REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DU GENIE ELECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes
De MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**

Filière : **Génie électrique**

Spécialité : **Télécommunication et Réseaux**

Présenté par

Yamina TAMI
Sadjia AGDOUR

Thème

Mise en place d'un IPS Suricata

Mémoire soutenu publiquement le 24 /09/2017. Devant les jurys composé de :

M Mourad LAZRI
Maître de conférences A, UMMTO, Président

M Fethi OUALLOUCHE
Maître de conférences B, UMMTO, Encadreur

M Djamel ALOUACHE
Maître de conférences B, UMMTO, Examinateur

Promotion 2016/2017

Remerciements

En premier lieu, on remercie Dieu le tout puissant, de nous avoir accordé la volonté et le courage pour réaliser ce travail.

On tient à exprimer nos sincères remerciements à notre promoteur Mr OUALLOUCHE de nous avoir guidé et orienté dans notre travail, et aussi pour sa patience, sa disponibilité et sa bienveillance.

On exprime également nos remerciements à Mr KHADIR pour son aide et son travail.

On tient aussi à remercier le personnel du Centre des Systèmes et Réseaux d'information, de Communication, de Télé-enseignement et enseignement à Distance Ex Centre de calcul de l'université Mouloud Mammeri de Tizi-Ouzou de nous avoir aidés dans nos recherches.

Enfin, nous tenons à exprimer notre profonde gratitude et réels sentiments à nos familles, qui nous ont toujours soutenues.

Dédicaces

Je dédie ce modeste travail à :

Mes chers parents, pour leurs sacrifices et leurs soutient.

Mon très cher frère GHILES

Mon cher frère KARIM et sa femme WISSEM

Mes grands-parents

Mes chères copines SAMIRA et AMINA

Tous mes ami(e) ainsi qu'à tous ceux qui me sont chers

YAMINA

Dédicaces

Je dédie ce modeste travail à :

La mémoire de mon défunt père,

Ma chère mère pour son soutien, ses encouragement qu'elle ma apporté tout au long de ma vie

Mes chers frères

Mes chères belles sœurs

Mon adorable neveu et nièce

Ainsi que tout mes amis et toute ma famille

SADJIA

Sommaire

Chapitre I : Généralités sur les réseaux informatiques

Chapitre II: Sécurité des réseaux informatiques

Chapitre III : Etude de l'IPS Suricata

Chapitre IV: Application

Résumé

Les réseaux et les systèmes d'information sont devenus actuellement des outils indispensables au fonctionnement des entreprises, donc la pérennité de toute entreprise passe aujourd'hui par une disponibilité permanente de ces derniers.

La stabilité des réseaux est due à l'implémentation de différentes technologies que se soit matériels ou logiciels au sein de leurs architectures. Cependant les principaux enjeux de l'IPS Suricata et ainsi de réussir à offrir des performances évoluées et fournir des services nouveaux et avancés sur les performances et la sécurité du réseau.

Durant notre travail qui s'est déroulé au sein du Centre des Systèmes et Réseaux d'information, de communication, de Télé-enseignement et Enseignement à distance Ex Centre de calcul de l'université Mouloud Mammeri de Tizi-Ouzou, en premier lieu nous nous sommes intéressées à l'étude détaillé de l'IPS Suricata, et afin de tester son efficacité de sécurisation, on a prie un exemple d'un réseau qu'on a sécurisé avec cet IPS. Tout d'abord on a installé l'IPS Suricata sur une machine virtuelle avec le logiciel de virtualisation VMware Workstation 12, et le système d'exploitation attribué est la distribution Debian8. Par la suite on a configuré l'IPS, et à la fin on a effectué quelques tests de fiabilités.

Mots clés : IPS, Suricata, Sécurité informatique, VMware Workstation, Debian

Liste des figures

Chapitre I : Généralités sur les réseaux informatiques

Chapitre II: Sécurité des réseaux informatiques

Chapitre III: Etude de l'IPS Suricata

Chapitre IV : Application

Liste des figures

Glossaire

ARP	Aderss Resolution Protocol
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DDOS	Distributed Denial-Of-Service
DHCP	Dynamic Host Configuration Protocol
DOS	Denial Of Service
DMZ	Demilitarized Zone
DNS	Domain Name Service
ET	Emerging Threats
FDDI	Fiber Distributed Data Interface
FTP	File Transfert Protocol
HTTP	Hyper Text Transfert Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
OSI	Open System Interconnexion
OSIF	Open Information Security Foundation
OSPF	Open Shortest Path First
PAN	Personal Area Network
P2P	Peer To Peer
RARP	Reverse Address Resolution Protocol
RIP	Routing Information Protocol
SMTP	Simple Mail Transfert Protocol
TCP	Transmission Control Protocol
Telnet	Terminal NETwork ou TELecommunication NETwork
UDP	User Datagram Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
YAML	Yet Another Markup Language

De nos jours, Les systèmes d'information mais aussi Internet, le réseau mondial qui interconnecte un nombre d'entre eux, jouent un rôle monumental dans la vie quotidienne et dans notre société en général, et sur lesquels reposent des domaines relevant de la vie privée tels que l'envoi de courrier ou bien le paiement à distance, mais aussi des domaines stratégiques comme le secteur bancaire ou encore les communications militaires.
Internet est un outil à la fois High-tech et démodé par sa technique, internet n'a pas su évoluer dans l'utilisation de ses protocoles. La plupart des protocoles utilisés ont plusieurs années d'existence et certains n'ont pas été crées dans une optique où le réseau prendrait une telle envergure. De ce fait, des attaques réalisées par des utilisateurs malveillants et visant à exploiter les vulnérabilités de ces systèmes d'information sont de plus en plus fréquentes [1].

Parmi les préceptes connus sur la sécurité informatique se trouve celui énonçant que pour une entreprise connectée à l'internet, le problème aujourd'hui, n'est plus de savoir si elle va se faire attaquer mais quand cela va arriver, une solution possible est alors d'essayer de repousser les risques dans le temps par la mise en œuvre de divers moyens destinés à augmenter le niveau de sécurité.

Les entreprises ont fait beaucoup d'effort pour sécuriser leurs systèmes d'information et leurs connexions externe en utilisant des mesures de sécurité tels que, les firewalls, DMZ, VPN, antivirus…etc. [2]. Le choix d'un outil de sécurité repose sur l'administrateur réseau. En effet, ce dernier doit d'abord étudier les failles de sécurité du réseau pour en proposer la solution.

Dans ce mémoire de fin d'étude, nous nous sommes intéressés à la problématique de sécurité des réseaux informatique. A cet effet, on a testé une méthode de sécurité sur un exemple d'un réseau, qu'on a réalisé durant notre stage au Centre des Systèmes et Réseaux d'information, de Communication, de Télé- enseignement à Distance Ex Centre de Calcul de l'université Mouloud Mammeri de Tizi-Ouzou. La méthode consiste à utiliser un IPS Suricata inline (Intrusion Prevention System), qu'on a installé puis configurer afin de bloquer des paquets de données malveillants, et cela selon des règles qui lui ont été attribuées. A la fin on a effectué des testes (des attaques) pour vérifier le bon fonctionnement de l'IPS Suricata.

Nous avons structuré notre mémoire en 4 chapitres.

Dans le premier chapitre, nous avons effectué une étude globale sur les réseaux informatiques, que ce soit, la classification des réseaux, les différents concepts des modèles en couche (TCP/IP et OSI) et aussi les différents protocoles de communication.

Le deuxième chapitre est consacré a la sécurité informatique, on a cité les différentes attaques aux quelles les réseaux sont exposés, puis les différentes méthodes de sécurité.

Le troisième chapitre est consacré à l'étude de l'IPS Suricata, les différentes sortes, les caractéristiques et les avantages de ce dernier.

Dans le quatrième chapitre les résultats de configuration et de test sur l'IPS Suricata sont donnés.

I.1 Préambule

Les réseaux informatiques sont nés du besoin de faire communiquer des terminaux distants entre eux. Ils sont beaucoup apportés pour les entreprises et les sociétés, ce qui les a rendus indispensables. Leur but est d'assurer l'interconnexion des ordinateurs afin qu'ils puissent communiquer entre eux et d'échanger des données.

Dans ce chapitre nous allons définir un réseau informatique et présenter les topologies et les protocoles les plus utilisés, et d'autres notions jugées nécessaires pour le déroulement de notre travail.

I.2 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'ordinateurs et d'autres dispositifs autonomes connectés entre eux grâce à des supports de transmission matérielles et logicielles.

Le réseau s'appuie sur deux notions fondamentales qui sont :

- L'interconnexion qui assure la transmission des données d'un nœud à un autre.
- La communication qui permet l'échange de données entre processus.

I.3 Intérêt d'un réseau

Pour les entreprises et les organisations [3] :

- Partage de ressources (programmes, matériels, données)
- Fiabilité / Résistances aux pannes (duplication des données)
- Réduction du coût
- Outil de communication (messagerie électronique, travail collaboratif)
- Commerce électronique

Pour les particuliers

- Accès à l'information répartie (WWW)
- Communication (email, messagerie instantanée, Forums, blogs …)
- Jeux
- Commerce électronique

I.4 Classification des réseaux informatiques

La classification se fait par rapport à un critère donné, ainsi nous pouvons classifier les réseaux informatiques de la manière suivante :

I.4.1 Classification selon l'étendue géographique

On compte généralement 4 catégories de réseaux informatiques différenciées par la distance maximale séparant les points les plus éloignés du réseau :

- **PAN** (Personal Area Network)

Les réseaux personnels, généralement mis en œuvre dans un espace d'une dizaine de mètres interconnectant des équipements personnels tels que : GSM, téléphones portables…etc.

- **LAN** (Local Area Network)

Les réseaux locaux représentent un ensemble d'ordinateurs interconnectés dans une petite aire géographique, tels qu'un domicile, un bureau, un bâtiment, pour l'échange de données et le partage de ressources. Ils ne dépassent pas généralement les centaines de machines et ne dessert jamais au-delà du kilomètre, et les vitesses de transmissions vont de 10 à100Mb/s.

- **MAN** (Métropolitain Area Network)

Les réseaux métropolitains permettent l'interconnexion des entreprises ou des départements sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole.

- **WAN** (Wide Area Network)

Les réseaux étendus sont destinés comme leurs noms l'indiquent, à transporter des données numériques sur des distances à l'échelle d'un pays voir d'un continent ou de plusieurs continents, le plus grand WAN est le réseau internet.

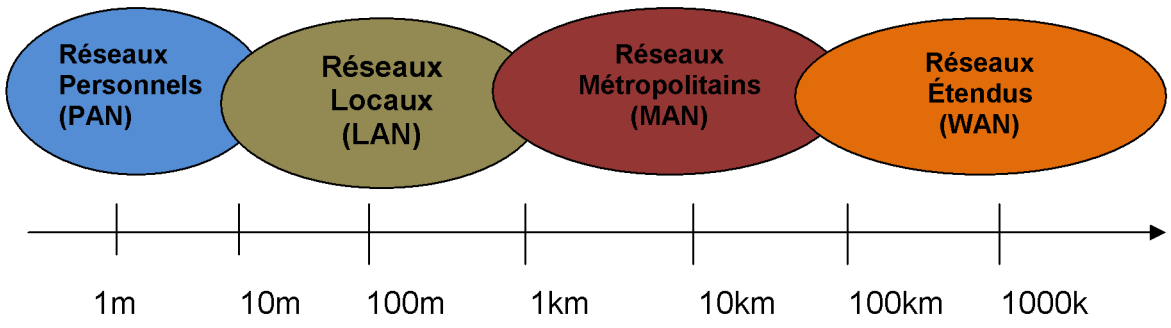


Figure I.1 : Classification des réseaux informatiques selon la taille

I.4.2 Classification selon la topologie

Les réseaux se différent selon leur structure et plus précisément leur topologie. La topologie est l'organisation physique d'un réseau.

La topologie physique est en fait la structure physique d'un réseau, C'est la forme, l'apparence du réseau. Il existe plusieurs topologies physiques (le bus, l'étoile, maillée, l'anneau…).

a. Topologie en bus

Le bus est un segment central ou circulent les informations, s'étend sur toute la longueur du réseau. Tous les équipements d'une topologie en bus sont connectés par un même câble généralement coaxial, qui passe d'un ordinateur à un autre. L'extrémité du segment de câble principal doit comporter un terminateur (bouchon) qui absorbe le signal lorsque ce dernier atteint la fin du câble. L'avantage du bus est sa simplicité de mise en œuvre par contre si un câble est en panne le réseau ne fonctionne plus.

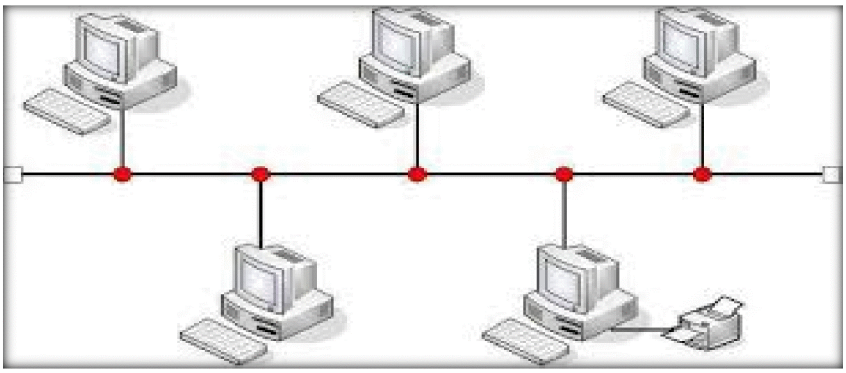


Figure I.2 : Topologie en bus

b. Topologie en anneau

Dans cette topologie les équipements sont reliés entre eux en formant une boucle, l'information circule dans une même direction le long du support. Chaque station reçoit le message, mais seule la station à qui le message est adressé le traite.

L'avantage est que l'anneau offre deux chemins pour aller d'un point a l'autre, ceci permet à l'information de passer malgré une coupure sur le câble.

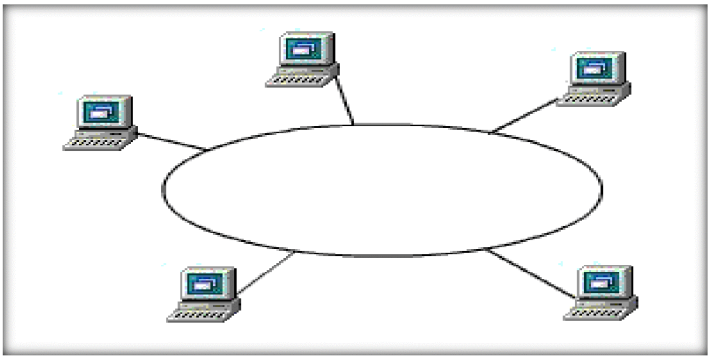


Figure I.3 : Topologie en anneau

c. Topologie en étoile

La topologie en étoile est la plus utilisée sur les réseaux locaux Ethernet. Elle est composée d'un point de connexion central, il s'agit d'un équipement comme un hub ou un commutateur, où tous les segments de câble se connectent. Chaque hôte du réseau est connecté à l'équipement central par son propre câble.

L'avantage de cette topologie est que la panne d'une station ne perturbe pas le fonctionnement du réseau et il est facile d'ajouter des stations ou de procéder à des modifications. L'inconvénient est que si le point central tombe en panne, le réseau devient inutilisable.

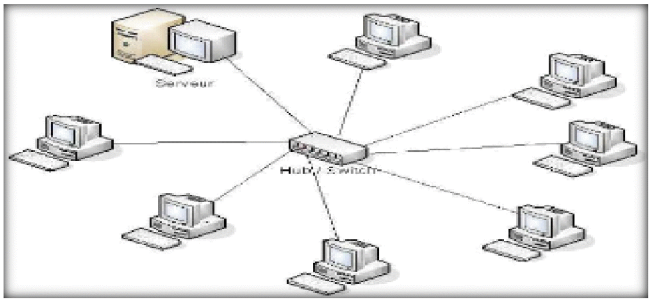


Figure I.4 : Topologie en étoile

d. Topologie en arbre

Dans une topologie en arbre il existe un hôte principal de haut niveau qui est connectée à plusieurs nœuds de niveau inférieur. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. L'inconvénient majeur avec cette topologie c'est que, si un câble casse, tous les ordinateurs connectés qui se trouvent en dessous seront paralysés.

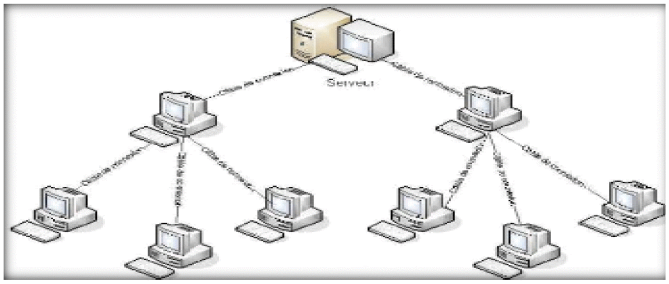


Figure I.5 : Topologie en arbre

e. **Topologie Maillée**

La topologie maillée est une évolution de la topologie en étoile. Elle permet de connecter tous les équipements, ou nœuds, entre eux afin d'obtenir une redondance et donc une tolérance aux pannes. Elle est utilisée sur les réseaux étendus (WAN) pour interconnecter les réseaux locaux. La mise en œuvre de la topologie maillée est difficile et onéreuse.

En cas de rupture d'un lien, l'information peut être acheminée, mais cette topologie nécessite beaucoup de câble.

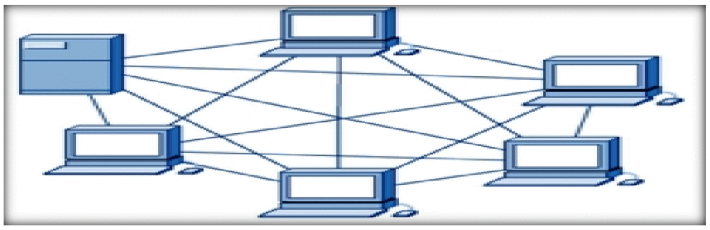


Figure I.6 : Topologie maillée

I.4.3 Classification selon la méthode d'accès

- **Méthode d'accès CSMA /CD**

CSMA (Carier Sense Multiple Access) c'est une méthode qui consiste à écouter le canal avant d'émettre. Ce protocole est de type persistant car la station persiste à écouter le canal jusqu'a ce que celui-ci devient libre, avant d'émettre sa trame.

- **Token ring**

La méthode du passage du jeton est une méthode propre aux réseaux en anneau. C'est une technologie d'accès au réseau basé sur le principe de la communication au tour à tour, c'est-à-dire que chaque ordinateur du réseau a la possibilité de parler à son tour. C'est un jeton, un paquet de données qui passe de station en station et qui détermine celle qui détient le droit d'émettre. Lorsqu'un ordinateur est en possession du jeton il peut émettre pendant un temps déterminé, après lequel il remet le jeton à l'ordinateur suivant.

- **Lan FDDI**

La technologie FDDI (Fiber Distributed data interface) est une technologie d'accès au réseau sur des lignes de type fibre optique. C'est un anneau à jeton à détection et correction d'erreurs.

I.5 Catégories des réseaux

Du point de vue architecture réseau, il existe deux grandes catégories de réseaux, réseau poste à poste (Peer to Peer) et réseau serveur dédicacé ou client-serveur (server based).

I.5.1 Le réseau Poste à Poste

C'est un réseau sans serveur dédié, chaque ordinateur connecté au réseau peut faire office de client ou serveur, les réseaux poste à poste sont valables que pour un petit nombre d'ordinateurs et pour des applications ne nécessitant pas une grande sécurité. L'architecture peer to peer est moins coûteuse par rapport à une architecture de réseau informatique de type client/serveur, elle ne nécessite pas un serveur puissant et un mécanisme de sécurité très poussée.

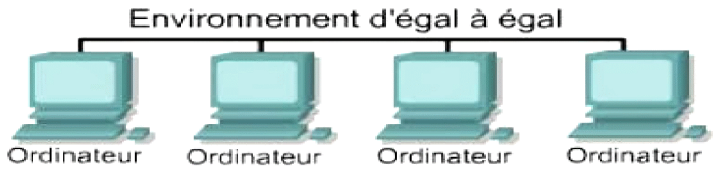


Figure I.7 : Architecture P2P

I.5.1.1 Avantages de l'architecture poste à poste

- Implémentation moins coûteuse.
- Ne requiert pas un système d'exploitation de réseau.
- Une simplicité à toutes épreuves.

I.5.1.2 Inconvénients de l'architecture poste à poste

- Le système n'est pas centralisé, ce qui le rend difficile à administrer.
- La sécurité est très peu présente.

I.5.2 Le réseau client /serveur

Dans une configuration client-serveur, les services de réseau sont placés sur un ordinateur dédié appelé serveur, qui répond aux requêtes des clients. Un serveur est un ordinateur central, disponible en permanence pour répondre aux requêtes émises par les clients et relatives à des services de fichiers, d'impressions, d'applications ou autres.

La plupart des systèmes d'exploitation de réseau adoptent des relations client-serveur. En règle générale, les ordinateurs de bureau agissent comme des clients, alors qu'un ou plusieurs ordinateurs équipés d'un logiciel dédié, qui sont dotés d'une puissance de traitement et d'une mémoire plus importantes assurent la fonction de serveurs. Les serveurs sont conçus pour gérer simultanément les requêtes de nombreux clients.

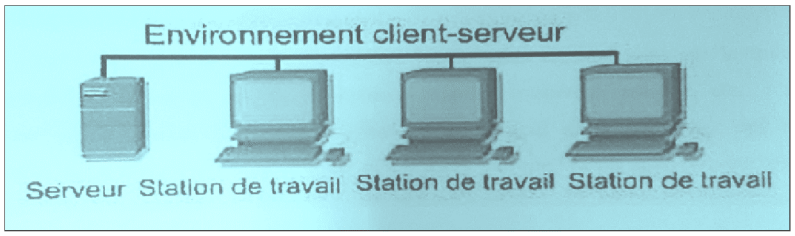


Figure I.8 : Architecture client/serveur

I.5.2.1 Avantages de l'architecture clients/serveur

- Garantit une meilleure sécurité.
- Plus facile à administrer lorsque le réseau est étendu car l'administration est centralisée.
- Possibilité de sauvegarder toutes les données dans un emplacement central.

I.5.2.2 Inconvénients de l'architecture clients/serveur

- Le serveur nécessite du matériel plus puissant et coûteux.

- Présente un point unique de défaillance s'il n'y a qu'un seul serveur ; si le serveur est en panne, les données de l'utilisateur risquent de ne plus être disponibles.

I.6 Les supports de transmission

Afin que les informations circulent au sein d'un réseau, il est nécessaire de relier les différentes Unités de communication à l'aide d'un support de transmission. Un support de transmission est un canal physique qui permet de relier des ordinateurs et des périphériques. Les supports de transmission sont nombreux, parmi ceux-ci on distingue [4]:

- ❖ Câble à paire torsadée
- ❖ Câble coaxial
- ❖ Fibre optique

I.6.1 Câble à Paire torsadée

I.6.1.1 Câble à paires torsadées non blindée

La paire torsadée non blindée est un support de transmission d'information entre les ordinateurs, c'est le type de câble le plus utilisé sur les réseaux. La paire torsadée non blindée peut être constituée de 2, 4, 6 ou 8 fils vrillés deux à deux, cette paire torsadée non blindée est extrêmement souple et légère, ce qui rend son installation facile.

Cette paire torsadée ne permet pas de relier des ordinateurs et des périphériques très éloignés les uns des autres, en effet, la transmission des signaux n'est possible que sur quelques dizaines de mètres.

I.6.1.2 Câble à paires torsadées blindée

La paire torsadée blindée est un support de transmission des informations utilisée pour relier des ordinateurs et des périphériques sur des réseaux comme Token-Ring. Elle est identique à la paire torsadée non blindée, mais contient en plus une protection contre les interférences constituée par une feuille ou une tresse métallique entre les paires torsadée et le revêtement externe du câble et aussi cette paire nécessite des connecteurs spécifique selon la nature du réseau.

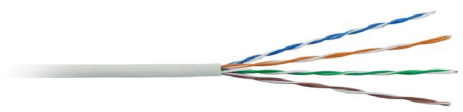


Figure I.9 : Câble à paires

I.6.2 Câble coaxial

Le câble coaxial est composé d'un fil de cuivre rigide enveloppé d'une couche en plastique, elle même entourer d'une feuille ou tresse métallique, l'ensemble du câble est recouvert d'une gaine plastique souple. Pour connecter les ordinateurs entre eux, il faut utiliser des connecteurs de type BNC [4].

Figure I.10 : Câble coaxial

I.6.3 Fibre optique

La fibre optique est un support de transmission d'informations entre les ordinateurs en utilisant des signaux lumineux au sein d'un réseau. Les informations échangées entre les ordinateurs se font à l'aide de signaux électriques, ces signaux sont convertis en signaux lumineux avant d'être transmis sur un câble optique. Le câble optique fait circuler les informations dans un conducteur central en verre ou en plastique, et le conducteur à son tour enveloppé de silicone ou de plastique pour empêcher la perte du signal, et l'ensemble est enveloppé par une gaine en plastique.

I.7 Les équipements d'interconnexion

L'interconnexion des réseaux est la possibilité de faire dialoguer plusieurs sous- réseau initialement isolés, par l'intermédiaire des périphériques.

I.7.1 La Carte réseau (Network Interface Card)

La carte réseau assure l'interface entre l'équipement ou la machine dans lequel est montée et un ensemble d'autres équipements connectés sur le même réseau.

La carte réseau est le composant le plus important, elle est indispensable, c'est par elle que transitent toutes les données à envoyer et à recevoir du réseau dans un ordinateur.

Chaque carte dispose d'une adresse MAC : c'est l'adresse physique de la carte, Elle permet d'identifier la machine dans un réseau.

I.7.2 Les concentrateurs (Hub)

Le hub, c'est un boitier qui a la fonction d'un répéteur, permettant de concentrer plusieurs lignes en une seules. Il prend les données binaires parvenant d'un port et de les diffuse sur l'ensemble des ports. Un commutateur fonctionne à peu près comme un hub, sauf qu'il est plus discret et intelligent. Il analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les rediriger vers les ports des hôtes destinataires. Ainsi les transmissions seront plus confidentielles et la bande passante sera plus libérée. Un commutateur transmet donc des données aux autres ordinateurs en se basant sur leurs adresses MAC.

I.7.3 Les commutateurs (Switch)

Un commutateur réseau est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique. Il s'agit d'un boitier disposant de plusieurs (entre 4 et 100) ports Ethernet.

Il a la même apparence qu'un concentrateur mais le Switch ne se contente pas de reproduire sur tous les ports chaque trames qu'il reçoit, il peut déterminer sur quel port il doit envoyer une trame, en fonction de l'adresse à laquelle cette trame est destinée.

I.7.4 Les routeurs

Un routeur est un matériel de communication de réseaux informatique, permettant d'acheminer les données dans les directions appropriées, entre les réseaux. Il est chargé de recevoir sur une interface des données sous forme de paquets et de les renvoyer sur une autre en parcourant le meilleur chemin possible. Il travaille au niveau de la couche trois du modèle OSI [5].

I.7.5 Répéteur (repeater)

Le répéteur est un équipement électronique contenant deux interfaces, il permet de régénérer le signal entrant afin d'étendre la distance de câblage d'un réseau local.

I.7.6 Les ponts (bridge)

Ces ont des dispositifs matériels ou logiciels permettant de relier des réseaux travaillant avec les mêmes protocoles. Le pont filtre les données et ne laisse passer que les données destinées aux ordinateurs situer de l'autre coté du pont.

Un pont possède deux connexions à deux réseaux distincts, lorsqu'il reçoit un paquet de données sur l'une de ses interfaces, il analyse l'adresse physique (mac) du destinataire et de

l'émetteur. Si jamais le pont ne connait pas l'émetteur, il stocke son adresse dans une table afin de se remémorer de quel coté du réseau se trouve l'émetteur.

I.7.7 Les passerelles (Gateway)

C'est un système matériel et/ou logiciel qui assure l'interconnexion de plusieurs réseaux de manière à permettre le passage de l'information d'un réseau à un autre. La passerelle est nécessaire pour changer de protocoles (passer du modèle OSI au TCP/IP) [5].

I.8 Le modèle OSI

OSI(Open Système Interconnexion ,) est un modèle de référence théorique décrivant le fonctionnement de communication réseau, élaboré par l'organisme ISO (International Standards Organisation _ L'organisation internationale De Normalisation) en 1984 pour garantir un maximum d'évolutivité et d'interopérabilité en les ordinateurs.

C'est une façon standardisée de segmenter en plusieurs blocs le processus de communication entre deux entités, Chaque bloc résultant de cette segmentation est appelé couche qui est un ensemble de services accomplissant un but précis. Le modèle OSI possède sept couches chaque couches est constituée d'éléments matériels et logiciels et accomplit un rôle particulier. Chaque couche est indépendante des autres et ne peut communiquer qu'avec une couche adjacente.

I.8.1 Les couches du modèle OSI

1. **Couche application :**

La couche applicative fait office d'interface entre l'utilisateur et le réseau, elle permet de transférer des fichiers, de rédiger un mail, établir une session à distance et de visualiser une page web.

2. **couche présentation :**

Cette couche s'occupe de tout aspect lié à la présentation des données, à savoir la syntaxe, la sémantique des informations, le cryptage, le formatage et la compression des données.

3. **La couche session :**

Le but de cette couche est de gérer, sécuriser, et authentifier les communications, elle permet notamment, d'ouvrir et de clore des sessions entre les utilisateurs.

4. **La couche transport** :

La couche transport segmente les données envoyées par le système de l'hôte émetteur et les rassemble en flux de données sur le système de l'hôte récepteur.

Cette couche permet de choisir, en fonction des contraintes de communication, la meilleure façon d'envoyer une information.

La couche de transport modifie également l'en-tête des données en y ajoutant plusieurs informations comme les numéros de ports de la source et de la destination.

5. **La couche réseau :**

La couche réseau se charge du routage des données de la source à la destination et de l'dressage. Dans cette couche aussi, l'en-tête subit une modification.

6. **La couche liaison des données :**

La couche liaison établie une liaison physique entre les hôtes, elle détecte et corrige les erreurs de transmission et fragmente les données en plusieurs trames, qui sont envoyées une par une dans un réseau local.

7. **La couche physique ;**

Cette couche se charge de la conversion des trames en bits et elle effectue la transmission physique des données sur le média.

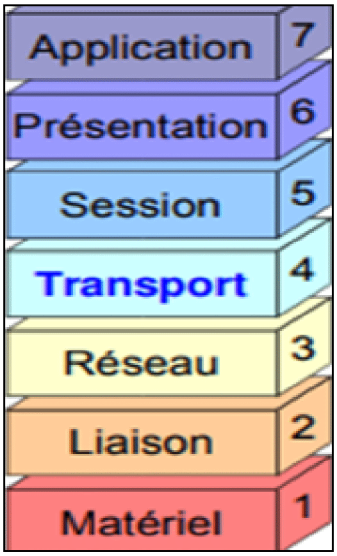


Figure I.11 : Les sept couches du modèle OSI

I.9 Encapsulations des données

Chaque couche a une fonction déterminée, la couche en cours utilise les services de la couche au-dessous d'elle qui, à son tour en offre pour la couche du dessous. Cette corrélation indique bien que certaines informations peuvent se retrouver d'une couche à une autre. Cela n'est possible que grâce au principe d'encapsulation.

L'encapsulation consiste à encapsule, en d'autres terme elle consiste à envelopper les données à chaque couche. Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête (c'est l'ensemble d'informations qui garantit la transmission). Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu puis supprimé c'est la décapsulation. Ainsi, à la réception le message est Dans sont états originales.

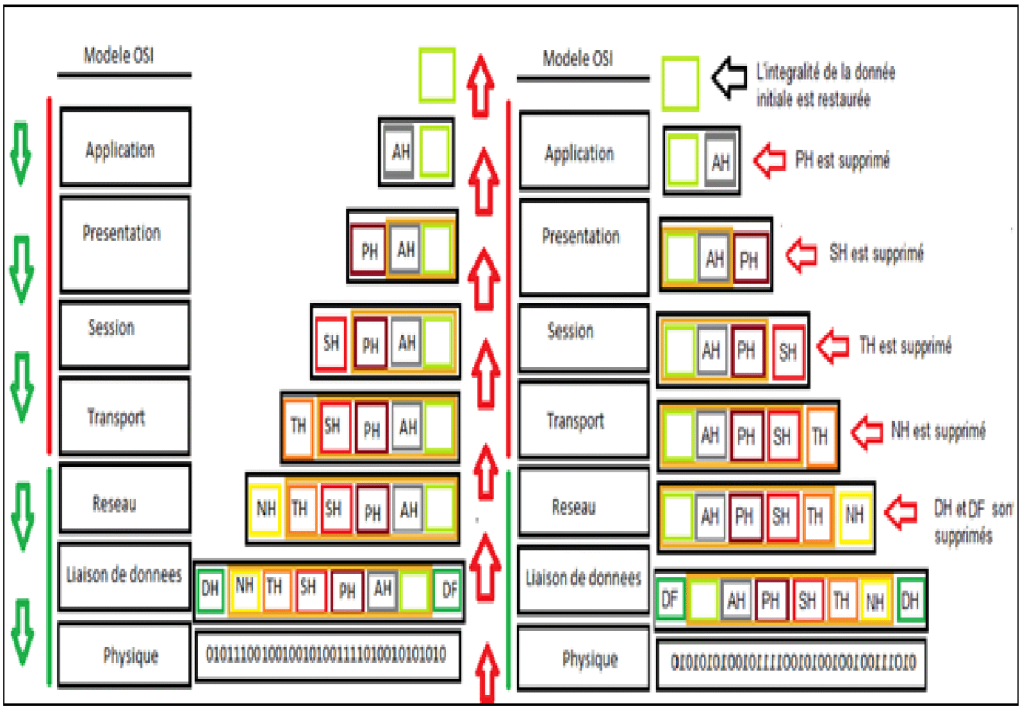


Figure I.12 : Encapsulation des données

I.10 Modèle TCP / IP

I.10.1 Description du modèle TCP /IP

Le modèle TCP/IP (Transmission Central protocole / Internet protocole) fut créé dans les années 1970 par le ministère américain de la défense car avait besoin d'un réseau pouvant résister à toutes les conditions, même à une guerre nucléaire c'est ce problème de conception qui a mené à la création du modèle TCP/ IP et de puis, il est devenu la norme sur laquelle repose internet.

TCP / IP est une suite des protocoles, qui provient des normes des deux protocoles majeurs TCP / IP. Il représente l'ensemble des règles de communication sur internet et se base sur la notion d'adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données.

Ce modèle est conçue pour rependre à un certain nombre de critères parmi les quels :

- Le fonctionnement des messages en paquets.
- L'utilisation d'un système d'adresses.
- L'acheminement des données sur le réseau.
- Le contrôle des erreurs de transmission de données.

Le système de protocoles TCP / IP inspiré du modèle OSI, reprend l'approche modulaire (Utilisation de modules de couches), alors il a été décomposé en plusieurs modules effectuant chacun une tache précise les uns après les autres dans un ordre précis, il est donc constitué de quatre couches, ce sont des couches d'abstraction, autrement dit des couches qui cachent les détails d'implémentation de la communication et leurs noms ne reflètent pas mot pour mot les fonctions qu'elles assurent.

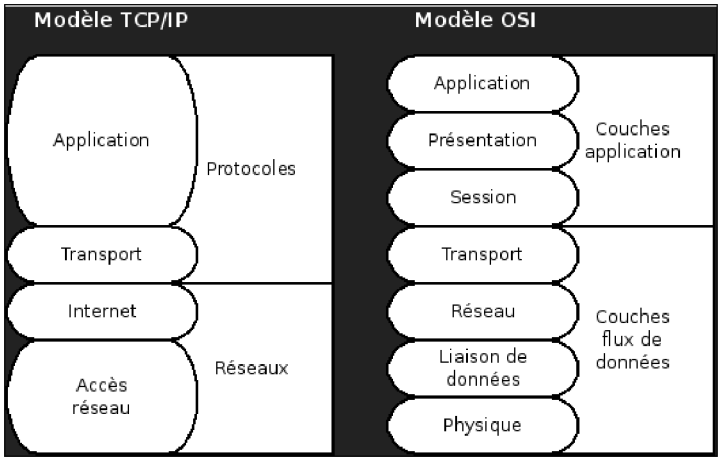


Figure I.13 : Présentation du modèle OSI et TCP/IP

I.10.2 Les couches du modèles TCP /IP

1) La couche application :

Elle contient tous les protocoles de haut niveau comme Telnet pour la connexion à un ordinateur distant, FTP (Fil transfert protocol) pour le transfert des données, SMTP (Simple Mail Transfert) pour les E-mail.

Le modèle TCP/IP regroupe en une seul couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.

2) La couche transport :

Elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaitre l'état de la transmission, elle gère les questions de qualité de service touchant la fiabilité, le contrôle de flux et la connections des erreurs.

Cette couche possède deux implémentations : Le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol).

3) La couche internet :

Cette couche réalise l'interconnexion des réseaux hétérogènes distants sans connexion son rôle consiste à envoyer des paquets sources à partir d'un réseau quelconque de l'inter réseau et à les faire parvenir à destination, indépendamment du trajet et des réseaux traversent pour y arriver. Le protocole qui régit cette couche est le protocole IP (Internet Protocole).

4) La couche d'accès au réseau :

Cette couche se charge de tout ce dont un paquet IP a besoin pour établir une liaison physique, permet d'envoyer et de recevoir physiquement les informations à transmettre sur un média et de spécifier la forme sous la quelle les données doivent être transmises.

I.10.3 Le protocole IP

Le protocole IP est une partie du protocole Internet TCP/IP

Il gère l'adressage et l'itinéraire des datagrammes IP (paquets de données) à travers un ensemble de réseau, afin d'arriver au destinataire approprié.

I.10.3.1 L'adressage IP

Une adresse IP est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque appareil connecté à un réseau TCP/IP.

L'adresse IP est parmi les moyens d'identification et de communication au sein d'un réseau et elle est relative à ce dernier.

I.10.3.1.a Structure d'une adresse IP

L'adresse IP d'une machine est unique, elle a une longueur de 32 bits, composée de quatre champs de 8 bits, qualifiés d'octets. Les octets sont séparés par des points et représentent un nombre en décimal pointée compris entre 0 et 255. Les 32 bits de l'adresse IP sont alloués à l'identificateur réseau (Network ID) et à l'Identificateur de l'hôte dans le réseau (Host ID)

- Network ID : décrit le numéro du réseau local auquel est rattachée la station.
- Host ID : correspond au numéro de la station dans le réseau local lui-même, appelé numéro d'hôte.

I.10.3.1.b Classes d'adresses IP

Il existe cinq classes d'adresses avec la version 4(version courante) selon la valeur du premier octet :

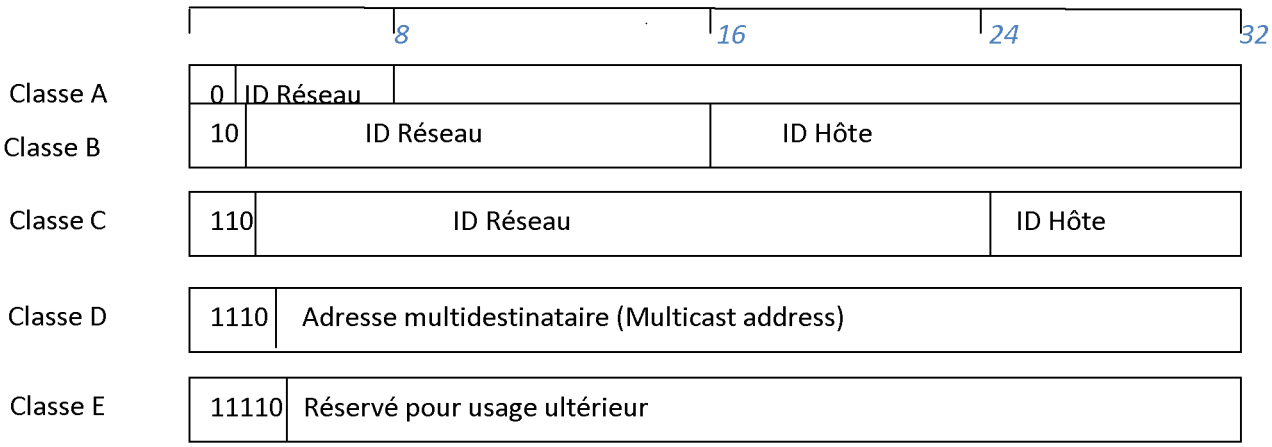


Figure I.14 Classes d'adresse IP

Le tableau ci – après donne l'espace d'adresses possibles pour chaque classe :

Classe	Adresse réseau
A	0.0.0.0 - 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 247.255.255.0

Tableau I.1 : L'espace d'adresse

I.10.3.1.c Le masque sous réseau

Chaque hôte d'un réseau TCP/IP nécessite un masque de sous-réseau. Un masque de sous-réseau est une adresse de 32 bits utilisée pour bloquer ou « masquer » une partie de l'adresse IP afin de distinguer l'ID de réseau à partir de l'ID d'hôte. Cela permet à TCP/IP de déterminer si une adresse IP se trouve sur un réseau local ou un réseau distant. Chaque hôte d'un réseau TCP/IP nécessite un masque de sous-réseau. Il peut s'agir d'un masque de sous-réseau par défaut, utilisé lorsque le réseau n'est pas divisé en sous-réseaux, ou d'un masque de sous-réseau personnalisé, utilisé lorsqu'un réseau est divisé en sous-réseaux.

Dans le masque de sous-réseau, tous les bits correspondant à l'ID de réseau sont à 1. La valeur décimale dans chaque octet est 255. Tous les bits correspondant à l'ID d'hôte sont à 0.

Classes d'dresses	Bits utilisés pour le masque sous - réseau	Notation décimale
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

Tableau I.2 : masque sous - réseau

I.11 Le protocole UDP

Le protocole UDP (*User Datagram Protocol*) est un protocole non orienté connexion de la couche transport du modèle TCP/IP, Le rôle de ce protocole est de permettre la transmission de données de manière très simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port. UDP est utilisé par des applications qui ne transfèrent que des petites quantités de données.

I.12 Le routage

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau afin d'acheminer des données d'un expéditeur jusqu'à un ou plusieurs destinataires. Il est appliqué dans plusieurs réseaux tels le réseau téléphonique, les réseaux de données électronique comme internet et les réseaux de transports.

I.12.1 Le routage IP

Le routage est l'une des fonctionnalités principales de la couche IP, et consiste à choisir la manière de transmettre un datagramme IP. Ainsi un routeur remettra des datagrammes venus d'une de ses interfaces vers une autre, alors que l'ordinateur sera soit l'expéditeur initial, soit le destinataire final d'un datagramme.

I.12.2 Table de routage

Un routeur utilise une table de routage pour déterminer le lieu d'expédition des paquets. La table de routage contient un ensemble de routes. Chaque route décrit la passerelle ou l'interface utilisée par le routeur pour atteindre un réseau donné.

D'un point de vue fonctionnel une table de routage contient des paires d'adresse du type (d,r) ou(d) est l'adresse IP d'une machine on d'un réseau de destination et (r) l'adresse IP du routeur.

I.12.3 Les protocoles de routage

I.12.3.1 Les protocoles de routage interne

- **RIP**

RIP (Routing Information Protocol) est un protocole de type vecteur de distance. C'est-à-dire que les messages échangés par des routeurs voisins contiennent un ensemble de distance entre routeur et destination qui permet de réactualiser les tables de routage. Ce protocole utilise une métrique simple : la distance entre une source et une destination est égale au nombre de sauts qui les séparent, elle est compris entre 1 et15, la valeur 16 réserver pour signaler une route infinie. Ceci implique que RIP est utilisé pour des réseaux de petite taille.

- **OSPF**

OSPF (Open Shortest Path First) est un protocole de type état de lien. Chaque routeur maintient une base d'informations sur les états des autres nœuds. Par rapport à RIP, il offre des mécanismes d'authentification, il peut calculer le plus court chemin selon plusieurs métriques. Pour un domaine de grande taille, OSPF peut fonctionner en mode hiérarchique (en structurant le domaine en deux niveaux) pour minimiser les échanges liés aux états de lien. C'est le protocole le plus déployé actuellement sur Internet.

I.12.3.2 Les protocoles de routage externe

- **BGP**

C'est le protocole de routage externe le plus utilisée, il améliore la capacité d'un système autonome à choisir entre différentes routes et a implémenter des politiques de routage.

I.13 Les protocoles réseaux

- **DHCP**

DHCP (Dynamic Host Configuration Protocol) est un protocole qui permet de configurer automatiquement les paramètres réseau des postes connectés.

- **ICMP**

ICMP (Internet Control Message Protocol) est un protocole dans la suite protocolaire TCP/IP utilisé pour envoyer des messages d'erreurs dans un réseau.

ICMP est le protocole de signalisation des problèmes utilisé par le protocole IP. Son but est de tester la connectivité réseau mais aussi d'apporter une aide au diagnostic en cas de problèmes ou de défaillances.

- **DNS**

Le DNS (Domain Name Service) est le mécanisme qui permet de convertir le nom des machines connectées à internet en adresse IP, il permet aussi aux utilisateurs d'ordinateurs client d'adopter des noms à la place des adresses IP numériques pour identifier les hôtes distants.

- **http**

HTTP (L'Hypertext Transfer Protocol) est un protocole de niveau application suffisamment léger et rapide, pour la transmission de documents distribués et multimédia à travers un système d'information multi-utilisateurs.

- **FTP**

FTP (File Transfer Protocol) s'occupe des transfères des fichiers sur un réseau TCP/IP, il permet une indépendance aux systèmes de fichiers des machines clientes et serveur.

- **ARP**

ARP (Adress Resolution Control) fait correspondre les adresses logiques(IP) avec les adresses physiques (MAC). Chaque machine connectée au réseau possède un numéro d'identification de 48 bits (adresse MAC). Ce numéro est un numéro unique qui est fixé dès la fabrication de la carte en usine. Pour faire correspondre les adresses physiques aux adresses logiques, le protocole ARP interroge les machines du réseau pour connaître leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans une mémoire cache.

- **RARP**

RARP (Reverse Address Resolution Protocol) permet à partir d'une adresse physique (adresse MAC) de déterminer l'adresse logique (adresse IP) d'une machine, il fait l'inverse d'ARP. Ce protocole est essentiellement utilisé pour les stations de travail n'ayant pas de disque dur et souhaitant connaître leur adresse logique.

- **Telnet**

Telnet (TErminaL NETwork ou TELecommunication NETwork) est un protocole de type client-serveur. Il fournit les règles de base pour permettre de relier un client à un interpréteur de commande (serveur), il s'appuie sur une connexion TCP pour envoyer des données.

I.14 Discussion

Ce chapitre est consacré à l'étude générale des réseaux informatiques, les réseaux sont différents et nombreux, chacun d'eux possède ses propres caractéristiques. Les réseaux permettent l'accès à de très nombreuses ressources et c'est pour cela qu'on observe une augmentation de la demande sur l'utilisation des réseaux.

II.1 Préambule

De nos jours l'utilisation de l'internet n'est plus sûre. Souvent, les transmissions de données ainsi que les sites web ne sont pas bien protégés, ils sont vulnérables à de nombreuses attaques intensionnelles ou accidentelles. La sécurité d'un réseau est un niveau de garantie pour que l'ensemble des machines fonctionnent d'une façon optimale. La mise en œuvre d'une politique de sécurité est indispensable au sein d'un réseau afin de le protéger de toute sorte d'attaques malveillantes.

Dans ce chapitre, nous allons présenter les faiblesses et les failles les plus exploitées et les notions de sécurité afin de contrer ces attaques.

II.2 Définition de la sécurité informatique

La sécurité informatique est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre les différentes attaques, ce qui implique la réalisation des fonctions essentielles suivantes :

- Intégrité
- Confidentialité
- Disponibilité
- Non répudiation
- Authentification

II.3 Objectifs de la sécurité informatique

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire Circuler, il représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

La sécurité informatique vise généralement cinq principaux objectifs :

- **L'intégrité**, c'est-à-dire garantir que les données sont bien celles que l'on croit être.
- **La confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.
- **La disponibilité**, permettant de maintenir le bon fonctionnement du système d'information.

- **La non répudiation**, permettant de garantir qu'une transaction ne peut être niée.
- **L'authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

II.4 Politique de sécurité

Une politique de sécurité informatique est un plan d'actions définies pour maintenir un certain niveau de sécurité.

Elle définit les objectifs de sécurité des systèmes informatiques d'une organisation.

Les politiques de sécurité sont mises en vigueur par des procédures techniques ou organisationnelles.

II.5 Les attaques informatiques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable aux attaques.

II.5.1 Définition

Une attaque désigne n'importe qu'elle a action intentionnelle, malveillante consistant à Contrôler les fonctions et les mesures de sécurité d'un système informatique, voler ses confidentielles et changer son comportement afin d'altérer son bon fonctionnement.

II.5.2 Types d'attaque

II.5.2.1 Les attaques directes

C'est la plus simple des attaques à réaliser, le hacker attaque directement sa victime à partir de son ordinateur par des scripts d'attaques faiblement paramétrable. Dans ce cas, il est possible de remonter à l'origine de l'attaque, identifiant par la même occasion l'identité de l'attaquant.

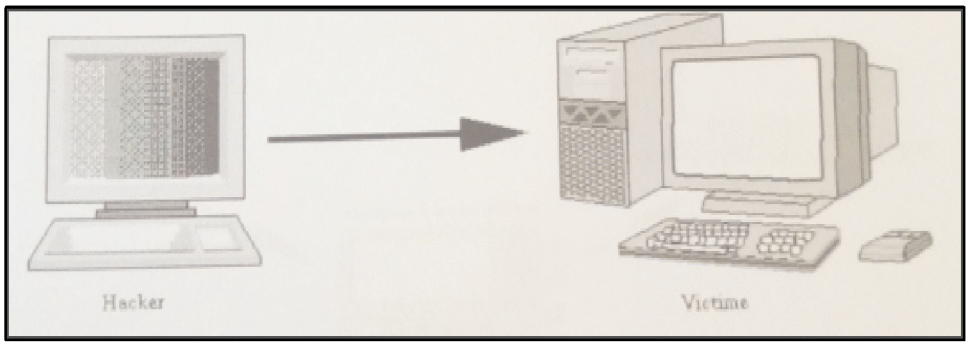


Figure II.15 : Attaque directe

II.5.2.2 Les attaques indirectes

II.5.2.2.a Les attaques indirectes par rebond

Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les attaques par rebond (par opposition aux attaques directes), consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui. (Telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond.

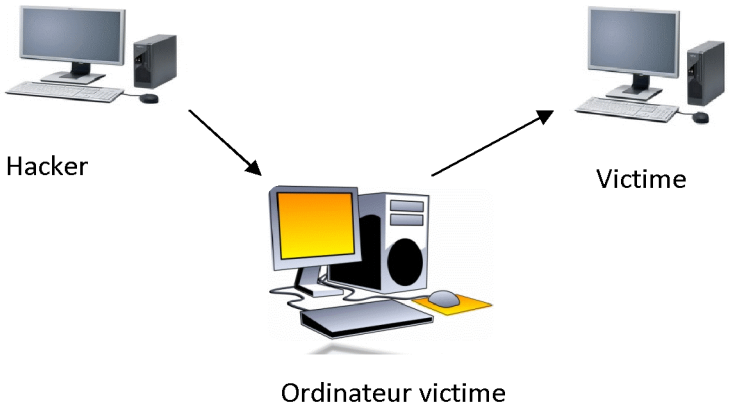


Figure II.16 : Attaque indirecte par rebond

II.5.2.2.b Les attaques indirectes par réponse

Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages que la précédente :

- Masquer l'identité du hacker.
- Exploité les ressources de l'ordinateur intermédiaire.

Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute l'attaquant va lui envoyer une requête, et c'est la réponse à cette requête qui va être envoyée à l'ordinateur victime.

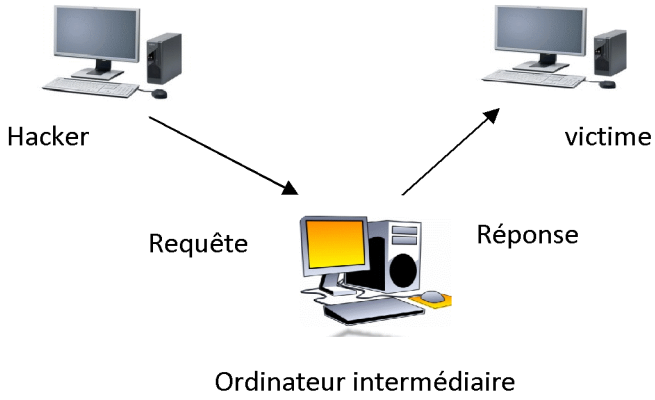


Figure II.17 : Attaque indirecte par réponse

II.5.3 Les étapes d'une attaque

Une attaque ne peut être réalisée en une seule action, elle doit être faite en plusieurs étapes. Les informations recueillies dans une étape vont être utilisés dans l'étape suivante pour faire avancer le processus.

✓ **Identification de la cible**

L'identification est un préalable à toute attaque, elle consiste à collecter des informations sur le système cible. Cette étape permet à l'attaquant de mettre en position des stratégies sur son attaque.

✓ **Scanning**

Le scanner réseau est utilisé pour collecter des informations plus détaillées sur le système cible, pour cela il existe une multitude d'outils et de programmes, la plupart téléchargeables depuis internet, comme par exemple le programme Nmap, qui permet de scanner des ports afin de connaitre la version des logiciels utilisés.

✓ **Obtenir l'accès**

Les informations récoltées et les vulnérabilités exposées au début de l'attaque seront utilisées pour accéder au système cible, au niveau du système d'exploitation ou bien au niveau du réseau.

✓ **Préserver l'accès**

Après avoir accéder au système cible, l'attaquant pourra créer un compte avec des droits d'un utilisateur afin de pouvoir se réinfiltrer ultérieurement, ou bien installer une application de contrôle à distance comme par exemple un chevale de Troie.

✓ **Passer à l'offensive**

Cette étape consiste à passer en action dans le réseau cible, c'est là que l'attaquant exécute ses motivations. Il peut par exemple voler des informations tels que des secrets industriels ou des propriétés intellectuelles, utiliser le serveur pour mener une attaque sur une autre machine, détruire des données ou encore endommager le système d'exploitation dans le but de planter le serveur.

✓ **Effacer les traces**

Lorsque l'intrus a concrétisé son attaque, il va essayer d'effacer les traces de son passage en supprimant les fichiers qu'il a créés et les messages d'erreur possibles qui peuvent avoir été générés par le processus d'attaque.

II.5.4 Les techniques d'attaques

II.5.4.1 Attaques logicielles

Un logiciel malveillant est un programme ou une partie de programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur infecté.

Il existe plusieurs types de logiciels malveillants nous citons les plus répandus [6] :

- **Virus**

Le virus représente la menace sur la sécurité la plus largement connue. C'est un programme informatique malicieux conçu et écrit par des programmeurs mal intentionnés et qui est placé dans des programmes sains. Il est capable d'infecter un autre programme en le modifiant de façon à ce qu'il puisse se reproduire à son tour.

Le virus peut s'avérer particulièrement dangereux et endommager plus ou moins gravement les machines infectées. Le virus peut se répandre à travers tout moyen d'échange de

données numériques comme Internet et notamment par l'intermédiaire des messages électroniques ou de leurs pièces attachées.

- **Vers**

Les vers sont des virus capables de se reproduire et se propager à travers un réseau.
La différence entre un ver et un virus est que le ver n'a pas besoin d'un autre programme pour se reproduire. La particularité de réplication et de duplication du ver peut affecter l'ordinateur et aussi dégrader les performances du réseau en provoquant la saturation de la bande passante.

- **Cheval de Troie**

Un cheval de Troie (trojan horse) est un programme informatique ouvrant une porte dérobée (Backdoor) dans un système, généralement pour permettre à son concepteur de s'introduire dans l'hôte infecté avec l'objectif de détruire ou de récupérer des informations confidentielles. Comme un virus le cheval de Troie est un code nuisible placé dans un programme sain mais qui n'a pas la capacité de se répliquer.

- **Spywares**

Un spyware est un programme conçu dans le but de collecter des informations sur l'ordinateur dans lequel il est installé et de les envoyer à son concepteur.
Les renseignements révéler peuvent être des adresses web des sites visités, des mots –clés saisis dans les moteurs de recherche ou même des informations personnelles, en d'autres termes les spywares peuvent également être une source de nuisances, comme par exemple la consommation de mémoire vive et d'espace disque, plantages d'autres applications...

- **Spam**

Le spam peut être définit comme un courrier électronique non sollicité (souvent de nature publicitaire) envoyer d'une manière intensive à des destinataires. L'objectif principal du spam est de faire de la publicité à moindre prix et cela engendre des inconvénients majeurs, tels que la consultation pénible des messages personnels ou professionnels parmi tant de messages non souhaités, le caractère violent ou dégradant des textes ou images véhiculés par les messages.

- **Bombe logique**

C'est une fonction malveillante cachée dans un programme informatique en apparence utile, qui se déclenchera à retardement lorsqu'une certaine date sera atteinte ou un certain événement survient.

Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise.

II.5.4.2 Attaques réseau

Les attaques réseau s'appuient sur des failles liées aux protocoles ou à leur implémentation. Observons quelques attaques [6] :

- **Scan**

Un scan de port a pour objectif d'indiquer quels sont les ports ouverts sur une machine. C'est une attaque passive qui consiste à récolter des informations pour en déduire les services qui sont exécutés sur la machine cible.

Il existe un nombre important de techniques de scan. Les plus répandues sont :

- le scan simple : Il consiste à établir une connexion TCP complète sur une suite de ports. S'il arrive à se connecter, le port est ouvert sinon, il est fermé. Cette technique n'est bien évidemment pas la meilleure vue qu'elle est facile à détecter.

- Le scan furtif : aussi appelé scan SYN, il n'établit pas complètement la connexion TCP ce qui veut dire pas de commande ACK (acquittement) après avoir reçu l'accord de se connecter.

- Le scan à l'aveugle : avec usurpation d'une machine intermédiaire. Le système attaqué pense que le scan est réalisé par la machine intermédiaire et non par un pirate.

- Le scan avec des programmes de scan : Le plus connue, Nmap, c'est un outil qui scanne de façon automatique toute une plage de ports et permet d'obtenir une foultitude de résultats.

- **Usurpation d'adresse IP (IP spoofing)**

C'est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet à un hacker d'envoyer des paquets IP d'une manière anonyme, alors il fait passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage de paquets.

- **DNS spoofing**

Le protocole DNS met en œuvre les mécanismes permettant de faire la correspondance entre le nom de la machine et son adresse IP. Le but de l'attaque DNS spoofing est de rediriger à leur insu des internautes vers des sites piratés. Il existe deux principales méthodes pour effectuer cette attaque :

DNS ID spoofing : pour communiquer avec une machine, il faut son adresse IP. On peut toutefois avoir son nom, et grâce au protocole DNS, il est possible d'obtenir son l'adresse IP, et cela en envoyant une requête DNS à un serveur DNS un numéro d'identification est placé dans la trame afin que le client et le serveur puissent identifier la requête. L'attaque consiste ici à récupérer ce numéro d'identification pour envoyer des réponses falsifiées au client avant le serveur DNS.

DNS cache poisoning : Les serveurs DNS possèdent un cache permettant de garder pendant un certain temps l'historique de correspondance entre un nom de machine et son adresse IP. L'attaque consiste à corrompre ce cache avec de fausses informations, pour cela le pirate doit avoir sous son contrôle un nom de domaine et le serveur DNS ayant autorité sur celui-ci.

II.5.4.3 Attaques Man in the middle

C'est une redirection complète d'une connexion entre deux machines. Chacun des interlocuteurs croient dialoguer directement avec l'autre mais en vrai le pirate, qui joue le rôle d'un intermédiaire écoute la communication entre eux et falsifie les échanges, ainsi tous les paquets passent par le pirate, qui les retransmet en toute transparence à l'autre machine [6].

Parmi les attaques Man in the middle, on trouve:

- **TCP session hijacking**

Le détournement de session TCP est une attaque qui consiste à intercepter une session TCP initiée entre deux machines afin de la détourner. Dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.

- **ARP spoofing**

L'ARP spoofing ou ARP cache poisoning est une technique utilisée pour attaquer tout réseau local utilisant le protocole de résolution d'adresse ARP. L'objectif de l'attaque consiste à s'interposer entre deux machines du réseau, et de transmettre à chacune d'elles un paquet ARP falsifié indiquant que l'adresse MAC de l'autre machine a été changée, et que la nouvelle adresse est celle de l'attaquant. La finalité est la même que l'IP spoofing mais le travaille s'effectue au niveau de la couche liaison de données.

II.5.4.4 Attaques Déni de service

Une attaque par déni de service (DOS, Denial of service) consiste à saturer les ressources d'un système de façon à empêcher son bon fonctionnement. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.

Parmi les attaques connues permettant de rendre indisponible un service on trouve :

- **UDP Flooding**

Le trafic UDP est prioritaire sur TCP. Le but de UDP flooding est donc d'envoyer un grand nombre de paquets UDP, ce qui va occuper toute la bande passante et ainsi rendre indisponibles toutes les connexions TCP.

- **Attaque par réflexion (smurfling)**

Cette attaque s'appuie sur l'utilisation de serveurs de diffusion (broadcast) qui un serveur capable de reproduire un message et de l'envoyer à toutes les machines présentes sur le même réseau. Le pirate fait des requêtes ICMP ECHO à des adresses de broadcast en spoofant l'adresse source (en indiquant l'adresse de la machine cible) ainsi l'ensemble des réponses des différents ordinateurs vont être routées sur la machine cible.

- **Déni de service distribué**

Le DDOS (Distributed denial-of-service) est un type d'attaque très évolué visant à faire planter ou à rendre muette une machine en la submergeant de trafic inutile. Plusieurs machines à la fois sont à l'origine de cette attaque (c'est une attaque distribuée) qui vise à anéantir des serveurs, des sous-réseaux. D'autre part, elle reste très difficile à contrer ou à éviter, c'est pour cela que cette attaque représente une menace que beaucoup craignent.

II.5.4.5 Intrusion

Signifie pénétration des systèmes d'information ou des réseaux par un intrus, qui est généralement vu comme une personne étrangère au système informatique, qui réussi à prendre le contrôle. Pour pouvoir s'introduire dans le réseau, le pirate à besoin d'accéder à des comptes valides sur les machines qu'il a recensées. Pour se faire différentes méthodes sont employées :

- **L'ingénierie sociale** C'est une technique qui a pour but d'extirper des informations à des personnes sans qu'elles ne s'en rendent compte. Contrairement aux autres attaques, elle ne nécessite pas de logiciel.
- **La consultation de l'annuaire** ou des services de messagerie afin de trouver des noms d'utilisateurs.
- **Les attaques par force brute** consistant à essayer d'une manière automatique différents mots de passe sur une liste de compte.

II.6 Les mécanismes de sécurité

Chaque ordinateur connecté à internet est susceptible d'être victime d'une attaque d'un pirate informatique, alors il faut mettre en place des mécanismes pour assurer la confidentialité, l'intégrité et la disponibilité des services. Parmi ces mécanismes, on peut citer :

II.6.1 La cryptographie

II.6.1.1 Définition

La cryptographie est une science permettant de convertir des informations compréhensibles en informations codées, (non compréhensibles) puis, à partir de ces informations codées, restituer les informations originales.

II.6.1.2 Objectifs

- **L'intégrité des informations** : Une bonne cryptographie doit pouvoir offrir une garantie de l'intégrité des informations. En effet, il ne doit pas être possible de pouvoir modifier des informations cryptées de façon totalement transparente. Un processus de vérification de l'intégrité du message (crypté et en clair) doit être mis en place.
- **L'authentification des correspondants :** Un aspect à ne pas négliger lorsque l'on désire faire des transactions sécurisées, il s'agit de l'authentification des correspondants.

II.6.1.3 Types de cryptographie

- **La cryptographie symétrique** : Egalement appelé cryptage à clé secrète, elle repose sur une clé partagée entre les deux entités communiquant pour chiffrer et déchiffrer le message. L'inconvénient majeur de ce cryptage est le partage de cette clé unique entre les personnes, si la clef secrète est dévoilée, alors n'importe qui pourra consulter les messages chiffrés avec celle-ci.

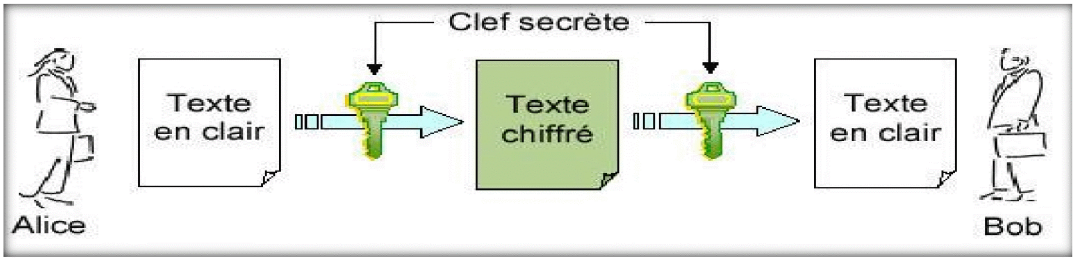


Figure II.18 : Le cryptage symétrique

- **Le cryptage asymétrique**

Il s'agit de clés utilisées dans le cas du chiffrement asymétrique, dans ce cas une clé différente est utilisé pour le chiffrement et pour le déchiffrement.

- Une première clé visible, appelé clé publique est utilisée pour chiffrer un texte.
- Une deuxième clé secrète, appelé clé privé, est connue seulement par le destinataire qui est utilisée pour déchiffrer un texte.

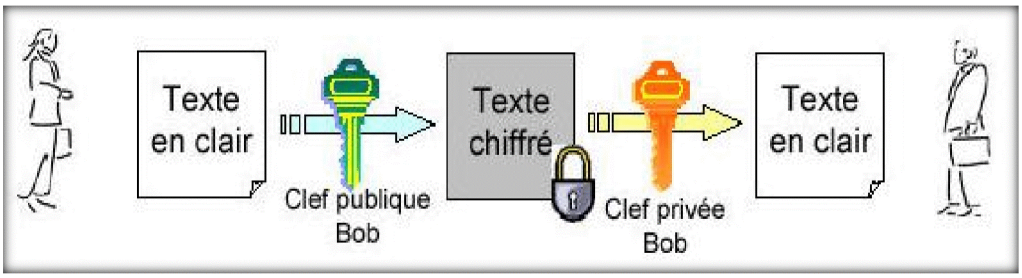


Figure II.19 : le cryptage asymétrique

II.6.2 L'antivirus

Un antivirus est un programme qui a pour but de détecter et d'éradiquer les virus présents dans un ordinateur. Un antivirus vérifie les fichiers et courriers électroniques, la mémoire vive de l'ordinateur, les médias amovibles (clef USB, CD, DVD, etc.), les données qui transitent sur les éventuels réseaux (dont internet), etc.

Pour détecter un virus, l'antivirus se sert de plusieurs techniques parmi elles on trouve :

- **Détection de la signature :** Aussi appelé scanning, c'est la méthode la plus ancienne et la plus utilisée. Elle consiste à analyser le disque dur à la recherche de la signature du virus, qui est un morceau de code du virus qui permet de l'identifier. Chaque virus possède sa propre signature qui doit être connue de l'antivirus. L'avantage de cette technique est qu'elle permet de détecter les virus avant leur exécution en mémoire, dès qu'ils sont stockés sur le disque et qu'une analyse est exécutée, mais elle n'est fiable que si l'antivirus possède une base virale à jour.
- **Le contrôle d'intégrité :** Vérifier l'intégrité d'un fichier consiste à contrôler qu'il n'a pas été modifié ou altéré au cours du temps. Le contrôleur d'intégrité construit une base de données contenant des informations sur les fichiers exécutables du système (la taille, la data et heure de la dernière modification).Ainsi lorsqu'un fichier change de caractéristiques, l'utilisateur est informé.

II.6.3 Le pare-feu (firewall)

II.6.3.1 Définition

C'est un logiciel ou un matériel constituant un intermédiaire entre un réseau interne et un réseau externe. Un pare-feu permet de fermer les ports d'un ordinateurs et de cette manière le rendre invulnérable (ou presque), il peut d'une part restreindre le trafic entrant dans le cas des attaques ou connexions suspectes, et d'une autre part il sert à éviter la fuite non contrôlée d'informations vers l'extérieur [2].

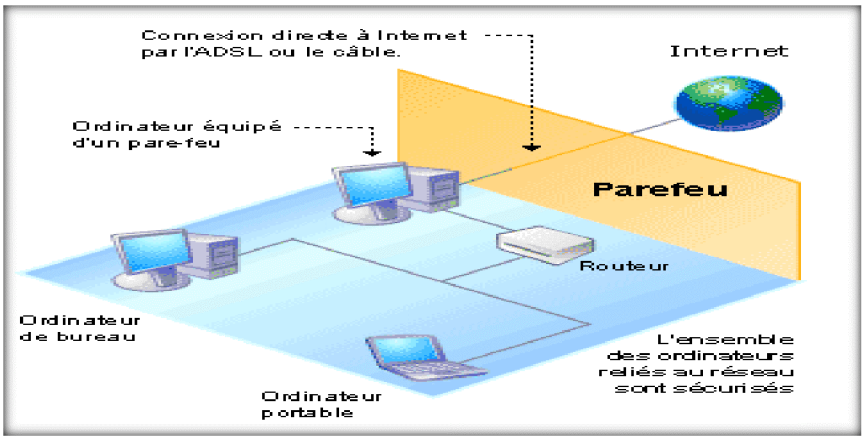


Figure II.20 : le fonctionnement d'un firewall

II.6.3.2 Types de pare-feu

- **Le pare-feu personnel** : C'est un logiciel installé directement sur l'ordinateur de l'utilisateur. Il est simple d'utilisation, il contrôle les données entrantes et sortantes.
- **Le routeur** : il masque l'adresse IP et les ports d'un ordinateur. C'est un périphérique matériel accompagné d'un logiciel. Ce n'est pas un vrai pare-feu dans le sens que ce n'est pas sa fonction première
- **Le pare-feu matériel :** destiné aux entreprises, il est souvent placé entre internet et un réseau d'entreprise, et il assure un bon niveau de sécurité. Ce firewall est généralement peu flexible et sa mise à jour dépend du constructeur.

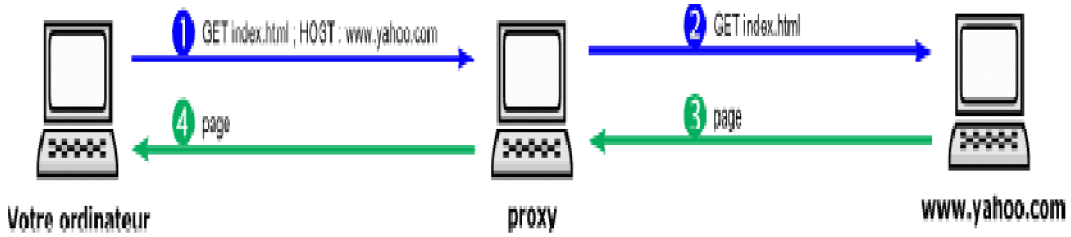
II.6.4 Le proxy

II.6.4.1 Définition

Un serveur proxy qui signifie un serveur mandataire est une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet.

II.6.4.2 Fonctionnement

Lorsqu'un utilisateur désire se connecter à internet en présence d'un proxy, l'ordinateur va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'ordinateur cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, et à son tour, il va la transmettre à l'utilisateur [2].



Figue II.21 : Le fonctionnement d'un proxy

II.6.5 Zone démilitarisée (DMZ)

La DMZ est un sous-réseau séparé du réseau local et isolé de celui-ci et d'internet(ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis internet. Le pare-feu bloque donc les accès au réseau local pour garantir sa sécurité, et les services susceptibles d'être accédés depuis internet seront situés en DMZ.

II.6.6 Les réseaux privés VPN

II.6.6.1 Définition

VPN (Virtual Private Network, réseau privé virtuel) est conçu pour établir des communications sécurisées en s'appuyant sur un réseau existant non sécurisé.

Le principe de cette technologie consiste à créer un chemin (tunnel) virtuel entre deux sites d'une organisation, et parvenir à faire circuler des données de façon cryptée d'un bout du tunnel à l'autre.

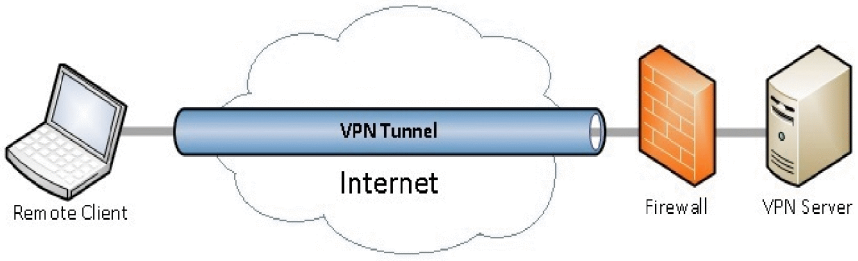


Figure II.22 : VPN dans un réseau

II.6.6.2 Principe de fonctionnement

Le VPN repose sur un protocole de tunnelisation (tunneling), c'est-à-dire un protocole qui permet le passage de données cryptées d'une extrémité du VPN à l'autre grâce à des algorithmes.

Dans le cas d'un VPN établie entre deux machine, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du cote utilisateur (client) et serveur VPN (ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrent les donnés du cotés de l'organisation.

De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en claire au système passerelle, qui va se connecte au réseau distant par L'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée .l'ordinateur distant va alors fournir les données au serveur VPN de son réseau locale qui va transmettre la réponse de façon chiffrée. A la réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur.

II.7 Discussion

Dans ce chapitre nous avons évoqué les risques et les différentes attaques qui scrutent les failles et les moindres faiblesses de sécurité des systèmes réseaux, mais pour faire face à ces attaques, des méthodes de protection ont été mise au point.

La sécurisation d'un réseau qu'il soit filaire ou sans fils est possible par de nombreux moyens matériels et/ou logiciels.

Cependant, en dépit des problèmes de sécurité, les réseaux informatiques continuent préalablement à ce développer, il est donc important de déterminer le niveau de sécurité souhaité afin de mettre en place des solutions adéquates.

III.1 Préambule

Aucun système d'information n'est complètement sûr. Parmi les préceptes connus sur la sécurité informatique se trouve celui énonçant que, pour une entreprise connectée à l'internet, le problème aujourd'hui, n'est plus de savoir si elle va se faire attaquer mais quand cela va arriver, une solution possible est alors d'essayer de repousser les risques dans le temps par la mise en œuvre de divers moyens destinés à augmenter le niveau de sécurité. Pour contrer les menaces d'intrusion, les entreprises se tournent de plus en plus vers les solutions de détection et de prévention d'intrusion. Les systèmes dits "passifs" de détection d'intrusion (IDS pour Intrusion Detection Systems) suivis aujourd'hui par des systèmes dits "actifs" de prévention d'intrusion (IPS pour Intrusion Prevention Systems), ce sont deux techniques permettant de détecter les intrusions et éventuellement de les prévenir.

Une intrusion se définit comme une série d'actions qui tentent de compromettre l'intégrité, la confidentialité ou la disponibilité d'une ressource.

La recherche en détection et prévention d'intrusion est toujours très active, notamment en raison des évolutions rapides et incessantes dans les technologies de l'information et de la communication.

III.2 Système de détection des intrusions (IDS)

On appelle IDS (Intrusion Detection System) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion [1].

III.2.1 Les différentes sortes d'IDS

III.2.1.1 La détection d'intrusion basée sur l'hôte (HIDS)

Les systèmes de détection d'intrusion sur hôte peuvent être classés dans deux catégories selon la provenance des données à examiner :

- Les H-IDS Basés Application : Les IDS de ce type reçoivent les données au niveau application, par exemple, des fichiers logs générés par les logiciels de gestion de bases de données, les serveurs web ou les firewalls. Cette technique souffre

Du fait que les vulnérabilités de la couche application peuvent agir sur l'intégrité de l'approche de détection Basée Application.

- H-IDS Basés Hôte : Les IDS de ce type reçoivent les informations de l'activité du système surveillé. Ces informations sont parfois sous forme de traces d'audit du système d'exploitation, elles peuvent inclure aussi des logs système, d'autres logs générés par les processus du système d'exploitation, et les contenus des objets système non reflétés dans l'audit standard du système d'exploitation.

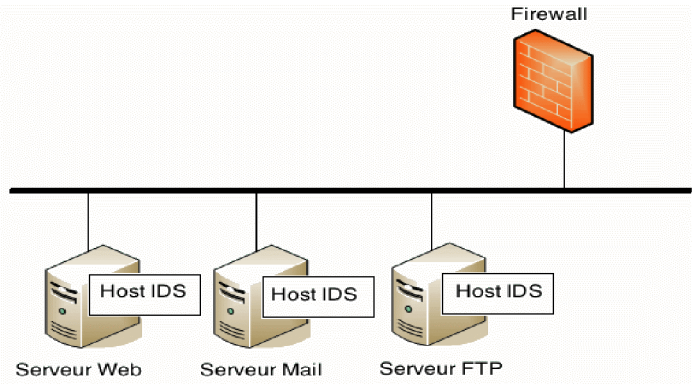


Figure III.23 : système de détection d'intrusion sur hôte (HIDS)

III.2.1.2 La détection d'intrusion réseau (NIDS)

Les N-IDS sont aussi appelés IDS passifs puisque ce type de systèmes se contente d'informer l'administrateur système qu'une attaque a ou a eu lieu, et c'est à ce dernier de prendre les mesures adéquates pour assurer la sécurité du système. Le principe de rendre compte après coup d'une intrusion, a vite évolué pour chercher des IDS capables de réagir en temps réel. Le constat des dégâts ne suffisait plus : il fallait réagir et pouvoir bloquer les trafics douteux détectés.

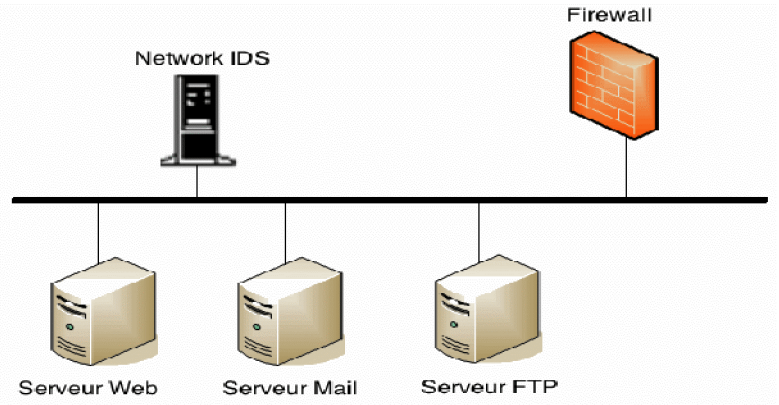


Figure III.24 : système de détection d'intrusion réseau

III.3 Système de prévention des intrusions (IPS)

La prévention d'intrusion est un ensemble de technologies de sécurité ayant pour but d'anticiper et de stopper les attaques. Elle est appliquée par quelques IDS récents. Au lieu d'analyser les logs du trafic, c'est-à-dire découvrir les attaques après qu'elles se soient déroulées, la prévention d'intrusion essaie de prévenir ces attaques. Là où les systèmes de détection d'intrusion se contentent de donner l'alerte, les systèmes de prévention d'intrusion bloquent le trafic jugé dangereux. La prévention d'intrusion est une technique relativement nouvelle par comparaison aux autres techniques. Cette approche fait interagir des technologies hétérogènes : pare-feu, VPN, IDS, anti-virus, anti-Spam, etc.

Les IPS sont souvent considérés comme des IDS de deuxième génération. Bien qu'il s'agisse d'un abus de langage, cette expression traduit bien le fait que les IPS remplacent petit à petit les IDS. En fait, les IPS ont avant tout été conçus pour lever les limitations des IDS en matière de réponse à des attaques, ce sont des IDS actifs : En cas de détection d'une attaque, l'IPS ne se contente pas de notifier l'administrateur réseau mais agit pour bloquer ou corriger les risques d'intrusions. Une action de prévention peut être, par exemple, le blocage de l'adresse IP du présumé attaquant [7]:

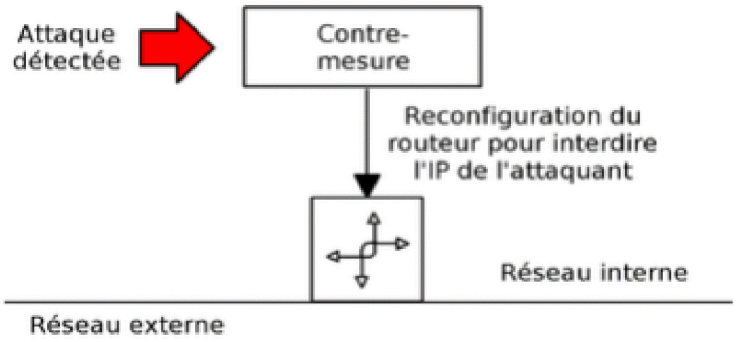


Figure III.25 : démonstration d'une contre

L'IPS se met en ligne sur le réseau, d'où il surveille le trafic et le contenu de la couche 2 jusqu'à la couche 7 et intervient activement en temps réel par limitation ou suppression du trafic jugé hostile, par interruption des sessions suspectes ou par d'autres mesures en réaction à une attaque ou une intrusion. Un IPS s'appuie sur la technologie IDS et cela se traduit par l'analyse des contextes de connexion, l'automatisation d'analyse des logs et la coupure des connexions suspectes.

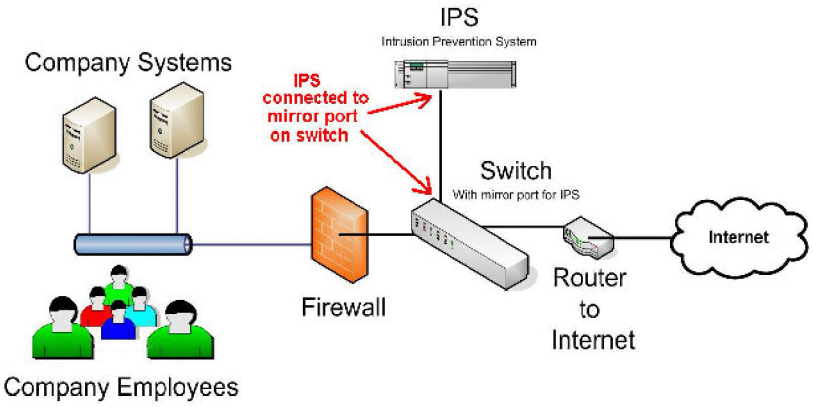


Figure III.26 : exemple d'un IPS dans un réseau

III.3.1 Les caractéristique d'un IPS

1. La technologie IPS peut être déployée en tant que capteur, le capteur IPS peut être l'un des périphériques suivants :
   - Un routeur configurable.
   - Un appareil spécialement conçu pour fournir des services IPS dédiés

- Un module réseau installé dans un appareil de sécurité, un commutateur ou un routeur adaptatif.

2. L'IPS surveille généralement les activités malveillantes en deux endroits :
   - Les activités malveillantes sont surveillées sur le réseau pour détecter les attaques contre un réseau, y compris les attaques contre les hôtes et les périphériques, en utilisant IPS réseau.
   - L'activité malveillante est surveillée sur un hôte pour détecter les attaques lancées depuis ou sur des machines cibles, en utilisant le système de prévention des intrusions hôtes (HIPS). Les attaques basées sur l'hôte sont détectées en lisant des journaux d'événements de sécurité, en vérifiant les modifications apportées aux fichiers système critiques et en vérifiant les registres du système pour les entrées malveillantes.

3. L'IPS utilise les signatures pour détecter les profils de mauvaise utilisation du trafic réseau .Une signature est un ensemble de règles qu'un IPS utilise pour détecter une activité intrusive.

III.3.2 Les fonctionnalités d'un IPS

1) La surveillance du comportement d'application se rapproche des IDS basés sur une application, c'est-à-dire que le comportement de l'application est analysé et noté (quelles données sont normalement demandées, avec quels programmes elle interagit et quelles ressources sont requises, etc.)

2) La création de règles pour l'application, dérivée de la surveillance du comportement d'application, cet ensemble de règles donne des informations sur ce que peut faire ou non une application.

3) La fonctionnalité d'alerte suite aux violations permet d'envoyer une alerte en cas de déviation (c'est-à-dire lorsqu'une attaque est détectée). L'alerte peut aller d'une simple entrée dans un journal à un blocage de ressources.

4) La corrélation avec d'autres événements implique un partage d'informations entre des senseurs coopératifs, afin de garantir une meilleure protection contre les attaques.

5) Bonne citoyenneté sur le réseau. Le système IPS n'est pas un observateur : il fait partie intégrante du réseau. De ce fait, il doit supporter toutes les contraintes que l'organisation peut lui imposer. Il doit être un bon citoyen sur le réseau, en termes de performance, fiabilité et disponibilité. La performance décrit la capacité de l'IPS à laisser le trafic circulé sur le réseau. Une performance médiocre dans un environnement où le trafic est dense causera une baisse de la performance du réseau, voir des pertes de paquets. La fiabilité fait référence à la capacité du système IPS à exécuter correctement ses fonctions, sans interférence avec les autres systèmes présents sur le réseau. La disponibilité relève de la durée d'immobilisation du produit due aux arrêts, aux blocages ou à la maintenance.

III.3.3 Les différentes sortes d'un IPS

III.3.3.1 Systèmes de prévention des intrusions réseaux (NIPS)

Lors de la détection d'une attaque, le système réagit et modifie l'environnement du système attaqué. Cette modification peut être le blocage de certains flux, de certains ports ou l'isolation pure et simple de certains systèmes du réseau. Le point sensible de ce genre de dispositif de prévention est qu'en cas de faux positif, c'est le trafic du système qui est directement affecté. Les erreurs doivent donc être les moins nombreuses possibles car elles ont un impact direct sur la disponibilité des systèmes. En cas de détection de trafic dangereux lié à une intrusion potentielle, l'IPS bloque ce trafic comme un firewall. Néanmoins, ce même trafic se déroulant dans une configuration non dangereuse (pas d'enchaînement spécifique de trafic signalant une intrusion) ne sera pas bloqué. On pourrait comparer un IPS à un firewall «intelligent», qui aurait des règles dynamiques [1].

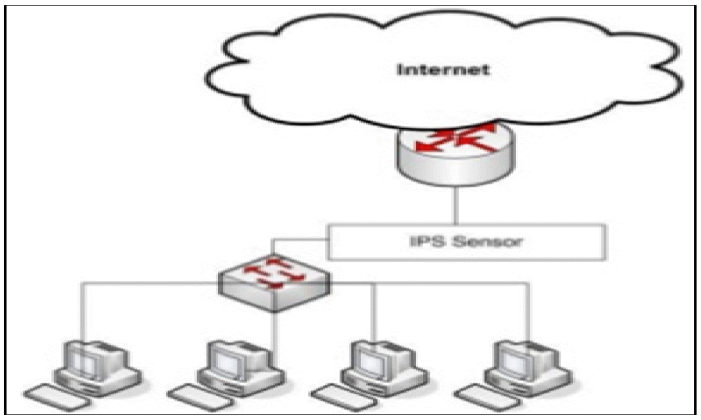


Figure III.27 : système de prévention d'intrusion réseau

III.3.3.1.a Avantages des systèmes NIPS

- **Blocage rapide des intrusions,** Un événement d'intrusion est le début d'un processus d'atteintes aux ressources informatiques d'une organisation, sans parler des responsabilités juridiques potentielles. En intervenant dès la détection, un système IPS bloque rapidement l'intrusion et minimise la durée totale avant que le réseau ne revienne à la normale.

- **Détection précise et fiable.** A l'aide de plusieurs méthodes de détection, et tirant parti de sa position en ligne, le système IPS peut détecter les attaques et intrusions avec une précision et une fiabilité supérieures. Moins dépendant des signatures et davantage des méthodes intelligentes de détection, le système IPS génère beaucoup moins de fausses alarmes. Ainsi le temps et les efforts de l'organisation sont exclusivement concentrés sur les véritables menaces.

- **Prévention active.** Alors qu'un système NIDS prévient simplement de la présence d'un trafic suspect ou anormal, un système IPS peut lancer divers mécanismes de réaction, comme décrit précédemment. Pour les organisations, les coûts d'administration de la sécurité réseau en sont réduits d'autan

III.3.3.2 SYSTEMES DE PREVENTION DES INTRUSIONS SUR HOTE (HIPS)

Aujourd'hui, les menaces évoluent rapidement, il est nécessaire de disposer d'une protection capable d'arrêter les malwares avant la publication d'une mise à jour de la détection spécifique.

Un système de prévention d'intrusions sur l'hôte ou HIPS (Host Intrusion Prevention System) est destiné à arrêter les malwares, avant qu'une mise à jour de la détection spécifique ne soit publiée, en surveillant le comportement du code. La majorité des solutions HIPS surveillent le code lors de son exécution et interviennent si le code est considéré suspect ou malveillant.

HIPS précède l'action des HIDS en ce sens qu'il est « résident », c'est à dire actif en Permanence, dès le lancement du système et jusqu'à son arrêt. Comme un HIDS, il se doit de protéger l'intégrité du système d'exploitation, des logiciels applicatifs lancés, des informations stockées, soit en mémoire RAM soit dans le système de fichiers, les fichiers journaux ou ailleurs, et de vérifier que leur contenu demeure intègre, mais en permanence.
Il doit contrôler instantanément 'tout ce qui change' dans l'ordinateur et veiller à ce que rien ne contourne la politique de sécurité, que l'agression vienne de l'intérieur ou de l'extérieur (Surveillance des activités en réseau intranet ou internet). En plus, un HIDS cherche à détecter des anomalies qui indiqueraient un risque potentiel en vérifiant les activités du PC et prend des mesures protectrices.

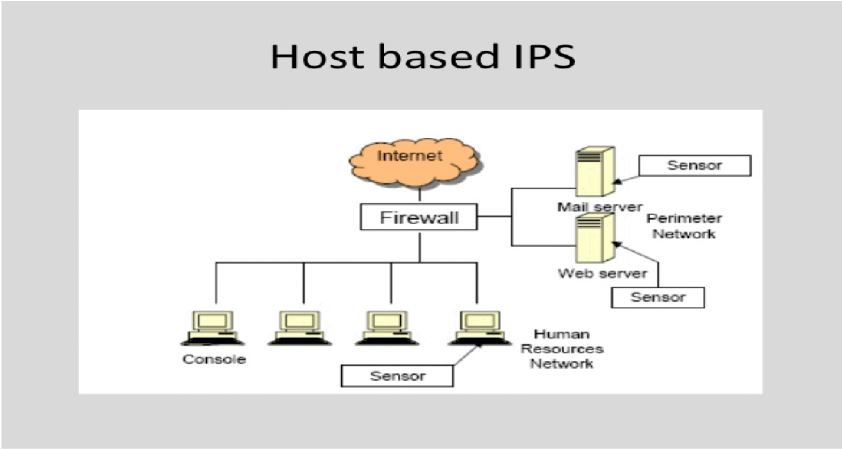


Figure III.28 : système de prévention d'intrusion sur hôte

III.3.4 Les critères d'un IPS

III.3.4.1 La méthode d'analyse

Le premier critère d'un IPS est la méthode d'analyse, deux approches sont possibles :

- **L'approche par scénario** : Cette approche consiste à rechercher dans l'activité de l'élément surveillé les empreintes (ou signatures) d'attaques connues. Ce type d'IPS est purement réactif, il ne peut détecter que les attaques dont il possède la signature. De ce fait, il nécessite des mises à jour fréquentes.

- **L'approche comportementale** : Elle consiste à détecter des anomalies. La mise en œuvre comprend toujours une phase d'apprentissage au cours de laquelle les IDS/IPS vont "découvrir" le fonctionnement "normal" des éléments surveillés. Ils sont ainsi en mesure de signaler les divergences par rapport au fonctionnement de référence. Les modèles comportementaux peuvent être élaborés à partir d'analyses statistiques. Ils présentent l'avantage de détecter des nouveaux types d'attaques. Cependant, de fréquents ajustements sont nécessaires afin de faire évoluer le modèle de référence de sorte qu'il reflète l'activité normale des utilisateurs et réduire le nombre de fausses alertes générées.

Chacune de ces deux approches peut conduire à des faux positifs (détection d'attaque en absence d'attaque) ou à des faux négatifs (absence de détection en présence d'attaque).

III.3.4.2 Fiabilité

Les alertes générées doivent être justifiées et aucune intrusion ne doit pouvoir lui échapper.

III.3.4.3 Réactivité

Un IPS doit être capable de détecter et d'empêcher les nouveaux types d'attaques le plus rapidement possibles; pour cela, il doit rester constamment à jour. Des capacités de mise à jour automatique sont pour ainsi dire indispensables.

III.3.4.4 mise en œuvre et adaptabilité

Un IPS doit être facile à mettre en œuvre et surtout s'adapter au contexte dans lequel il doit opérer.

III.3.4.5 Performance : La mise en place d'un IPS ne doit en aucun cas affecter les performances des systèmes surveillés.

III.4 IPS Suricata

Suricata est un moteur de détection et de prévention de menaces réseau gratuit et ouvert mature, rapide et robuste, le moteur Suricata est capable de détecter l'intrusion en temps réel (IDS), la prévention des intrusions en ligne (IPS), la surveillance de la sécurité du réseau (NSM) et le traitement de la pcap hors ligne.

Suricata inspecte le trafic réseau en utilisant un langage de règles et de signature puissant et étendu.

Le projet et le code Suricata sont détenus et soutenus par Open Information Security Foundation (OISF), une fondation à but non lucratif qui s'est engagée à assurer le développement de Suricata et le succès soutenu en tant que projet open source.

Un IPS à base de signatures, il offre des possibilités intéressantes en termes d'analyse protocolaire et de suivi de l'activité réseau.

III.4.1 Caractéristiques de suricata

- **IDS / IPS**

Suricata met en œuvre une langue de signature complète pour correspondre aux menaces connues, aux violations des règles et aux comportements malveillants. Suricata détectera également de nombreuses anomalies dans le trafic qu'il inspecte. Suricata est capable d'utiliser le jeu de règles Suricata Emerging Threats spécialisé et le jeu de règles VRT .

- **Haute performance**

Une seule occurrence de Suricata est capable d'inspecter le trafic multi-gigabit. Le moteur est construit autour d'une base de code multi-thread, moderne, propre et hautement évolutive. Il existe un support natif pour l'accélération matérielle de plusieurs fournisseurs et via PF_RING et AF_PACKET.

- **Détection automatique des protocoles**

Suricata détecte automatiquement des protocoles tels que HTTP sur n'importe quel port et applique la logique de détection et de journalisation appropriée. Cela aide grandement à trouver des logiciels malveillants.

Lua scripting

Analyse avancée et fonctionnalités disponibles pour détecter des éléments qui ne sont pas possibles dans la syntaxe de la configuration.

III.4.2 Les avantage de Suricata :

Suricata offre de nombreux avantages pour lutter contre les menaces de sécurité actuelles qui se présente comme ceux-ci :

- **Un moteur Open Source:** le pouvoir de la communauté fonctionne bien dans les défenses de sécurité informatique, car une communauté est plus efficace qu'une organisation unique pour capturer les caractéristiques des menaces émergentes.

- **Multi-thread :** Multithreading est la capacité d'un programme ou d'un processus de système d'exploitation à gérer plusieurs demandes, sans avoir plusieurs copies de programmation en cours d'exécution dans l'ordinateur.

L'architecture Multi-thread de Suricata est unique car elle peut supporter des systèmes multi-core et multi-processeurs haute performance. Les principaux avantages d'une conception multi-thread est qu'il offre une vitesse et une efficacité accrues dans l'analyse du trafic réseau et peut également aider à diviser la charge de travail IDS / IPS en fonction des besoins de traitement.

- **Prise en charge de la réputation IP:** en incorporant la réputation et les signatures dans son moteur, Suricata peut repérer le trafic à partir de mauvaises sources connues.

- **Détection automatisée de protocole:** les préprocesseurs identifient automatiquement le protocole utilisé dans un flux réseau et appliquent les règles appropriées, quel que soit le port numérique. La détection automatisée du protocole empêche également les erreurs de l'utilisateur qui sont en fait plus fréquentes.

III.4.3 Comparaison des fonctionnalités de Snort et suricata

III.4.3.1 Définition du moteur Snort

Snort est sans doute le système de détection d'intrusion gratuit le plus utilisé au monde (IDS) et le système de prévention des intrusions (IPS) conçu pour effectuer l'enregistrement des paquets et des analyses de trafic en temps réel des réseaux IP.

Snort est un IDS / IPS basé sur des signatures avec des packages disponibles pour toutes les plates-formes système d'exploitation et possède une communauté mondiale impressionnante d'utilisateurs.

III.4.3.2 Les propriétés de Snort

Il existe plusieurs moteurs du système de détection d'intrusion disponibles pour automatiser et simplifier le processus de détection d'intrusion, et Snort est l'une des meilleures options. Snort est devenu la technologie de détection et de détection d'intrusion la plus largement déployée et de confiance dans le monde. SC Magazine a déclaré que le succès de Snort IDS est dû au fait que les utilisateurs de la communauté de sécurité open source du monde entier peuvent détecter et répondre à des bugs, des vers, des attaques de logiciels malveillants et d'autres menaces de sécurité plus rapidement et plus efficacement que les autres moteurs IDS. En outre, il existe une grande variété de guides de référence disponibles pour l'installation, la configuration, le déploiement et la gestion des capteurs Snort IDS et des signatures basées sur des règles sur un réseau.

En résumé, Snort, un moteur IDS, offre de nombreux avantages:

a) Snort peut être déployé avec succès sur n'importe quel environnement de réseau.
b) Flexibilité et facilité d'utilisation: Snort peut fonctionner sur différents systèmes d'exploitation, y compris Linux, Windows et Mac OS X.
c) Live and Real-Time: Snort peut fournir des informations sur les événements de trafic réseau en temps réel.
d) Flexibilité dans le déploiement: il existe plusieurs milliers de façons dont Snort peut être déployé et une myriade de bases de données, de systèmes d'enregistrement et d'outils avec lesquels il peut fonctionner.
e) Vitesse dans la détection et la réponse aux menaces de sécurité: Utilisé en conjonction avec un pare-feu et d'autres couches d'infrastructure de sécurité, Snort

aide les entreprises à détecter et à réagir aux crackers système, les vers, les vulnérabilités du réseau, les menaces à la sécurité et les agresseurs de politiques qui visent à réduire le réseau et systèmes informatiques.

f) Moteur de détection modulaire: les capteurs Snort sont modulaires et peuvent surveiller plusieurs machines à partir d'un emplacement physique et logique. Snort doit être placé devant le pare-feu, derrière le pare-feu, à côté du pare-feu, et partout ailleurs pour surveiller un réseau entier. En conséquence, les organisations utilisent Snort comme une solution de sécurité pour savoir s'il existe des tentatives non autorisées de piratage dans le réseau ou si un pirate informatique a acquis un accès non autorisé dans le système réseau.

III.4.3.3 Les propriétés de Suricata

Suricata est un système de détection d'intrusion open source c'est le résultat de plus de quatre années de développement menées par Open Information Security Foundation (OISF) et un certain nombre de développeurs organisés pour aider à construire le moteur IDS open source de nouvelle génération. L'objectif de l'OISF est d'apporter de nouvelles idées de sécurité et des innovations technologiques à l'industrie de la détection des intrusions. L'organisme a un but non lucratif, accepte les contributions du gouvernement et du secteur privé, et le financement initial vient des sources gouvernementales, car la principale mission de l'entreprise est de protéger les documents gouvernementaux contre les adversaires étrangers et domestiques. Avec l'aide financière du département américain de la sécurité intérieure, un alternatif multi-thread à Snort a été créé pour aider à sécuriser les réseaux contre les intrusions de sécurité avancées. L'architecture multi-thread de Suricata est unique car elle peut supporter des systèmes multi-core et multiprocesseurs haute performance. Les principaux avantages d'une conception multi-thread est qu'il offre une vitesse et une efficacité accrues dans l'analyse du trafic réseau et peut également aider à diviser la charge de travail IDS / IPS en fonction des besoins de traitement. En plus de l'accélération matérielle (avec les limitations de la carte matérielle et réseau), le moteur est conçu pour utiliser l'augmentation du pouvoir de traitement offerte par les derniers ensembles de puce CPU multi-core.

Bien que Suricata soit encore un produit nouveau et moins répandu par rapport à Snort, la technologie prend de l'ampleur parmi toutes les entreprises et les utilisateurs informatiques. Les performances accrues, le support IPv6 natif, la détection d'anomalie

statistique des modèles multiples, sont quelques-uns des principaux points de vente de Suricata.

Suricata est conçu pour être compatible avec les composants de sécurité réseau existants, Suricata est également conçu pour fonctionner avec les jeux de règles Snort. Par ailleurs, Suricata intègre également des techniques révolutionnaires. Le moteur intègre un normalisateur et un analyseur HTTP (bibliothèque HTP) qui fournit un traitement très avancé des flux HTTP, ce qui permet de comprendre le trafic au 7ème niveau du modèle OSI.

III.4.4 Les règles de suricata

Les signatures jouent un rôle très important dans Suricata. Dans la plupart des cas, les utilisateurs utilisent des jeux de règles existants. Les plus utilisés sont Emerging Threats , Emerging Threats Pro et Sourcefire's VRT .

Une règle / signature se compose des éléments suivants :

- L'action
- L'en-tête
- Les options de règles

Une signature se présente comme ceux- ci :

Figure III.29 : Exemple de signature suricata

III.4.4.1 Action-commande

Toutes les signatures ont des propriétés différentes. L'une d'entre elles est la propriété Action. Celui-ci détermine ce qui se passera lorsqu'une signature correspond. Il existe quatre types d'actions. Un résumé de ce qui se passera lorsqu'une signature correspond et contient une de ces actions:

- Passer

Si une signature correspond et contient un passage, Suricata arrête de numériser le paquet et saute à la fin de toutes les règles (uniquement pour le paquet actuel).

- Ignorer

Cela concerne uniquement le mode IPS / en ligne. Si le programme trouve une signature qui correspond, contenant la suppression, elle s'arrête immédiatement. Le paquet ne sera plus envoyé. Inconvénient: le récepteur ne reçoit pas un message de ce qui se passe, ce qui entraîne un time-out (certainement avec TCP). Suricata génère une alerte pour ce paquet.

- Rejeter

Il s'agit d'un rejet actif du paquet. Le récepteur et l'expéditeur reçoivent un paquet de rejet. Il existe deux types de paquets de rejet qui seront automatiquement sélectionnés. Si le paquet offensif concerne TCP, ce sera un paquet de réinitialisation. Pour tous les autres protocoles, ce sera un paquet d'erreur ICMP. Suricata génère également une alerte. En mode Inline / IPS, le paquet offensant sera également supprimé comme avec l'action 'drop'.

- Alerte

Si une signature correspond et contient une alerte, le paquet sera traité comme tout autre paquet non menaçant, à l'exception de celui-ci, une alerte sera générée par Suricata. Seul l'administrateur système peut noter cette alerte.

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Dans cet exemple la partie rouge, représente l'action.

III.4.4.2 Protocole

Lorsqu' un nom de protocole est trouvé dans une signature, cela indique à Suricata quel est le protocole concerné. Vous pouvez choisir entre quatre paramètres. TCP (pour tcp-traffic), UDP, ICMP et IP. Suricata ajoute quelques protocoles: HTTP, FTP, DNS. Ce sont les protocoles dits de couche d'application ou les protocoles de couche 7.

Par exemple avoir une signature avec un protocole http, Suricata s'assure que la signature ne peut correspondre que si elle concerne le trafic http.

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Dans cet exemple la partie rouge, représente le protocole.

III.4.4.3 Source et destination

En source, des adresses IP sont assignées. Dans le fichier Yaml, des adresses IP pour des variables telles qu'EXTERNAL_NET et HOME_NET sont définies. Ces paramètres seront utilisés lorsque ces variables sont utilisés dans une règle.

Exemple de source et de destination dans une signature :

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Dans cet exemple la partie rouge, représente la source.

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Dans cet exemple la partie rouge, représente la destination.

III.4.4.4 Direction

La direction indique de quelle manière la signature doit correspondre. Presque chaque signature comporte une flèche vers la droite. Cela signifie que seuls les paquets avec la même direction peuvent correspondre.

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Dans cet exemple la partie rouge, représente la direction.

III.5 Discussion

En premier lieu, nous avons donné une idée générale sur les IDS/IPS, leurs définitions ainsi que leurs types. L'IDS/IPS réseau se révèlent être les plus simples à mettre en place étant donné qu'il n'ya qu'une configuration à faire. Ces systèmes ne sont pas infaillibles, la sécurité absolue n'existe pas, mais c'est un investissement raisonnable pour protéger le Système informatique.

Par la suite, on a présenté l'IPS Suricata, ses caractéristiques, avantages et fonctionnalités. C'est un système de prévention d'intrusion open source utilisant des règles de Snort.

IV.1 Préambule

Le but de ce chapitre est de tester l'IPS Suricata sur un exemple d'un réseau qu'on a réalisé durant notre stage au Centre des Systèmes et Réseaux d'information, de Communication, de Télé-enseignement et enseignement à Distance Ex Centre de Calcul de l'université Mouloud Mammeri de Tizi-Ouzou.

Cette application, nous permet de découvrir la capacité de sécurisation de l'IPS Suricata. Nous commençons par l'installation de l'IPS Suricata, puis on passe à la configuration et on termine par des tests des fiabilités.

IV.2 L'architecture réseau existante

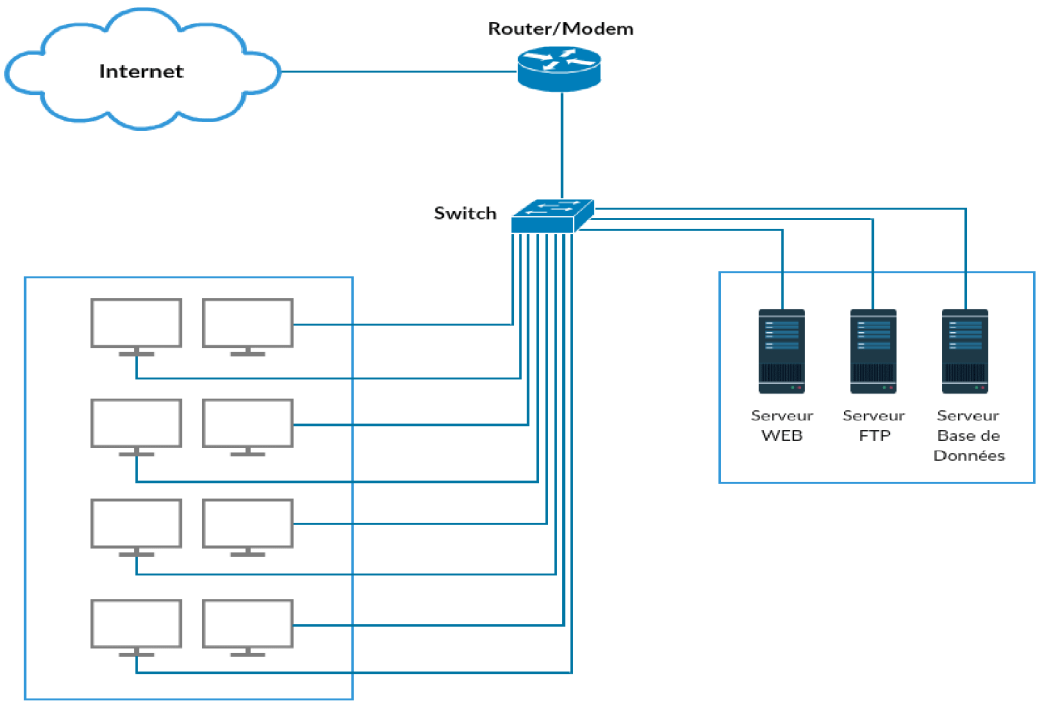


Figure IV.30 : Architecture du réseau de départ

Afin de sécuriser ce réseau, nous avons opté pour l'utilisation de l'IPS Suricata.

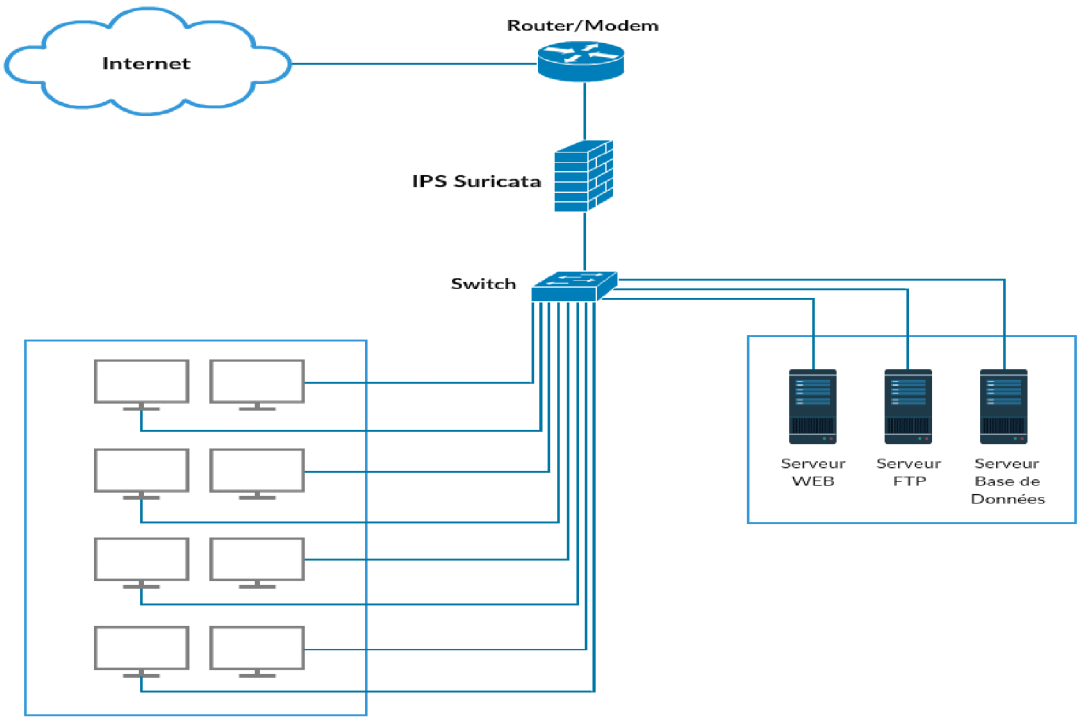


Figure IV.31 : Nouvelle architecture en utilisant l'IPS Suricata

IV.3 Installation de L'IPS Suricata

Avant que Suricata puisse être exploité, il doit être installé, il peut être installé sur différentes distributions à l'aide de paquets binaires comme Ubuntu, Debian, CentOS, Fedora ou bien RHEL.

IV.3.1 Installer les dépendances

Avant de pouvoir construire Suricata sur le système, nous devons d'abord installer plusieurs dépendances requises en exécutant la commande suivante :

```
Sudo apt-get -y install libpcre3 libpcre3-dbg libpcre3-dev \
build-essential autoconf automake libtool libpcap-dev libnet1-dev \
libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libmagic-dev libcap-ng-dev
```

Figue IV.32 : Installation des dépendances

IV.3.2 télécharger Suricata

Par défaut, Suricata fonctionne comme IDS. Si on souhaite l'utiliser comme programme IPS comme dans notre cas, on fait entrez la commande suivante :

```
apt-get -y install libnetfilter-queue-dev
```

Une fois que tous les paquets nécessaires sont installés, on a téléchargé le code source Suricata de http://suricata-ids.org/download/ .La version Suricata utilisé est 3.2.3

- Linux/Mac/FreeBSD/UNIX/Windows Source: suricata-3.2.3.tar.gz
- PGP Signature suricata-3.2.3.tar.gz.sig
- Ubuntu PPA beta (doc)
- Windows (win32) installer: Suricata-3.2.3-1-32bits.msid

Pour télécharger Suricata, on fait entrer ce qui suit:

```
wget http://www.openinfosecfoundation.org/download/suricata-3.2.3tar.gz

tar -xvzf suricata-3.2.3.tar.gz cd suricata-3.2.3
```

Figure IV.33 : Téléchargement de Suricata

IV.3.3 Génération des fichiers de configuration

Générer tous les fichiers nécessaires à l'installation de l'IPS suricata, en utilisant la commande autogen.sh

```
root@debian:/home/user/Documents/suricata# ./autogen.sh
Found libtoolize
autoreconf: Entering directory `.'
autoreconf: configure.ac: not using Gettext
autoreconf: running: aclocal --force -I m4
autoreconf: configure.ac: tracing
autoreconf: configure.ac: adding subdirectory libhtp to autoreconf
autoreconf: Entering directory `libhtp'
autoreconf: running: libtoolize --copy --force
libtoolize: putting auxiliary files in '.'.
libtoolize: copying file './ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt~obsolete.m4'
```

Figure IV.34 : Génération des fichiers

IV.3.4 Compilation et installation du programme

Installation de l'IPS suricata en activant le protocole nfqueue, et pour cela on fait entrer la commande suivante :

```
. /configure --enable-nfqueue --prefix=/usr --sysconfdir=/etc --
localstatedir=/var
```

Figure IV.35 : Commande pour l'installation de l'IPS

ET on continue avec:

```
make && make install-full
```

- **--prefix=/usr/**

  Installle le binôme Suricata dans / usr / bin /.

- **--sysconfdir=/etc**

  Installe les fichiers de configuration Suricata dans / etc / suricata /.

- **--localstatedir=/var**

  Setups Suricata pour ouvrir une session dans / var / log / suricata /. Défault

La figure suivante nous permet de visualiser les commandes utilisées pour l'installation de l'IPS suricata.

```
You can now run "./configure" and then "make".
root@debian:/home/user/Documents/suricata# ./configure --enable-nfqueue --prefix
=/usr --sysconfdir=/etc --localstatedir=/var
checking whether make supports nested variables... yes
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking for style of include used by make... GNU
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for gcc option to accept ISO C99... -std=gnu99
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
```

Figure IV.36 : compilation et installation de l'IPS suricata

Pour s'assurer que la liste existante avec les bibliothèques sera mise à jour avec la nouvelle bibliothèque, il suffit de faire entrer la commande suivante.

```
#sudo ldconfig
```

IV.4 Installation et Gestion de règles

Les signatures jouent un rôle très important dans Suricata. Dans la plupart des cas, les utilisateurs utilisent des jeux de règles existants. Les plus utilisés sont Emerging Threats (ET), Emerging Threats Pro et Sourcefire's VRT .Dans notre travail nous utilisons Emerging Threats(ET).

Il est possible de télécharger et d'installer des règles manuellement, mais il existe un moyen beaucoup plus simple et rapide de le faire. Il existe des programmes spéciaux que nous pouvons utiliser pour télécharger et installer des règles, comme par exemple pulledpork.

Pulledpork est un gestionnaire de règles Snort et Suricata, il peut déterminer la version de Snort et télécharger automatiquement les dernières règles.

Pulledpork doit savoir où de trouve les règles. C'est règles peuvent être trouvées à :

```
https://rules.emergingthreats.net/open/suricata-3.2/emerging.rules.tar.gz
```

Ouvrir pulledpork.conf pour ajouter le lien en entrant :

```
sudo  gedit/ etc / pulledpork. conf
```

IV.4.1 copier les fichiers de configuration

Dans la figure qui suit, pulledpork copie tous les fichiers avec l'extension .conf dans le répertoire /etc/suricata/

```
root@debian:/home/user/Documents/pulledpork/etc# cp -v *.conf /etc/suricata/
‘disablesid.conf’ -> ‘/etc/suricata/disablesid.conf’
‘dropsid.conf’ -> ‘/etc/suricata/dropsid.conf’
‘enablesid.conf’ -> ‘/etc/suricata/enablesid.conf’
‘modifysid.conf’ -> ‘/etc/suricata/modifysid.conf’
‘pulledpork.conf’ -> ‘/etc/suricata/pulledpork.conf’
```

Figure IV.37 : copier les fichiers dans un répertoire

IV.4.2 créer un répertoire pour les nouvelles règles

Exécuter la commande mkdir qui est une commande de gestion de fichiers, elle permet de gérer les fichiers présents sur le Debian GNU/Linux.
Elle est utilisée pour créer des répertoires, comme illustrer dans la figure suivante on a créé le répertoire /iplists dans /etc/suricata/, pour les règles de l'IPS suricata.

```
root@debian:/home/user/Documents/pulledpork/etc# mkdir /etc/suricata/rules/iplis
ts
```

Figure IV.38 : Création du répertoire iplists

IV.4.3 création du fichier default.blacklist

On poursuit avec la création d'un fichier nommé default.blacklist dans le répertoire iplists en exécutant la commande touch.

```
root@debian:/home/user/Documents/pulledpork/etc# touch /etc/suricata/rules/iplis
ts/default.blacklist
```

Figure IV.39 : Création du fichier default.black list

IV.4.4 Modification du fichier de configuration

Exécution de gedit, un éditeur de texte, qui permet d'éditer /etc/snort/pulledpork.conf pour modifier le fichier de configuration pulledpork, car c'est une configuration qui a été faite pour Snort. Comme illustré dans la figure suivante :

```
root@debian:/home/user/Documents/pulledpork# gedit /etc/suricata/pulledpork.cont
```

Figure IV.40 : Modification du fichier de configuration

IV.4.5 Initialisation de pulledpork

Après la modification du fichier pulledpork.conf, on peut lancer l'installation de pulledpork c'est-à-dire la création des règles pour l'IPS suricata.

```
root@debian:/home/user/Documents/pulledpork# ./pulledpork.pl -c /etc/suricata/pu
lledpork.conf

    https://github.com/shirkdog/pulledpork

     _____ ____
     `-----,\    )
      `--==\\  /    PulledPork v0.7.3 - Making signature updates great again!
       `--==\\/
     .-~~~~~-.Y|\\_  Copyright (C) 2009-2016 JJ Cummings
  @_/        /  66\_  cummingsj@gmail.com
    |    \   \   _(")
     \   /-| ||'--'  Rules give me wings!
      \_\  \_\\
 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Use of uninitialized value $Snort_path in -B at ./pulledpork.pl line 1785.
Use of uninitialized value $Snort in pattern match (m//) at ./pulledpork.pl line
 1994.
Use of uninitialized value $Snort in pattern match (m//) at ./pulledpork.pl line
 1998.
Checking latest MD5 for emerging.rules.tar.gz....
Rules tarball download of emerging.rules.tar.gz....
```

Figure IV.41: création des règles pour l'IPS Suricata

Dans le nouveau répertoire de règles, on trouve une classification.config, ce répertoire doit être ajouté dans le fichier suricata.yaml.

```
#sudo  gedit  / etc / suricata / suricata. yaml
```

Figure IV.42 : Ajout de règles

Les règles provenant de Emerging Threats :

```
ET-botcc
ET-botcc.portgrouped
ET-ciarmy
ET-compromised
ET-drop
ET-dshield
ET-emerging-activex
ET-emerging-attack_response
ET-emerging-chat
ET-emerging-current_events
ET-emerging-deleted
ET-emerging-dns
ET-emerging-dos
ET-emerging-exploit
ET-emerging-ftp
ET-emerging-games
ET-emerging-icmp
ET-emerging-icmp_info
ET-emerging-imap
ET-emerging-inappropriate
ET-emerging-info
ET-emerging-malware
ET-emerging-misc
ET-emerging-mobile_malware
ET-emerging-netbios
ET-emerging-p2p
ET-emerging-policy
ET-emerging-pop3
ET-emerging-rpc
ET-emerging-scada
ET-emerging-scan
ET-emerging-shellcode
ET-emerging-smtp
ET-emerging-snmp
ET-emerging-sql
ET-emerging-telnet
ET-emerging-tftp
ET-emerging-trojan
ET-emerging-user_agents
ET-emerging-voip
ET-emerging-web_client
ET-emerging-web_server
ET-emerging-web_specific_apps
ET-emerging-worm
ET-tor
```

Figure IV.43 : les règles de Suricata

IV.4.6 Mise à jour des règles

Après le téléchargement du jeu de règles, place à la mise à jour des règles, en faisant entrer :

```
#sudo pulledpork-C /etc/pulledpork.conf -o /etc/suricata/rules
```

Figure IV.44 : mise à jour des règles

Il est recommandé de mettre à jour régulièrement les règles. Les menaces émergentes sont modifiées quotidiennement, le VRT est mis à jour chaque semaine ou plusieurs fois par semaine.

On peut modifier les règles dans pulledpork.conf en entrant ce qui suit :

```
#sudo gedit pulledpork.conf
```

Figure IV.45 : Modification des règles

Puis on continue avec :

```
modifysid …… rules| “drop”
```

Le mot-clé sid (signature id) donne à chaque signature son propre identifiant. Cet identifiant est indiqué avec un nombre.

Dans la figure suivante comme on peut le voir, on n’a pas effectué des modifications pour les règles :

```
Processing /etc/suricata/enablesid.conf....
        Modified 0 rules
        Skipped 0 rules (already disabled)
        Done
Processing /etc/suricata/dropsid.conf....
        Modified 0 rules
        Skipped 0 rules (already disabled)
        Done
Processing /etc/suricata/disablesid.conf....
        Modified 0 rules
        Skipped 0 rules (already disabled)
        Done
Setting Flowbit State....
        Enabled 111 flowbits
        Done
Writing /etc/suricata/rules/snort.rules....
        Done
Generating sid-msg.map....
        Done
Writing v2 /etc/suricata/sid-msg.map....
        Done
Creating backup at: /suricata/backup/pulled-pork.1500815618.tgz
```

Figure IV.46 : états des règles (aucune modification de règles)

La figure suivante affiche un résumé des règles :

```
Writing /var/log/suricata/sid_changes.log....
        Done
Rule Stats...
        New:-------24327
        Deleted:---0
        Enabled Rules:----18790
        Dropped Rules:----0
        Disabled Rules:---5537
        Total Rules:------24327
IP Blacklist Stats...
        Total IPs:-----7360

Done
Please review /var/log/suricata/sid_changes.log for additional details
Fly Piggy Fly!
```

Figure IV.47 : Le résumé des règles

IV.4.7 Choix de la configuration

Une fois qu'on a installé Suricata et créé les règles, on passe à la compilation de Suricata avec le support NFQ utiliser dans les règles iptables pour envoyer des paquets à Suricata.

Pour vérifier si le NFQ est activé dans Suricata, on fait entrer la commande :

```
suricata  - build - inf
```

Figure IV.48 : vérification de l'activation de NFQ dans Suricata

Il est important de connaître le trafic qu'on souhaite envoyer à Suricata. Pour notre travail nous avons opté pour le premier scénario, le mode passerelle.

- Suricata peut s'exécuter sur une passerelle et est destiné à protéger les ordinateurs derrière cette passerelle, alors on rencontre le premier scénario : forward_ing

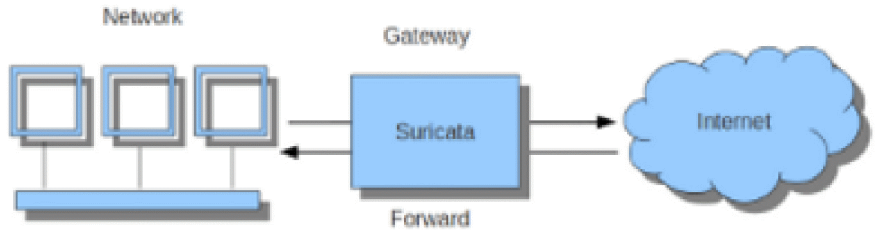


Figure IV.49 : le cas où Suricata est une passerelle

La règle la plus simple dans le cas du scénario de passerelle pour envoyer du trafic à Suricata est :

```
sudo  iptables  - I  FORWARD  - j  NFQUEUE
```

Figure IV 50 : règle iptable dans le cas de la passerelle

- Suricata protège l'ordinateur en cours d'exécution, c'est le deuxième scénario : hôte.

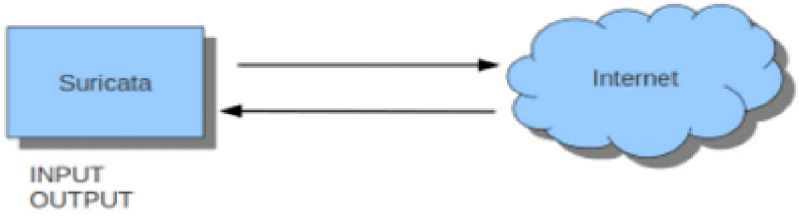


Figure IV.51: le cas où Suricata est l'hôte

Dans le cas de la situation de l'hôte, il s'agit de deux règles iptables, comme le montre-la Figure suivante :

```
sudo  iptables  - I  INPUT  - j  NFQUEUE
sudo  iptables  - I  OUTPUT  - j  NFQUEUE
```

Figure IV.52 : le cas où suricata est l'hôte

IV.5 Test

Dans le but de vérifier l'efficacité le l'IPS Suricata, on a effectué les tests suivants :

La variable HOME_NET, pour laquelle on a attribué l'adresse IP de notre machine virtuelle, qui se présente comme ceci :

```
HOME_NET : '' [192.168.1.250 /24]''
```

Figure IV.53 : attribution d'adresse IP

IV.5.1 Faire un Ping

Le premier test qu'on a effectué après l'activation de suricata est un Ping.

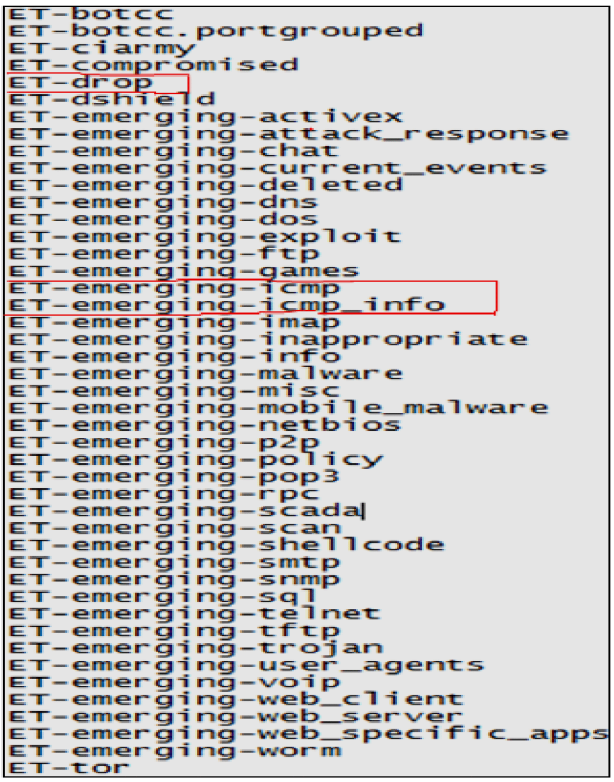


Figure IV.54 : règles spécifiques du Ping

Pour effectuer un Ping vers la machine virtuelle, il faut d'abord mettre les règes icmp Et icmp-info dans le fichier dropsid.conf

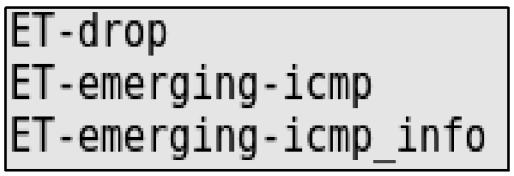


Figure IV.55 : Les règles à copier dans dropsid.conf

La figure suivante nous montre le Ping vers la machine virtuelle :

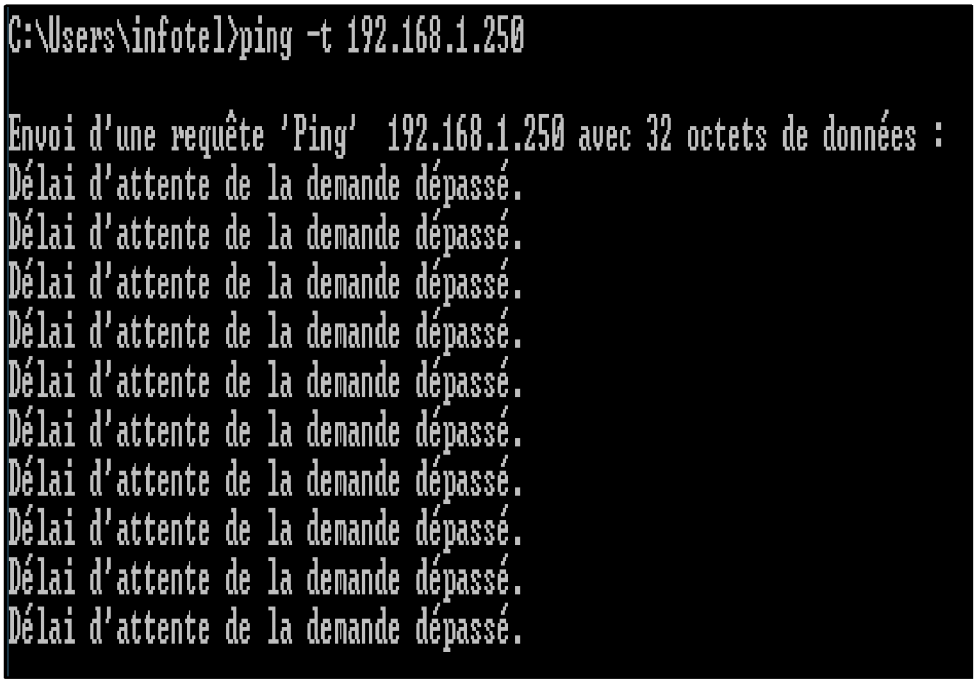


Figure IV.56 : effectuer le Ping

Le blocage du Ping est réussit, comme on peut le voir dans cette figure :

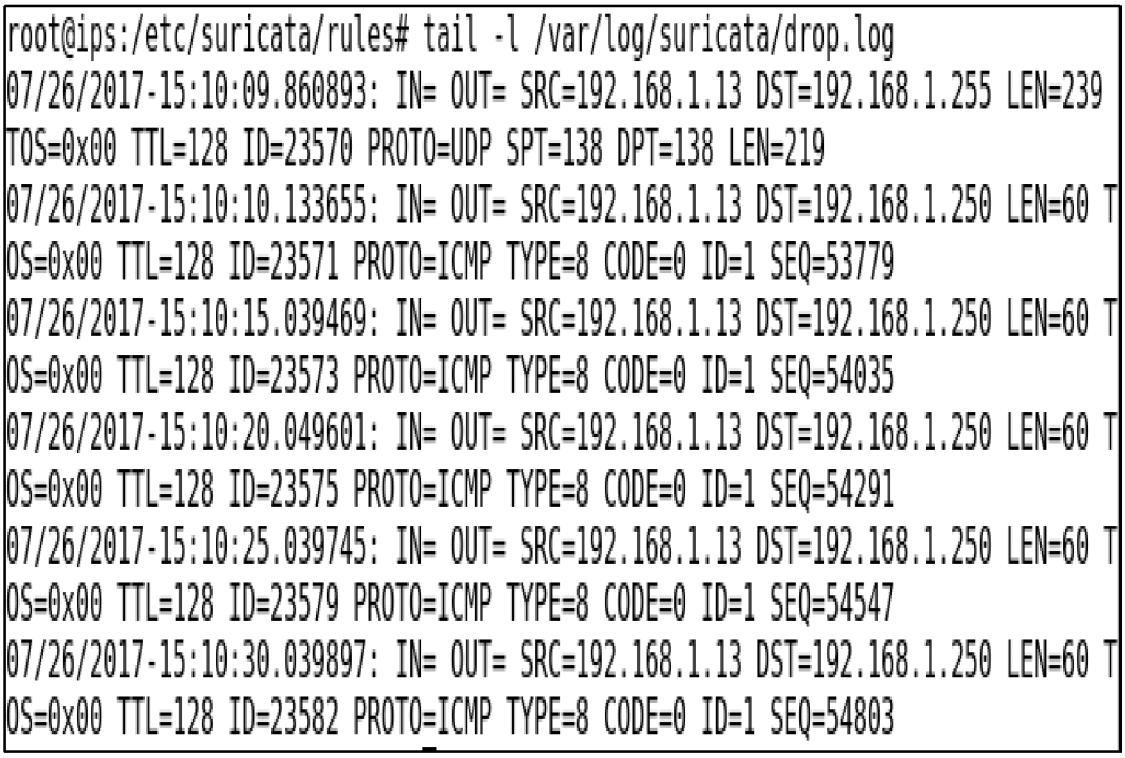


Figure IV.57 : Résultat du Ping

Dans la figure suivante comme on peut le voir, après avoir fait le Ping, le protocole ICMP est bloqué, 48 règles sont modifiées dans le fichier dropsid.conf

Figure IV.58 : états des règles (modification de 48 règles)

IV.5.2 effectuer un test de scan réseau

Pour notre deuxième test on a effectué un scan réseau pour la machine virtuelle, et pour celle on a utilisé Nmap qui est une source libre et gratuite pour la découverte de réseau et l'audit de sécurité.

Nmap utilise des paquets IP bruts de manières nouvelles pour déterminer quels hôtes sont disponibles sur le réseau, quels services (nom et version de l'application) que ces hôtes offrent, sur quels systèmes d'exploitation ils fonctionnent, quel type de filtre / firewalls de paquets sont utilisés…etc.

Afin de bloquer le scan, suricata doit copier la règle ET- emerging-scan dans le fichier dropsid.conf.

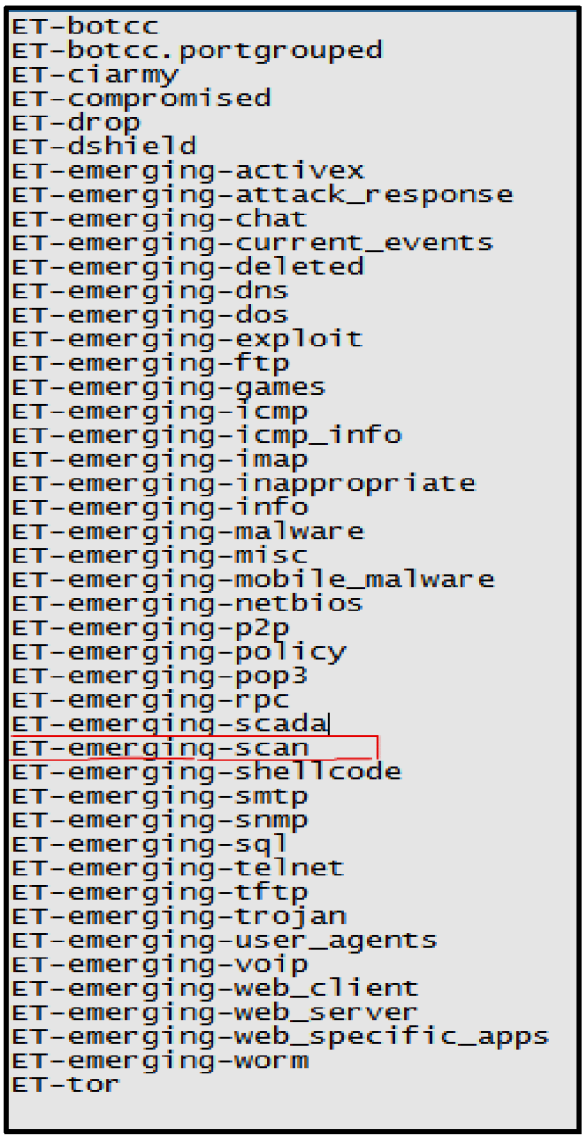


Figure IV.59 : La règle spécifique du scan

Le scan réseau de la machine virtuelle a été lancé, comme on peut voir dans la figure qui suit l'adresse IP de notre machine virtuelle, mais le scan a été aussi vite boqué par l'IPS suricata.

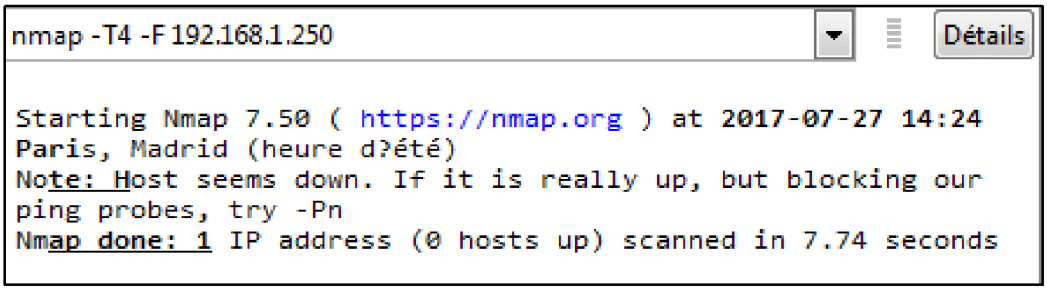


Figure IV.60 : Blocage de scan

IV.5.3 effectuer un test pour un trojan

Pour notre troisième test on a utilisé Le fichier de test Eicar, qui est une chaîne de caractères, écrite dans un fichier informatique, destiné à tester le bon fonctionnement des logiciels antivirus.

Afin de bloquer l'accès vers www.eicar.org, suricata doit copier la règle ET- emerging-trojan dans le fichier dropsid.conf.

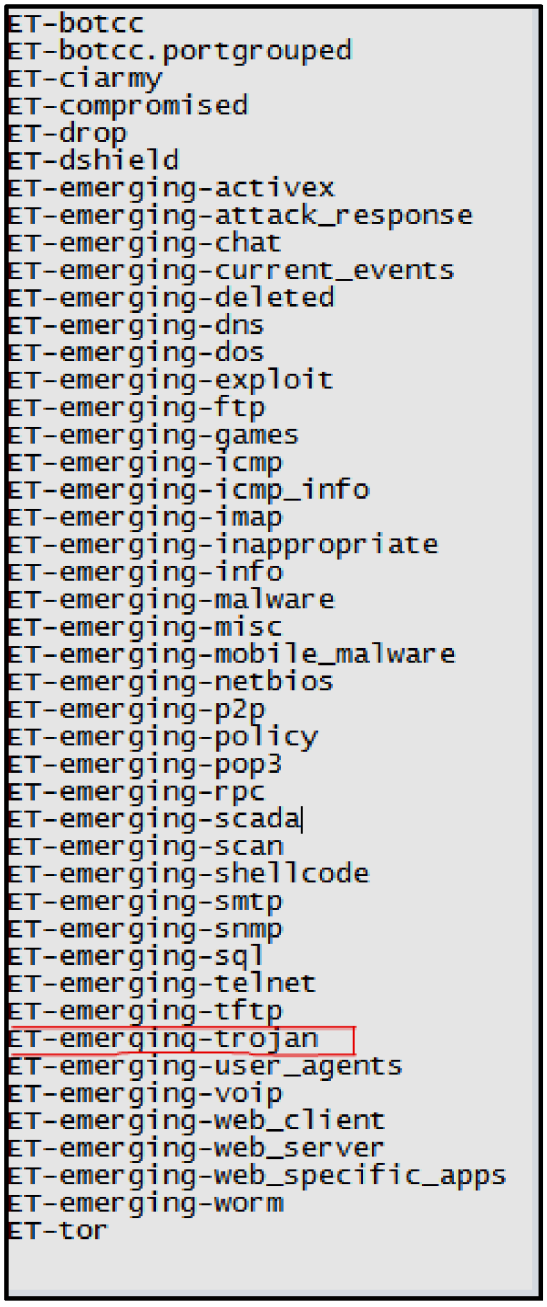


Figure IV.61: La règle spécifique du trojan

Le navigateur de la machine virtuelle a fait un Ping vers www.eicar.org, et on peut voir dans la figure suivante que le Ping est bloqué.

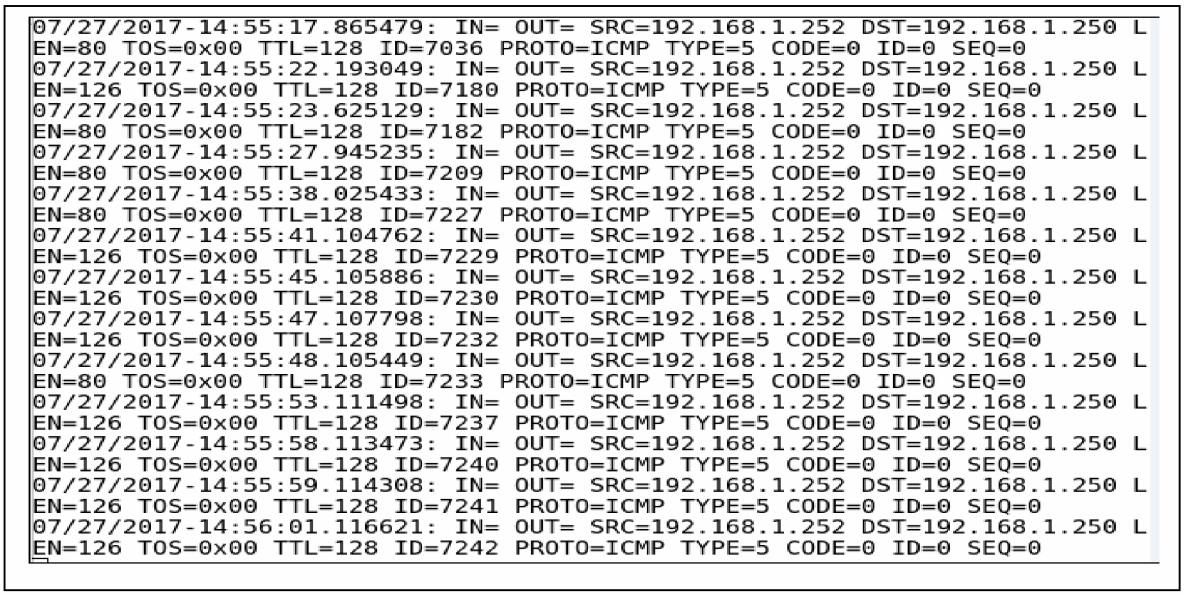


Figure IV.62 : Résultat du Ping vers le site eicar.org

Comme on peut le voir dans la figure suivante le navigateur de notre machine virtuelle n'arrive pas à se connecter à www.eicar.org , car ce lien a été bloqué par l'IPS suricata.

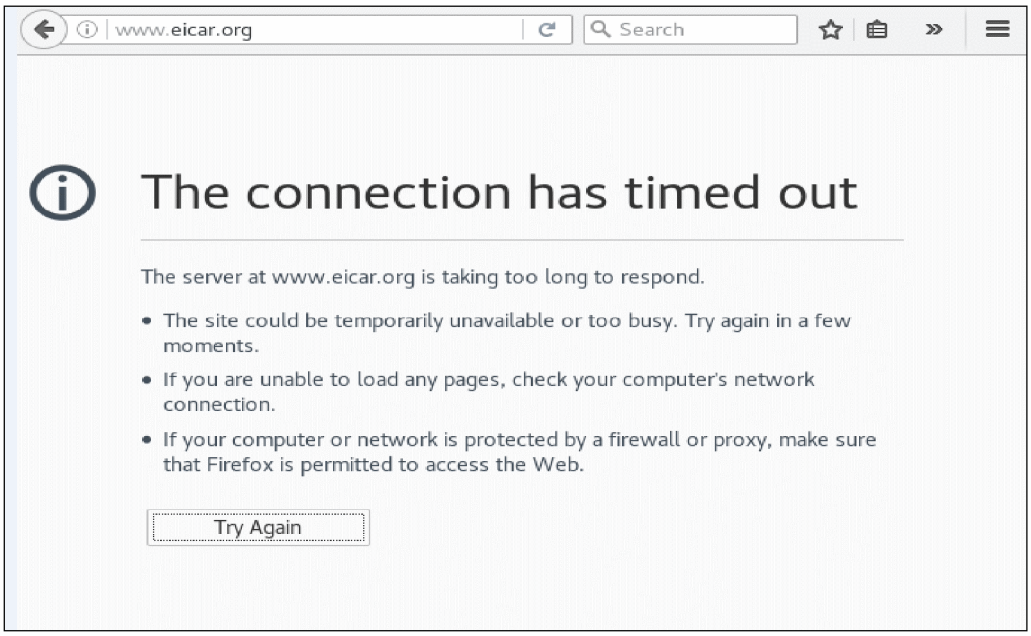


Figure IV.63 : échec de connexion à eicar.org

IV.6 Discussion

A la fin de ce projet, nous pouvons dire qu'on a réussit à sécuriser le réseau, en utilisant l'IPS Suricata, qui a pu prévenir et bloqué les attaques. Alors on peut déduire que l'IPS Suricata est fiable, il a su contré aux différentes attaques, mais il reste à tester son efficacité dans un contexte de production.

Avec la multiplication des réseaux d'entreprise et l'importance croissante d'Internet au niveau consommateur, les entreprises cherchent à se rendre de plus en plus présentes et visibles sur Internet. Cette présence sur Internet, que ce soit à travers des sites Internet, de la vente en ligne ou même les courriels se fait souvent au détriment de la sécurité du ou des réseaux de l'entreprise et de ses données. Comme nous l'avons vu, de nombreux systèmes permettent de renforcer la sécurité des réseaux d'entreprise. Que ce soit les firewalls, qui filtrent l'entrée des réseaux, les IDS qui écoutent le trafic réseau de manière furtive afin de repérer des activités anormales, ou même les IPS qui agissent pour bloquer ou corriger les risques d'intrusions.

Dans notre projet, une architecture a été choisie afin de la sécurisée avec un IPS Suricata. D'abord on a installé l'IPS Suricata, puis on la configuré en mode passerelle afin de filtrer tout les paquets entrants et sortants, et à la fin on a effectué des tests (des attaques) pour tester le bon fonctionnement de l'IPS.
Les résultats ont été satisfaisants prouvant que l'IPS Suricata a sécurisé le réseau.

Cependant, nous avons pu constater que les IPS ne sont pas encore suffisamment efficaces pour être utilisés dans un contexte de production, notamment en ce qui concerne les faux positifs et les faux négatifs, et aussi qu'ils restent lourds à administrer. Ils sont actuellement utilisés dans des environnements de tests afin d'évaluer leurs fiabilités.

Néanmoins, cette technologie est amenée à se développer dans les prochaines années du fait des besoins de sécurité croissants des entreprises et de l'évolution des technologies.

[1] Yousef FARHAOUI, « Evaluation des Systèmes de Détection et de Prévention des Intrusions et la Conception d'un BiIDS », thèse de doctorat, Faculté des Sciences d'Agadir, 2012.

[2] Elie MABO, « La sécurité des systèmes informatiques » (Théorie), support de cours, 2010

[3] M.BALLASTERONS, « les technologies sans fil », ED Eyrolles, juin 2002.

[4] Guy PUJOLLE, » les réseaux sans fils », ED Eyrolles, 5éme édition, 2006.

[5] G.PUJOLLE, O.SALVATORI, « Les réseaux et télécommunication », édition Eyrolles, paris, 2004.

[6] Jean-François PILLOU, Jean-Philippe Bay, « Tout sur la sécurité informatique », 2éme édition, Edition Dunod, Paris, 2009.

[7] Etienne Duris, « NT réseaux-IDS et IPS », support de cours, 2003-2004.

Site Web

- https://www.securiteinfo.com/conseils/introsecu.shtml
- https://suricata-ids.org (consulté le 25/08/2017)

I .Mise en place d'une machine virtuelle

La virtualisation est une technique consistant à faire fonctionner en même temps, sur un seul ordinateur, plusieurs systèmes d'exploitation comme s'ils fonctionnaient sur des ordinateurs distincts, à l'aide d'un logiciel de virtualisation appelé VMware Workstation.

- **VMware Workstation 12**

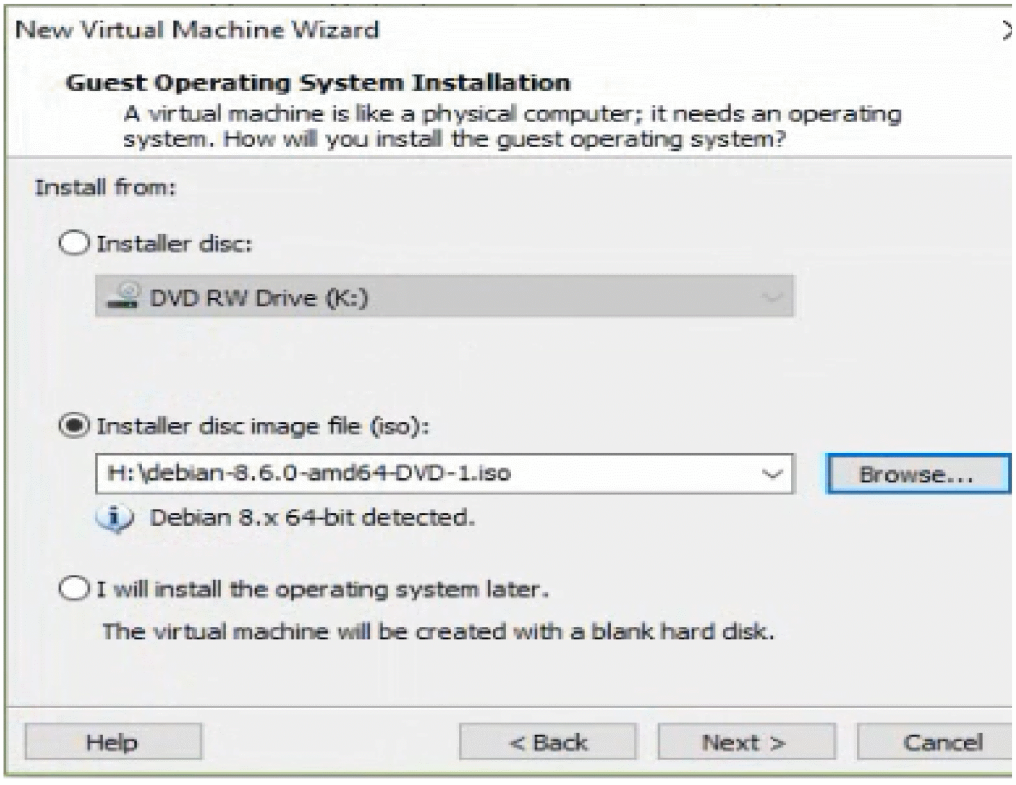
C'est la version station de travail du logiciel. Il permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique.

- **Installation de Debian 8.6 sur la VMware Workstation 12 :**

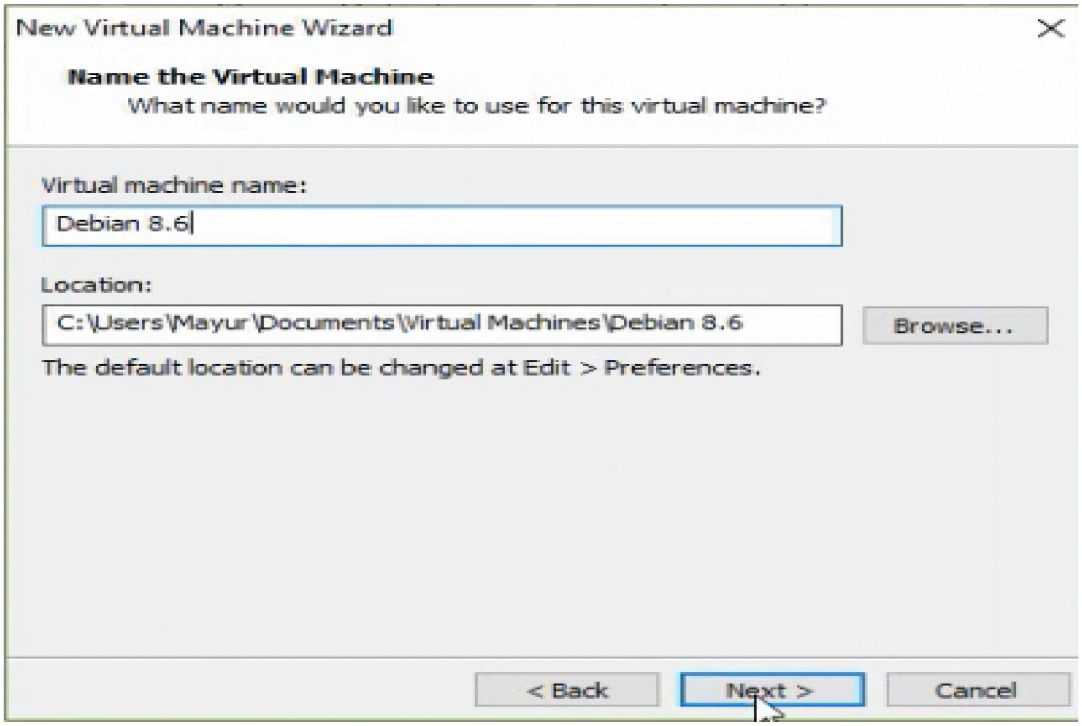
1. Lancer le programme VMware Workstation 12 et sélectionner dans le menu présenté sur l'interface si dessous, créé une nouvelle machine virtuelle.

2. Sélectionner le premier choix « Typical (recommended). »

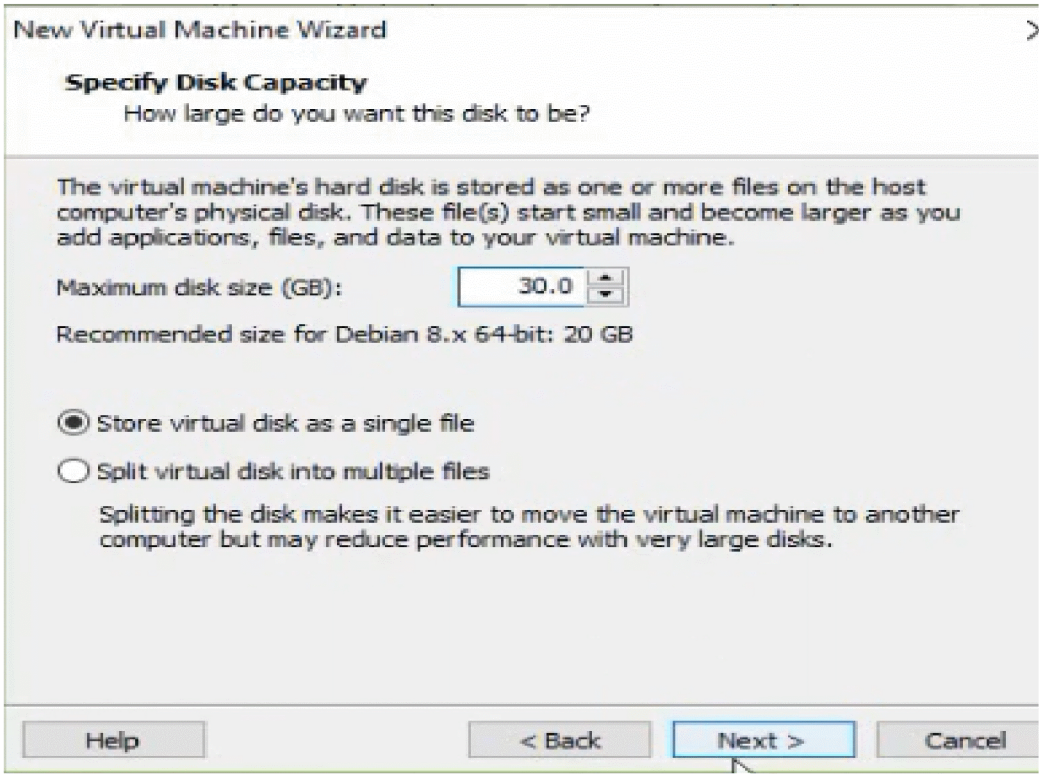
3. Choisir l'option «installer un fichier image ISO » et télécharger l'image existante sur notre machine, puis cliquer sur Next.



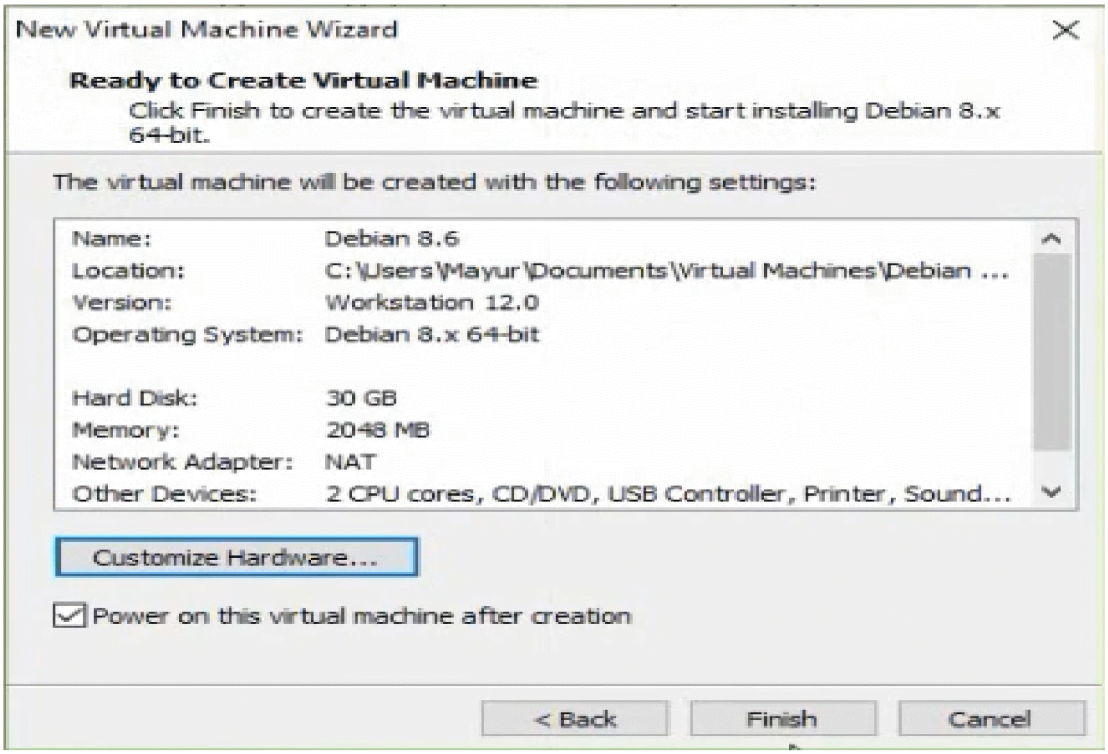
4. Donner un nom à la nouvelle machine crée puis cliquer sur NEXT.



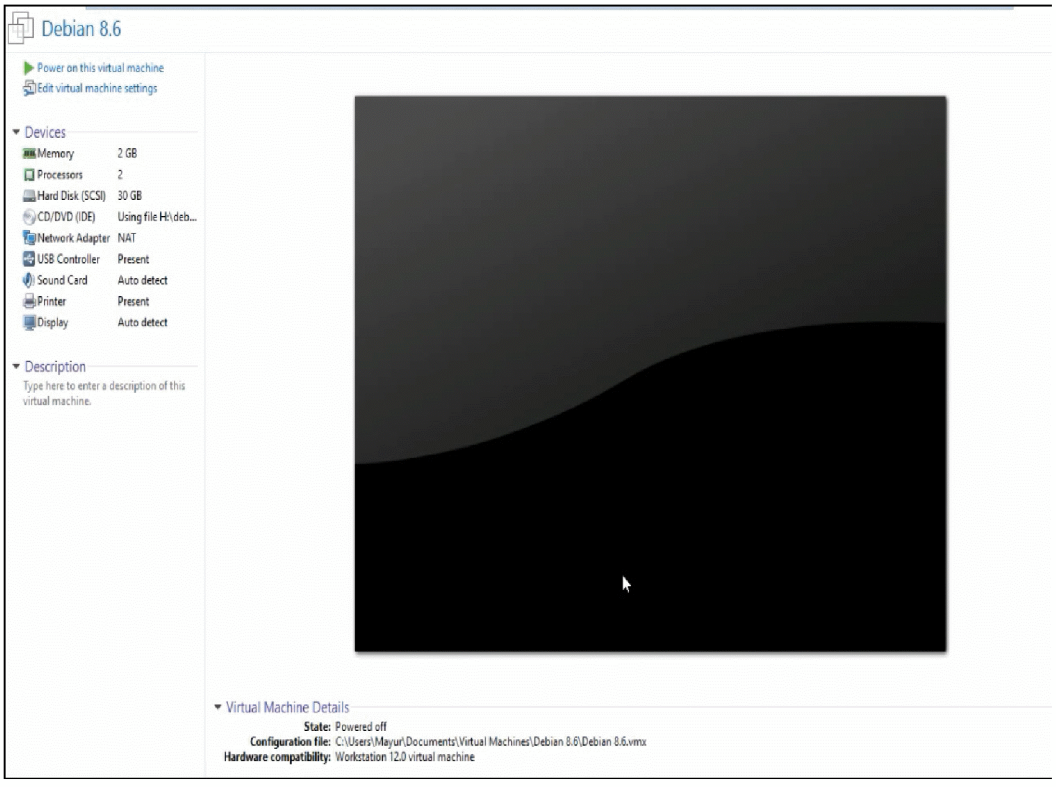
5. Choisir une capacité pour le disque, 30GB recommandé



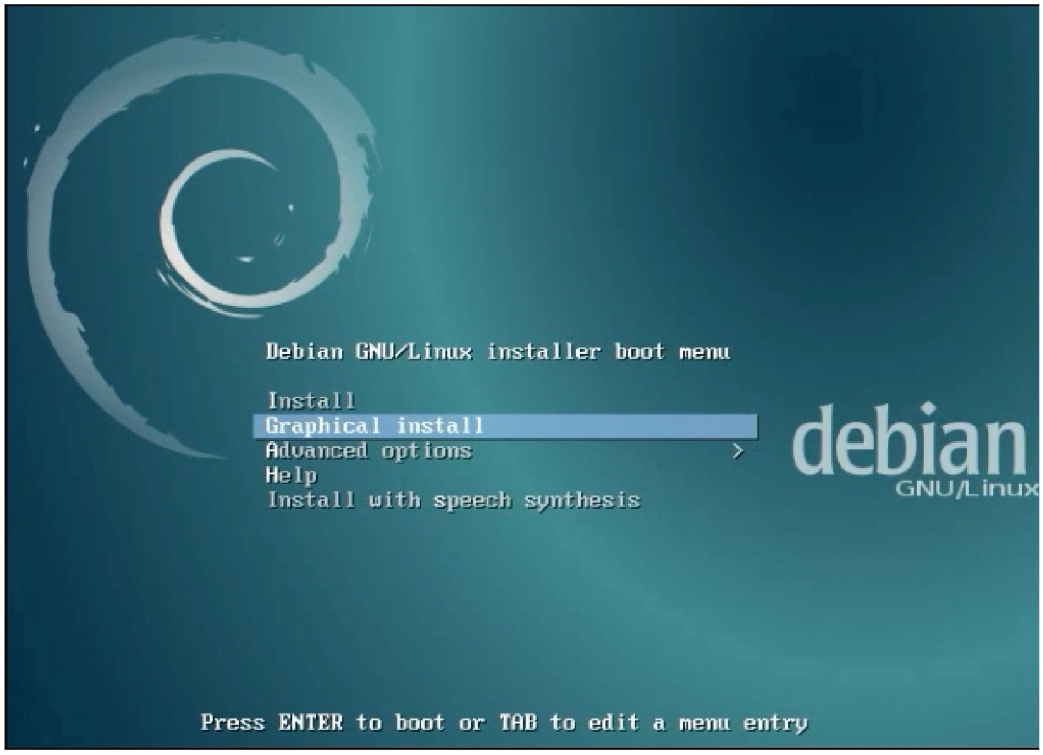
6. Cliquer sur Finish .



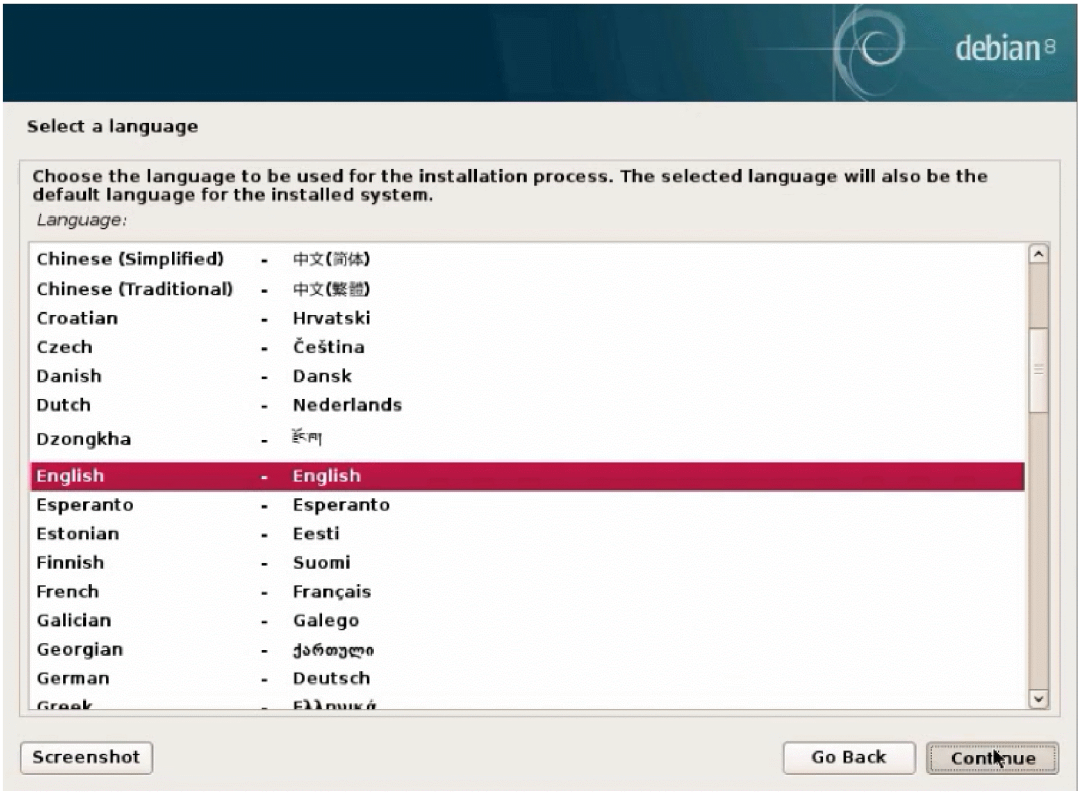
7. Cliquer sur Power this virtual machine pour commencer l'installation de Debian.



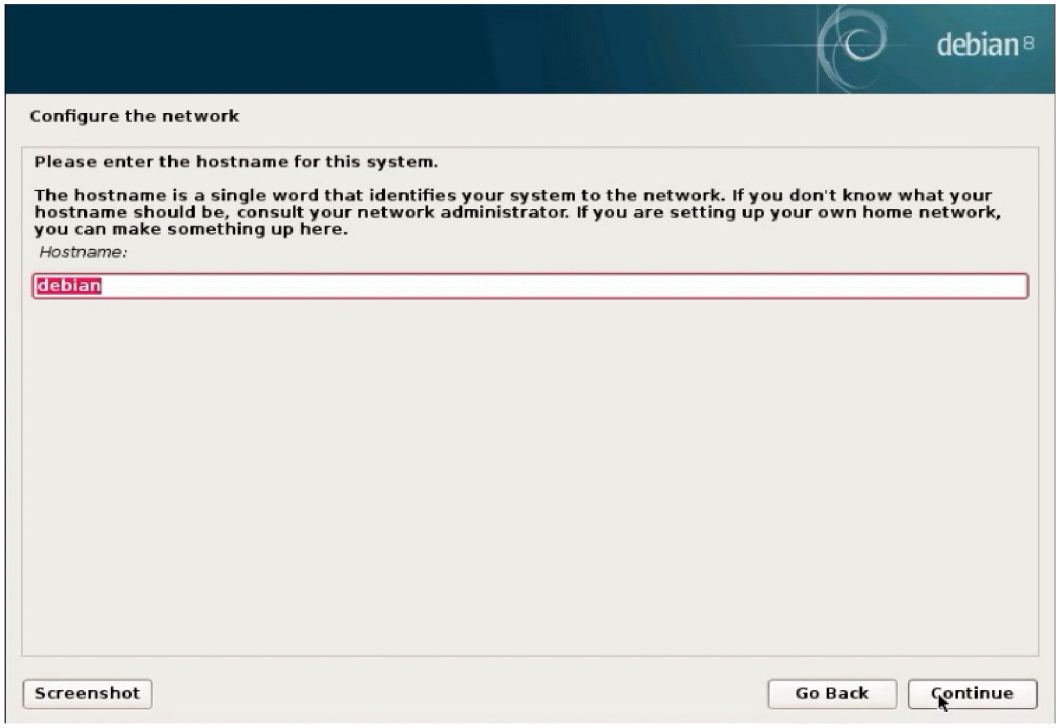
8. Choisir Graphical install puis appuyer sur entrée pour démarrer.



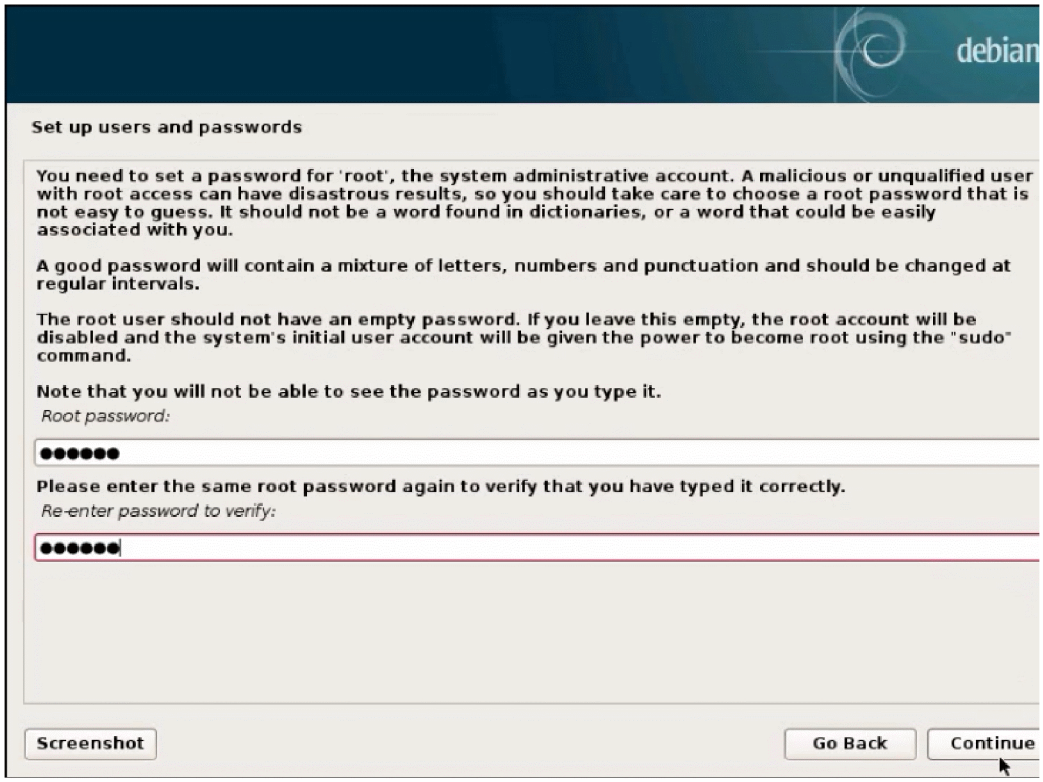
9. Choisir la langue d'installation puis continue.



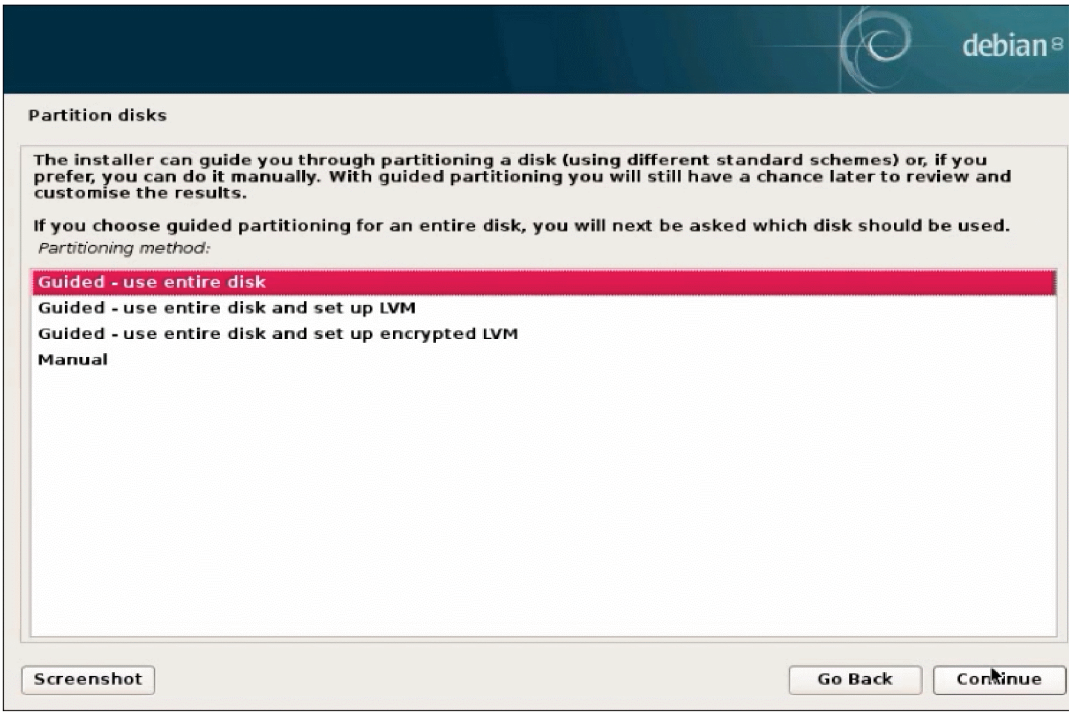
10. Donner un nom pour la machine. Puis cliquer sur continue.



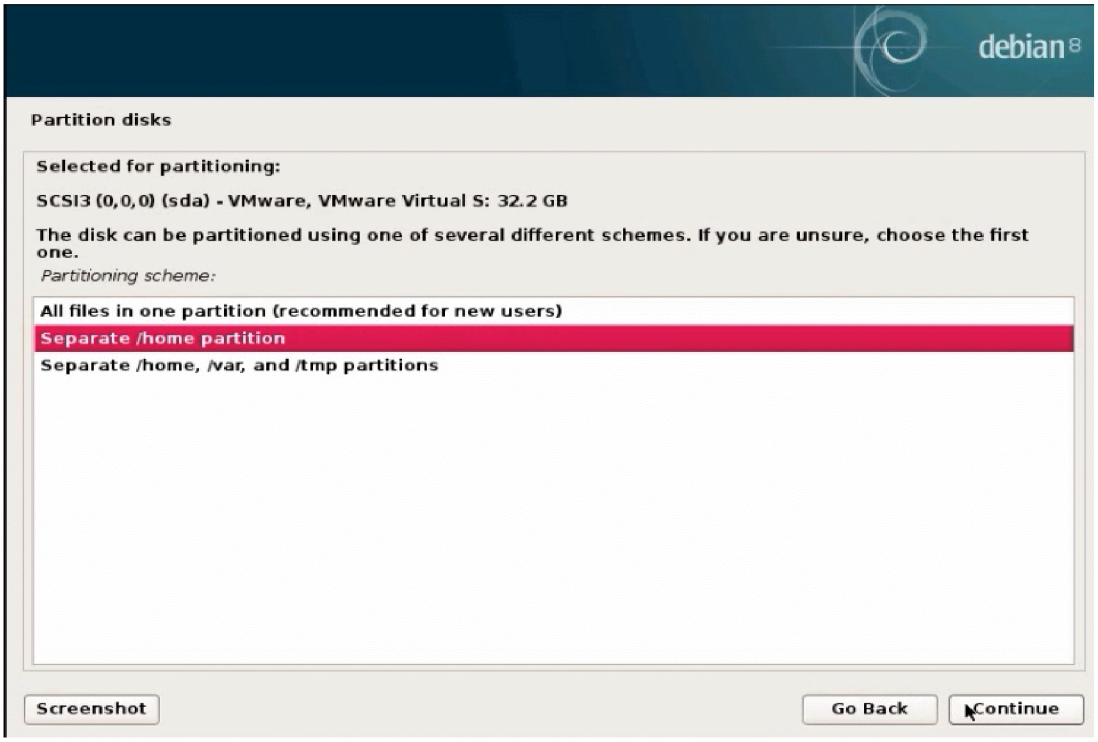
11. Entrer un mot de passe pour le compte administrateur.



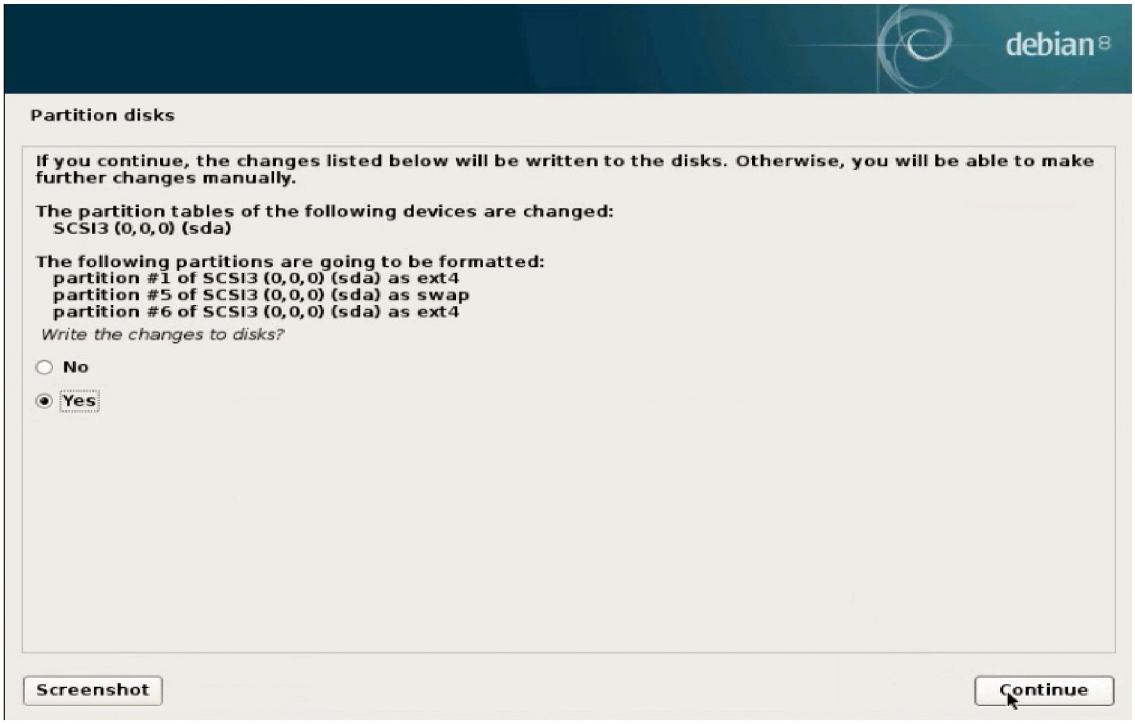
12. Guide – use entier disk (Utiliser un disque entier). Puis cliquer sur continue.



13. Choisir separete /home partition (partition /home séparée) qui est recommandé. Puis poursuivre l'installation.

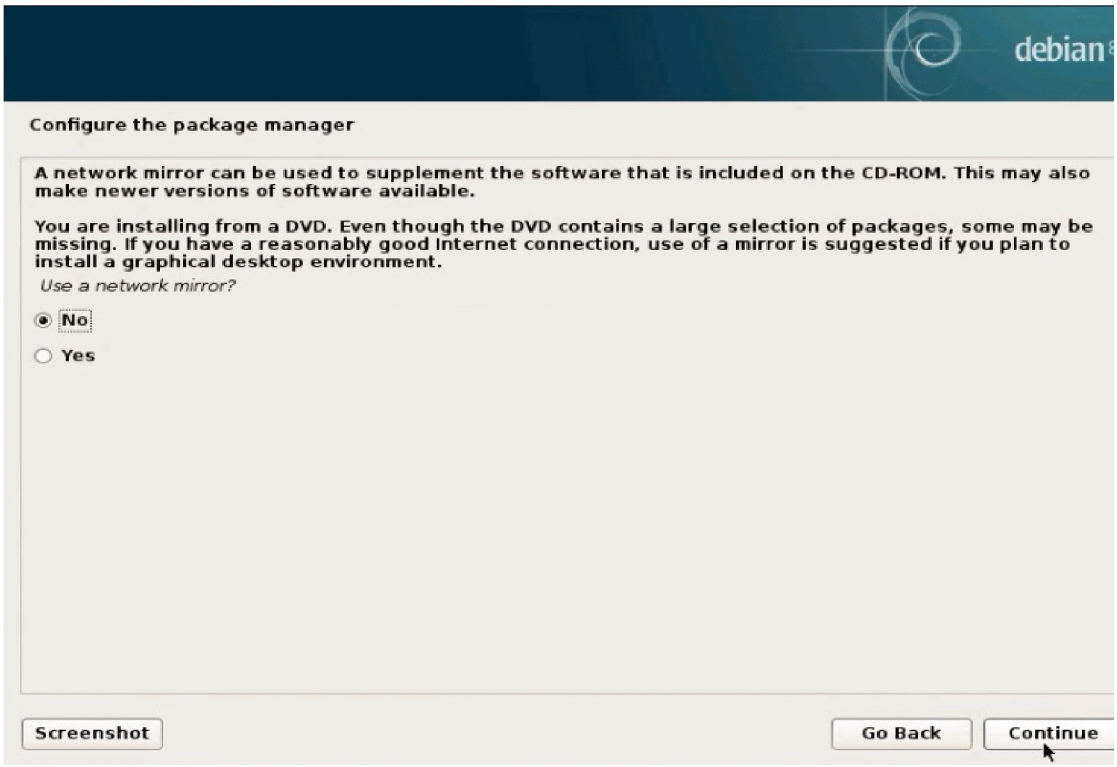


14. Une possibilité de réviser les changements avant de continuer cette opération irréversible. Cliquer sur continue.



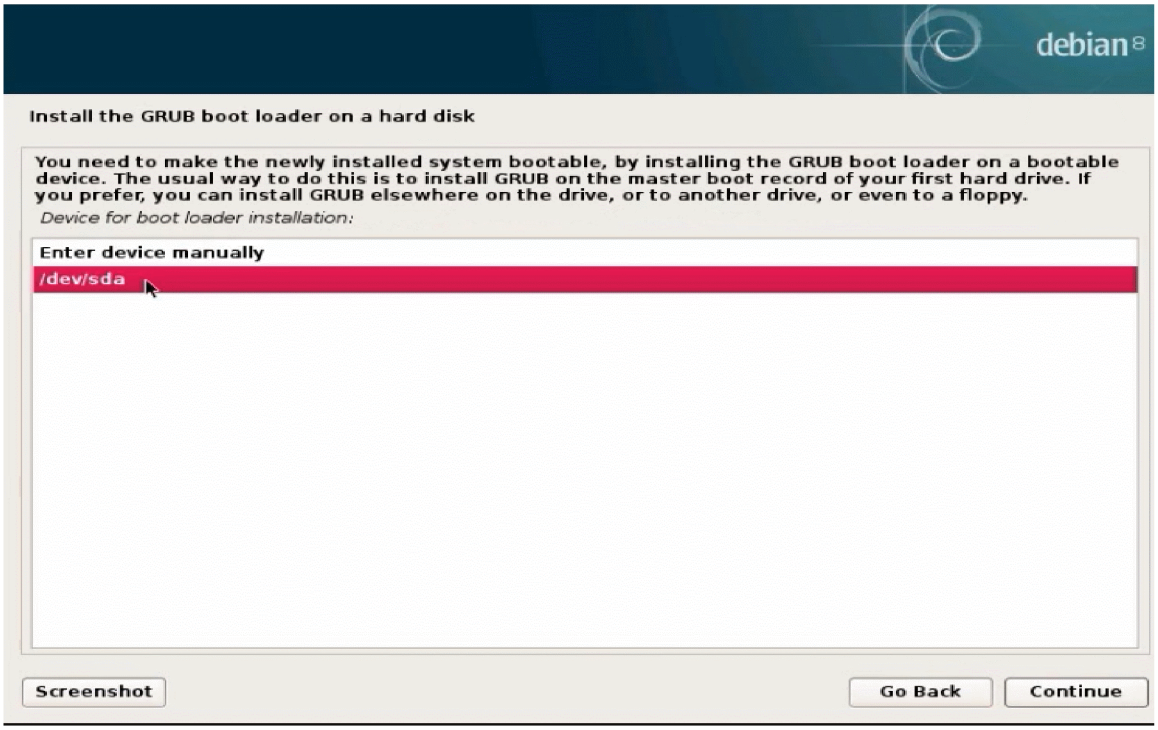
15. Cliquer sur continue.

16. Cliquer sur Continue.

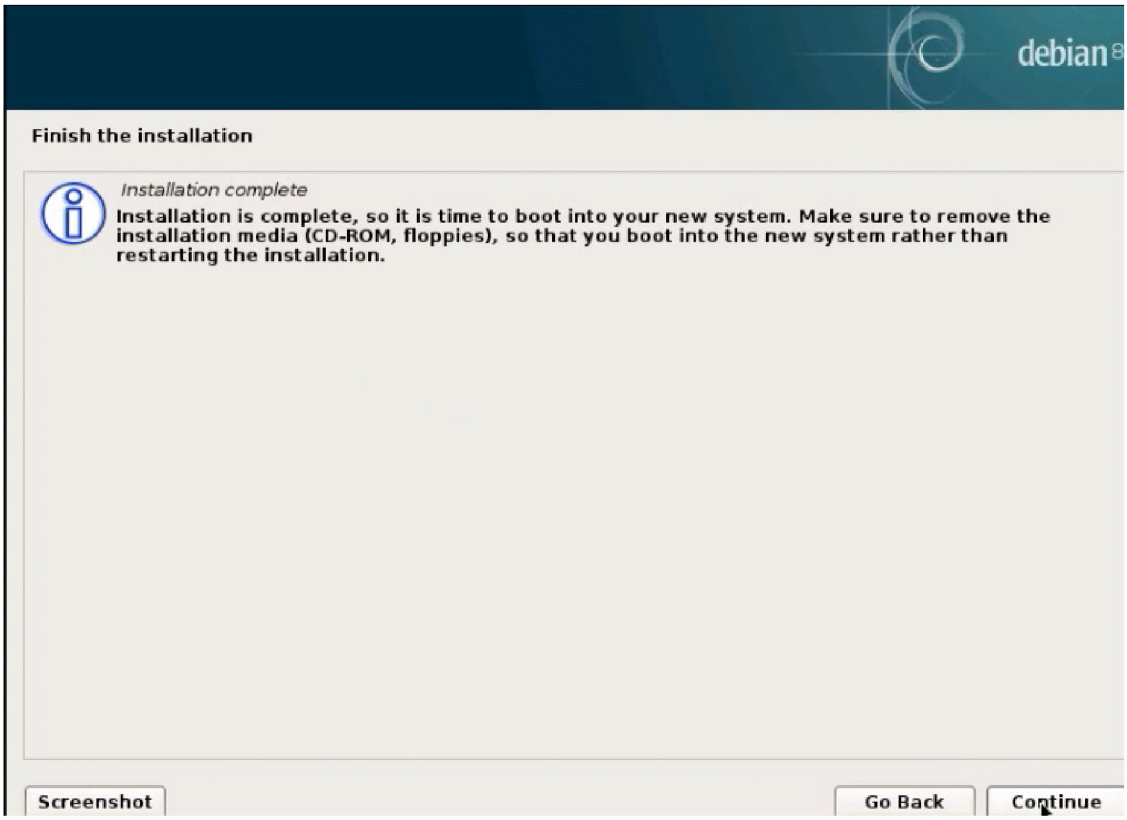


17. Choisir d'installer GRUB qui donne à l'utilisateur la possibilité de démarrer plusieurs programmes.

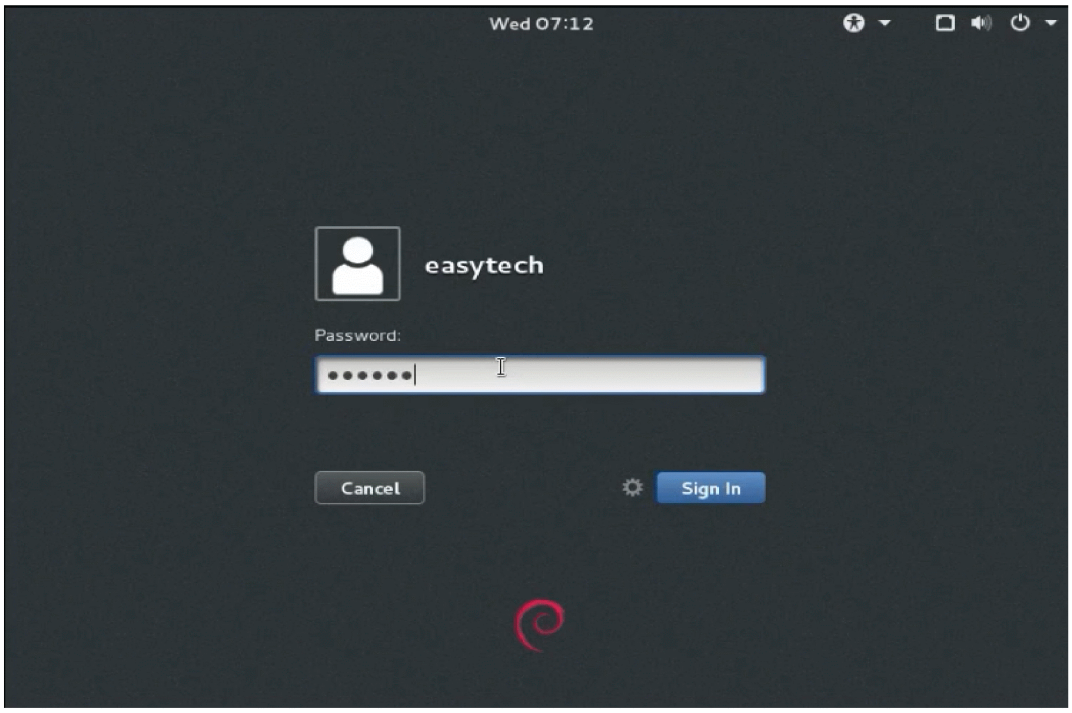
18. Cliquer sur continue.



19. Reste seulement à sélectionner continue et Debian va démarrer automatiquement.



20. Après le démarrage de Debian , il nous reste qu'a saisir le nom d'utilisateur.



21. Voici maintenant le bureau de Debian 8.