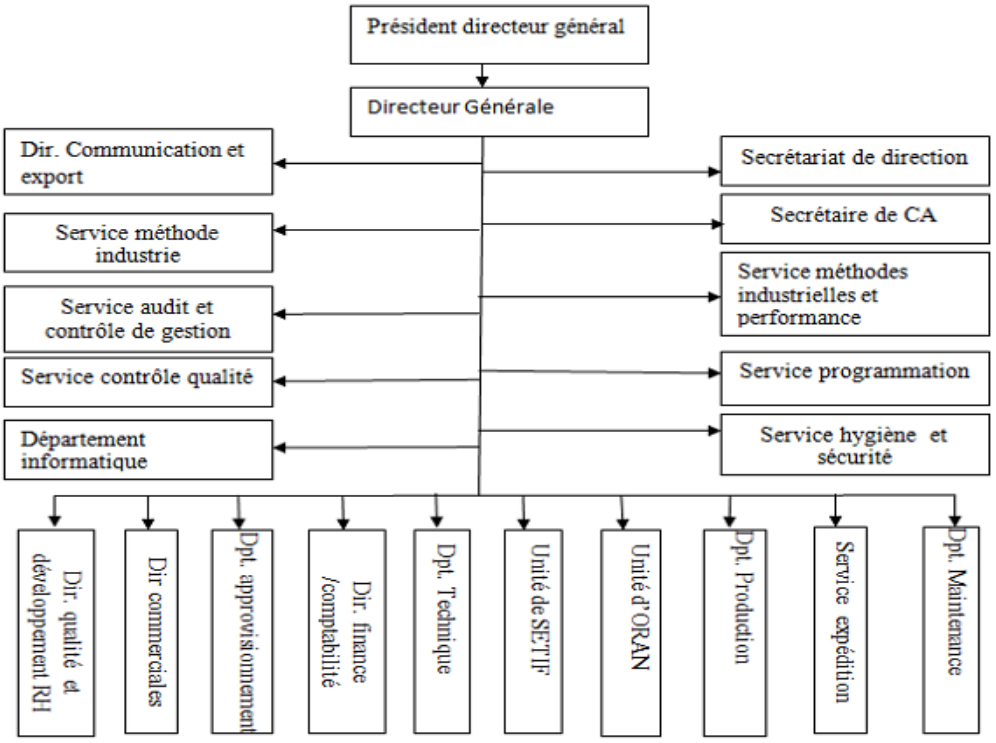

Figure 1.11: organigramme de général emballage.

1.13 L'informatique dans Général Emballage

Général Emballage est parmi les entreprises possédant une direction informatique et donne une grande importance au domaine de l'informatique.

1.13.1 Présentation de service informatique

Notre étude se focalise au niveau de Général Emballage d'AKBOU dont nous avons effectué notre stage, dans le service réseau.

1.13.2 Organigramme service informatique

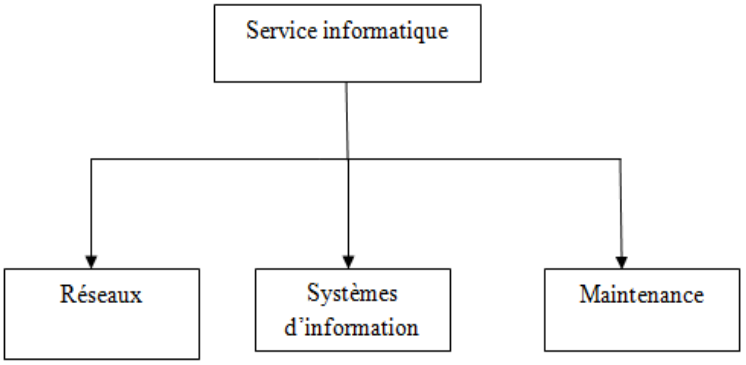

Figure 1.12: organigramme de service informatique dans Général Emballage.

1.13.3 Infrastructure matériel

Centre d'information (data center) est le coeur de Général Emballage, il contient tous les équipements physiques et tous les serveurs dont Général Emballage a besoin.

Le data center est une pièce très importante pour cela le droit d'accès est limite que pour l'équipe du système d'informations.

1.13.4 Les équipements physiques de Data Center

✓ **Onduleur** : Assure le bon fonctionnement et la continuité et la stabilité du courant électrique, il en existe plusieurs.

✓ **Climatiseur** : Il y a deux climatiseurs pour éviter l'échauffement des équipements physiques.

✓ **Un routeur** : Assure le fonctionnement et la liaison avec les réseaux des groupes qui se trouvent à Oran et Sétif.

✓ **Switch** : il existe plusieurs Switch dans général emballage, et chaque Switch est relie à un service, que ce soit service informatique, commerciale, laboratoire, unité serveurs...etc.

✓ **Un firewall** : Pour la gestion de protection Internet et pour l'autorisation d'accès à un nombre de site internet le ASA55 10-EDG.

1.13.5 Architecture du réseau

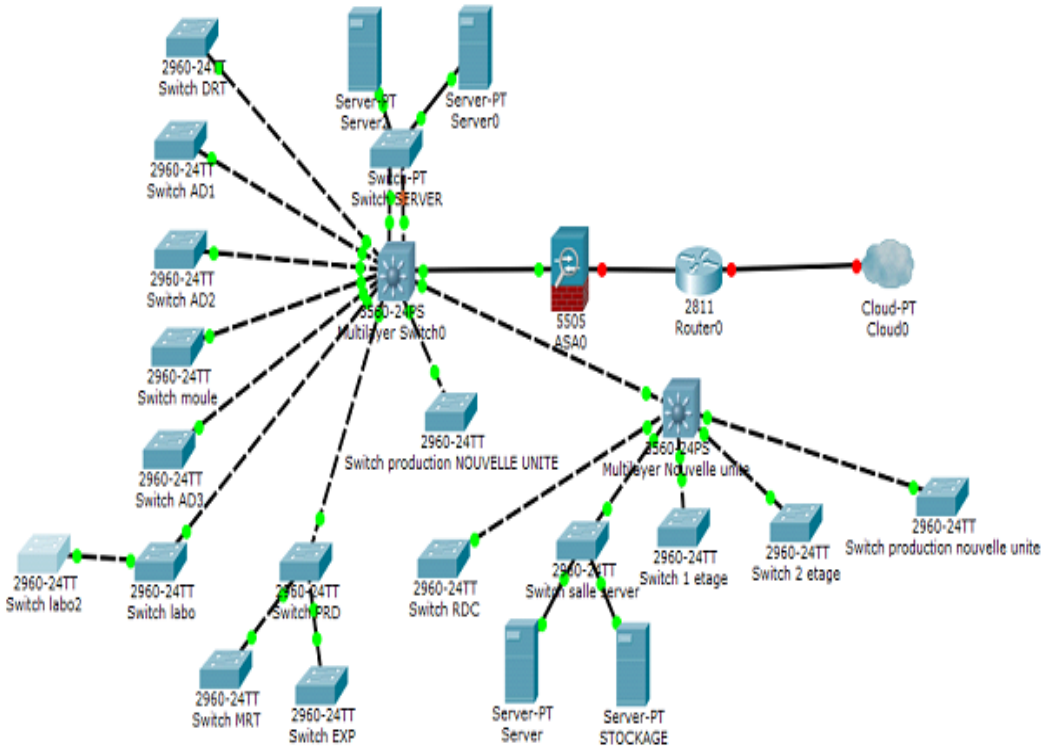

Figure 1.13: architecture du réseau.

1.14 Problématique

le systéme informatique en dépit de son déploiment dans tous les secteurs professionnels et son développement phénoménal, s'avére accompagné par une croissance frappante d'utilisateurs qui ne révèlent pas forcément de bonnes intentions vis-à-vis ce systéme informatique, vu que Firewall et d'autres antivirus ne suffisent point à garantir la sécurité des réseaux informatiques, des systémes de détction et de prévention d'intrusion sont mis en place. toute foi on a constaté au cours de notre stage au sein de l'entreprise de Général Emaballage des anomalies relatives à la sécurité de leur réseau, par rapport au manque d'un mécanisme de détection et de prévention d'intrusion.

De ce fait, durant notre stage au sein de Général Emballage nous avons constaté des anomalies relatives à la sécurité de leur réseau, à savoir le manque d'un mécanisme de détection et de prévention d'intrusion.

1.15 Objectif

La configuration d'IDS et d'IPS augmente le degré de la capacité de la sécurité informatique, car ils permettent de détecter et de prévenir des attaques venant de l'intrus, donc les IDS et les IPS jouent un role complémentaire pour le pare-feu (firewall), ils permettent d'analyser le trafic du réseau.

Enfin pour résoudre le problème que nous avons traité à la problématique, nous avons choisir de mettre en place un IDS et IPS sous Pfsense qui utilise le système d'exploitation freeBSD qui sera integré dans le pare-feu entre le réseau WAN et le réseau LAN, pour cela on a suivi ces quatre étapes :

- Etude du réseau existant et identification des besoins.
- Installation et mise en place d'IDS et d'IPS.
- Configuration d'IDS et d'IPS.
- Test de la configuration de systéme de détection et de prévention d'intrusion.

Conclusion

Les techniques de protection contre les attaques Internet permettent de réaliser les bases de la sécurité : confidentialité, intégrité, authentification, disponibilité.

Mais malgré toutes ces techniques utilisées pour empêcher les attaques Internet, un système n'est jamais totalement sûr.

Dans le deuxième chapitre, nous sommes intéressés par la présentation du systéme de détection et de pévention d'intrusion.

2

Systéme de détection et de prévention d'intrusion

Introduction

De nos jours, les attaques sont si rapides qu'avant, et tout le monde est exposé aux pertes des données essentielles. Malheureusement, les systèmes antivirus ou les pare-feux sont la plupart du temps inefficaces face à ces nouvelles menaces. C'est pour pallier ce manque que sont apparus récemment des nouveaux composants de sécurité appelés systèmes de détection et de prévention des intrusions.

En effet, le but de ce chapitre est tout d'abord, de présenter la notion de système de détection d'intrusion, et par la suite le système de prévention d'intrusion.

2.1 Systéme détection d'intrusion

Le premier modèle de détection d'intrusion est développé en 1984 par Dorothy Denning et Peter Neuman, qui s'appuie sur des règles d'approche comportementale. Ce système appelé IDES (Intrusion Detection Expert System), en 1988 Il est développé à un IDS(système de détection d'intrusion). [26]

Ce dernier est un ensemble de composants logiciels et/ou matériels destiné à repérer des activités anormales ou suspectes sur la cible analysée, un réseau ou un hôte, son rôle est de surveiller les données qui transitent sur ce système. Il permet ainsi d'avoir une action d'intervention sur les risques d'intrusion. Afin de détecter les attaques que peut subir un système ou réseau informatique. [27]

2.1.1 Type de système détection d'intrusion

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

2.1.1.1 La détection d'intrusion basée sur l'hôte

L'HIDS (Host Based IDS) surveille le trafic sur une seule machine. Il analyse les journaux systèmes, les appels, et enfin vérifie l'intégrité des fichiers. Un HIDS a besoin d'un système sain pour vérifier l'intégrité des données. Si le système a été compromis par un pirate, le HIDS ne sera plus efficace [10].

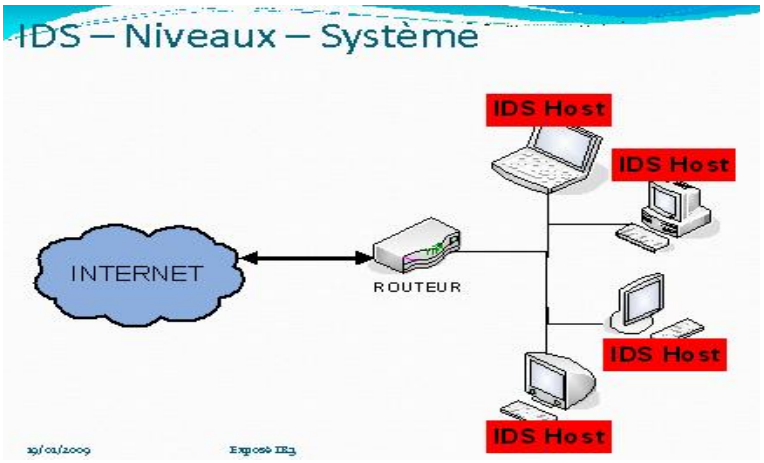

Figure 2.1: Exemple de HIDS [10].

2.1.1.2 La détection d'intrusion réseau NIDS

Les NIDS sont des IDS utilisés pour protéger un réseau. Ils comportent généralement une sonde (machine par exemple) qui écoute et surveille en temps réel tout le trafic réseau, puis analyse et génère des alertes s'il détecte des intrusions ou des paquets semblent dangereux [10].

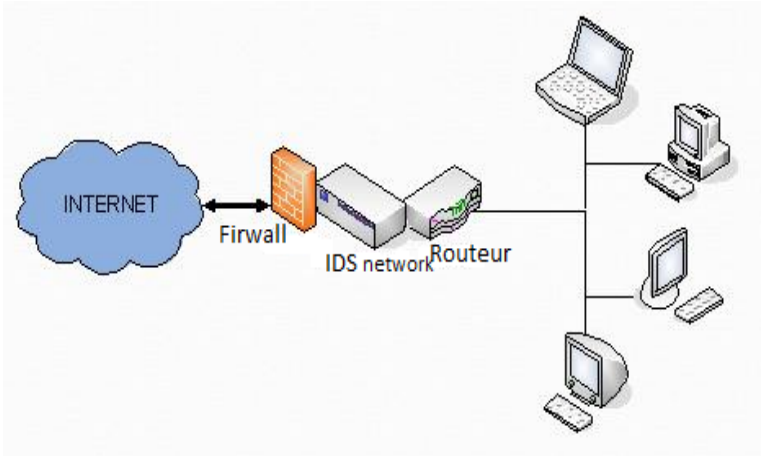

Figure 2.2: Exemple de NIDS [10].

2.1.1.3 Système de détection d'intrusion Hybride

IDS hybrides rassemblent les caractéristiques des NIDS et HIDS. Ils permettent, de surveiller le réseau et les terminaux. 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 lier les informations d'origines multiples. Ainsi, on comprend que les IDS hybrides sont basés sur une architecture distribuée, ou chaque composant unifie son format d'envoi. Cela permet de communiquer et d'extraire des alertes plus exactes [10].

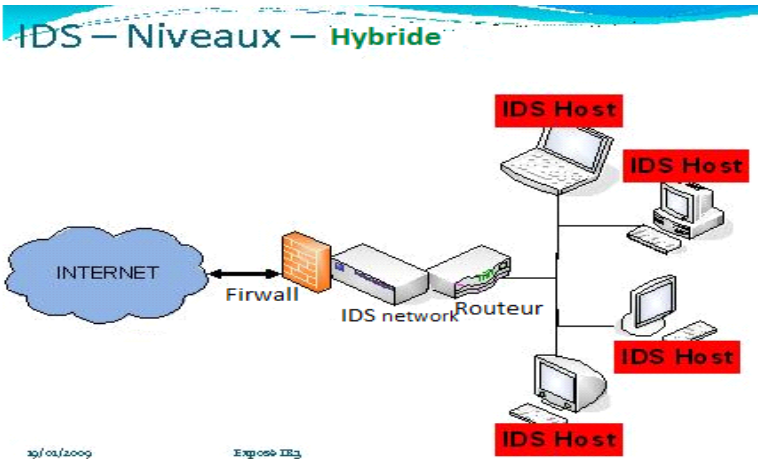

Figure 2.3: Exemple d'Hybride [10].

2.1.2 Comparaison entre les types d'IDS

	Avantages	**Inconvénients**
NIDS	-Les capteurs peuvent être bien sécurisés puisqu'ils se contentent d'observer le trafic. -Détecter plus facilement les scans grâce aux signatures. -Filtrage de trafic. -assurer la sécurité contre les attaques puisqu'il est invisible.	-La probabilité de faux négatifs (attaques non détectées) est élevée et il est difficile de contrôler le réseau entier. -Ils doivent principalement fonctionner de manière cryptée d'où une complication de l'analyse des paquets. -A l'opposé des IDS basés sur l'hôte, ils ne voient pas les impacts d'une attaque.
HIDS	-Découvrir plus facilement un Cheval de Troie puisque les informations et les possibilités sont très étendues. -Détecter des attaques impossibles à détecter avec des IDS réseau puisque le trafic est souvent crypté. -Observer les activités sur l'hôte avec précision.	-Ils ont moins de facilité à détecter les scans. -Ils sont plus vulnérables aux attaques de type DoS. -Ils consomment beaucoup de ressources CPU.
hybrides	-moins de faux positifs. -meilleure corrélation (la corrélation permet de générer de nouvelles alertes à partir de celles existantes). -possibilité de réaction sur les analyseurs.	-taux elevé de faux positifs.

Table 2.1: la comparaison entre types d'IDS.

2.1.3 Architecture fonctionnelle des IDS

Nous décrivons dans cette section les trois composants qui constituent classiquement un système de détection d'intrusion. La Figure ci-dessous illustre les interactions entre ces trois composants [11].

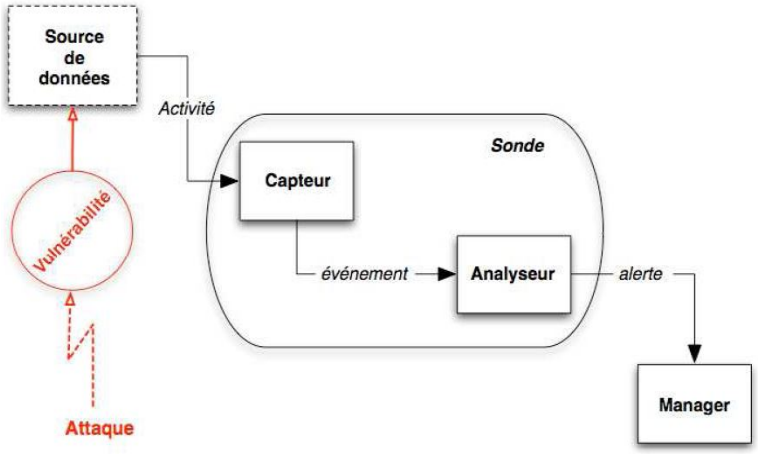

Figure 2.4: architecture fonctionnelle d'un IDS [11].

2.1.3.1 Capteur

Le capteur observe l'activité du système par le biais d'une source de donnée et fournit à l'analyseur une séquence d'événements qui renseignent de l'évolution de l'état du système.

Le capteur peut se contenter de transmettre directement ces données brutes, mais en général un prétraitement est effectué. Et pour cela on distingue trois types de capteurs en fonction des sources de données utilisées pour observer l'activité du système : les capteurs système, les capteurs réseau et les capteurs applicatifs.

2.1.3.2 Analyseur

L'objectif de l'analyseur est de déterminer si le flux d'événements fourni par le capteur contient des éléments caractéristiques d'une activité malveillante.

2.1.3.3 Manager

Le manager collecte les alertes produites par le capteur, les met en forme et les présente à l'opérateur[1]. Eventuellement, le manager est chargé de la réaction à adopter qui peut être :

- Isolement de l'attaque, qui a pour but de limiter les effets de l'attaque.
- Suppression d'attaque, qui tente d'arrêter l'attaque.
- Recouvrement, qui est l'étape de restauration du système dans un état sain.
- Diagnostic, qui est la phase d'identification du problème.

[1] administrateur

2.1.4 Classification des systèmes de détection d'intrusion

Les différents systèmes de détection d'intrusion disponibles peuvent être classés selon plusieurs critères qui sont : [12]

- La méthode de détection.
- Le comportement du système après la détection.
- La source des données.
- La fréquence d'utilisation.

La figure ci-dessous illustre les détailles de chaque critère.

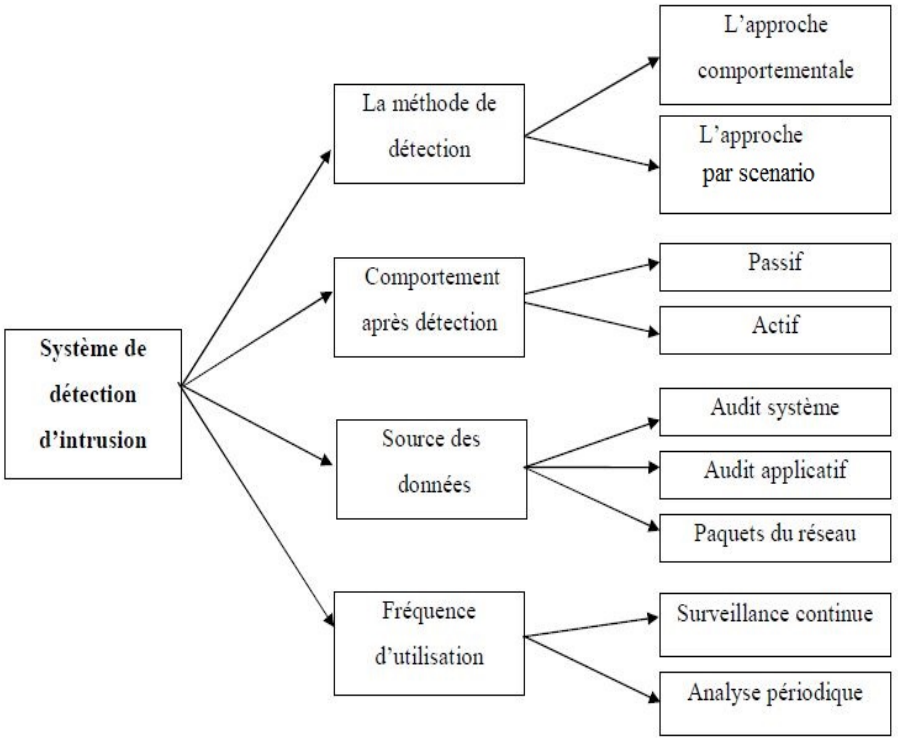

Figure 2.5: classification d'un système de détection d'intrusion [12].

2.1.4.1 Méthodes de détection des IDS

Il existe deux méthodes de détection: [13]

✓ **Approche par scénario ou par signature** : Cette technique s'appuie sur les connaissances des techniques utilisées par les attaquants contenues dans la base de donnée, elle compare l'activité de l'utilisateur à partir de la base de

donnée, ensuite elle déclenche une alerte lorsque des événements hors profil se produisent.

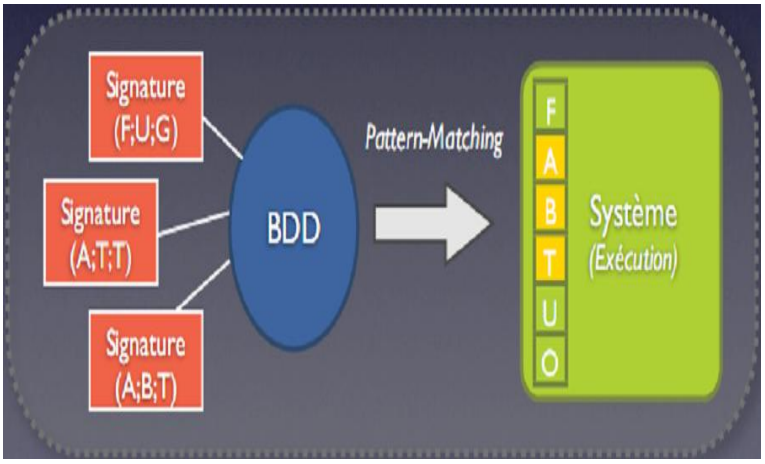

Figure 2.6: illustration de l'approche scénario [13].

✓ **L'approche comportementale** : Cette technique consiste à détecter une intrusion en fonction du comportement de l'utilisateur ou d'une application, autrement dit c'est créer un modèle basé sur le comportement habituel du système et surveiller toute déviation de ce comportement.

Plusieurs paramètres sont possibles : la charge CPU, le volume de données échangées, la durée et l'heure de connexion sur des ressources, la répartition statistique des protocoles et applications utilisés...etc.

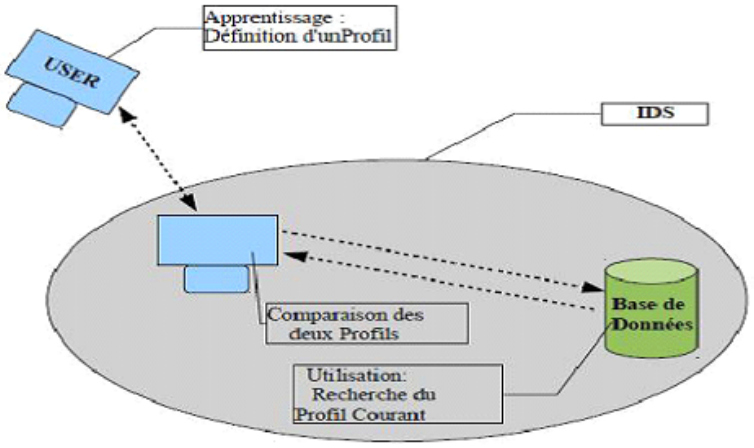

Figure 2.7: illustration de l'approche comportementale [14].

2.1.4.2 Comportement après la détection d'intrusion

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

✓ **Réponse passive** : Lorsqu'une attaque est détectée, le système d'intrusion ne prend aucune action, il génère seulement une alarme en direction de l'administrateur système sous forme d'une alerte lisible qui contient les informations à propos de chaque attaque. Les réponses passives se traduisent la plupart du temps par des opérations de reconfiguration automatique d'un firewall afin de bloquer les adresses IP source impliquées dans les intrusions. Mais si le pirate prend une adresse IP sensible telle qu'un routeur d'accès ou un serveur DNS, l'entreprise qui implémente une reconfiguration systématique d'un firewall risque tout simplement de se couper du monde extérieur.[13]

✓ **Réponse active** : La réponse active consiste à répondre directement à une attaque, elle implique des actions automatisées prises par un IDS qui permet de couper rapidement une connexion suspecte quand le système détecte une intrusion. Par exemple interrompre le progrès d'une attaque pour bloquer ensuite l'accès suivant de l'attaquant. Mais cella risque de se voir exposer à une contre attaque part le pirate.[28]

2.1.4.3 La nature des données analysées

La nature des données analysées sont composées de : [13]

✓ **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.

✓ **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.

✓ **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.

2.1.4.4 La fréquence d'utilisation

La fréquence d'utilisation d'un système de détection d'intrusion peut exister selon deux formes :

✓ **Surveillance périodique** : Ce type de système de détection d'intrusion analyse périodiquement les différentes sources de données à la recherche d'une éventuelle intrusion ou une anomalie passée.

✓ **Surveillance en temps réel** : Les systèmes de détection d'intrusions en temps réel fonctionnent sur le traitement et l'analyse continue des informations produites par les différentes sources de données. Elle limite les dégâts produits par une attaque car elle permet de prendre des mesures qui réduisent le progrès de l'attaque détectée.

2.1.5 Limite des IDS

✓ **N-IDS** : Ils sont basés sur une bibliothèque de signatures d'attaques connues, cette bibliothèque devra être mise à jour à chaque nouvelle attaque sera affichée. Si l'attaque ne contient pas la signature d'une attaque spécifique et récente, cette dernière passera au travers des mailles du filet et la sécurité des données et le réseau en général sera menacé.[29]

✓ **H-IDS** : Il génère une alerte si une activité sur l'hôte s'éloigne de la norme, mais si dans un cas exceptionnel une requête justifiée mais non prévue par le système venaient à arriver en masse, cette méthode de protection risquerait de générer des alertes infondées. Dans ce cas les H-IDS ne sont pas fiables car ils ne font que générer des alertes, et ce sera à un administrateur en charge de la sécurité du réseau de dire si telle ou telle requête est valable ou pas.[29]

2.1.6 Efficacité des systèmes de détection d'intrusions

L'efficacité d'un système de détection d'intrusions est déterminée par les mesures suivantes : [12]

✓ **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 [30].

2.2 Système de prévention d'intrusion

En effet, l'IPS est un outil de protection et sécurité des systèmes d'information contre les intrusions, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque. C'est un IDS actif, il empêche toute activité suspecte détectée au sein d'un système [31].

2.2.1 Types d'IPS

2.2.1.1 La détection 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 : [31]

- 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.

2.2.1.2 La prévention d'intrusion basée sur le 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.[31]
Deux types de NIPS :

✓ **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.

✓ **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.

Avantage de NIPS :
Protection active.

Inconvénients de NIPS :

- Point sensible du réseau.
- Faux positifs (risque de blocage de trafic légitime).
- Coût complexité additionnelle / Exploitation supplémentaire.

2.2.1.3 La détection d'intrusion basée sur noyau KIPS

Les KIPS (Kernel Intrusion Prevention System) leur particularité est de s'executer dans le noyau d'une machine, pour y bloquer toute activité suspecte. Si cela est pratique pour empecher des tetavees d'appels systéme 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]

2.2.2 Les inconvénients d'IPS

Un IPS possède des nombreux inconvénients : [20]

- 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.

2.2.3 Architecture foncionnelle 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 [15].

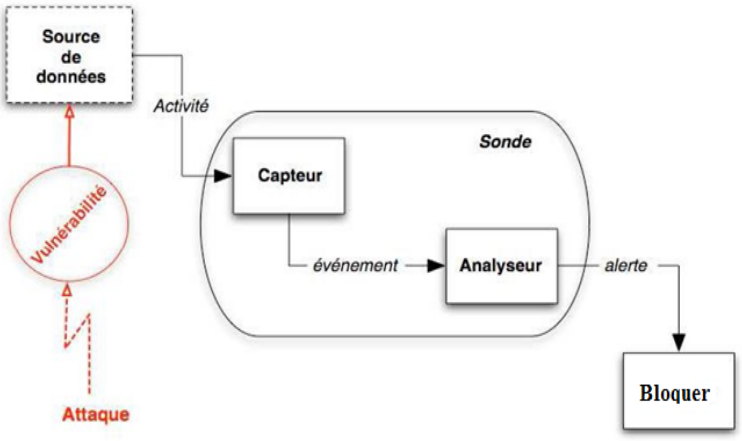

Figure 2.8: architecture fonctionnelle d'un IPS [15].

2.2.4 Dispositifs d'un NIPS

Un NIPS a quatre caractéristiques principales : [32]

- 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 partie 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.

2.2.5 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 [33].

2.2.6 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 : [34]

✓ **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.

2.2.7 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 : [32]

✓ **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.

2.2.8 La Différence entre IPS et Firewall

Firewall est un système de contrôle d'accès basé sur des règles statiques autorisant ou refusant certains flux. Il travaille essentiellement au niveau des couches du modèle OSI (de 1 à 4) ce qui est insuffisant pour les intrusions.

Contrairement à un IPS qui doit être complètement discret. Ceci implique que les interfaces de la sonde ne doivent pas être visibles (pas d'adresse IP, pas d'adresse MAC), et l'IPS analyse l'intégralité des paquets en transit, depuis les couches réseaux jusqu'au niveau applicatif [35].

Conclusion

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

le chapitre suivant nos renseigne comment réussir la configuration, après installation, du système de détection et de prévention d'intrusion afin de mieux sécuriser le réseau, Nous allons montrer également un test permettant la confermation les bonnes installation et configuration de notre systéme.

3

Tests et mise en place

introduction

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

En final, nous allons donner quelques tests que nous avons réalisés en lançant quelques attaques et quelques virus et voir comment ces derniers sont détectés et bloqués.

3.1 Présentation de PfSense

Basé sur FreeBSD, pfSense est un logiciel de filtrage de flux (Firewall). Comme iptables sur GNU/Linux, il est réputé pour sa fiabilité. Nous y retrouvons la plupart des fonctionnalités incluses dans des firewalls commerciaux et quelques autres complémentaires [36].

3.1.1 Les services proposés

Plusieurs services peuvent être gérés par pfSense. Ils peuvent être arrêtés ou activés depuis son interface.

Voici la liste des services :[36]

- Système de basculement (Failover) par le protocole CARP.
- VPN site à site OpenVPN et IPSec.
- VPN client PPTP.
- Proxy et Blacklist SQUID et SQUIDGuard.
- IDS-IPS Snort.
- Répartition de charge avec LoadBalancer.
- Vue sur la Consommation de Bande Passante avec Bandwithd et Ntop pour plus de détails.
- VPN point à point Stunnel.
- Partage de bande passante Traffic Shaper.

3.2 Configuration des adresses IP sous pfsense

Apres avoir créé la machine virtuelle et installé le pfsense, nous allons configurer les adresses IP.

Sur le menu suivant on choisit l'option n°2 pour configurer les interfaces, puis deux options apparaissent, celle de WAN et celle de LAN.

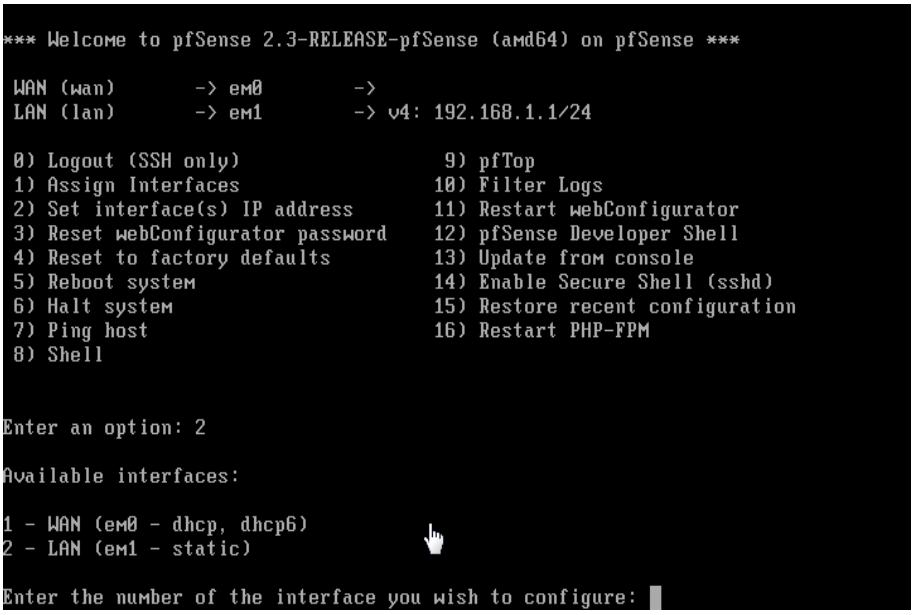

Figure 3.1: configuration l'interface du WAN.

Nous commençons par la configuration du WAN on tapant 1, et nous aurons deux options soit le DHCP qui délivre l'adresse IP du WAN ou en l'attribuant une adresse manuellement comme dans notre cas 192.168.43.200, puis en choisissant le masque, dans notre cas sera 24, après nous attribuerons l'adresse IP de la passerelle.

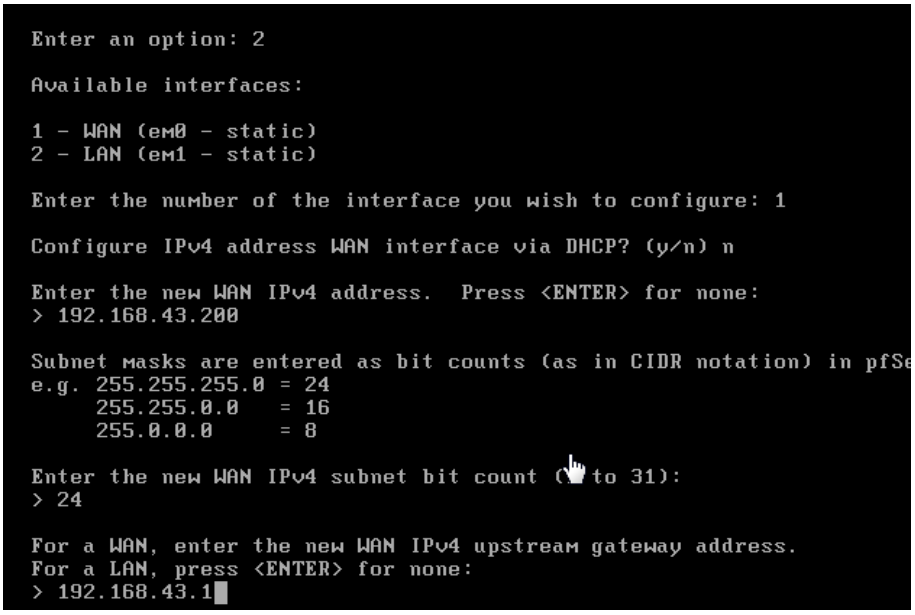

Figure 3.2: attribution d'une adresse ip pour l'interface du WAN.

Pour l'adresse IP de ipv6, nous n'avons pas besoin de la configurer, alors nous tapons sur entrer directement. Quant au navigateur web nous choisissons le http et nous validons par « y » ou bien en le convertissant en https et en tapant « n », suivi par entrer.

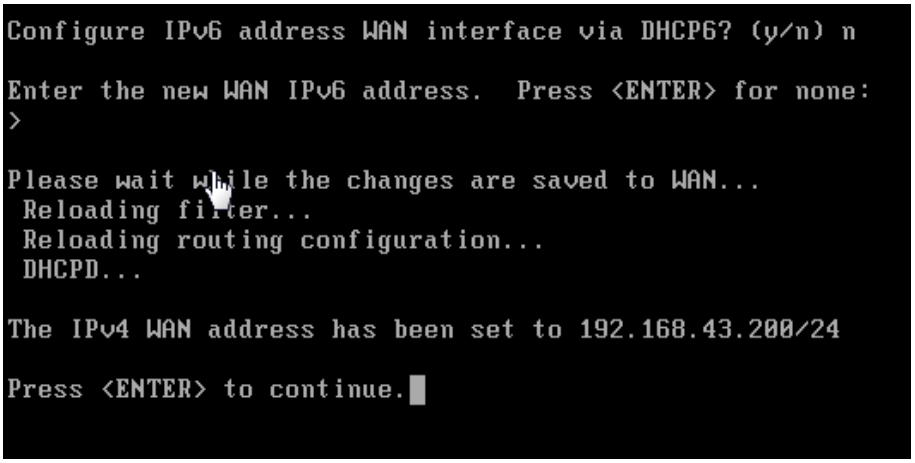

Figure 3.3: attribution d'une adresse ipv6 pour l'interface du WAN.

Et maintenant nous configurons le LAN en suivant les mêmes instructions que le WAN.

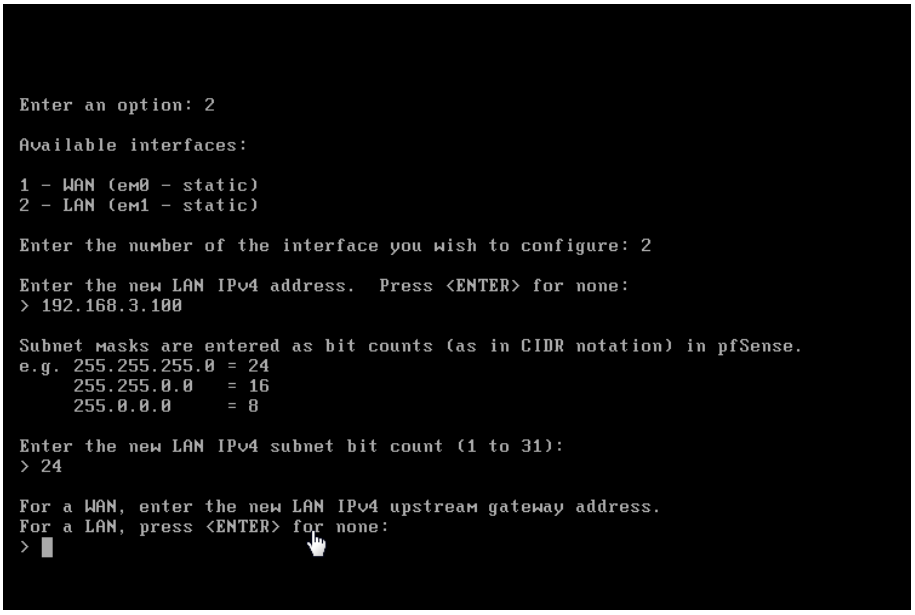

Figure 3.4: configuration l'interface du LAN.

Nous allons respecter le plan réseau suivant :
Wan : 192.168.43.200/24
Lan : 192.168.3.100/24

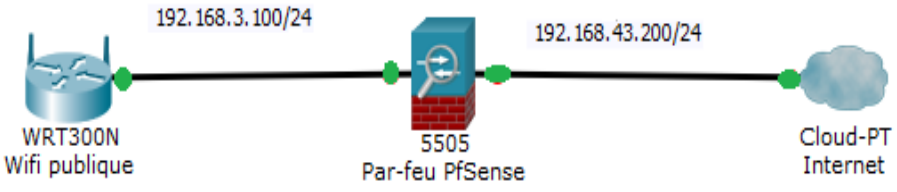

Figure 3.5: l'enchainement du reseau.

3.2.1 Configuration de l'interface

Accéder à l'interface web en entrant l'adresse IP du LAN dans un navigateur dans notre cas : 192.168.3.100. Nous arrivons sur la page de connexion de PfSense dont les identifiants sont :
Login : admin
mot de passe : pfsense

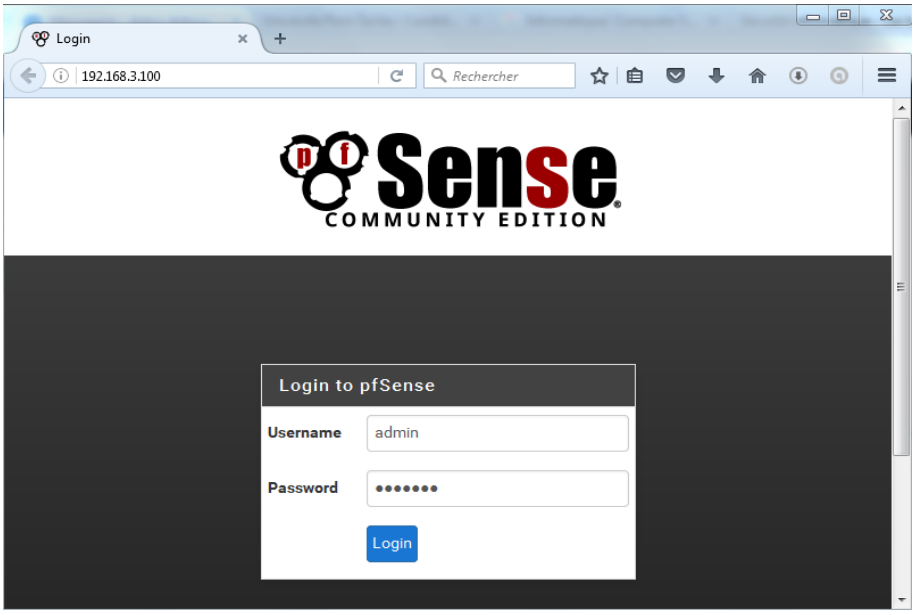

Figure 3.6: configuration l'interface de pfsense.

3.3 Installation et configuration de snort

3.3.1 Présentation de snort :

SNORT est un outil open source de NIDS, il est capable d'écouter sur une interface afin d'effectuer une analyse du trafic en temps réel, de logger les paquets IP, de rechercher des correspondances de contenu , le but étant de détecter une grande variété d'attaques connues.

SNORT peut fonctionner en quatre modes différents : SNIFFER (capture et affichage des paquets, pas de log), PACKET LOGGER (capture et log des paquets), NIDS (analyse le trafic, le compare à des règles, et affiche des alertes) puis IPS (détection d'attaques et prévention de celles-ci).

3.3.2 Maquette de test :

Voici la maquette qui nous permettra de tester SNORT afin de mettre en avant ses fonctions de NIDS et d'IPS :

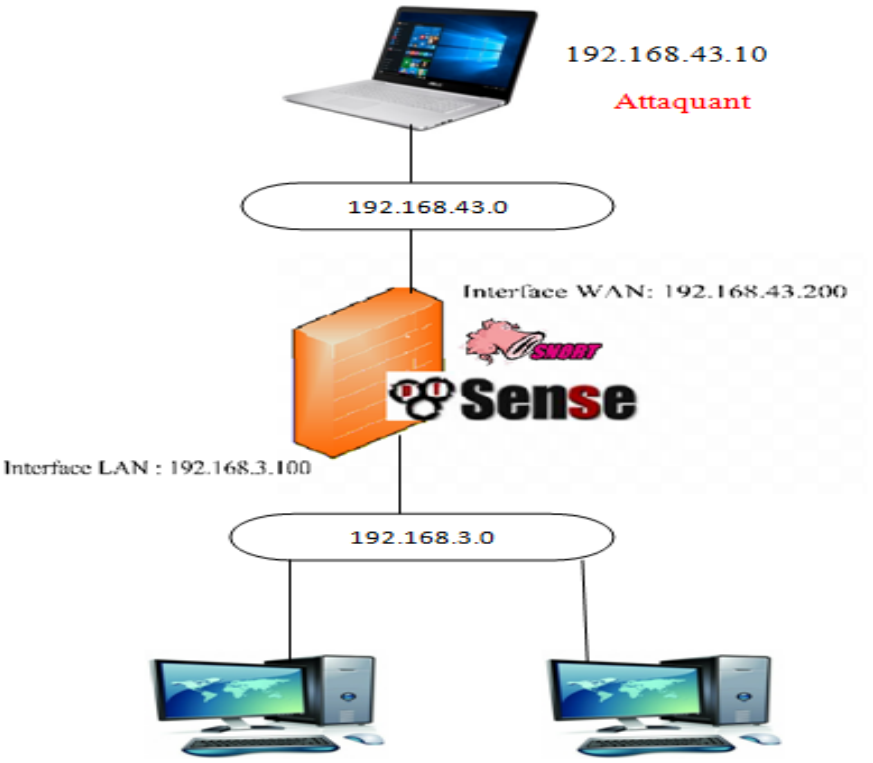

Figure 3.7: maquet de test.

Installation et configuration de snort La première étape est l'installation du package SNORT dans pfSense (system->packages->SNORT) :

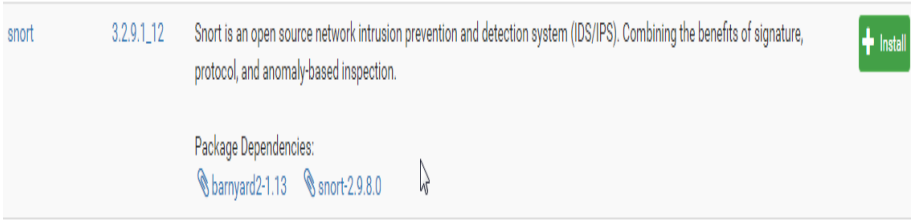

Figure 3.8: installation package de snort.

L'installation étant maintenant faite, la seconde étape importante est la création d'un compte sur http://snort.org, afin de pouvoir récupérer les règles prédéfinies en temps voulu.

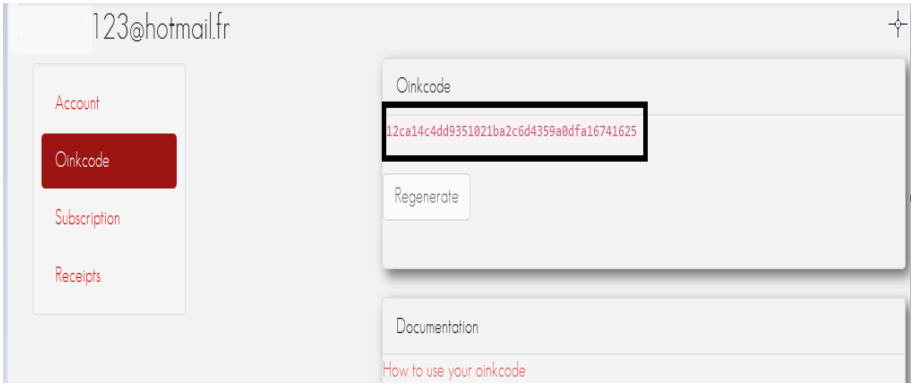

Figure 3.9: création de compte sur le site de snort.

Cliquez sur l'onglet Paramètres globaux et activer l'ensemble des règles de téléchargements à utiliser.

Soit nous utilisons le Snort VRT (comme dans notre cas), soit Emerging Threats (ET) Rules. Après, une zone de texte sera affichée pour entrer le code unique de l'abonné obtenu avec l'abonnement ou l'enregistrement.

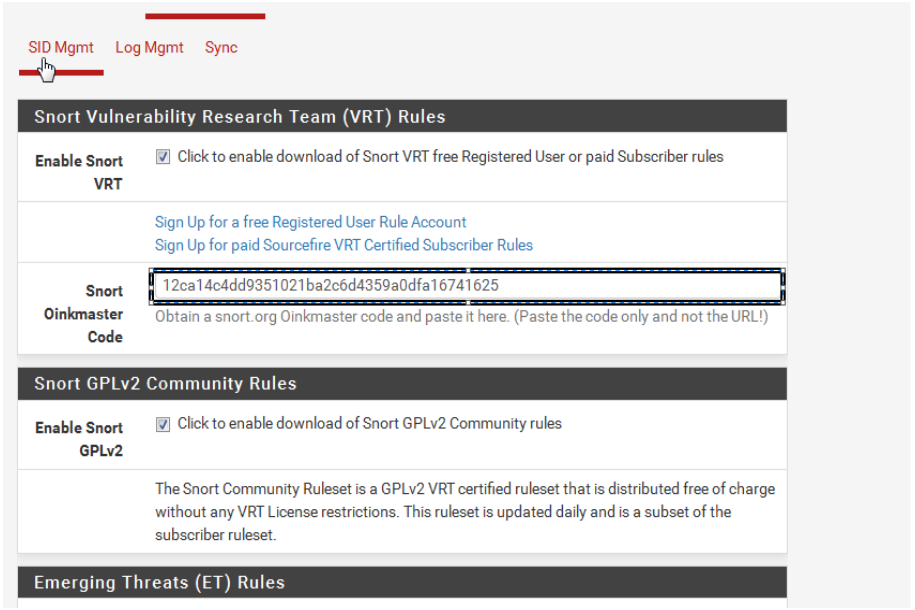

Figure 3.10: code d'activation des régles de snort.

Donc avec un intervalle de 12 heures visant la mise à jour sélectionnée, Snort vérifiera la Snort VRT 3 minutes après minuit et 3 minutes après midi chaque jour pour toutes les mises à jour des paquets des règles affichés.

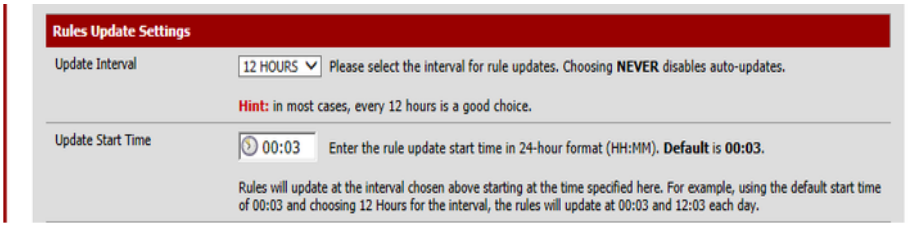

Figure 3.11: mise à jour des paquets des règles.

nous Validons ensuite en cliquant sur le bouton « save » en bas de page. SNORT va automatiquement télécharger les règles (premium rules) depuis snort.org grâce à notre Oinkmaster code :

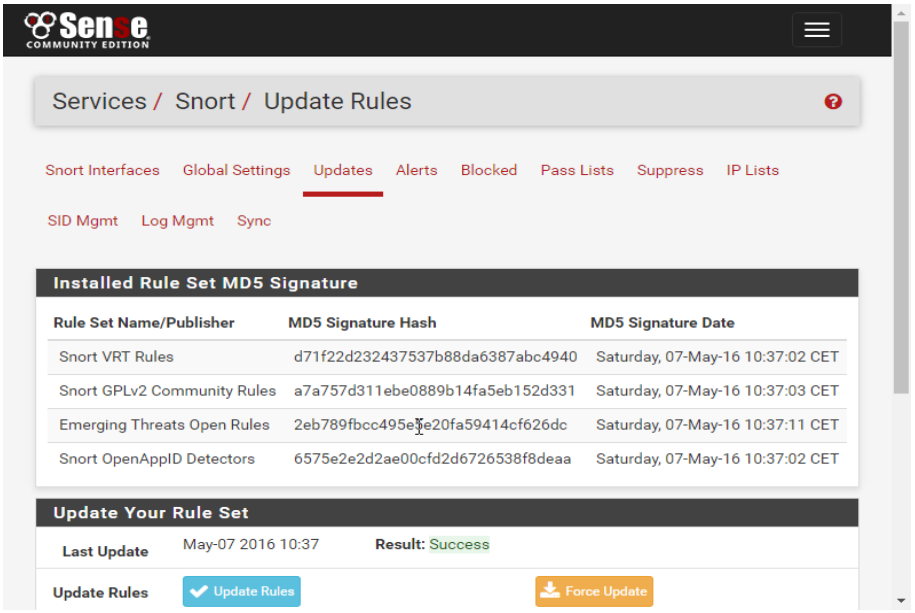

Figure 3.12: télécharger les règles de snort.

Toutes les règles ainsi téléchargées sont regroupées sous forme de catégorie dans l'onglet «Wan categories », à nous de sélectionner celles qui correspondent aux attaques que nous voulons détecter sur notre réseau.

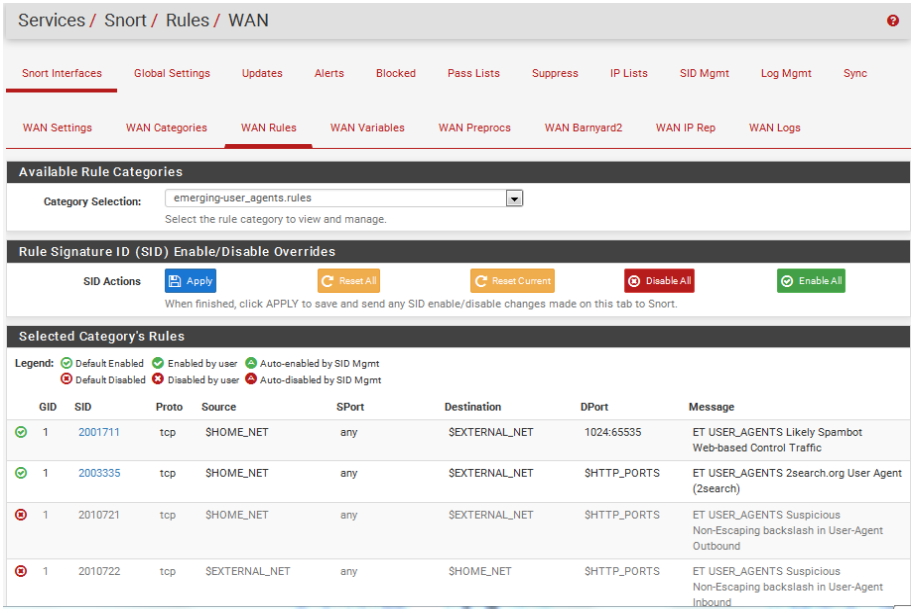

Figure 3.13: activation des règles.

Maintenant, nous allons ajouter une nouvelle interface. Pour cela, nous cliquons sur l'onglet Snort Interfaces puis sur ajouter.

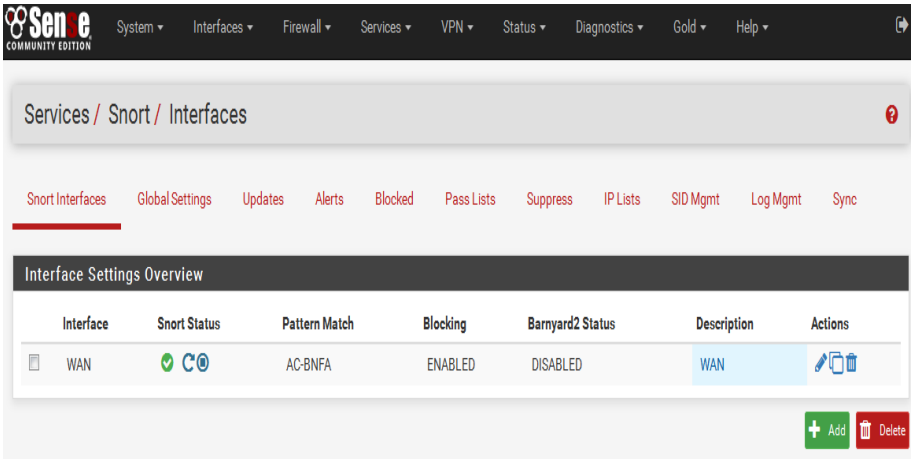

Figure 3.14: ajouter l'interface du WAN.

Nous allons configurer l'interface du WAN et modifier que ce qui est nécessaire.

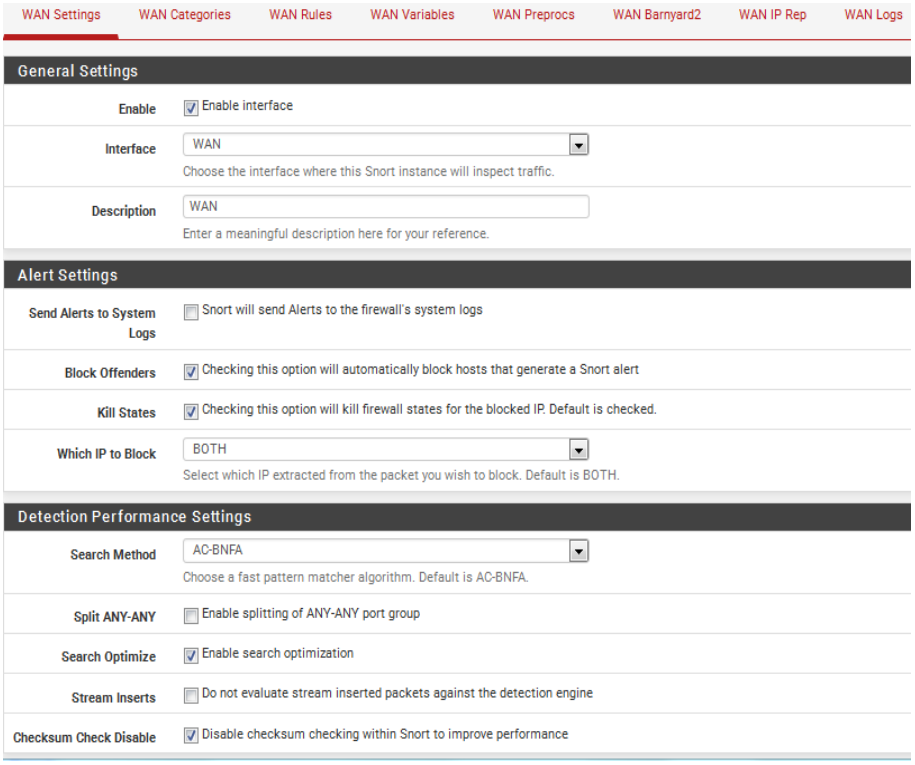

Figure 3.15: modification les paramétres du WAN.

La configuration de systéme de détection et de prévention d'intrusion est désormais terminée, la machine de supervision peut d'hors et déjà consulter les alertes ainsi que la liste des adresses IP bloquées.

La liste des alertes .

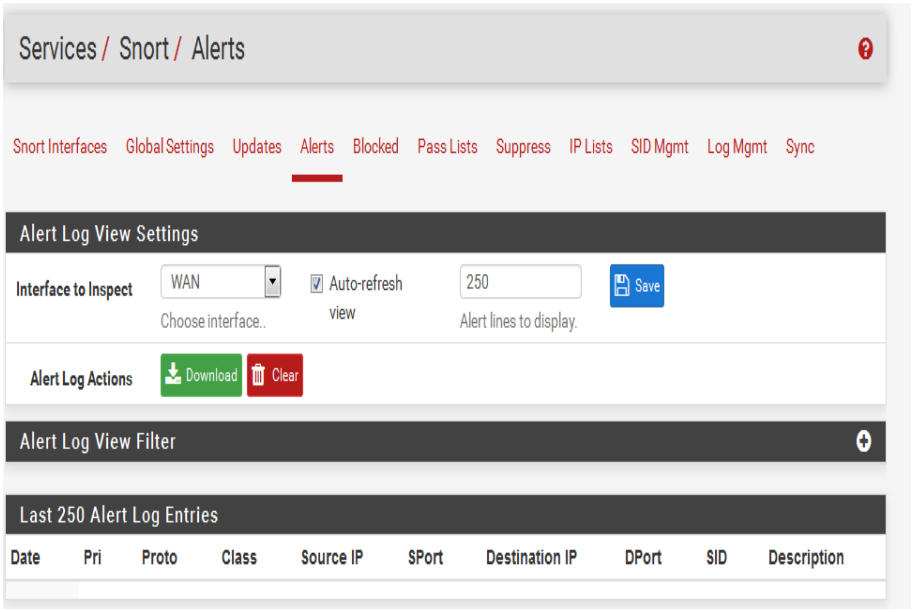

Figure 3.16: La liste des alertes.

La liste des adresses IP bloquées

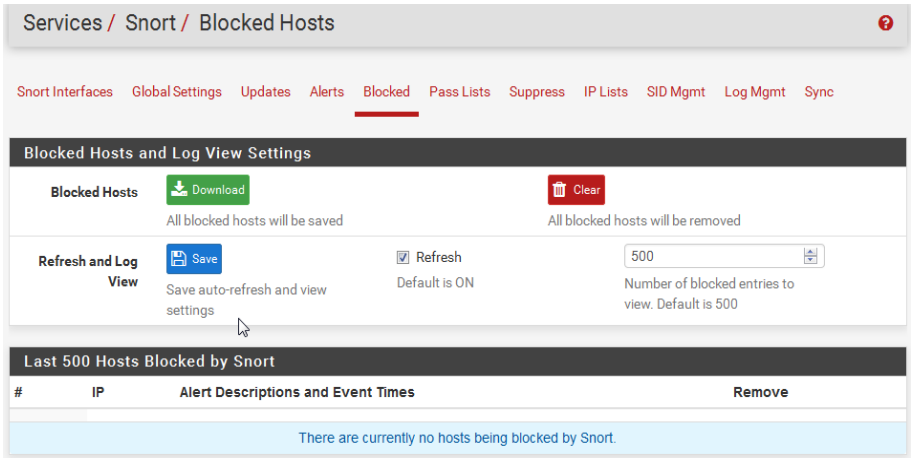

Figure 3.17: La liste des adresses IP bloquées.

3.4 Test de la solution

3.4.1 Zenmap

Nmap a été conçu pour détecter en scannant les portes ouvertes sur le réseau et obtenir des informations sur l'OS d'un systéme distant, il utlise plusieurs protocoles (UDP,TCP,IP,ICMP) pour générer un audit de sécurité.

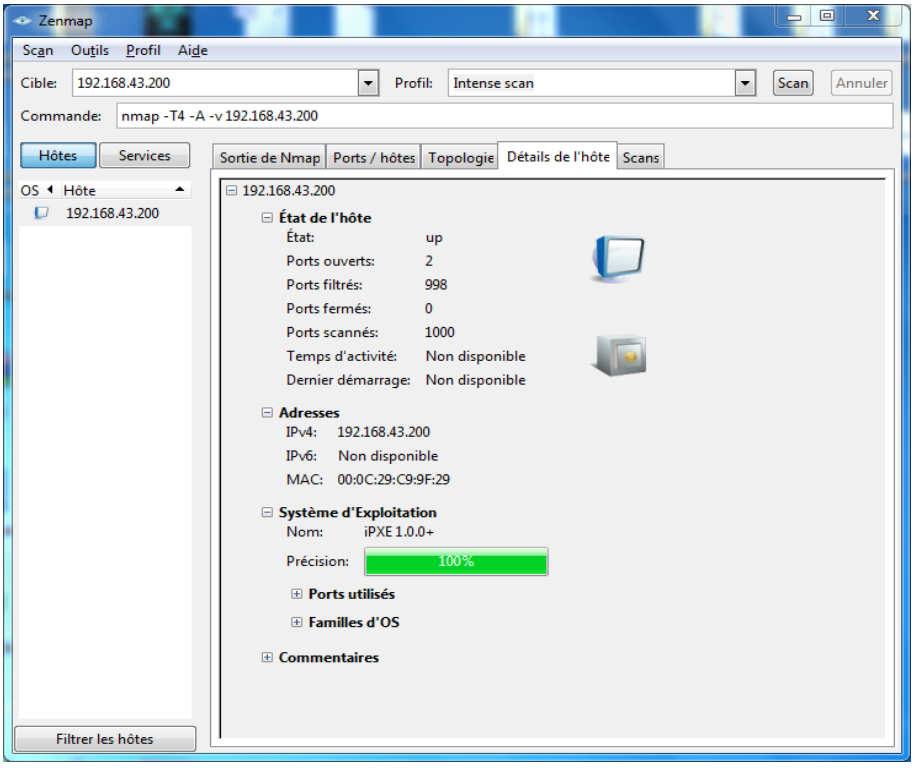

Figure 3.18: test de fiabilité d'IDS et IPS.

Une fois le scan de port lancé, la station de supervision peut très rapidement constater des alertes ainsi que l'IP 192.168.43.159 (notre attaquant) a été bloquée :

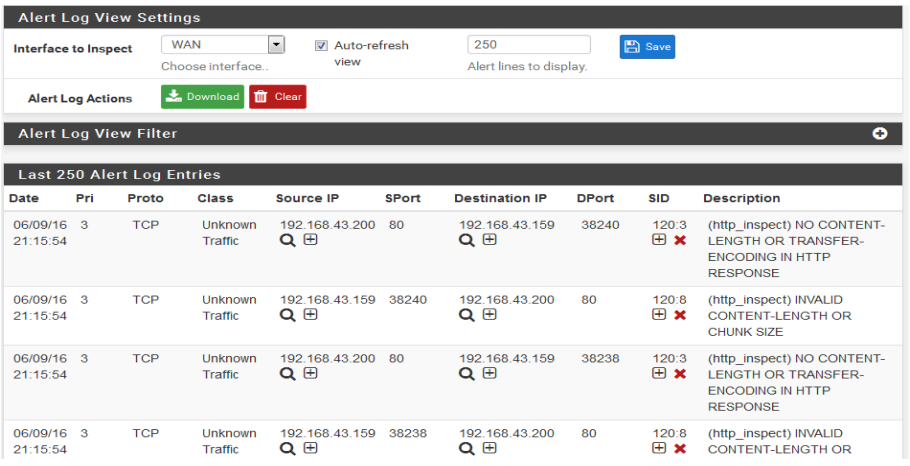

Figure 3.19: La liste des alertes aprés le test.

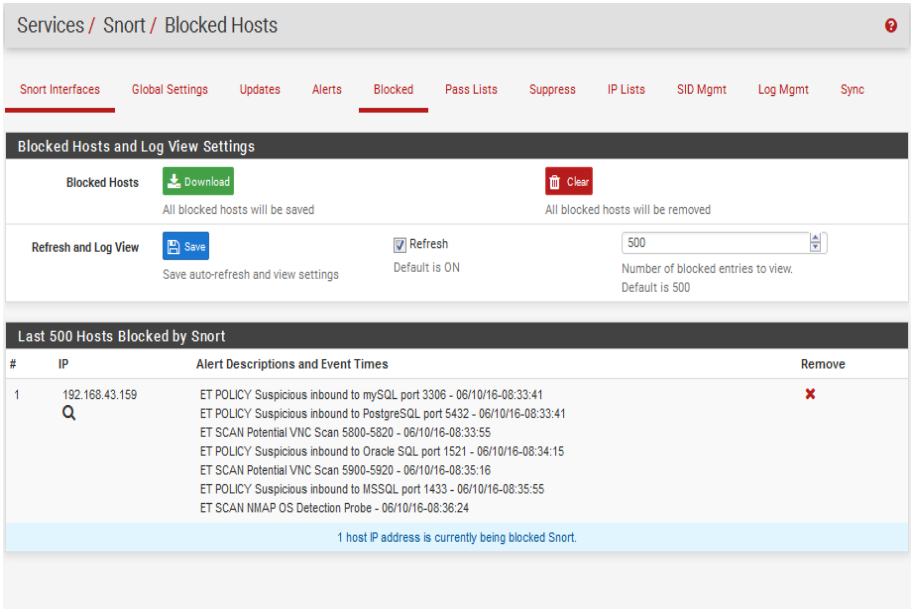

Figure 3.20: La liste des adresses ip bloquées aprés le test.

Conclusion

Dans ce chapitre, nous avons présenté des outils importans pour la détection et la prévention d'intrusion. À savoir PfSense et Snort. Nous avons donné toutes les étapes d'installation et configuration de ces outils.

Les systèmes de détection et de prévention d'intrusions, en particulier snort, peuvent être assimilés à des simples alarmes qui se déclenchent une fois une intrusion détectée et bloquée.

Conclusion générale

Conclusion générale

La sécurité des réseaux informatiques demeure encore un sujet très sensible voir complexe, pour les acteurs du monde informatique, car les variables qui tournent autour de ce sujet sont souvent difficiles à maitriser.

Ce projet nous a permis de découvrir les systèmes de détection et de prévention d'intrusions. Nous avons étudié les fonctionnements d'IDS et d'IPS de type réseau, ainsi nous avons pris comme exemple le snort sous le pare-feu pfsense qui est un trés bon outil pour la détection et la prévention d'intrusion, il effectue en temps réel des analyses du trafic et journalise(log) les paquets IP transitant sur le réseau, Ce qui nous a offert l'occasion de travailler sous l'environnement Free BSD.

Le résultat des tests de notre système est satisfaisant, 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% .

Bibliography

[1] https://www.securiteinfo.com/attaques/hacking/typesattaques.shtml.

[2] http://rene-reyt.fr/documents/informatique/petit-resume-de-securite-informatique/securite-informatique-les-techniques-dattaque/.

[3] http://www.info-virus.com/comprendre-les-virus-informatiqu.htm.

[4] Gunadiz.Safia. Algorithme d'intelligence artificielle pour la classification d'attaques réseaux à partir de données tcp. 2010-2011.

[5] Cedric Llorens. Denis valois et laurent levier, tableau de bord de la sécurité réseau.

[6] Mohammed EL-Sayed GADELRAB. Evaluation des systémes de détection d'intrusion.

[7] JABOU Chaouki. Ter détection d'anomalies sur le réseau. 2009.

[8] http://www.commentcamarche.net/contents/610-serveur-proxy-et-reverse-proxy.

[9] LESCOP Yves. La sécurité informatique,.

[10] http://igm.univ-mlv.fr/dr/XPOSE2009/Sonde-de-securite-IDS-IPS/IPS.html.

[11] J. Timmis. Artificial immune systems: A novel data analysis technique inspired by the immune network theory. 1999.

[12] H. Debar. Wespi, a revised taxonomy for intrusion detectionsystems,. 1999.

[13] LABED Ines. Proposition d'un systéme immunitaire artificiel pour la détection d'intrusions. 2005-2006.

[14] Abderrahim ESSAIDI. Conception d'une zone démilitarisée (dmz). 2006-2007.

[15] Osman SALEM. La protection des réseaux contre les attaques dos.

[16] Apporter les notions essentiels pour l'interconnexion de réseau dans des environnements de communication hétérogéne basé sur tcp/ip.

[17] Arnould.Gerard. Etude et conception d'architectures haut-débit pour la modulation et la démodulation numériques. Décembre 2006.

[18] TATEB Dehia. Mise en oeuvre d'une solution de sécurité basé sur ids cas d'étude : entreprise algérie télécom, mémoire de master en informatique. juin 2014.

[19] http://xenod.free.fr/0-La-securite-informatique.htm.

[20] CHIKH Asma. Sécurité d'une application web à l'aide d'un systéme de détection d'intrusions comportementale. 2011-2012.

[21] Jean-Christophe GALLARD. Sécurité et réseaux,v 2.0.

[22] Michaël AMAND. Etude d'un systéme de détection d'intrusion comportemental pour l'analyse du trafic aéroportuaire.

[23] BIONDI Philippe. Architecture expérimentale pour la détection d'intrusions dans un systéme informatique. avril- septembre 2001.

[24] Serge Aumont. L'accés sécurité aux données,.

[25] Denis de REYNAL. présentation sur les vpn. février 2004.

[26] http://mrproof.blogspot.com/2010/11/les-systemes-de-detections-dintrusions.html.

[27] DABOUR Imane. Etude et mise en place d'un système de détection/prévention d'intrusion (ids/ips) réseau etude de cas snort. 2013-2014.

[28] Emira MHAROUECH. Etude et développement d'un outil d'analyse de sécurité des logs. juin 2005.

[29] timoDavid Burgermeister. Les systémes de détection d'intrusions.

[30] Ahmim Ahmed. Systéme de détection d'intrusion adaptatif et distribué.

[31] Guillaume Lehembr. Prévention d'intrusion convention sécurité management.

[32] David Burns. Ccnp security ips 642-627.

[33] Nathalie Dagorn. Détection et prévention d'intrusion : présentation et limites.

[34] http://www.leblogduhacker.fr/techniques-de-prevention-dintrusion/.

[35] https://wapiti.telecom-lille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesrio200
marcant/syst.html.

[36] KAANICHE MED RIDHA. Ids/ips, securiday access control.