République Algérienne Démocratique Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université d'Ibn Khaldoun – Tiaret

Faculté des Mathématiques et de l'Informatique

Département Informatique

Thème

Mise en place de Snort sur un réseau local

Pour L'obtention du diplôme de Master II

Spécialité : Réseau et Telecom

Rédigé par :

REZIG Sabrine

KHELLADI Nacera

Dirigé par : Mr. BAKAR Khaled

Année universitaire: 2015-2016

Dédicace

C'EST AVEC PROFONDE GRATITUDE ET SINCERES MOTS, QUE NOUS DEDIONS CE MODESTE TRAVAIL DE FIN D'ETUDE A NOS CHERS PARENTS ; QUI ONT SACRIFIE LEUR VIE POUR NOTRE REUSSITE ET NOUS ONT ECLAIRE LE CHEMIN PAR LEURS CONSEILS JUDICIEUX.

NOUS ESPERONS QU'UN JOUR, NOUS POURRONS LEURS RENDRE UN PEU DE CE QU'ILS ONT FAIT POUR NOUS, QUE DIEU LEUR PRETE BONHEUR ET LONGUE VIE.

NOUS DEDIONS AUSSI CE TRAVAIL A NOS FRERES ET SŒURS, NOS FAMILLES, NOS AMIS, TOUS NOS PROFESSEURS QUI NOUS ONT ENSEIGNE ET A TOUS CEUX QUI NOUS SONT CHERS.

Remerciement

Nous remercions en premier lieu notre dieu qui nous a éclairé le chemin du savoir et qui nous a donné la volonté et la patience d'achever ce travail de mémoire, notre grand salut sur le premier éducateur notre prophète Mohamed (satisfaction et salut de dieu soit sur lui)

Nous adressons nos vifs remerciements et nos sincères gratitudes à tous ceux qui nous ont aidés de près ou de loin à élaborer ce travail.

Nous remercions en particulier notre encadreur

Monsieur BAKAR Khaled qui nous a fait l'honneur d'avoir la charge d'encadrer notre travail de mémoire avec grande patience, pour la confiance qu'il a eu en notre projet et surtout pour ses orientations, ainsi que son aide précieuse et ses conseils pour réaliser ce mémoire.

Ainsi que tous nos professeurs qui nous ont enseigné durant nos études à la faculté

I b n K h a l d o u n

Nous tenons à remercier tous nos collègues d'étude, particulièrement notre promotion.

A la fin nos profonds remerciements pour les membres de jury qui ont accepté d'évaluer ce Travail.

RESUME :

Notre projet d'étude immerge dans le domaine de la sécurité informatique. Aujourd'hui l'information est la sève de l'entreprise et de toute organisation, sa protection contre toute menace est par ailleurs plus que nécessaire, d'où l'intérêt de notre travail qui, en partant de quelques connaissances de base sur la sécurité informatique et la détection d'intrusions, consiste à mettre en place un système de détection d'intrusions (le SNORT).

LISTE DES FIGURES :

SOMMAIRE

CHAPITRE II

SYSTEMES DE DETECTION D'INSTRUCTION.

CHAPITRE III

INSTALLATION ET CONFIGURATION DE «SNORT »

INTRODUCTION GENERALE

INTRODUCTION GENERALE :

La fulgurante de l'Internet et l'ouverture des systèmes ont fait que les attaques dans les réseaux informatiques soient de plus en plus nombreuses. Les vulnérabilités en matière de sécurité s'intensifient, d'une part au niveau de la conception des protocoles de communication ainsi qu'au niveau de leur implantation et d'autre part, les connaissances, les outils et les scripts pour lancer les attaques sont facilement disponibles et exploitables. D'où la nécessité d'un système de détection d'intrusions (IDS).

Cette technologie consiste à rechercher une suite de mots ou de paramètres caractérisant une attaque dans un flux de paquets. Les systèmes de détection d'intrusion sont devenus un composant essentiel et critique dans une architecture de sécurité informatique.

Un IDS doit être conçu dans une politique globale de sécurité. L'objectif d'un IDS est de détecter toute violation liée à la politique de sécurité, il permet ainsi de signaler les attaques. Ainsi pour créer un IDS nous allons utiliser un logiciel open source nommé SNORTS.

Dans le cas du système SNORT, la reconnaissance des attaques est basée sur le concept d'analyse de chaînes de caractères présentes dans le paquet. Pour que le système puisse être capable de détecter une attaque, cette dernière doit être décrite par une signature. C'est avec cette signature qu'on pourra d'écrire la règle que l'IDS va utiliser pour la détection.

CHAPITRE I

LA SECURITE RESEAU

INTRODUCTION

Les bienfaits de l'informatique sont évidents et en train de transformer les sociétés. Les nouvelles technologies comportent leurs parts de fragilités, de faiblesse et peuvent aussi être détournés de leurs usages premiers.

Il est donc très nécessaire et très important de nos jours de mettre au premier plan la sécurité de tout système informatique pour faire face aux attaque qui pèsent sur les données à cause de la fragilité des supports, des technologies, et de l'automatisation des traitements.

I.1. DEFINITIONS :

1- La sécurité Informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu Il n'est pas aussi facile de définir la sécurité Informatique de façon exhaustive vu la très grande diversité des domaines de l'informatique. Néanmoins, pour nous aider à mieux cerner la portée du sujet, voyons cette autre définition qui parait plus cadrée [1].

2- la sécurité informatique peut être définie comme l'ensemble des moyens matériels, logiciels, et humains mis en œuvre pour minimiser les vulnérabilités d'un système d'informatique [2].

La sécurité informatique a plusieurs objectifs:

I.2. OBJECTIF DE SECURITE :

- Confidentialité;
- Authenticité;
- Intégrité;
- Non-répudiation;
- Contrôle d'accès;
- Disponibilité.
- Confidentialité

I.2.1. La confidentialité:

Est la protection contre les attaques passives des données transmises. Plusieurs niveaux de protection de la confidentialité sont envisageables. Le service le plus général protège toutes les données transmises entre deux utilisateurs pendant une période donnée. Des formes restreintes de ce service peuvent également être définies, incluant la protection d'un message élémentaire ou même de champs spécifiques à l'intérieur d'un message. Un autre aspect de la confidentialité est la protection du flot de trafic contre l'analyse. Cela requiert qu'un attaquant ne puisse observer les sources et destinations, les fréquences, longueurs ou autres caractéristiques du trafic existant sur un équipement de communication **[3]**.

I.2.2. Authentification:

Le service d'authentification permet évidemment d'assurer l'authenticité d'une communication. Dans le cas d'un message élémentaire, tel un signal d'avertissement, d'alarme, ou un ordre de tir, la fonction du service d'authentification est d'assurer le destinataire que le message a bien pour origine la source dont il prétend être issu. Dans le cas d'une interaction suivie, telle une connexion d'un terminal à un serveur, deux aspects sont concernés. En premier lieu, lors de l'initialisation de la connexion, il assure que les deux entités sont authentiques (c'est-à-dire, que chaque entité est celle qu'elle dit être). Ensuite, le service dont assurer que la connexion n'est pas perturbée par une tierce partie qui pourrait se faire passer pour une des deux entités légitimes à des fins de transmissions ou de réceptions non autorisées**[3]**.

I.2.3. Intégrité :

À l'instar de la confidentialité, l'intégrité s'applique à un flux de messages, un seul message, ou à certains champs à l'intérieur d'un message. Là encore, la meilleure approche est une protection totale du flux. Un service d'intégrité orienté connexion, traitant un flot de messages, assure que les messages sont reçus aussitôt qu'envoyés, sans duplication, insertion, modification, réorganisation ou répétition. La destruction de données est également traitée par ce service. Ainsi, un service d'intégrité orienté connexion concerne à la fois la modification de flux de messages et le refus de service. D'un autre côté, un service d'intégrité

non orienté connexion, traitant des messages individuels sans regard sur un contexte plus large, fournit généralement une protection contre la seule modification de message **[3]**.

I.2.4. Non-répudiation:

La non-répudiation empêche tant l'expéditeur que le receveur de nier avoir transmis ou reçu un message. Ainsi, lorsqu'un message est envoyé, le receveur peut prouver que le message a bien été envoyé par l'expéditeur prétendu. De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le message a bien été reçu par le receveur prétendu **[3].**

I.2.5. Contrôle d'accès:

Dans le contexte de la sécurité des réseaux, le contrôle d'accès est la faculté de limiter et de contrôler l'accès à des systèmes et des applications via des maillons de communications. Pour accomplir ce contrôle, chaque entité essayant d'obtenir un accès doit d'abord être authentifiée, ou s'authentifier, de telle sorte que les droits d'accès puissent être adaptés à son cas **[3]**.

I.2.6. Disponibilité :

De nombreuses attaques peuvent résulter en une perte ou une réduction de la disponibilité d'un service ou d'un système. Certaines de ces attaques sont susceptibles d'être l'objet de contre-mesures automatiques, telle que l'authentification et le chiffrement, alors que d'autres exigent une action humaine pour prévenir ou se rétablir de la perte de disponibilité des éléments d'un système **[3]**.

I.3. ATTAQUES RESEAUX :

Les attaques portées à la sécurité d'un ordinateur ou d'un réseau sont mieux caractérisées en considérant le système en tant que fournisseur d'information. En général, il existe un flot d'information issu d'une source (un fichier ou une zone de la mémoire centrale vers une destination) à un autre fichier ou utilisateur.
Il existe quatre catégories d'attaques : interruption, interception, modification, fabrication **[4]**.

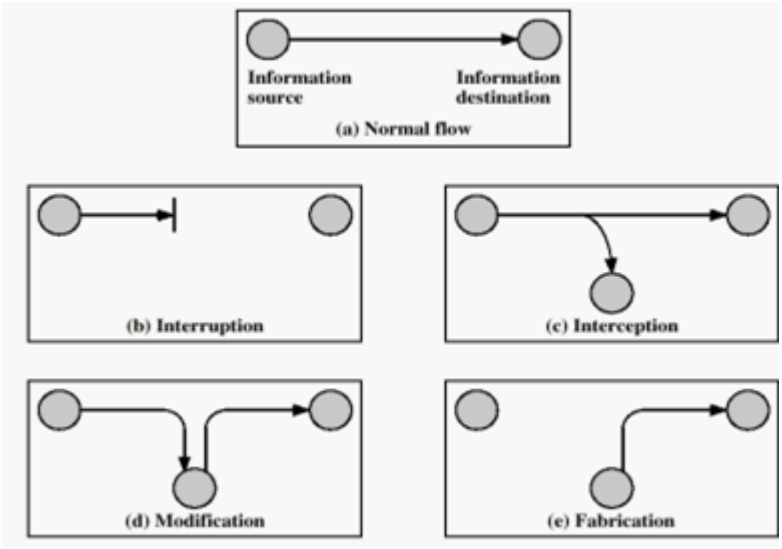


Figure 1 : Attaque réseau.

- **Interruption:**

Un atout du système est détruit ou devient indisponible ou inutilisable. 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.

- **Interception:**

Une tierce partie non autorisée obtient un accès à un atout. 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 programmes en sont des exemples.

- **Modification**:

Une tierce partie non autorisée obtient accès à un atout et le modifie de façon (presque) indétectable. 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.

- **Fabrication**:

Une tierce partie non autorisée insère des contrefaçons dans le système. 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.

I.3.1. Attaques passives et attaques actives:

Il peut être utile de distinguer deux catégories d'attaques : les attaques passives et les attaques actives **[4]**.

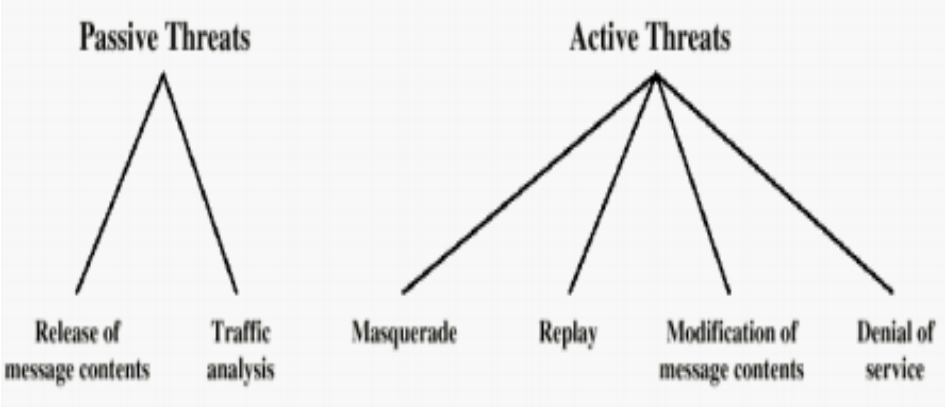


Figure 2: Deux types d'attaques (active et passive)

I.3.1.1. Attaques passives :

Écoutes indiscrètes ou surveillance de transmissions sont des attaques de nature passive. Le but de l'adversaire est d'obtenir une information qui a été transmise. Ces attaques passives sont la capture du contenu d'un message et l'analyse de trafic. La capture du contenu de messages est facilement compréhensible. Une conversation téléphonique, un courrier électronique ou un fichier transféré peuvent contenir une information sensible ou confidentielle.

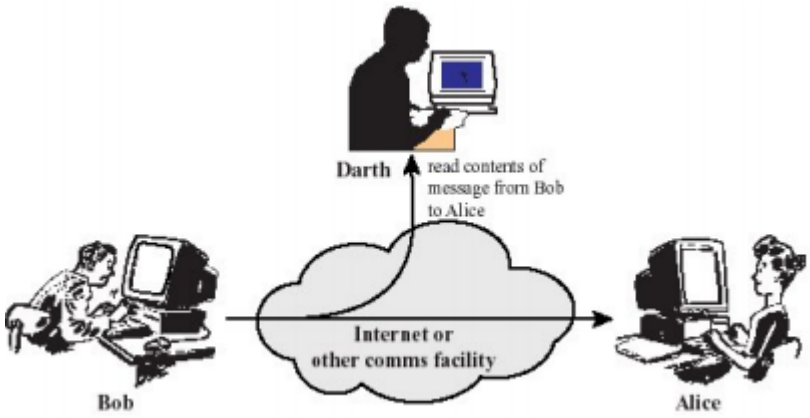


Figure 3 : Description des attaques ; capture

La seconde attaque passive, l'analyse de trafic, est plus subtile. Supposons qu'un moyen de masquer le contenu des messages ou des informations soit à disposition (par exemple, un système de chiffrement), de sorte que les adversaires, même en cas de capture, ne pourront en extraire l'information contenue. Cependant l'adversaire pourra être en mesure d'observer le motif de ces messages, déterminer l'origine et l'identité des systèmes en cours de communication, et observer la fréquence et la longueur des messages échangés. Cette information peut être utile pour deviner la nature de la communication. Les attaques passives sont très difficiles à détecter car elles ne causent aucune altération des données **[4]**.

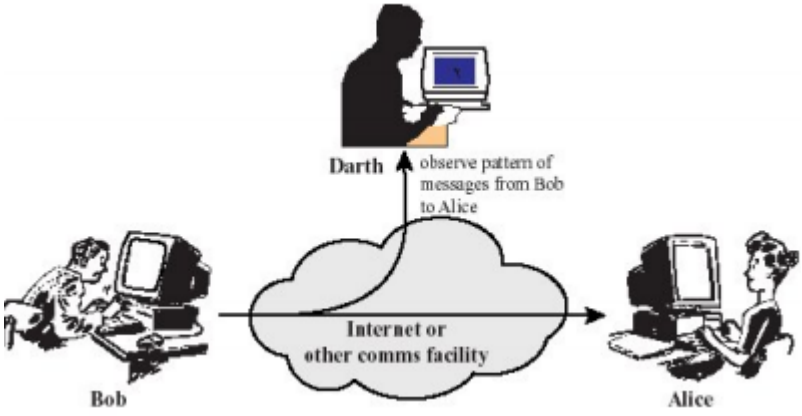


Figure 4 : Description des attaques ; analyse de trafique

I.3.1.2. Attaques actives :

La seconde catégorie d'attaques est l'attaque active. Ces attaques impliquent certaines modifications du flot de données ou la création d'un flot frauduleux ; elles peuvent être subdivisées en quatre catégories : mascarade, rejeu, modification de messages et déni de service. Une mascarade a lieu lorsqu'une entité prétend être une autre entité. Une attaque de ce type inclut habituellement une des autres formes d'attaque active. Par exemple, des séquences d'authentification peuvent être capturées et rejouées, permettant ainsi à une entité autorisée munie de peu de privilèges d'en obtenir d'autres en usurpant une identité possédant ces privilèges. Le rejeu implique la capture passive de données et leur retransmission ultérieure en vue de produire un effet non autorisé **[4]**.

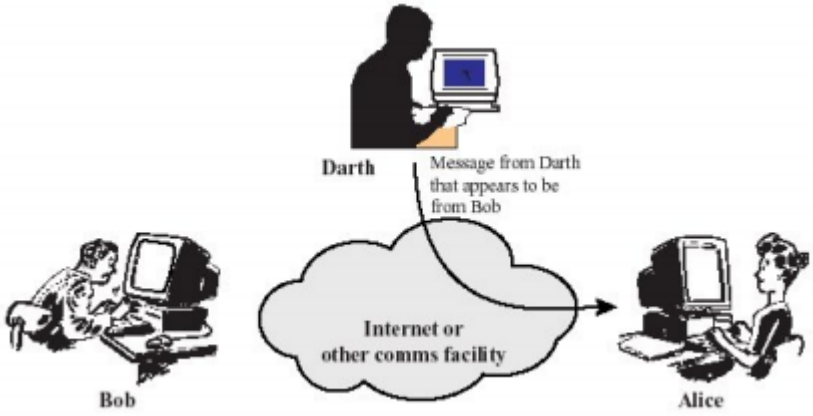


Figure 5 : Description des attaques ; mascarade

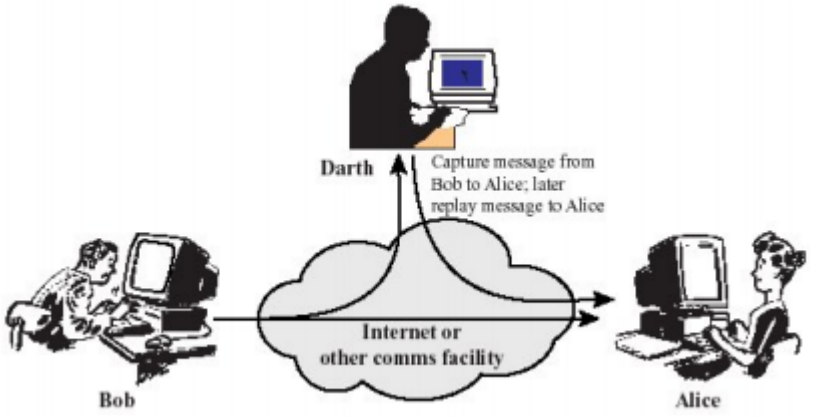


Figure 6 : Description des attaques ; rejeu

La modification de messages signifie que certaines portions d'un message légitime sont altérés ou que les messages sont retardés ou réorganisés. Par exemple, le message " autoriser X à lire le fichier confidentiel comptes " est modifié en " autoriser Y à

lire le fichier confidentiel comptes ". Le déni de service empêche l'utilisation normale ou la gestion de fonctionnalités de communication. Cette attaque peut avoir une cible spécifique ; par exemple, une entité peut supprimer tous les messages dirigés vers une destination particulière. Une autre forme de refus de service est la perturbation d'un réseau dans son intégralité, soit en mettant hors service le réseau, soit en le surchargeant de messages afin de dégrader ses performances.

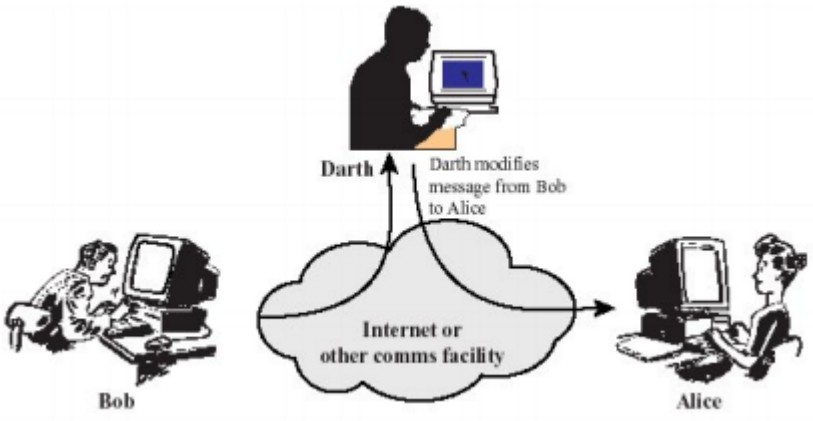


Figure 7 : Description des attaques ; modification

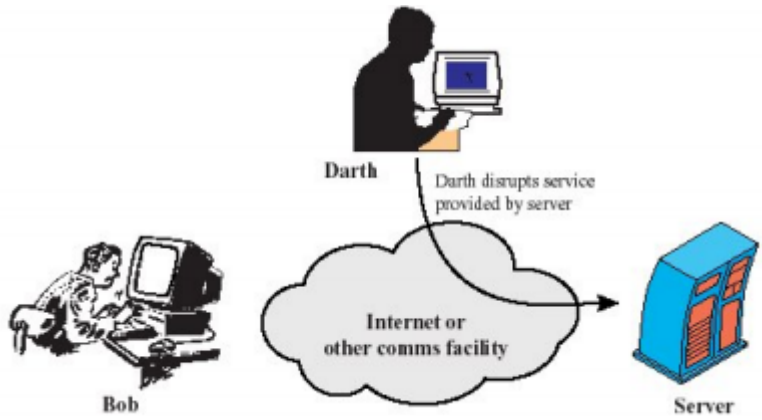


Figure 8 : Description des attaques ; déni de service

I.4. MECANISMES DE SECURITE :

On a imaginé plusieurs mécanismes pour mettre en œuvre et offrir les services de sécurité énumérés précédemment. Il s'agit principalement du chiffrement qui intervient dans presque tous les mécanismes de la signature numérique, des techniques d'utilisation d'identificateur et de mots de passe, de bourrage et de notarisation **[3]**.

I.4.1. Chiffrement:

Le chiffrement transforme tout ou une partie d'un texte dit clair en cryptogramme, message chiffré ou protégé. Si une communication utilise des dispositifs de chiffrement, les données sont transmises sous une forme « brouillée » de manière qu'elles ne puissent être comprises par un tiers **[3]** .

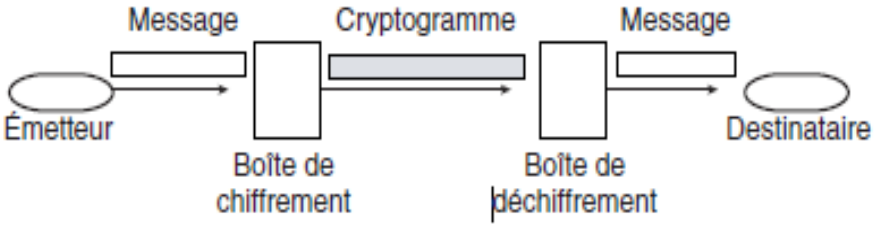


Figure 9 : Message en clair au cryptogramme.

- **Cryptage symétrique :**

Autrement appelée cryptage à clé privée, ce type se base sur l'utilisation d'une clé pour crypter et décrypter les messages. La sécurité de cette solution repose sur le fait que la clé est connue uniquement par l'émetteur et le récepteur du message.

Les algorithmes les plus courants du type symétrique sont DES (Data Encryptions Standard) et ses variantes, RC4, 5 et 6, IDEA (International Data Encryption Algorithme) et AES (Advanced Encryption Standard) **[3]** .

- **Cryptage asymétrique** :

Contrairement au symétrique, ce type se base sur l'utilisation des 2 clés : publique (pour crypter, elle est accessible publiquement) et privée (pour décrypter le message, elle est gardée secrète).
Les algorithmes les plus connus du type asymétrique sont RSA (Rivest Shamir Adleman) et ECC (Elliptic Curve Cryptosystem). Ils utilisent des éléments de mathématiques de très haut niveau.

I.4.2. Signature numérique :

La signature numérique consiste à utiliser un chiffrement particulier appelé chiffrement irréversible. Celui-ci transforme un message (a priori long) en un bloc de données (de petite taille) tel qu'il est impossible de reconstruire le message à partir du bloc. Les algorithmes utilisés sont appelés fonction de hachage ou fonction de condensation. Le bloc est appelé condensé ou signature.

Les algorithmes les plus connus du type irréversible sont MD5 (Message Digest5) et SHA1 (Secure Hash Algorithm1) **[3]**.

I.4.3. Mots de passe :

Lorsque les entités homologues et les moyens de communication sont sûrs, l'identification des entités homologues peut se faire par un identificateur d'utilisateur (login) et un mot de passe. La sécurité ne peut pas se fonder sur l'identificateur seul. Le choix du mot de passe est essentiel. Il doit avoir au moins huit caractères combinant majuscules, minuscules, chiffres, caractères spéciaux. Il doit être robuste. Il ne doit jamais être communiqué à autrui **[3]**.

I.4.4. Liste de contrôle d'accès:

Le mécanisme des listes de contrôle d'accès (ACL, Access Control List) utilise l'identité authentifiée des entités et des informations fiables pour déterminer leurs droits d'accès au réseau ou aux ressources sur le réseau. De plus, il est susceptible d'enregistrer sous forme de trace d'audit et de répertorier les tentatives d'accès non autorisées.

Le mécanisme de contrôle d'accès peut avoir lieu aux deux extrémités de la communication (équipement d'accès et ressource du réseau) **[3]**.

I.4.5. Le pare-feu (*firewall)* :

Est un système aux fonctions de filtrage évoluées. Indépendamment des fonctions de routage et de translation d'adresses, chaque paquet reçu est examiné, une décision de rejet ou d'acceptation est prise en fonction de nombreux critères :

- l'adresse destination,
- l'adresse source,
- le protocole transporté (ICMP, UDP…),
- le port destination,
- le port source,
- la valeur de certains flags (ACK, SYN…)…

La décision est prise pour chaque datagramme, il n'y a pas de notion de contexte. Il existe deux types de pare-feu :

Le pare-feu à séparation des réseaux segmente le réseau en deux tronçons : le réseau interne et le réseau externe. Il contrôle le trafic et peut réaliser une translation d'adresses (NAT) **[3]**.

Figure 10 : Pare-feu à séparation de réseau

Le pare-feu au fil de l'eau n'effectue aucune séparation physique des réseaux. Cependant, comme le pare-feu à séparation des réseaux, il réalise l'isolation des trafics. Les postes ne communiquent qu'avec le pare-feu (passerelle par défaut) et le routeur ne voit que le pare-feu.

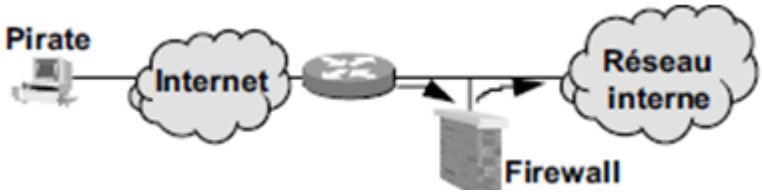


Figure 11 : Pare-feu au fil de l'eau

I.5. LA ZONE DEMILITARISEE (DMZ):

La mise à disposition d'un serveur public (service Web, messagerie...) est généralement réalisée par la constitution d'une zone de sécurité dite **DMZ (*DeMilitarized Zone*).**

Différentes zones de sécurité peuvent être constituées, chacune accessible selon des critères spécifiques (filtres).

La zone démilitarisée accueillera les différents serveurs accessibles à la fois par le personnel de l'entreprise et par le monde extérieur.
Pour différencier les services offerts et les règles de filtrage, il est possible de définir plusieurs DMZ, dans ce cas généralement l'une est accessible à tous (DMZ publique), et l'autre aux personnels de l'entreprise (DMZ privée).

La définition des filtres est similaire à celle réalisée pour les routeurs, seule, la portée de l'analyse est plus profonde. Tout datagramme non autorisé est rejeté. En cas de tentative de violation d'une règle, les pare-feu émettent des alertes. Un fichier (logs) conserve une trace de tous les événements [3].

I.6. IDS :

Un système de détection d'intrusion (ou IDS : Intrusion Detection System)est un mécanisme destiné à repérer des activités anormalesou suspectes sur la cible analysée (un réseau ou unhôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.
Il faut distinguer deux aspects dans le fonctionnement d'un IDS : le mode de détection utilisé et la réponse apportée par l'IDS lors de la détection d'une intrusion.

CONCLUSION :

Dans ce chapitre nous avons dégagé les principes fondamentaux, les domaines d'application de la sécurité Informatique ainsi que les dis positives de protection notamment les firewalls et les Systèmes de Détection des Intrusions, ces derniers nous les aborderons dans le chapitre qui suit.

CHAPITRE II

LES SYSTEME DE DETECTION D'INTRUSION.

INTRODUCTION

Un système de détection d'intrusion a été introduit comme ligne de défense afin de renforcer la sécurité des systèmes informatique, ce concept a été introduit en 1980 par James. Anderson dans le fameux rapport « COMPUTER SECURITY THREAT MONITORING AND SURVEILLANCE ». Mais le sujet n'a pas eu beaucoup de succès. Il a fallu attendre la Publication d'un modèle de détection d'intrusions par Dorothy E. Denning en 1987 pour marquer réellement le départ du domaine**.** En 1988, il existait déjà quelques prototypes : *Haystack*, *NIDX* .... La recherche dans le domaine s'est ensuite développée, le nombre de prototypes s'est énormément accru.

Un nouveau modèle de gestion de la sécurité des systèmes a émergé.

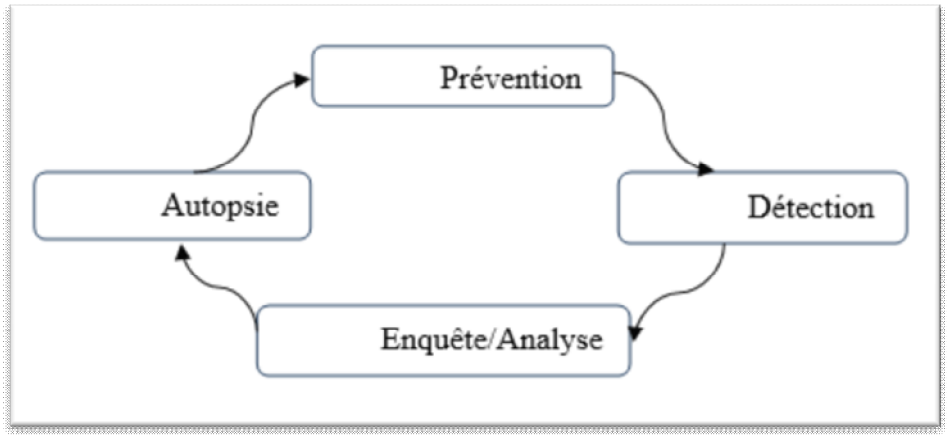


Figure 12 : Un modèle de gestion de la sécurité d'un système informatique

Dans cette approche plus réaliste, la prévention n'est qu'une des quatre parties de la gestion de la sécurité. La partie détection est à la recherche de l'exploitation de nouvelles trouées. La partie enquête/analyse essaye de déterminer ce qui est arrivé, en s'appuyant sur les informations fournies par la partie détection. La partie autopsie consiste à mener un examen minutieux et à chercher comment empêcher des intrusions similaires dans le futur [5].

Dans ce chapitre, nous étudierons les systèmes de détection d'intrusions de façon générale.

II.1. DEFINITION :

II.1.1. L'intrusion :

Avant d'entamer les systèmes de détection d'intrusion, il faut éclaircir la notion d'intrusion qu'on prise la défini par toute séquence active d'évènement en relation qui texte de causer du tort comme interrompe le fonctionnement d'un système, usurper l'identité d'un utilisateur ou modifier les informations, cette définition comprend toutes les tentatives qui réussissent ou celles qui échouent **[6]**.

II.1.2. La détection d'intrusion :

La détection d'intrusions est définie comme étant l'ensemble des pratiques et des mécanismes utilisés qui permettent de détecter des problèmes pouvant conduire à des violations de la politique de sécurité dans un système informatique.

La détection peut être effectuée de façon non-systématique. Dans ce cas l'administrateur du système procède à un examen (analyse) du système, ce qui est la tâche fastidieuse et ennuyante à l'administrateur qui peut ne pas être présent lors d'une tentative d'intrusion.

Donc un système qui détecte, surveille l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion et si possible de réagir à cette tentative de façon automatique est appelé « Système de Détection d'Intrusion » (SDI), en anglais « Intrusion Detection System » (IDS) [4].

II.2. LE MODELE DE BASE D'UN SYSTEME DE DETECTION D'INTRUSION :

Il existe plusieurs outils de détection d'intrusion, chaque outils utilise propre technique de détection et ses propres sources de données, il est très intéressant de se disposer d'un modèle général qui englobe et standardise la structure d'un système de détection d'intrusion. Ce sujet a été le centre d'intérêt du groupe IDWG (Intrusion Detection Working Group) de l'IETF. IDWG a proposé le modèle général des systèmes de détection d'intrusion qui se compose de senseur (collecteur), analyseur, manager (administrateur). La figure suivante montre en détailles composants d'IDS

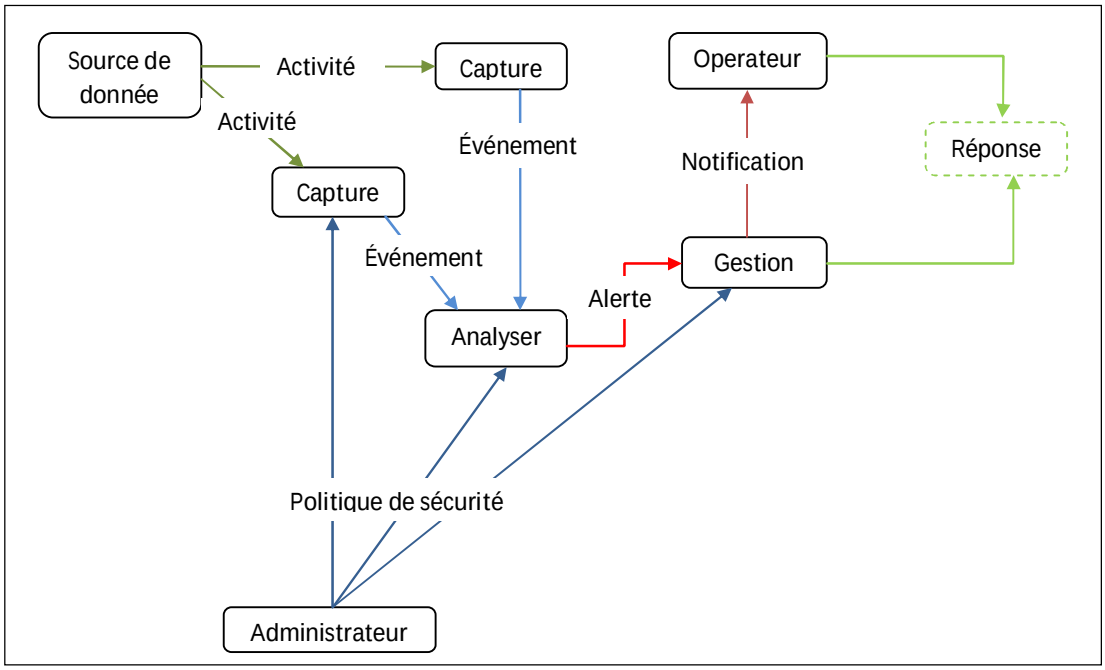


Figure 13 : Modèle générique de la détection d'intrusions proposé par l'IDWG **[10]**.

- **L'activité :**

C'est les éléments de la source ou les occurrences au sein de la source de données qui sont identifiés par le capteur ou l'analyseur comme étant à intérêt pour l'opérateur.

- **L'administrateur :**

C'est le responsable de l'établissement de la politique de sécurité de l'organisation, donc celui qui déploie et configure l'IDS. Cette personne peut ou peut ne pas être l'opérateur de l'IDS.

- **L'alerte :**

C'est un message qui passe de l'analyseur au gestionnaire pour lui informer qu'un événement d'intérêt a été détecté. une alerte contient généralement des informations sur l'activité inhabituelle qui été détecté ainsi que ces détails.

- **L'analyseur :**

C'est le composants clé, il analyse les données recueillies par le capteur pour signaler les activités non autorisées ou indésirables ou les événements qui pourraient avoir un intérêt pour l'administrateur de sécurité dans la plupart des IDS existants, le capteur et l'analyseur font partie d'un même composant.

- **La source de données :**

C'est les informations brutes utilisées par le système de détection d'intrusion pour détecter les activités non autorisées ou non désirées.

- **L'événement :**

C'est toute occurrence détectée dans la source des données par un capteur et qui peut donner lieu à un alerte, par exemple une attaque.

- **Le gestionnaire :**

C'est l'élément clé ou le processus à partir de laquelle l'opérateur gère les différents composants du système les fonctions du gestionnaire comprennent la configuration de l'analyseur la gestion de la notification d'événements la consolidation des données et la gestion des rapports.

- **La notification :**

C'est la méthode avec laquelle le gestionnaire de l'IDS informe l'opérateur de la survenance d'une alerte dans des nombreux IDS, la notification se fait via l'affichage d'une icône colorée sur l'écran du gestionnaire de l'IDS la transmission d'un e-mail ou un message ou la transmission d'un simple Network Management Protocol (SNMP)……..etc.

- **L'opérateur :**

C'est l'utilisateur principal du gestionnaire de l'IDS. L'opérateur surveille souvent la sortie du système de détection d'intrusion et déclenche ou recommande d'autres actions.

- **La réponse :**

C'est les mesures prises comme réponse à un événement, les réponses peuvent être effectuées automatiquement par une entité dans l'architecture de l'IDS ou peuvent être initiées par un humain l'envoi d'une notification à l'opérateur est une réponse très commune. Autres réponses incluent (mais ne sont pas limités) la journalisation de l'activité, l'enregistrement des données brutes (à partir de la source de données) qui ont caractérisé l'événement, l'arrêt du réseau ou de l'utilisateur ou la session de l'application, la modification des contrôles d'accès réseau ou système.

- **La capture :**

C'est le composant qui collecte des données à partir de la source de données. La fréquence de la collecte des données varie selon la configuration de l'IDS .le capteur est mis en place pour transférer des événements à l'analyseur.

II.3. EFFICACITE DES SYSTEMES DE DETECTION D'INTRUSIONS :

D'après Debar nous conclusion que il existe cinq critères pour évaluer l'efficacité des systèmes de détection d'intrusion :

- **La précision :**

On parle de la précision quand le système de détection d'intrusion détecte les attaques sans faire des fausses alarmes.

- **La performance de traitement :**

La performance de traitement d'un système de détection d'intrusion est mesurée par la vitesse avec laquelle les évènements d'audit sont traités.
Si la performance est faible alors la détection en temps réel est impossible

- **Complétude :**

Est la capacité d'un IDS de détection toutes les attaques .mais ce critères est le plus difficile par rapport aux autres critères, parce qu'il est impossible d'avoir une connaissance globale sur les attaques. Ce critère correspond au faux négatif.

- **La tolérance aux fautes :**

Le système de détection d'intrusion doit lui-même résisté aux attaques. Particulièrement au déni de service, Donc IDS devrait être conçu avec cette objectif.
Ceci est important parce que plusieurs systèmes de détection s'exécutent sur des matériels ou logiciels. Connus comme vulnérables aux attaques.

- **La rapidité :**

Système de détection d'intrusion doit exécuter et propager son analyse le plus rapidement possible pour permettre à l'agent, de sécurité de réagir afin de minimiser les dégâts possibles et aussi pour empêcher l'attaquant d'altérer la source de vérification ou interrompre le fonctionnement du système de détection d'intrusion. Parce qu'il ne s'agit pas seulement de temps de traitement des évènements, mais aussi de temps nécessaire pour la propagation et la réaction à cet évènement.

II.4. Classification Des Systèmes De Détection D'intrusions :

Il existe de nombreux systèmes de détection d'intrusion les IDS peuvent être classifiés d'après plusieurs critères. Quatre critères de classification des systèmes de détection

d'intrusion ont été introduits par Hervé Debar et Marc Dacier et Andreas Wespi. Ces critères sont **[9]** :

- La méthode d'analyse.
- Le comportement de la détection.
- Emplacement de la source d'audit.
- La fréquence d'utilisation.

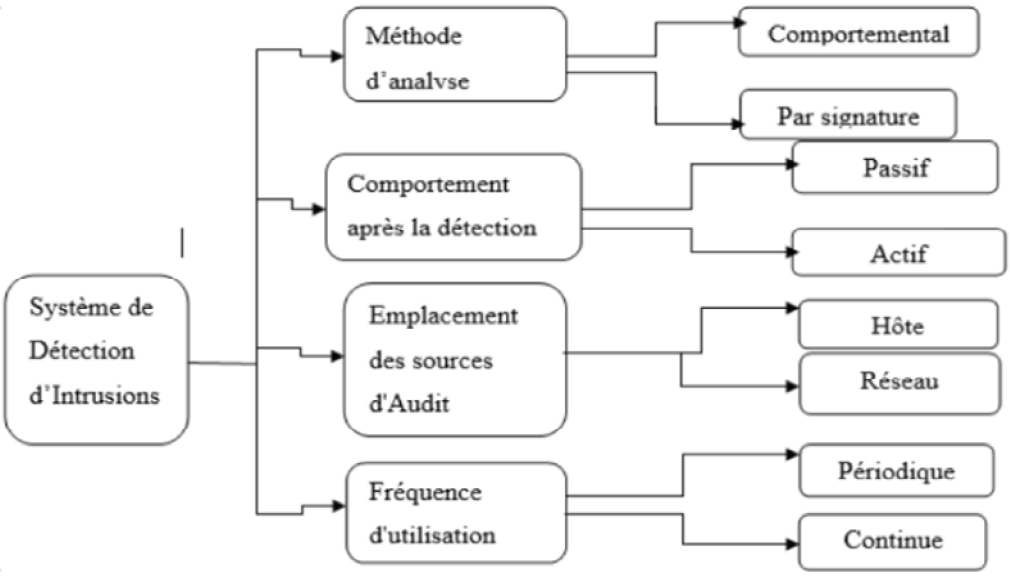


Figure 14 : Taxonomie des systèmes de détection d'intrusion.

II.4.1. La méthode d'analyse :

Une autre différenciation se fait sur la manière de détecter une attaque. Elle peut se baser sur ses signatures (aussi appelée approche par scénario) ou en se basant sur des profils normaux d'utilisation (aussi appelée approche comportementale). Dans le premier cas, on regarde la suite d'actions effectuées par une personne et on la compare à une attaque connue. Dans le deuxième cas, on regarde le comportement d'une personne et on le compare à son comportement normal.

II.4.1.1. Approche par scénario :

Elle se base sur les connaissances accumulées sur les attaques spécifiques et les vulnérabilités et cherche toute tentative de les exploiter si l'IDS détecte une tentative, une alarme est déclenchée, En d'autres termes toute action qui n'est pas explicitement reconnue

comme une attaque est considérée comme acceptable par conséquent, la précision des systèmes de détection d'intrusion basée sur l'approche par scénario est bonne. Cependant, cette précision dépend toujours de la mise à jour des connaissances sur les attaques qui doit être régulière **[9].**Elle se fait de la forme : si Evènement matche Signature alors Alerte.

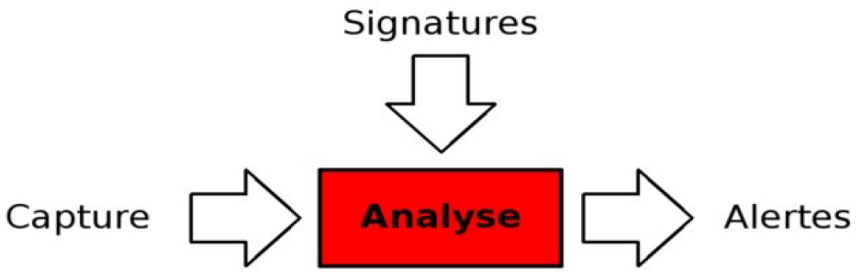


Figure 15 : Méthode de détection par signatures

Un avantage de cette approche est la normalisation possible de la description des signatures et ainsi la possibilité de diffuser et de configurer rapidement et facilement les IDS. De plus, ceci permet d'avoir un faible taux de fausses alarmes. Néanmoins, la problématique est le besoin d'une mise à jour régulière de la base de données des signatures pour détecter de nouvelles attaques. Ils sont donc faillibles aux attaques *0day* qui sont des exploitations d'une faiblesse le jour de leur publication. De plus, une même attaque peut être faite de plusieurs manières légèrement différentes. Ainsi, le *pattern matching* ne semble pas très efficace. A sa place, on peut utiliser la *machine learning* pour apprendre leurs signatures de manière générique et ainsi les repérer même si celles-ci évoluent légèrement au cours du temps.

II.4.1.2. Approche comportementale :

Le but de cette technique est la prédiction de comportement. Pour cela, cette technique utilise une base de données des comportements normaux des utilisateurs, d'un groupe d'utilisateurs, des services ou d'un système entier pour constituer un profil. Au début, le modèle du comportement normal est extrait à partir des informations de référence recueillies par divers moyens. Puis le système de détection d'intrusion compare ce modèle avec l'activité actuelle. Si une déviation est détectée, une alerte sera déclenchée, on peut dire que cette approche considère tout comportement qui n'est pas précédemment enregistré

comme intrusion. Par conséquent cette approche peut être complète, mais la précision reste son plus grand souci.

Le point fort de cette approche est qu'elle arrive à détecter les nouvelles formes d'attaques qui exploitent les nouvelles formes de vulnérabilités non connues auparavant, pour agrandir la base de données des attaques connues de la méthode par scénario. Cette approche est moins dépendante du système d'exploitent par rapport à l'approche par scénario pour augmenter l'efficacité. Elle peut aussi détecter les attaques d'abus prérogative de qui n'exploite aucune vulnérabilité **[14]**.

II.4.2. Comportement après la détection d'une intrusion (la réponse) :

Le comportement d'un IDS après la détection d'une intrusion est l'ensemble des actions prises par le système lorsqu'il détecte une attaque. Ces actions peuvent être passives ou actives selon les capacités de l'IDS.

II.4.2.1. Réponse passive :

Après la détection d'une intrusion, certains IDS mènent certaines actions passives vis-à-vis de l'attaquant et du système attaqué. Ces actions peuvent êtres :

- **Alarme :**

Les alarmes sont produites par les IDS pour informer les administrateurs réseau lorsque des attaques sont détectées. La forme la plus commune est d'afficher un message d'alerte contenant des informations détaillées de l'intrusion détectée sur la console du responsable de la sécurité. Une autre option très utile consiste à envoyer ces alertes au téléphone du responsable. Il peut aussi envoyer des e-mails, ou générer des alertes sonores**.**

- **SNMP Trap :**

Certains IDS sont conçus pour produire des alertes et envoyer les rapports au système de gestion de réseau (*network management system*). Ils utilisent le protocole SNMP *(Sample Network Management Protocol*), qui est un protocole dédié à la gestion du réseau**.**

- **L'archivage :**

Le système enregistre les informations concernant l'attaque dans un fichier log. L'archivage (*logging*) permet aux analystes de faire des analyses approfondies, et de faire des corrélations avec l'historique dont ils disposent concernant les évènements qui se sont produits auparavant.

II.4.2.2. Réponse active :

D'autres systèmes de détection d'intrusions peuvent, en plus de la notification à l'opérateur, prendre automatiquement des mesures pour stopper l'attaque en cours. Il y a trois catégories de réponses actives :

- **Rassembler des informations additionnelles :**

Il est très important de rassembler des informations additionnelles sur une attaque afin de l'identifier avec précision. Chacun de nous a fait probablement l'équivalant de cela une fois réveillé par un bruit étrange pendant la nuit. La première chose à faire dans une telle situation est d'écouter d'avantage, recherchant l'information additionnelle qui nous permet de décider si on doit agir ou non.

Dans le cas des IDSs, cela se traduira par l'exigence d'analyse des informations additionnelles, faire des corrélations, ou bien communiquer avec d'autres types d'IDSs installés sur le réseau .

- **Changer l'environnement :**

Une autre réponse active doit stopper une attaque en progression et puis bloquer l'accès de l'attaquant. Typiquement, les IDSs n'ont pas les capacités de bloquer l'accès d'une personne spécifique, mais ils peuvent uniquement rompre des connexions ou bloquer certains paquets spécifiques en s'appuyant sur les mécanismes des protocoles Internet. Cela est dû à la capacité du hacker expert de construire des paquets falsifiés (*forging packets*).Parmi ces actions on trouve :

- L'envoi des paquets TCP de type *Reset* ou des paquets *ICMP* au système de l'attaquant pour arrêter la connexion.
- La configuration des routeurs et des *Firewalls*pour bloquer les paquets provenant de l'adresse IP de l'attaquant.
- La configuration des routeurs et des *Firewalls*pour bloquer les paquets selon le numéro de port, le protocole, ou le service utilisé par l'attaquant.

➢ **Agir contre l'intrus** :

La première option dans la réponse active est d'agir contre l'intrus. En effet, la forme la plus agressive de cette réponse implique le lancement des contre-attaques ou d'essayer d'obtenir activement les informations sur l'hôte ou l'emplacement de l'attaquant.

Toutefois, il apparait que ce type de fonctionnalité automatique, est potentiellement dangereux car, il peut mener à des dénis de service provoqués par l'IDS. Un attaquant déterminé peut, par exemple, tromper l'IDS en usurpant des adresses du réseau local qui seront alors considérées comme la source de l'attaque par l'IDS. Il est préférable de proposer une réaction facultative à un opérateur humain (qui prend la décision finale).

II.5. Emplacement des sources d'audit :

L'emplacement des sources d'audits est le critère généralement utilisé pour classifier les IDS, ainsi, Il existe deux grandes familles distinctes d'IDS :

▪ **Les N-IDS :** (*Network Based Intrusion Detection System*), ils assurent la sécurité au niveaudu réseau.

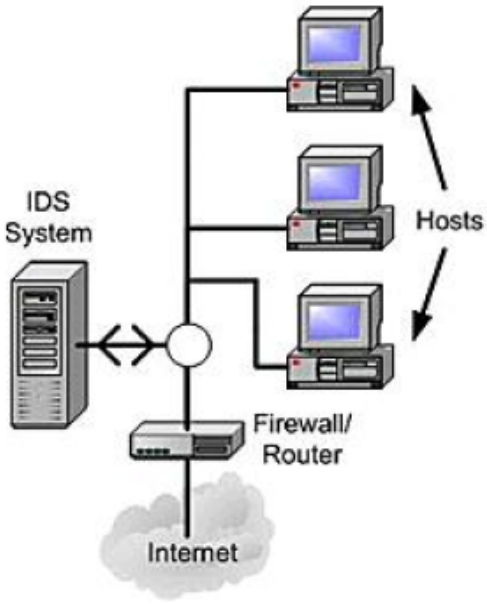


Figure 16 : Architecture d'un NIDS

- **Les H-IDS** (*Host Based Intrusion Detection System*), ils assurent la sécurité au niveau des hôtes (machines).

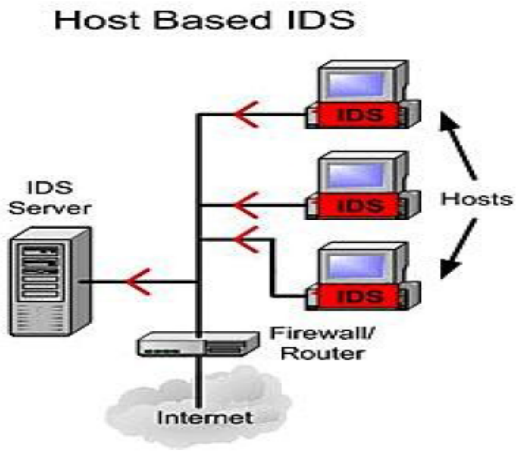


Figure 17 : Architecture d'un HIDS

II.5.1. HIDS :

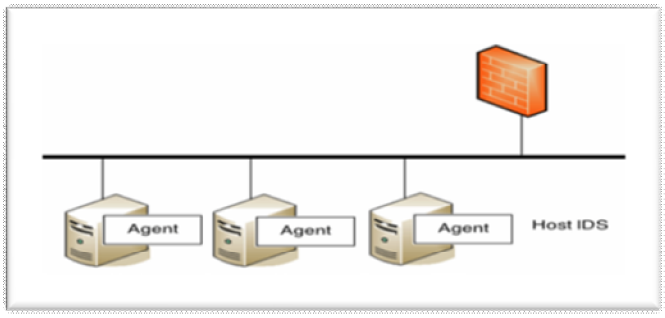


Figure 18 : HIDS**[12]**

Un H-IDS réside sur un hôte (machine) particulier et la gamme de ces logiciels couvre donc une grande partie des systèmes d'exploitation tels que Windows, Solaris, Linux, HP-UX, Aix, etc…Le H-IDS se comporte comme un démon ou un service standard sur un système hôte.Traditionnellement, le H-IDS analyse des informations particulières dans les journaux de logs (syslogs, messages, lastlog, wtmp…) et aussi capture les paquets réseaux entrant/sortant del'hôte pour y déceler des signaux d'intrusions (Déni de Services, Backdoors, chevaux de Troie,tentatives d'accès non autorisés, exécution de codes malicieux, attaques par débordement de buffeurs…)**[14]**.

II.5.2. NIDS :

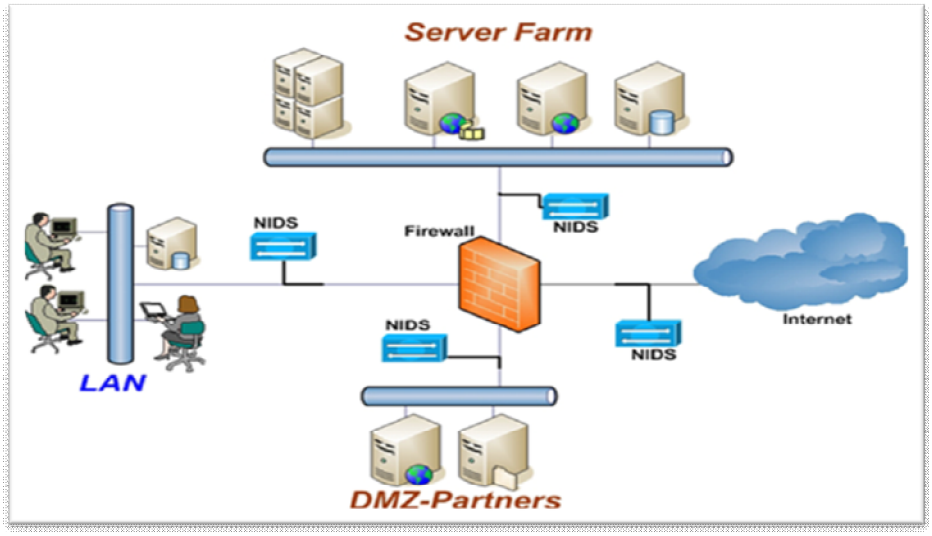


Figure 19: Network-based Intrusion Detection System **[12]**

Le IDS Réseau est un logiciel qui, installé sur un matériel généralement dédié, place la carte réseau du système hôte en mode promiscuité ; NIDS est un système de détection des intrusions travaille sur les trames réseau aux niveaux (couches réseau, transport, application), il est capable de détecter des paquets malveillants conçus pour outrepasser un pare-feu aux règles de filtrage trop laxistes, et de chercher des signes d'attaque à différents endroits sur le réseau [14].

II.5.3. IDS Hybrides [13]

Les IDS hybrides rassemblent les caractéristiques des NIDS et HIDS. Ils permettent, en un seul outil, 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 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 (par exemple IDMEF[1]).

Cela permet de communiquer et d'extraire des alertes plus pertinentes.

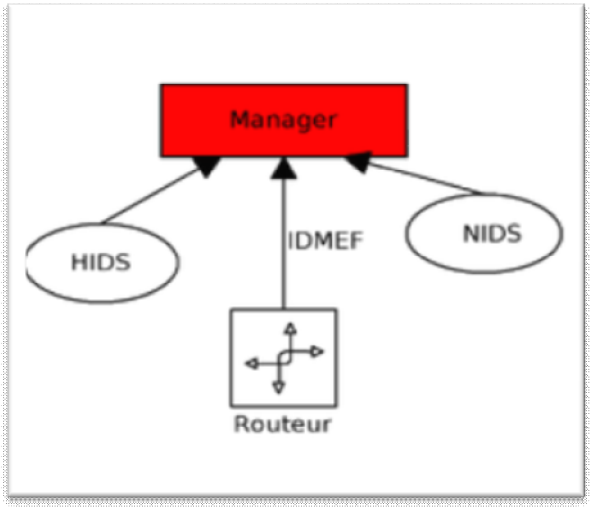


Figure 20 : Principe de l'IDS hybride

- Les avantages des IDS hybrides sont multiples :
  - 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

[1] Est une norme qui spécifie le format des messages d'alertes échange entre IDS.

II.5.4. Fréquence d'utilisation (la synchronisation) :

La synchronisation se rapporte au temps écoulé entre les évènements qui sont surveillés et l'analyse de ces évènements. Elle est réalisée en temps réel ou différé. **[11]**

II.5.4.1. En temps différé (périodique) :

Ce type de système de détection d'intrusions, analyse périodiquement les différentes sources de données, à la recherche d'une éventuelle intrusion ou une anomalie passée. Cette approche est employée surtout, dans les Host-IDS, qui scrutent les logs du système d'exploitation dans des intervalles de temps réguliers. **[11]**

II.5.4.2. En temps réel (continue) :

Les IDS en temps réel, traitent des flux continus d'informations à partir des différentes sources d'informations. C'est la technique prédominante de synchronisation pour les IDS réseau, qui recueillent l'information du trafic réseau. Par conséquent Les IDS peuvent prendre des actions pour affecter la progression d'une attaque détectée. **[11]**

Conclusion :

Dans ce chapitre, nous avons fait une étude générale des systèmes de détection d'intrusions en procédant notamment à une étude sur les critères d'évaluation de l'efficacité des IDS et une étude sur la classification des IDS en se basant sur un certain nombre de critère.

Dans le chapitre qui suit, nous effectuerons une étude de cas de système de détection d'intrusion libre sous licence GNU GPL « *le Snort* ».

CHAPITRE III

INSTALLATION ET CONFIGURATION DE «SNORT».

INTRODUCTION

Devant la complexité croissante des réseaux qui est de plus en plus importante et étendu et suite aux attaques de plus en plus nombreuses; Outre la mise en place des pare feu et de système, il est nécessaire de mettre en place un système de détection d'intrusion.
Dans ce qui suit, nous étudierons un cas de système de détection d'intrusion celui de Snort.

III.1. PRÉSENTATION :

III.1.1. Snort :

Snort est un outil de détection d'intrusion basé publié sous licence (définissant le mode d'utilisation et de distribution des logiciels libres). Initialement développé par Martin Roesh il est désormais une référence par sa forte communauté.

Snort permet d'analyser le trafic réseau en fonction d'un ensemble de règle et de signatures d'attaques contenues dans sa base de signatures pour déterminer s'il faut générer des actions (log, alerte, …) [15]

Snort peut être configuré pour fonctionner en quatre modes :

Le mode sniffer : « hors ligne » qui se contente de lire les paquets qui circulent sur le réseau et de afficher de manière continue à l'écran. Il s'agit d'écouter le réseau, en tapant une ou plusieurs lignes de commande qui indiqueront à Snort le type de résultat à afficher.

Le mode « packetlogger » : dans ce mode snort journalise le trafic réseau dans des répertoires sur le disque.

Le mode détecteur d'intrusion réseau (NIDS) : plus configurable, qui permet d'analyser le trafic sur le réseau, compare ce trafic à des règles déjà définies par l'utilisateur et établi des actions à exécuter ;

Le mode Prévention des intrusions réseau (IPS): c'est SNORT-inline. Le mode IPS n'est plus Snort à proprement parler. Il s'agit d'une autre version basée sur Snort 2.6. Cette version permet de modifier ou de rejeter des paquets [16].

Snort, comme nous venons de le dire, est un NIDS, et son emplacement physique sur le réseau à un impact considérable sur son efficacité. Il utilise pour cela des règles pour détecter les intrusions, il existe aujourd'hui environ 2000 Quant règles différentes (on 2014), s'adaptant à un cas particulier, on peut créer des règles pour observer une activité particulière sur le réseau : ping, scans, faille dans un script, tentative de prise de contrôle à distance, les alertes peuvent être enregistrées dans un fichier particulier ou directement dans le syslog ou encore dans une base de données.

III.1.2. Positionnement de snort dans le réseau :

L'emplacement physique de la sonde snort sur le réseau a un impact considérable sur son efficacité.

Dans le cas d'une architecture classique composé d'un firewall et d'une DMZ, trois positions sont généralement envisageables :

- **Avant le firewall ou le routeur filtrant :** sur cette position, l'IDS va pouvoir détecter l'ensemble des attaques frontales. Ainsi, beaucoup d'alertes seront remontées ce qui rendra les logs difficilement consultables.

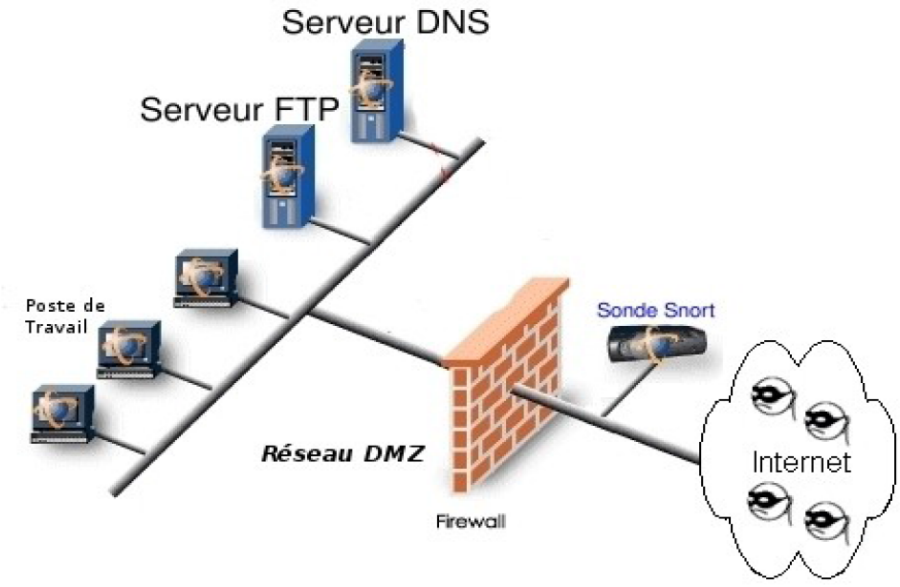


Figure 21: Positionnement du Snort avant le firewall

- **Sur la DMZ :** dans cette position, la sonde peut détecter tout le trafic filtré par le Firewall et qui a atteint la zone DMZ. Cette position de la sonde permet de surveiller les attaques dirigées vers les différents serveurs de l'entreprise accessibles de l'extérieur.

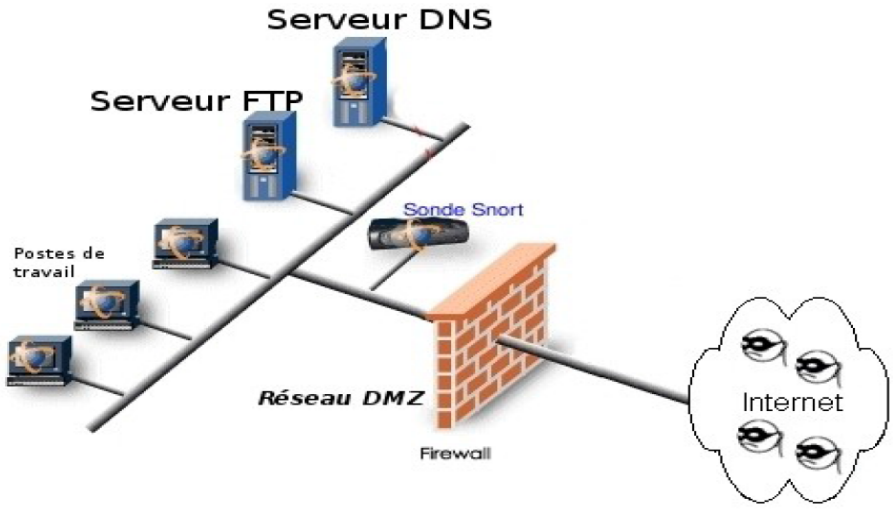


Figure 12 : Positionnement dusnort après le firewall

- **Sur le réseau interne** : le positionnement du NIDS à cet endroit nous permet d'observer les tentatives d'intrusion parvenues à l'intérieur du réseau d'entreprise ainsi que les tentatives d'attaques à partir de l'intérieur. Dans le cas d'entreprises utilisant largement l'outil informatique pour la gestion de leurs activités ou de réseaux fournissant un accès à des personnes peu soucieuses de la sécurité cette position peut revêtir un intérêt primordial. [17]

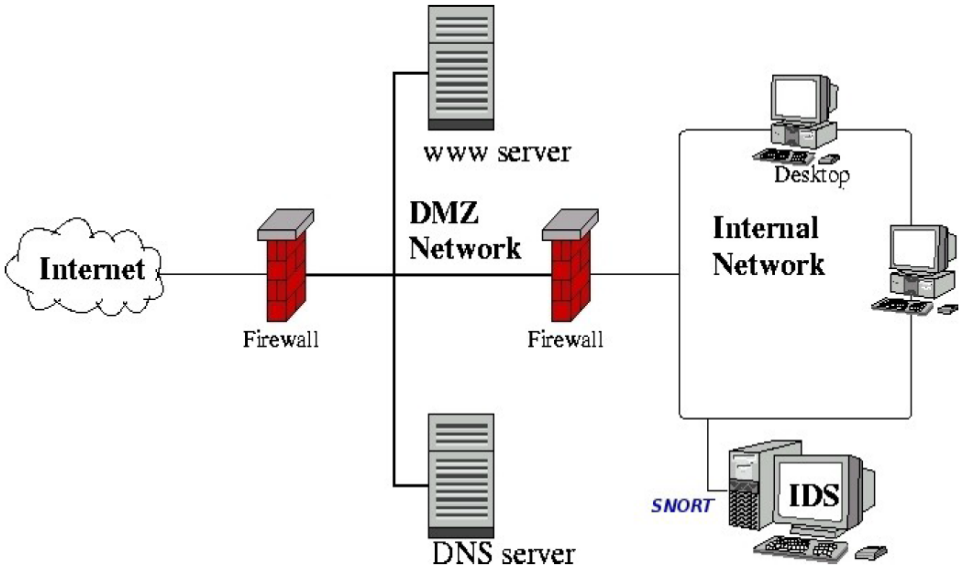


Figure 23: Positionnement du Snort sur le réseau interne

III.1.3. Architecture de snort :

L'architecture de Snort est modulaire et est composée de :

Décodeur de paquet (Packet Decoder) : il capture les paquets de données des interfaces réseaux, les prépare afin d'être prétraitées ou envoyées au moteur de détection. **[16]**

Pré processeur (Pre processor) : ce sont des composants utilisés avec SNORT afin d'améliorer les possibilités d'analyse, et de recomposition du trafic capturé. Ils reçoivent les paquets, les retraitent et les envoient au moteur de détection.

- Les préprocesseurs sont chargés et configurés avec le mot-clé preprocessor.
- Le format de la directive préprocesseur de Snort est :

preprocessor<nom> : <options>
Exemple de préprocesseur :
Le détecteur portscan permet de :
Enregistrer le début et la fin d'un scan de ports à partir d'une seule adresse IP.
Lorsqu'un fichier de log est spécifié, ce préprocesseur journalise les IP et les ports scannés ainsi que le type du scan.

Exemple :
Preprocessorportscan 192.168.1.0/24 /var/log/snort

Une série d'analyses est ensuite appliquée aux paquets. Ces analyses se composent principalement de comparaisons de différents champs des headers des protocoles (IP, ICMP, TCP et UDP) par rapport à des valeurs précises.

Après la détection d'intrusion, une série de fichiers de sortie (output plugins) permet de traiter cette intrusion de plusieurs manières : envoie vers un fichier log, envoie d'un message d'alerte vers un serveur syslog, stocker cette intrusion dans une base de données.**[16]**

Moteur de détection (DetectionEngine) : c'est le composant le plus important de SNORT. Son rôle consiste à détecter les éventuelles intrusions qui existent dans un paquet.

Pour se faire, le moteur de recherche se base sur les règles de SNORT. En effet, ce moteur consulte ces règles et les compare une à une avec le paquet de données. S'il y a conformité, le détecteur l'enregistre dans le fichier log et/ou génère une alerte. Sinon le paquet est laissé tomber.

Système d'alerte et d'enregistrement des logs (Logging and Alerting System) : il permet de générer les alertes et les messages log suivant ce que le moteur de détection a trouvé dans le paquet analysé.

Output modules (ou plugins) : permet de traiter l'intrusion générée par le système d'alertes et de notation de plusieurs manières : envoie vers un fichier log, génère un message d'alerte vers un serveur syslog, ou stocke cette intrusion dans une base de données comme MySQL ou Oracle. [16]

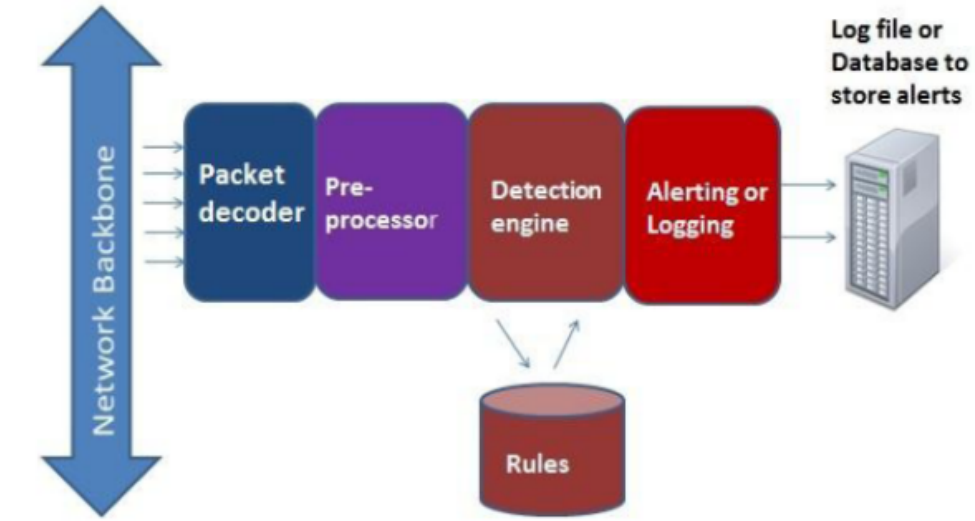


Figure 24 : Schéma de l'architecture de Snort**[16]**

III.1.4. Les règle de Snort:

Les règles de Snort sont composées de deux parties distinctes : header (options).

Header	(options)

Figure 2: Structure de base des règles de snort

Le header contient des informations qui définit la règle, et permet de spécifier le type d'alerte à générer (alerte, log et pass)et d'indiquer les champs de base nécessaire au filtrage : le protocole ainsi que les adresse IP et ports sources et destination [18].

- **Action :**

C'est le premier élément de règle, cette partie représente l'action à effectuer si la détection est réussie. Elle peut prendre les valeurs*log, pass, alert, activate et dynamic,* ou des valeurs définies par l'utilisateur [18]

- *Log :* enregistre le paquet avec le module d'archivage.
- *Pass* : ignore le paquet qui correspond à la description.
- *Alert* : plus d'archiver le paquet, génère une modification grâce au module d'alarme.
- *Activate* : alerte, puis tourné sur une autre règle dynamique.
- *Dynamic* : reste inactif jusqu'à activé par une règle d'activation, alors agir comme une règle de journal.

Exemple simple de règle qui enregistre tout le trafic àdestination de l'adresse 192.168.159.140 via le port 79 : *logtcpanyany -> 192.168.159.140 79*

- **Protocole :**

Le protocole est la deuxième partie d'une règle snort. Qui montre le type de paquets, il existe quatre protocoles: TCP, IP, UDP, et ICMP ; dans le futur il pourrait être plus comme : ARP, IGRP, GRE, OSPF, RIP, IPX etc [20]

Par exemple : considérons la règle suivante ou le protocole est ICMP

alerticmpanyany -> (msg : "Ping with TTL=100";\ ttl : 100 ;)

- **Adresse :**

Il y’a deux parties d’adresse dans règle Snort, ces adresse sont utilisées pour vérifier la source de laquelle provient le paquet et la destination du paquet l’adresse peut être une adresse IP unique ou une adresse réseau[19].
Par exemple : une adresse 192.168.159.0/24
192.168.159.0 Avec 24 bits dans le masque de réseau, il est un réseau de classe C.

- **Porte :**

Le port est utilisé pour appliquer une règle sur les paquets qui proviennent ou aller à un port privé ou une plage de ports. Par exemple, nous pouvons utiliser le port 23 à appliquer une règle aux paquets qui proviennent d'un serveur Telnet.

Nous pouvons utiliser le mot-clé *any* pour appliquer la règle sur tous les paquets quel que soit le port. Le port de communication associé à l’adresse IP, le port ne joue aucun rôle[19].
Exemple :

La règle suivante est appliquée à tous les paquets qui proviennent d'un serveur Telnet en 192.168.2.0/24, qui est un réseau de classe C et contient le mot «confidentiel»:

a*lerttcp 192.168.159.0/24 23 ->anyany \ (Contenu: «confidentiel»; msg: "Détecté confidentiel";)*

Les numéros de port sont essentiels lorsque nous souhaitons poser une règle uniquement pour un type particulier de paquet de données. Par exemple, si une vulnérabilité est liée à un seul protocole HTTP (Hyper Text Transfer Protocol) du serveur Web, nous pouvons utiliser le port 80 dans la règle pour détecter toute personne essayant pour l'exploiter. De cette façon, Snort appliquera cette règle que pour le trafic du serveur Web et non à un autre paquet TCP. La rédaction de bonnes règles améliore toujours les performances de l'IDS.

Les ports connus :

Numéros de port bien connus sont utilisés pour des applications fréquemment utilisées. Une partie de ces numéros de port et leurs applications sont répertoriées dans le tableau suivant :

Numéro de port	Description
20	FTP data
21	FTP
23	Telnet
25	SMTP, utiliser pour 'email server'
37	NTP(Network Time Protocol)
53	DNS server
67	Booptp/DHCP client
68	Bootp/DHCP server
69	TFTP
80	http
110	PoPS
161	SNMP
162	SNMP Traps
443	HTTPS
514	Syslog
330	MySQL

Tableau 1:Numéros port bien connus **[20]**

- **Direction :**

Le champ de direction détermine les adresses source et de destination et les numéros de port dans une règle. Les règles suivantes sont applicables dans le domaine de la direction:

- A -> symbole indique que l'adresse et les numéros de port sur le côté gauche du champ de direction sont la source du paquet alors que l'adresse et le numéro de port sur le côté droit du champ sont la destination.
- A <- symbole dans le champ de direction indique que le paquet se déplace à partir de la adresse et numéro de port sur le côté droit du symbole à l'adresse et numéro de port sur le côté gauche.
- Un symbole <> montre que la règle sera appliquée aux paquets circulant sur deux direction. Ce symbole est utile lorsque vous souhaitez surveiller les paquets de données pour à la fois client et serveur. Par exemple, en utilisant ce symbole, vous pouvez contrôler tous le trafic en provenance et à un serveur POP ou Telnet. **[19]**

- **Options:**

Cette section est le cœur du moteur de détection d'intrusion. Elle sert à décrire le contenu que l'on souhaite vérifier dans diverses sections du paquet. Dans la version 2.9.8 (d'près) de Snort, on compte plus de cinquante mots clés regroupés dans quatre catégories majeures que sont : générale, charge utile (payload), charge non utile (non-payload), post-détection :

1-Générale : cette catégorie regroupe les options que fournissent de l'information, mais qui n'ont aucun effet sur la détection. Voilà quelques options :

- *msg* : spécifie le message qui sera affiché dans le log et dans l'alerte
  Format : *Msg :* "<*message text*>" *;*
- *reference* : fait référence aux sites expliquant l'attaque détectée.
  Exemple :
  *alerttcpanyany ->any 7070 (msg:"IDS411/dos-realaudio"; *
  flags:AP; content:"|fff4 fffd 06|"; reference:arachnids, IDS411;)
- *classtype* : définit la classe de l'attaque (troyen, shellcode …etc).

Format :ClassType :<class name>

Exemple :

alerttcpanyany -> any25(msg: :"SMTP expnroot"; flags:A+; \ content:"expnroot"; nocase; classtype:attempted-recon;)

2-Payload: cette catégorie regroupe les options permettant d'accéder à l'information utile continue dans les paquets.Par exemple :

- *content* :permet à l'utilisateur de définir des règles qui recherchentle contenu spécifique de la réponse de la charge utile des paquets et de déclenchement sur la base de ces données.

Format : content : [!]"<Content String >" ;

Exemple :

Alerttcpanyany ->any 80 (content : ! "GET";)

3-Non-payload : cette catégorie regroupe les options qui font référence aux contenus du paquet qui ne sont pas de type payload.

- *ttl* : spécifie la valeur du TTL(Time-To-Live) du paquet,cette option prend numéro entre 0 et 225.

Format :

ttl:[<, >, =, <=, >=] <number>;

ttl:[<number>]-[<number>];

Exemple :

Cet exemple vérifie pour une valeur time-to-live qui est inférieure à 3.

Ttl :<3 ;

- *flags* : spécifie la présence d'un flag TCP dans les paquets suivants :
  - F - FIN - Terminer (LSB dans Drapeaux TCP byte)
  - S - SYN - Synchroniser les numéros de séquence
  - R - RST - Réinitialiser
  - P - PSH - poussoir
  - A - ACK - Acquittement
  - U - URG - Urgent
  - C - CWR - CongestionWindowReduced(MSB dans Drapeaux TCP byte)
  - E - ECE - ECN-Echo
  - 0 - Pas de TCP Flags Set

  Les modificateurs suivants peuvent être réglés pour modifier les critères de correspondance:
  - + - Match sur les bits spécifiés, ainsi que tous les autres
  - - Match si une quelconque des bits spécifiés sont mis
  - ! - Match si les bits spécifiés ne sont pas réglés

Cet exemple vérifie si juste le SYN et les bits FIN sont réglés, ignorant CWR (1 bit réservé) et ECN (réservé 2bit) :

Alerttcpanyany ->anyany(flags : SF,CE ;)

4-Post-détection: c'est un ensemble d'options qui désignent des actions à exécuter une fois que la règle est satisfaite.

- *session* : indique à Snort d'extraire les données de la session TCP,Il y a trois mots clés argument disponibles pour l'option session: *printable*, *binary*, ou*all*.

Exemple : pour enregistre toutes les chaînes imprimables dans un paquet de Telnet.

logtcpanyany<>any 23(session : printables ;) **[19]**

II.2. INSTALLATION DE SNORT :

III.2.1. Environnement de travail

Logiciel de virtualisation VMware Workstation, version 12.1-1 build -3770994 Copyright © 1998-2016 : C'est la version station de travail du logiciel. Il permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique.

Figure 25: Fenêtre de VMware

Distribution linux ubuntu -14.04.4 LTS

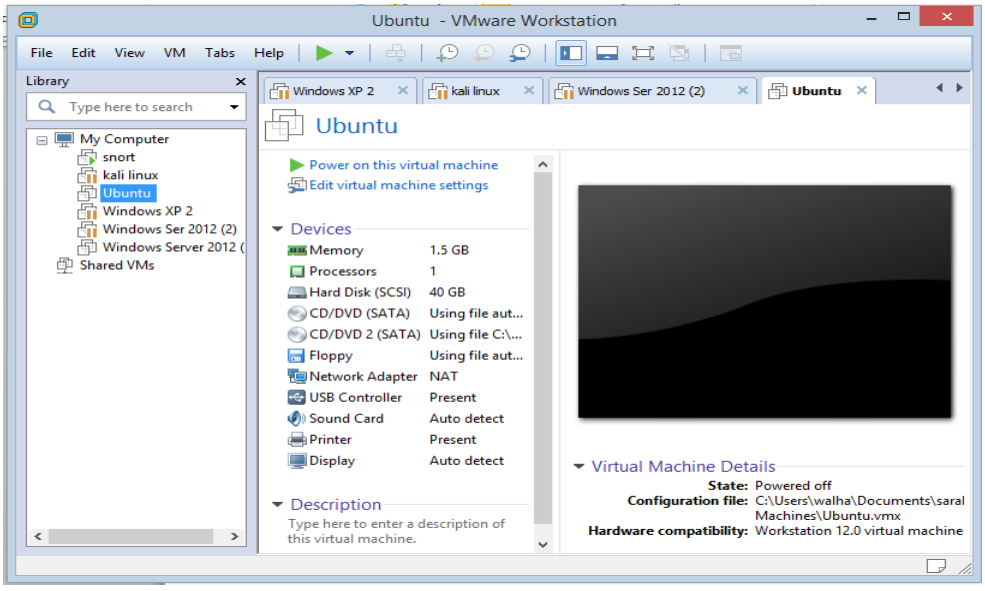


Figure 26: Fenêtre de VMware avec 4 machines

III.2.2. Préparation ubuntu et installation snort

Nous avons installé la distribution linux ubuntu :

Figure 27 :l'lancement l'installation ubuntu

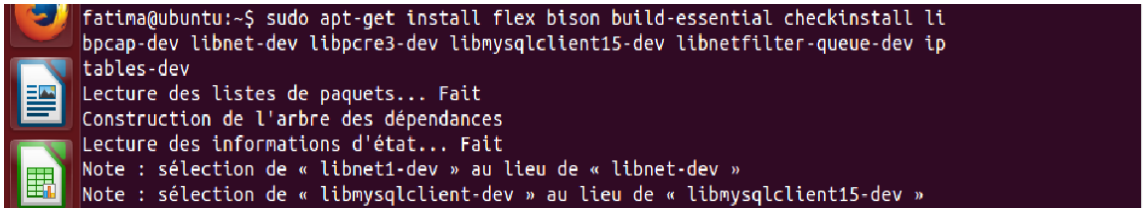
Après l'installation de la distribution de linux, il est nécessaire de mettre à jour les différents paquets installés.

#apt-get update

#apt-get dist-upgrade

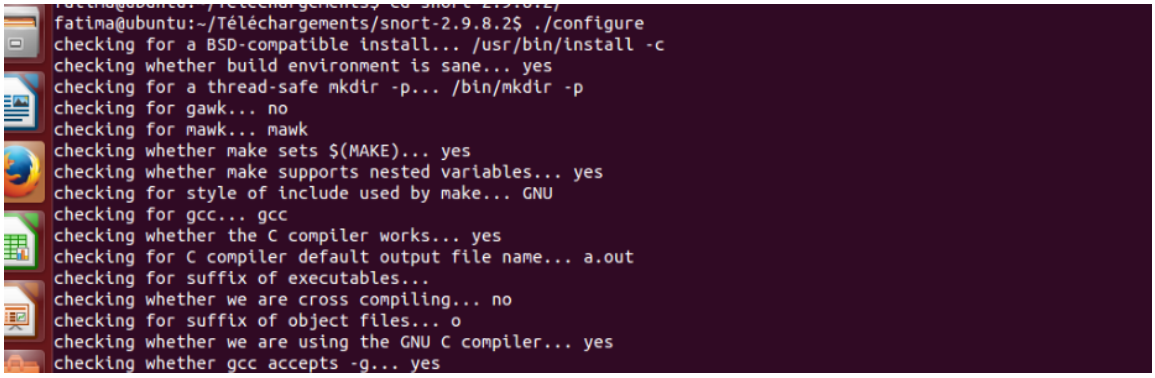
II.2.3. Installation des dépendances de Snort

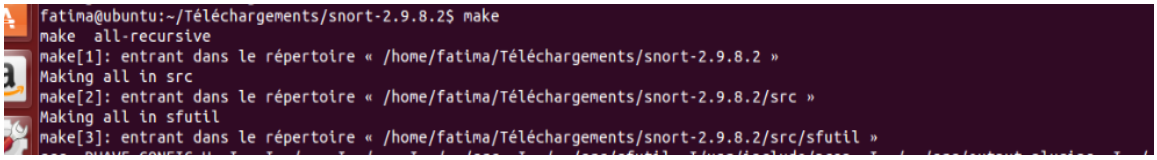
Pour le bon fonctionnement de Snort, il est nécessaire d'installer certains paquets entre autre en tapant la commande :



III.2.4. Téléchargement et installation de Snort

Nous avons téléchargé Snort sur le site officiel www.snort.org/snortdownloads , décompresser le fichier , compiler …etc.





Nous avons vérifié que Snort installé correctement en exécutent « snort –v ».

III.3. CONFIGURATION SNORT :

D'abord éditions le fichier snort.conf , Ouvrons le fichier de configuration de snort avec nano/pico

sudo pico /etc/snort/snort.conf

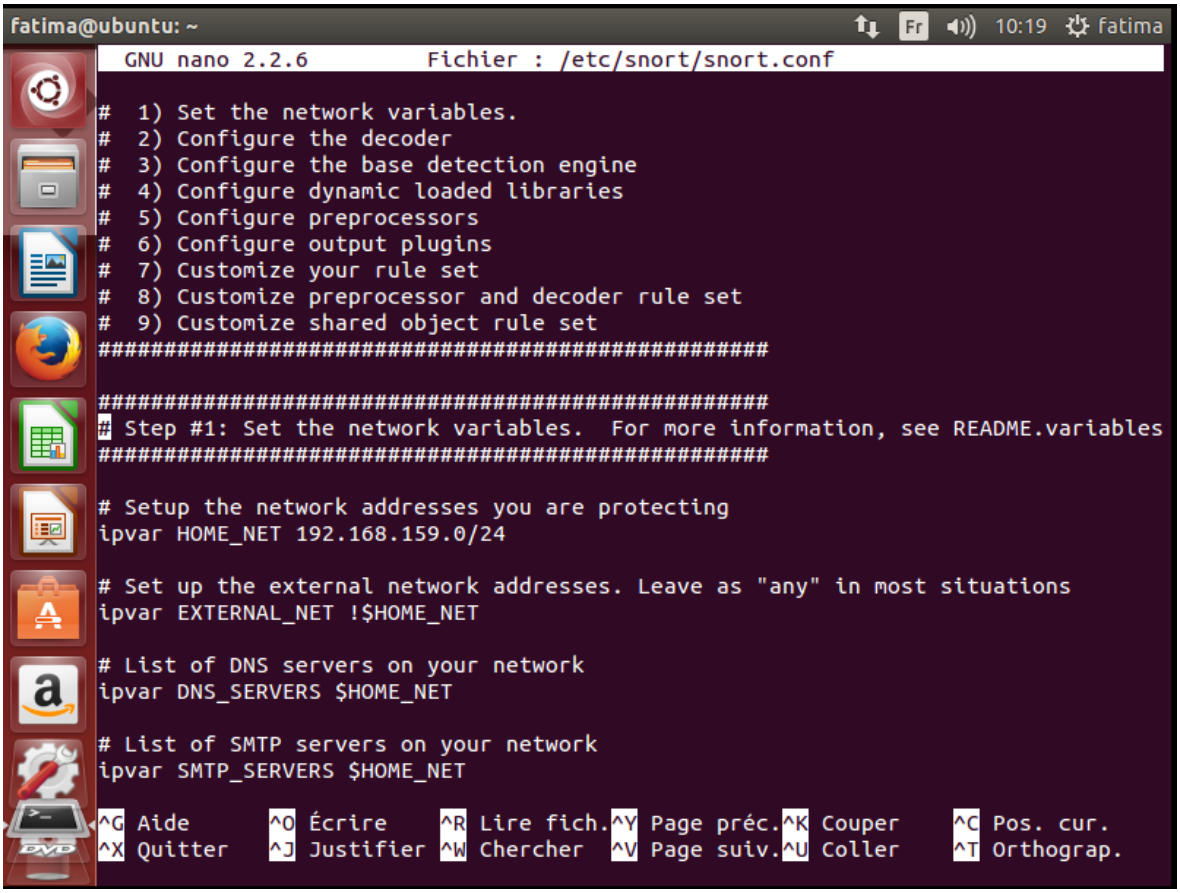


Figure 28: Fichier de configuration

Comme vous pouvez le voir dans la capture d'écran ci-dessus, le fichier de configuration est composé de six (6) sections :

- Définissez les variables sur votre réseau
- Configurer la bibliothèque dynamique chargée
- Configurez les préprocesseurs
- Configurez les plugins de sortie
- Ajoutez les directives de l'exécution de configuration
- Personnalisez vos règles

Nous devons d'abord définir les variables de notre réseau interne et externe. Celles-ci sont définies par les lignes:

- var HOME_NET
- var EXTERNAL_NET

Nous devons régler le HOME_NET à notre sous-réseau interne, comme 192.168.159.0/24.

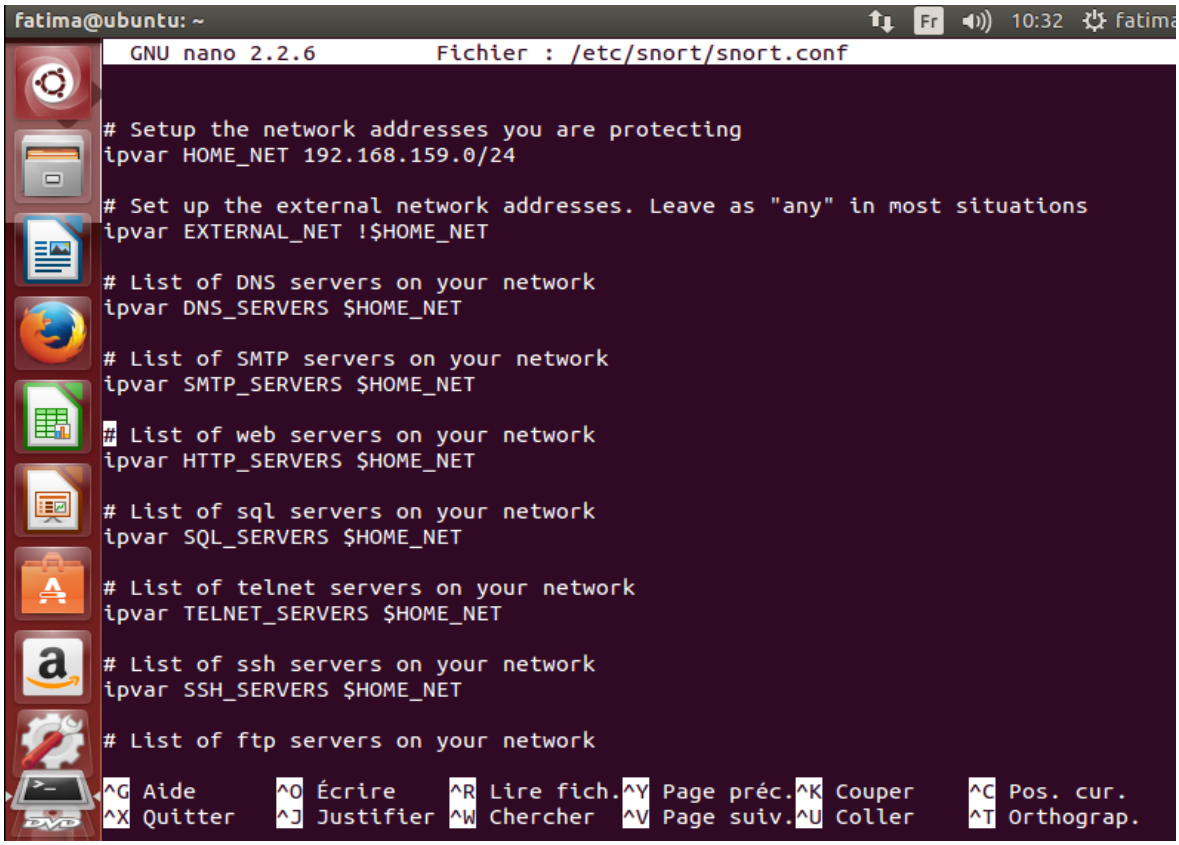


Figure29 : modification de réseau dans le fichier

Dans le fichier de configuration de SNORT (/etc/snort/snort.conf), vous avez toute une série de inclue. Il s'agit des règles utilisées par SNORT pour détecter d'éventuelles intrusions. Il y a des règles de Telnet, ICMP, FTP, ...

III.4. AJOUT DES RÈGLES SNORT :

Nous devons définir notre chemin à nos règles. Comme nous pouvons le voir dans la capture d'écran ci-dessous: var RULE_PATH /etc /snort /rules

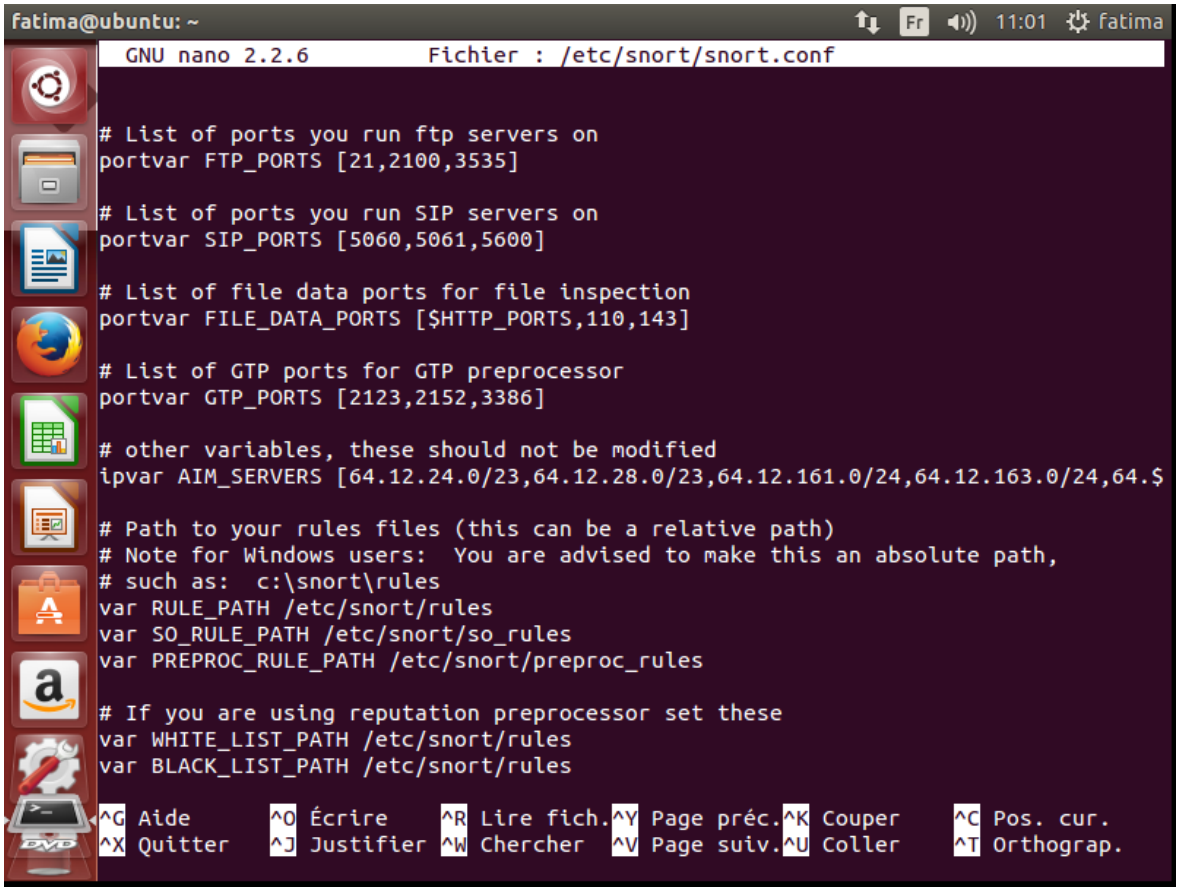
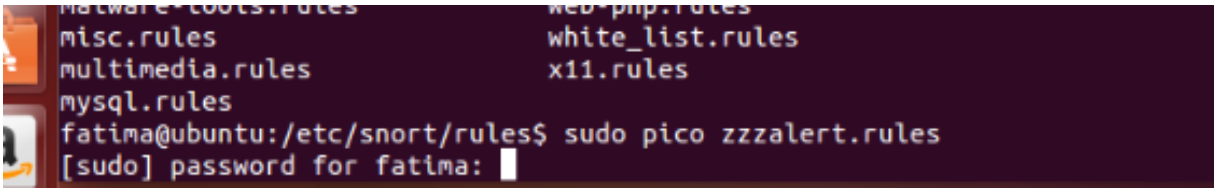


Figure 30: modification effectué dans le fichier

Après avoir configuré Snort, nous écrivons nos propres règles. Pour simplifier l'analyse des sorties produites par Snort, nous utilisons que les règles que nous écrivons.

a. Création 'alertrule ' personnalisé pour snort

Accéder au répertoire ou se trouvent toutes les règles snort, et créer.



Notre règle:

alerttcp any any -> any any (content:"www.facebook.com";msg:"Someone is accessing Facebook!!";sid:1000001;)

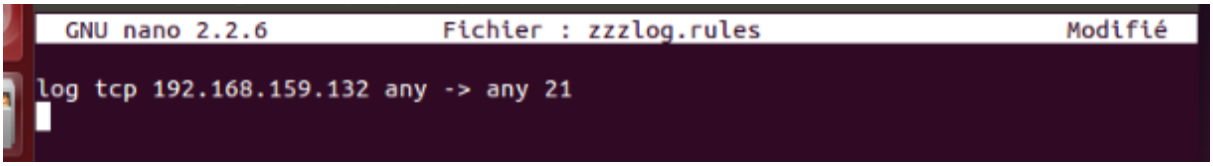
Si quelqu'un accède à www.facebook.com , puis un message apparait que quelqu'un tente d'y accéder.

a. Création 'log rule ' personnalisé pour snort

Nous avons tapé et puis enregistre la règle suivante :

Log tcp 192.168.159.132 any ->any 21

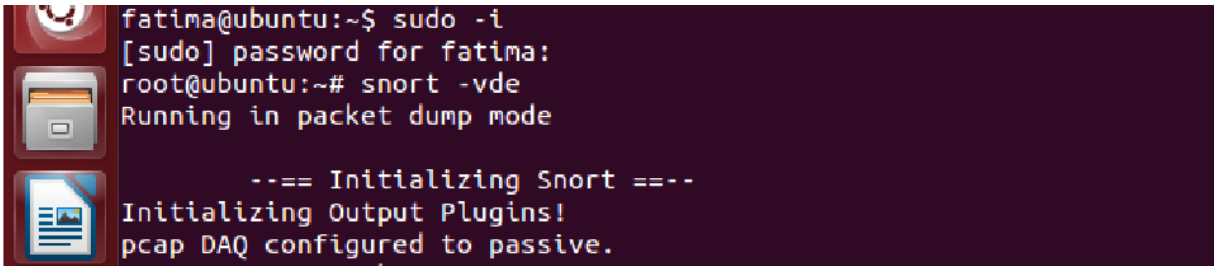
Cette règle permet que la machine avec l'adresse 192.168.159.132 essaie de FTP, le paquet sera connecté.



III.5. LANCEMENT DE SNORT :

Il est possible d'exécuter snort en trois modes :

En mode Sniffer : SNORT lit les paquets circulant sur le réseau et les affiche d'une façon continue sur l'écran.



En mode packetlogger : ce mode en tout point similaire au précédent à ceci près que les logs ne s'affiche plus à l'écran, mais s'inscrivent directement dans un fichier de log, qui se trouve dans /var/log/snort, le fichier est écrit dans ascii.

```
root@ubuntu:/var/log/snort# snort -vde -l /var/log/snort -K ascii
Running in packet logging mode
```

L'exécution de snort avec le fichier de configuration

```
root@ubuntu: ~
root@ubuntu:~# snort -A console -i eth0 -c /etc/snort/snort.conf -l /var/
log/snort -K ascii
```

b. Résultats

Mode Packet logger :

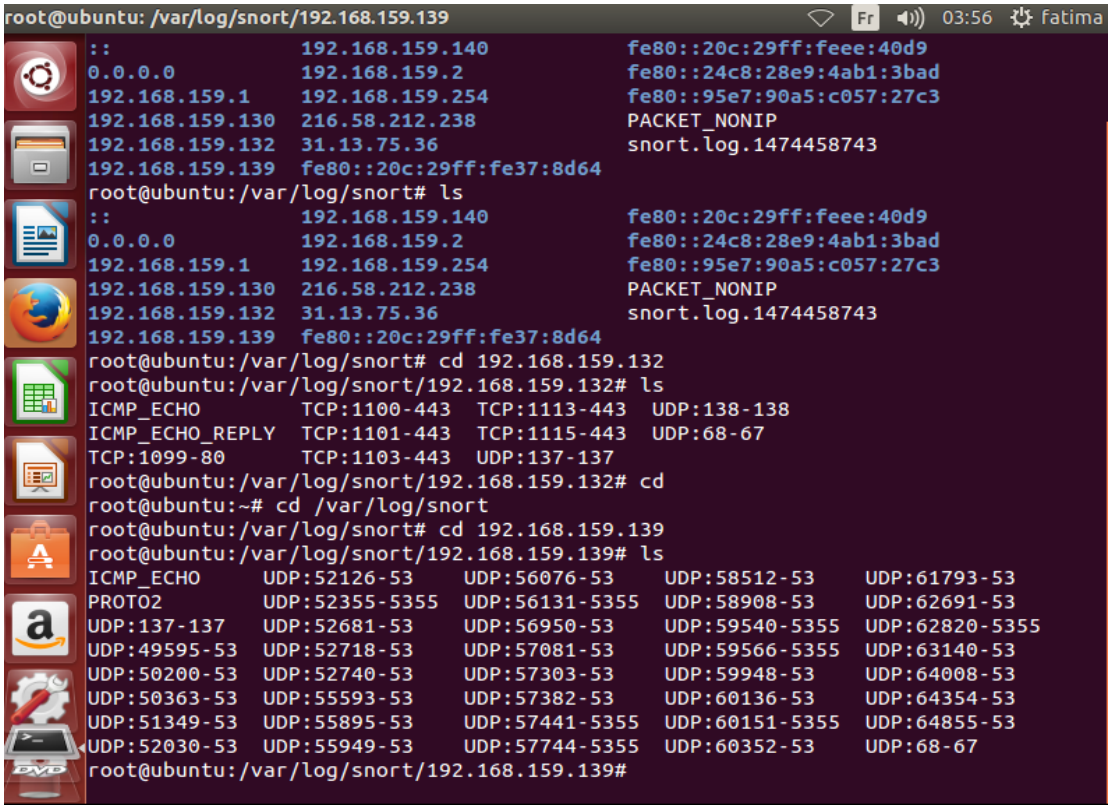
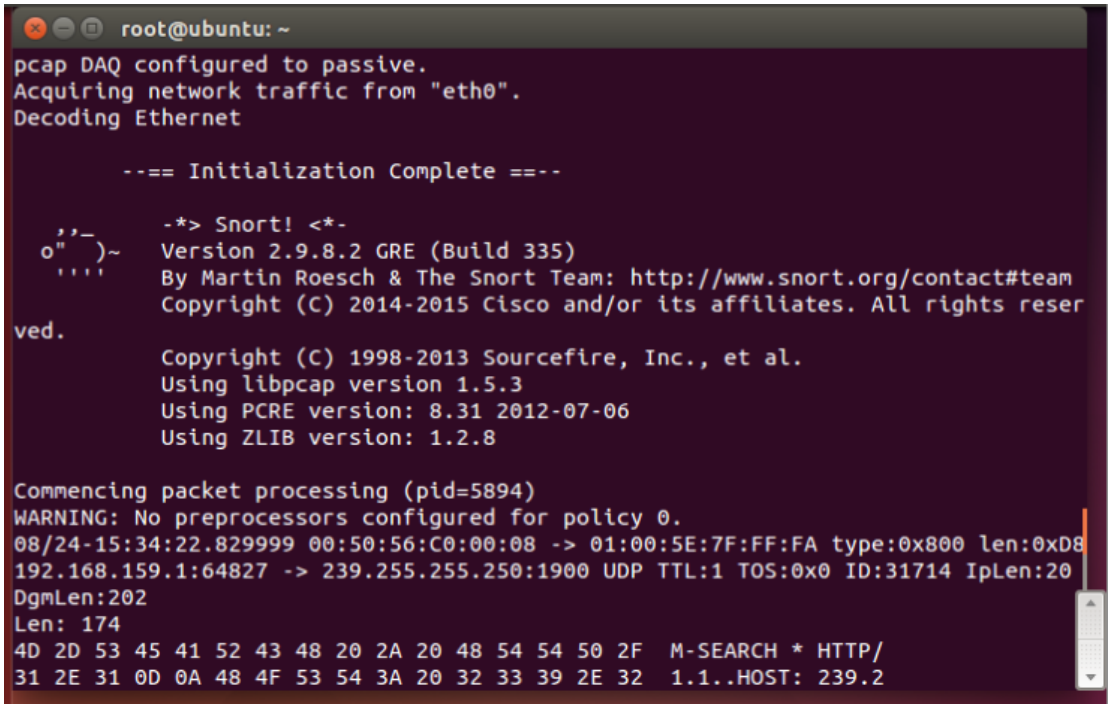


Figure 31:Un fichier log

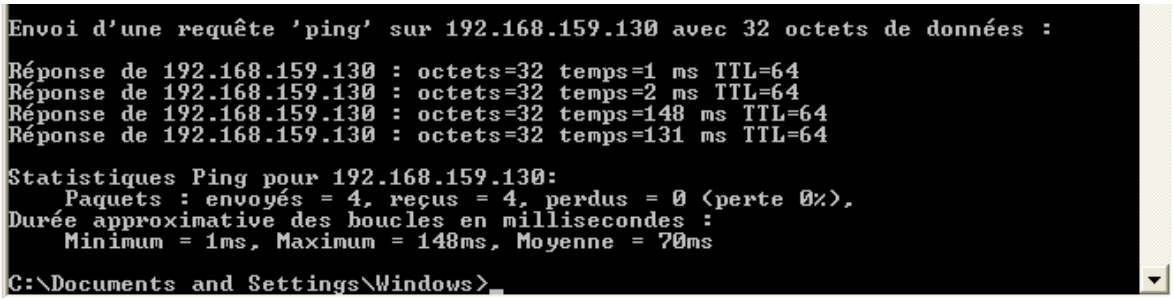
Mode sniffer :



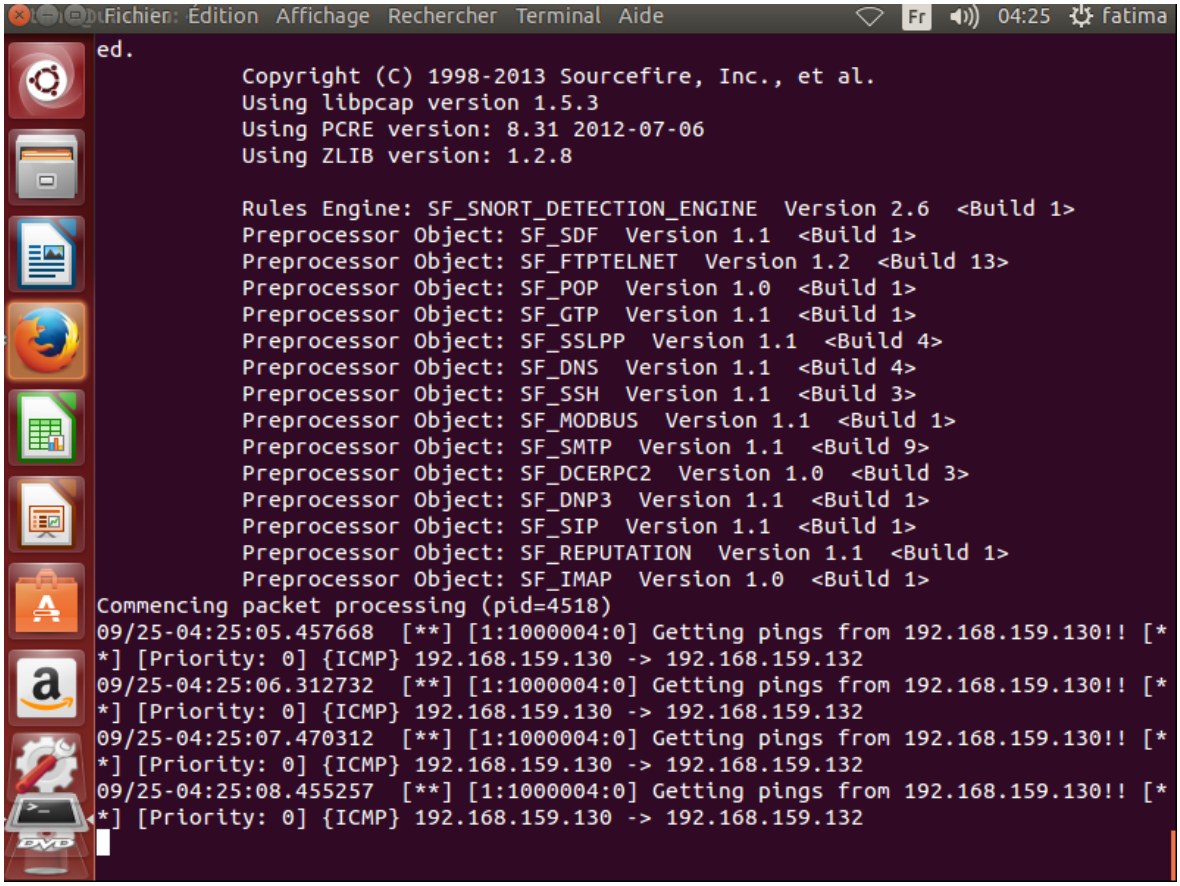
Test ping :

Nous allons tester si snort peut détecter une intrusion

Machine XP son adresse IP est 192.168.159.132



Ubuntu (Snort) son adresse IP 192.168.159.130



Donc l'IDS Snort a bien détecté l'intrusion

Conclusion

Dans ce chapitre, nous avons faire une étude de cas du système de détection d'intrusion Snort, en présentant sa position dans un réseau, son architecture détaillée ainsi que son processus d'installation.

De nombreux problèmes ont été rencontrés et maîtrisés lors de l'installation du nombre important des packages complémentaires à Snort.

Ce chapitre nous a permis de découvrir un outil de détection d'intrusion très intéressant.

CONCLUSION GENERALE

La sécurité reste encore un sujet à discussion vu qu'aucune solution fiable à part entière n'a encore été trouvée.

Nous venons de montrer que la détection d'intrusion sur les réseaux ne vient pas concurrencer les autres systèmes de sécurité mais au contraire les compléter.

On a également présenté les principes mises en œuvre par les IDS pour atteindre leur but.

Cependant le seul bémol est qu'un système ne peut jamais être sécurisé à 100 %, alors le but recherché serait de pouvoir détecter le maximum d'intrusions et de toutes les boquer dans le futur ; C'est dans ce cas que Snort est déclaré efficace.

Capable de détecter et de bloquer plusieurs intrusions à la fois de par ses règles régulièrement mises à jour par « le monde du gratuit », Snort est un vrai portail anti-intrusion.

Cependant, comme tout autre système de sécurité, cette technologie (les IDS) n'est pas encore arrivée à maturité et les outils existants tels que Snort ne sont pas toujours à la hauteur des besoins

REFERENCES BIBLIOGRAPHIQUES

[3]:Ahmed Mehaoua, Architecture des réseaux, 2e édition, Pearson éducation France Paris, 2010

[4]: Ghernaouti-Hélié S. « Sécurité Informatique et réseaux », Dunod 2ème édition, p. 231.

[5] :Biondi P., « Architecture expérimentale pour la détection d'intrusions dans un système informatique », Avril-Septembre 2001, p.8.

[6]Endorf C ,Schultw E , Mellande J(2004) Instrusion Detection and Prevention»

[7]Lerman L les systemes de detection d'instruction basés sur du machine learning »

[8]Boulares M system de d »tection des intrusions»

[9]Debar H ,Dacier M,Wespi A(2000) A Revised Tasronomy or intrusion-Detection Systemes

[10]Wood ,M .Erlinger,M(2012) Instruction detection message exchange requirements,The RFC

[11]T .Kenaza Modeles graphiques probqbilistes pour la corr »lation d'alertes en d »tection d'instrusion»

[13]M .Amand et M.NSIRI, Etude d'un système de détection d'instrusions comportemental pour léanalyse du traic aéroportuaine » ,IENAC08 ,rapport de projet tutoré 27 janvier 2011

[15]M .KHALID « SNORT-System de détection d'intrusion »

[16]Mohamed D « Mettre enplace un IDS snort et un pare-fou IPtables »2013

[18]E .Farman,Rapport de stage,Cursus AFPA TSRT 2011-2012,lieu :Hotel de ville de Pertuis du 30 Janvier 2012 au 16 février 2012.

[19]Rafeeq Ur Rehman, Intrusion Detection systems with Snort, Pearson Education, Inc publishing as pretice Hall PTR, Upper Saddle River, New Jersey, 2003.

[20]Martin Roesch, Snort User Manual 2.9.8.0, November 18th, 2015

Webographie:

[1]*http://www.larousse.fr/dictionnaires/francais/%C3%A9v%C3%A9nement/*

[2] *http://www.ivision.fr/audit-informatique/*

[12] *http://www.informatique-securite.fr/systemes/ids.html*

[14] *http://www.commentcamarche.net/contents/237-systemes-de-detection-d-intrusion-ids*,

[17] *http://fr.wikipedia.org/wiki/Snort*