REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET D'INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études
DE MASTER ACADEMIQUE

Domaine : Sciences et Technologies
Filière : Génie électrique
Spécialité : Télécommunication et Réseaux
Présenté par : Melle SEBA SABRINA

THEME :

Simulation d'attaque sur des ressources protégées dans un environnement Suricata

Mémoire soutenu publiquement le ……/……/2015 devant le jury composé de :

Président :……

Encadreur :……

Co-encadreur :……

Examinateur :……

Examinateur :……

Promotion : 2015-2016

Dédicaces

Je tiens à dédier ce modeste travail à mes chers parents pour leur présence, leur soutien inconditionnel et leur confiance.

A toutes mes sœurs : Warda, Chahrazed, Mounira, Fatima, Souhila et la petite dernière Ikram.

A mon très chère frère Fethi.

A toutes mes tantes et oncles pour leurs présences et leurs encouragements.

A ma très chère tante Samia qui as toujours été présente pour moi.

A la mémoire de « Yemma Djamila » et « Yemma Habou » qui aurais été très fière de moi.

A tous mes ami (e)s.

SABRINA

Remerciements

Aucun travail digne de ce nom ne s'accomplit dans la solitude, alors que je ne peux qu'être consciente de ma dette de reconnaissance a l'égard de tous ceux qui ont contribué de prés ou de loin à la réalisation de ce modeste labeur

Pour cela, Je remercié mes promoteurs à savoir ***Mr K.AKKOUCH*** *et* ***MR Y. Ait Bachir*** *pour leur aide précieuse tout au long de cette recherche de même que messieurs FATAH et WALID sans oublier tout le personnel de la GTP.*

Nos remerciements vont aussi à toute l'équipe pédagogique du département électronique. Ainsi qu'aux enseignants qui ont contribué à ma formation durant toute ma carrière estudiantine.

Sommaire

Introduction générale

Nous vivons actuellement l'air du numérique où l'informatique occupe une très grande place au sein des entreprise, institution et même à l'échelle de l'individu.Les enjeux liés à la sécurité informatique ne sont pas les même que l'ont soit, un gouvernement ; un acteur économique ou bien un simple individu. Là ou un simples antivirus est préconisé pour sécurisé une machine ; ailleurs par exemple dans les entreprises économiques, il nous faut mettre en place tout un dispositif pour assurer la sécurité des données ; une politique de sécurité est souvent instaurée au sein des entreprise et respectée par l'ensemble des employés ;

L'entreprise ENGTP (Entreprise National des Grand Travaux Pétrolier) est au même titre que les entreprises dans le monde, s'intéresse à sécuriser ses données. C'est au sein de cette entreprise que nous avons effectué notre stage autour de cette thématique.

GPT publie un serveur de messagerie, accessible depuis internet avec un pare-feu classique, donc des règles de pare-feu qui permettent la connexion aux ports SMTP et pop3 (25 et 110) du serveur depuis n'importe quel client , ce qui rend le serveur vulnérable aux attaques externes.

Comment alors devons nous procéder pour protéger le réseau interne de l'entreprise ?qu'elle stratégie de sécurité adopter ? Et comment la mettre en œuvre ? Ce sont les questions aux quelles répond notre travail.

Pour sécuriser les accès externes au réseau et au serveur de messagerie GPT en particulier, nous avons opté à explorer un système de détection d'intrusion et de supervision de trafic appelé Suricata.

Nous avons organisé notre mémoire en cinq chapitres :

Le premier chapitre **« Présentation de l'organisme d'accueil »** décrit l'entreprise, sa situation informatique ainsi que l'architecture du réseau.

Dans le deuxième chapitre **« généralités sur les réseaux informatiques»**,nous avons voulu abordée les notions fondamentales liées aux réseaux informatique ;les composants d'un réseau ,les différentes architectures physiques et logiques ;ainsi que la pile des protocoles OSI et TCP/IP .

Le troisième chapitre **« la sécurité des réseaux informatiques »**se veut un aperçu sur les différentes notions de la sécurité des réseaux informatiques.

Quant au quatrième chapitre, il est dédié aux « systèmes **de détection d'intrusion »** ; c'est cet utilitaire que nous avons choisi pour notre étude afin de contrer les éventuelles attaques venues de l'extérieur. Suricata est actuellement le logiciel Open source le plus utilisé dans le domaine de la prévention et de la détection d'intrusions ; dans ce chapitre on définit les systèmes de détection d'intrusion ; leur architecture, leurs modes de fonctionnement, leurs avantages et leurs inconvénients.

Le dernier chapitre résume la simulation d'attaques de type « force brute »sur un serveur de messagerie dans un environnement protégée par l'IDS Suricata.

Le mémoire se termine par une conclusion générale et quelques perspectives pour de futurs travaux.

Chapitre I :

Présentation de l'organisme d'accueil

Introduction

La présentation de l'organisme d'accueil est une étape très importante pour le choix de la solution réseau ainsi que sa supervision.

Dans ce chapitre, nous allons présenter notre cadre d'étude qui c'est fait dans l'Entreprise National de Grand Travaux Pétroliers, ses missions et ses activités et son organigramme, ensuite nous présenterons la situation informatique de notre champ d'étude et nous terminons par son architecture réseau.

1. présentation de l'organisme d'accueil (E.N.G.T.P)

L'entreprise National de grands travaux pétroliers « **ENGTP** » est une société par actions créé le 19 février 1989, ces actions étaient détenues d'une part par la société mère Sonatrach à 51% et d'autre part par la société de gestion de participation à 49% jusqu'au **13 Décembre 2005** ou toutes ces actions sont détenues à 100% par Sonatrach.

Son capital social est actuellement **6.390.000.000 DA**. Son activité principale est l'étude et la réalisation des projets d'installation matérielle notamment dans les domaines des Hydrocarbure, de l'hydraulique, de l'énergie de l'agroalimentaire, des matériaux de construction et des industries s'y rapportant, à l'intérieur du territoire et à l'étranger, la maintenance d'installations industrielles en exploitation. La formation dans ce domaine de soudage, contrôle et activités annexes.

Son siège social est fixé à : Boulevard 38, zone industrielle de Réghaia, Alger. Elle est implantée sur le territoire national d'est en ouest et du nord au sud, notamment à Skikda, Arzew, HassiR'mel, Hassimessaoud et In amenas où elle est représentée par des directions régionales.

Sa présence sur le marché depuis plus de 40 année, lui a permet de développer un large portefeuille d'activités et d'accumuler un savoir-faire, une expertise et des capacités qui l'on Hissé au statut d'entreprise leader en Algérie.

2. Evolution du statut

Année 1968 : SONATRACH et le groupe français UIE () créent une société de canalisation et de montage industriel dénommée ALTRA. Cette étape a vu la naissance d'ALTRA (entreprise algérienne de grands travaux) société d'économie mixte dans laquelle SONATRACH détient 51% des actions. Le siège social était fixé au 1 Boulevard Mahmoudi à Alger. L'activité principale est domiciliée dans les régions Hassi-Messouad et arzew.

Les effectifs de l'entreprise environ 600 personnes et le chiffre d'affaire est de 24 millions de DA.

Année 1972 : ALTRA devient filiale de SOATRACH à 100% ;Fin de la société mixte par rachat des actions détenues par le partenaire étranger.ALTRA se transforme en unité

SONATRACH, son siège est fixé au 2 Bd Mohamed V- Alger. Elle réalise avec succès son premier gros projet (LPG Nord et sud à Hassi Messaoud) ses effectifs passent à 1 500 agents et son chiffre d'affaire à 122 M DA.L'entreprise GTP devient une entreprise autonome affranchie de toute tutelle, l'E.P.E (Entreprise Publique Economique).

A la tète de GTP un Président Directeur Général qui a pour mission de gérer et d'administrer l'entreprise sous la responsabilité et le contrôle du conseil d'administration.

Année 1980 : Création de GTP qui hérite du patrimoine d'ALTRA.La restauration de SONATRACH donne naissance à l'Entreprise Nationale de grands travaux pétroliers (ENGTP) dont le siège social est fixé à Réghaia. C'est une entreprise socialiste à caractère économique.

Son implantation sur le territoire national s'est amplifiée par la création de bases régionales (Hassi Messaoud, HassiR'mel, Skikda, Arzew, In Amenas).Ses effectives environ 6 700 agents et son chiffre d'affaire est de 600 MDA, elle est sous tutelle du ministère de l'énergie et des industries pétrolières.

Année 1989 : statut EPE/SPA pour GTP, GTP devient une société par action le 19 février 1989, son actionnaire principale est le fond de participation des mines et d'hydrocarbures.

Année 2004 :démarche HSE

GTP a certifié son système à la norme ISO 9001 version 2000, certification obtenue auprès de l'organisme certificateur AIB Vinçotte international (organisme Belge).

La démarche en vue de la certification de ses systémes de management environnemental et management HSE selon respictivement, les normes 14001 version 2004 et 18001, selon en cours.

Année 2005 :GTP devient filiale du Groupe Sonatrach Holding SPP à 100%

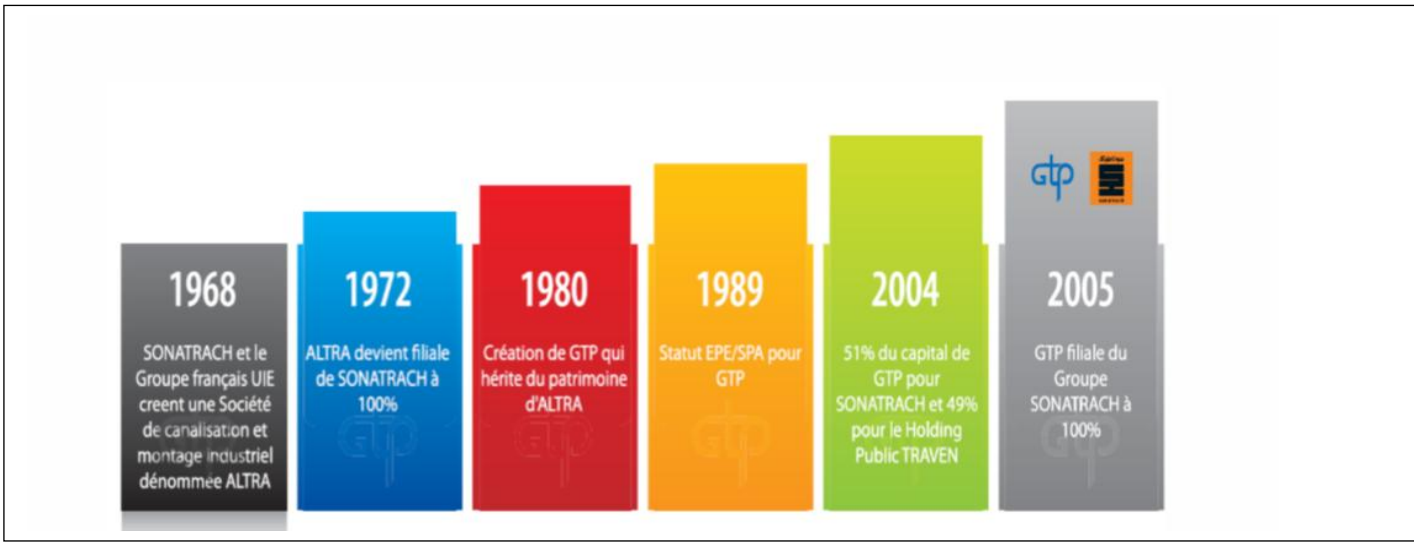


Figure I.1 : Evolution du statut de la GTP

3. Missions et activités de « ENGTP » :

3.1 –Les missions de l'ENGTP :

Les missions de l'ENGTP se résument principalement dans les axes suivants :

- Etude et réalisation des projets d'installations matérielles dans le domaine des hydrocarbures et des industries s'y rapportant.
- Etude générale industrielle, résolution des problèmes technico-économiques et expertise Contrôle et réception de tous matériaux, matériels et installations industrielles.
- La réalisation des grands ensembles industriels dans le domaine des Hydrocarbure et des industries se rapportant à son objet.
- Réalisation de réseaux de collecte et désertes d'Hydrocarbures liquides et gazeux et des installations de surfaces y afférents.

Ses différents domaines d'intervention sont :

- Secteur Hydrocarbures.
- Secteur chimie et pétrochimie.
- Secteur Energie Electrique.
- Secteur Agroalimentaire.
- Secteur Matériaux de construction.

3.2 Les activités de « ENGTP» :

GTP est spécialisée dans la construction des installations industrielles destinées à la production, transformation, transport est distribution des Hydrocarbures avec une capacité de réalisation de l'ordre de 09 millions d'heures, soutenue par un effectif de 7000 agents et 4000 équipements de construction.

Les domaines d'activités de l'ENGTP :

A travers son implantation au niveau des principaux pôles industriels au nord, dans l'ensemble des champs pétroliers et gaziers au sud, GTP dispose d'une capacité de réalisation annuelle de l'ordre de 8.5 Millions d'heures.

Elle intervient dans les activités :

A-Engineering-procurement :

- Etude de base et de détails
- Contrôle de la construction
- Mise en service des installations de stockage des hydrocarbures
- Processing

B-Géni-civil et bâtiments :

- Terrassements
- Fondations des équipements et des structures
- Bâtiments, technique, industriels et administratifs
- Infrastructures sociales nécessaires à l'exploitation des unités industrielles
- Géni-civil lié à la pose des canalisations

C-Montage industriel :

- Montage des structures métalliques
- Montage des tuyauteries et supports
- Montage des équipements mécaniques
- Réservoirs et sphère
- Installation d'équipements électriques et instrumentation
- Pose et raccordement câbles MT et BT

D-Préfabrication :

- Préfabrication des structures métalliques
- Préfabrication des tuyauteries

E-Canalisation :

- Collectes et dessertes
- Pipe d'expédition
- Ouvrages concentrés
- Points spéciaux

F-Soudage Procédés

- SMAW : Soudage à l'arc manuel
- GTAW : Soudage TIG
- GMAW : Soudage semi-auto.fil plein
- FCAW : Soudage semi-auto.fil fourré
- SAW : Soudage auto.sous flux

G-Contrôle et essais :

- Non destructif par rayons X, GAMMA
    - Ultrasons ,ressuage,magnétoscopie
- Destructif par traction, pilage, résilience Macrographie et micrographie

H-Traitement thermiques :

En Atelier et sur Chantier pour :

- Tout type de tuyauterie
- Réservoirs sphériques (Partiel ou Intégral)
- Colonnes

I-Maintenance industrielles :

La maintenance industrielle est un complément de service que nous offrons à nos clients. Nous réalisons des ensembles industriels et intervenons dans les prestations d'entretien et de maintenance depuis plus de 20 ans par la mise à disposition des moyens humains et matériels qualifiés.

Nous avons réalisé plus de 20 conventions représentant 2 500 000 heures d'activité annuelle.

- Interventions régulières et continues (Contrats pluriannuels)
- Interventions programmées (Arrêts d'entretien annuel)
- Interventions d'urgence (incidents)

4. Moyens humains et matériels de GTP :

En raison de son caractère de grande entreprise de réalisation GTP, possède actuellement un effectif moyen de **9176** agents, et qui évolue selon les besoins de l'Entreprise.

Vu son vaste champ d'intervention, GTP est implanté aux quatre points du pays à savoir ARZEW à l'ouest, SKIKDA à l'est, HassiMassaoud, et HassiR'mel au sud du pays, ce qui nécessite des moyens matériels très importante, et de ces moyens :

- Equipement informatique très sophistiqué.
- 22 bâtiments, atelier et magasins.
- 12 bâtiments divers.
- 09 ateliers de travail et de maintenance.
- Un important parc roulant déployé à travers les régions ou elle est implantée des bases de vie.
- D'importants moyens de réalisation (grues, pipe layer, postes de soudures, compresseurs…etc).

5. La stratégie d'affaire de GTP :

La stratégie d'affaire de GTP repose sur des piliers solides :

- Maximiser notre expertise reconnue dans nos marchés principaux, les hydrocarbures, l'Energie et la pétrochimie
- Se servir de notre expertise pour acquérir des marchés dans les secteurs de l'industrie et l'hydraulique

- Développer à travers un partenariat nos unités dans le cadre de la maintenance industrielle
- Confirmer nos capacités dans la préfabrication de tuyauterie et de chaudronnerie

6. Les objectifs de GTP :

Le président directeur général fixe à l'ensemble du personnel de l'entreprise les objectifs suivant :

- Développer et maintenir l'écoute permanente de leurs clients dans le but de mieux les satisfaire,
- Améliorer en permanence la qualité de leur produit et services,
- Mieux maitriser leurs couts notamment par la réduction des charges, la diminution des rebuts, des réparations et des stocks
- Perfectionner leurs rendements afin de rester leader dans leurs domaines d'activités,
- Développer la compétence des personnels par la formation continue.
- Améliorer en permanence le système de management de la qualité mis en place et certifié conforme aux exigences de la norme ISO 9001 versions2000.(ISO : organisation internationale de normalisation).
- Implanter un système de management environnemental conforme aux exigences de la norme ISO 14001 versions 2004, ainsi qu'à celles de la législation et de la réglementation environnementale.

7. Structure organisationnelle de l'ENGTP

L'organigramme ci-dessous montre les différentes structures ayant la responsabilité et l'autorité, pour exécuter et vérifier le travail accompli par la GTP.

Les unités régionales ne sont pas structurées toutes de la même manière. Malgré l'existence de fonctions similaires, les unités régionales sont organisées différemment en fonction de l'importance de l'unité et sa capacité.

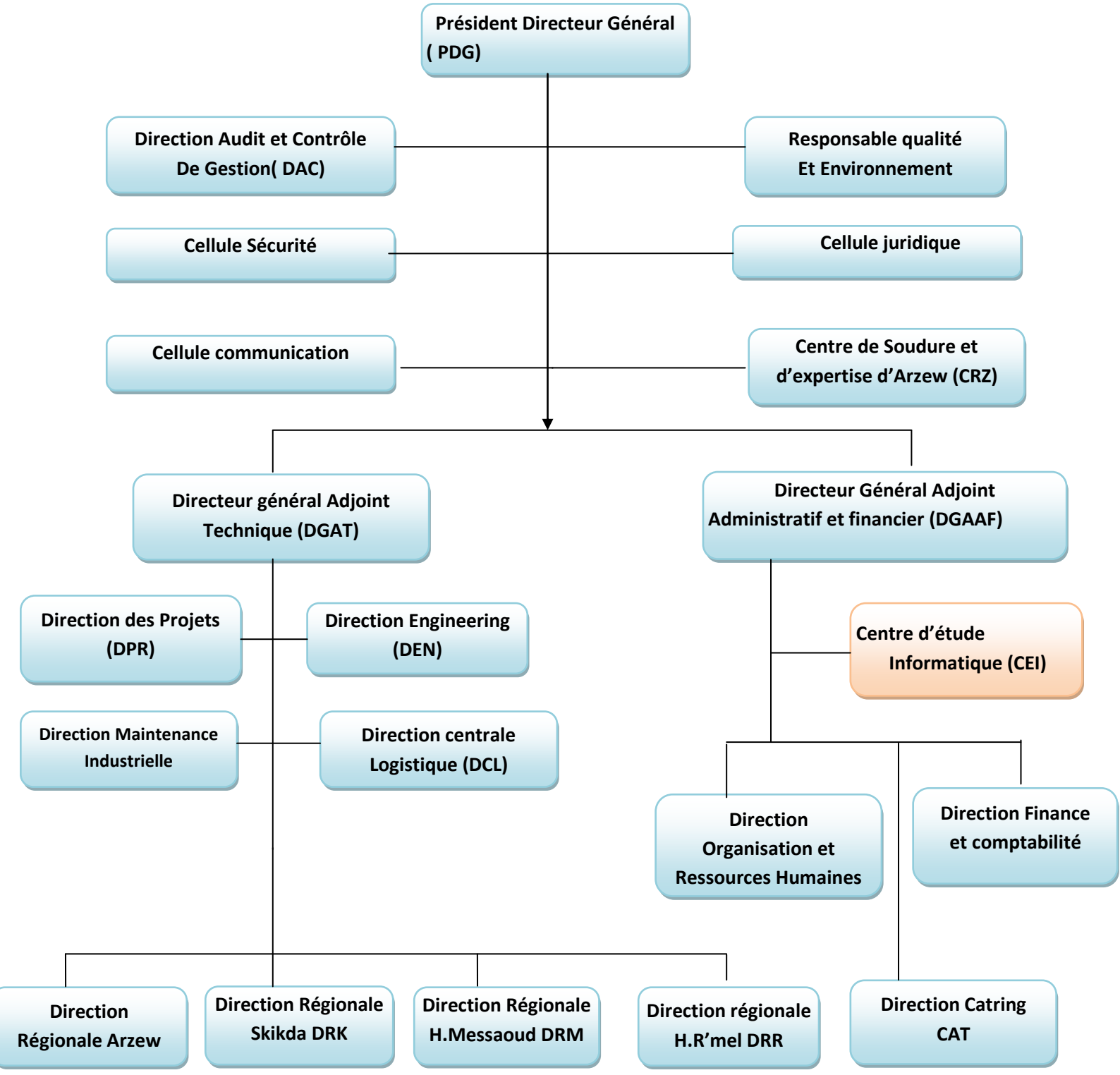


Figure I.2 : Structure organisationnelle de l'ENGTP

8. La normalisation au sein de la GTP

8.1 GTP et ISO 9001 :

L'ambition de GTP, telle qu'affichée dans sa politique qualité, est l'amélioration continu de ses performances. Ainsi la mise en place d'un système de management de la qualité qui satisfait à l'ensemble des exigences de la norme ISO 9001/2000.Elle adopte une démarche qualité, qui se veut globale et cohérente, dont la finalité est la satisfaction du client et de toutes les autres parties intéressées qui sont :

- Le personnel
- GTP elle même
- Le p
- propriétaire (SONATRACH)
- Les autorités

8.2 GTP et ISO 18001 :

L'amélioration de la santé et la sécurité du personnel demeure une préoccupation majeure pour GTP et constitue une priorité dans tous ses projets de réalisation.

Des progrès significatifs ont été réalisés en matière de prévention des accidents de travail. Des actions entreprises à ce sujet mettent en œuvre des mesures de sensibilisation, de formation, d'information et d'investissement.

Son objectif étant non seulement de réduire le taux de fréquence des accidents de travail mais aussi d'atteindre « ZERO ACCIDENT ».

Cette préoccupation est appuyé par la mise en place d'un système de management santé et sécurité OHSAS 18001, avec l'accompagnement international spécialisé.

9. Direction du centre informatique de l'entreprise

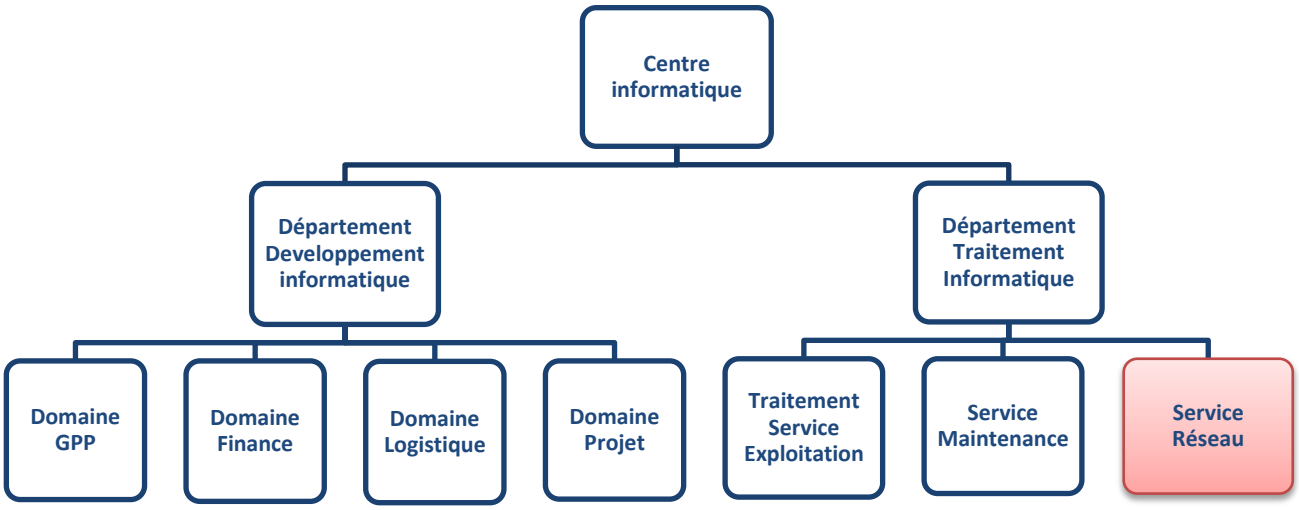


Figure I.3 : Organigramme du centre informatique

10.Architecture du réseau informatique

Le réseau informatique :

Un réseau est une configuration de plusieurs micros ordinateurs reliés à un serveur ou une application stockée au niveau du serveur peut être utilisée par un ou plusieurs utilisateurs en même temps.

Des réseaux LAN (local area network) sont installés au niveau siège et dans toutes les régions de l'entreprise.

Caractéristiques : (réseau, base de données)

- Réseau local de type Ethernet.
- Architecture étoile
- La plate-forme de serveur : Intel biprocesseur avec un contrôleur RAID pourvu d'un lecteur de bandes pour la sauvegarde des données et contient 6 disques durs de capacité 18 gigat Octet pour chacun avec la technologie SCSI
- Système d'exploitation
    - Serveur (Windous NT4)
    - Client (XP professionnel).
- Le Protocol utilisé : TCP/IP
- SGBD oracle 8.0 (en mode client/serveur).

Les données :

L'entreprise dispose d'une base de données centrale contenant l'ensemble des données et des bases de données régionales sont identiquesà la centrale mais ne sont accessible en mode mise à jour que pour les données de la région concernée. Les bases de données sont installées sur des serveurs : un serveur central entreprise et des serveurs régionaux.
Les postes de travail qui ont accès aux bases de données sont reliés aux serveurs à travers des réseaux locaux. Ces postes de travail sont appelés client par rapport aux serveurs. C'est le mode client/serveur.
L'accès aux bases de données se fait à travers des applications développées par le centre informatique et installées sur les postes clients conformément au schéma suivant :
Des postes clients et un serveur de données entreprises au niveau siège interconnectés via un Réseau local.
Des postes clients et un serveur de données régional implanté au niveau de chacune des quatre directions régionales interconnectés via des réseaux locaux.

Conclusion

Dans ce chapitre, nous avons présenté l'organisme d'accueil en présentant l'environnement dans lequel il évolue. Nous avons effectué notre stage au sein du centre d'étude en informatique, en particulier nous avons été accueillie spar l'équipe réseau.

Le chapitre suivant portera donc sur les généralités des réseaux informatiques.

Chapitre II :

Généralités sur les réseaux informatiques

Introduction

Les réseaux informatiques sont destinés à transporter des données d'une machine terminale vers une autre machine terminale .Cependant, il est nécessaire de définir un environnement physique et un environnement logiciel assurant le service de communication entre celles-ci.

Le présent chapitre va présenter des concepts généraux sur les réseaux, en particulier les réseaux informatiques.

1. Définition d'un réseau informatique [9]

Un réseau informatique est un ensemble d'ordinateurs (ou de périphériques) autonomes connectés entre eux dans le but d'échanger des informations sous forme de données numériques. (Valeurs binaires, c'est-à-dire codées sous forme de signaux pouvant prendre deux valeurs : 0 et 1).

2. Avantages et inconvénients des réseaux

Les réseaux sont d'un grand bénéfique pour l'homme, néanmoins ils présentent certains inconvénients. Voici quelques avantages et inconvénients des réseaux.

2.1 Avantage des réseaux [9]

Un réseau permet de partager des ressources entre plusieurs ordinateurs, données ou périphériques ; il permet : le partage de fichiers ; Le partage d'application : compilateur, système de gestion de base de données (SGBD) ; Le partage de périphérique : imprimante, modem, scanner,…

Il permet aussi :

- Le transfert de fichiers ;
- Le traitement à distance ;
- La réduction des couts grâce aux partages des données et des périphériques ;
- La garantie de l'unicité de l'information grâce à une centralisation de la base de données sur un serveur ;
- Une grande fiabilité grâce à la duplication des données sur deux ou trois machines ; ainsi au cas de défectuosité matérielle les autres copies peuvent être utilisées.

2.2 Inconvénients des réseaux [9]

Le principal inconvénient d'un réseau est sa complexité, ce qui nécessite impérativement l'intervention d'un personnel spécialisé au cas de pannes.

3. Composants d'un réseau

Un réseau est constitué d'ordinateurs reliés par un ensemble d'éléments matériels et logiciels.

3.1 Le matériel

Le matériel permettant d'interconnecter les ordinateurs est bien évidemment indispensable pour transmettre des signaux d'un émetteur vers un récepteur. On distingue trois types de composants matériels :

- Le support physique de transmission ;
- Les équipements intermédiaires ;
- Les équipements d'interconnexion.

3.1.1 Le support physique de transmission

Le support physique de transmission, c'est le support (généralement filaire, c'est-à-dire sous forme de câble) permettant de relier les ordinateurs entre eux. On distingue généralement :

- **La paire torsadée :** Un câble à paire torsadée est constitué de deux brins de cuivre, isolés et entrelacés. La vitesse de transmission de l'information de ceux-ci est assez réduite, et la sensibilité à l'environnement électromagnétique est relativement élevée.
  On retrouve deux variantes pour ce type de câble : la paire torsadée et non blindée.
- **Le câble coaxial :** Un câble coaxial est constitué de deux conducteurs cylindriques de même axe, l'âme et la tresse, séparés par un isolant. Cet ensemble offre une structure isolée qui résiste aux interférences externes.(perturbation électrique ou électromagnétiques).
- **La fibre optique :** Une fibre optique se compose d'un cylindre de verre extrêmement fin d'une couche de verre concentrique. Ce support achemine des données numériques sous forme de faisceaux lumineux. Ce qui présente l'avantage de véhiculer des informations, sur de très longues distances, sans y ait altération de

celles-ci (la fibre étant insensible aux perturbations électromagnétiques).La bande passante est très large et le débit est de l'ordre de giga bits par seconde (Gbps).
Notons que la fibre optique est un support unidirectionnel, il faut donc deux fibres pour assurer une liaison bidirectionnelle.

3.1.2 Les équipements intermédiaires

Comme leur noms l'indiquent, les équipements intermédiaires servent à relier les supports de transmission, que nous venons de citer, aux machines terminales. Les principaux équipements intermédiaires les plus usités sont :

- **La prise :** il s'agit de l'élément permettant de réaliser la jonction mécanique entre la carte réseau et le support physique (la prise RJ-45 à huit contactes, en est un exemple)
- **La carte réseau :** (parfois appelé coupleur ou encore carte d'accès) : constitue l'interface entre l'ordinateur et le câble du réseau. Chaque carte dispose d'une adresse unique, appelée adresse MAC, affectée par le concentrateur de la carte, ce qui lui permet d'être identifiée de façon unique dans le monde parmi touts les autres cartes réseaux. La fonction d'une carte réseau est de préparer, d'envoyer et de contrôler les données sur le réseau.
- **Le transformateur :**(appelé aussi adapteur ou tranciver) : Les données se déplacent dans un ordinateur en parallèle, en empruntant des bus sur 8 bites, 16 bites ou 32 bites. Toutefois sur un câble les données circulant sur le support physique (électrique ou optique), en signaux logiques manipulable par la carte réseau, aussi bien à l'émission qu'à la réception. Notons que le transformateur est parfois intégré au coupleur.

3.1.3 Les équipements d'interconnexions

Les équipements d'interconnexion sont utilisés pour relier des réseaux locaux entre eux. On compte principalement les équipements suivant :

- **Le répéteur :**Un répéteur permet de régénérer un signal afin d'étendre la distance de câblage d'un réseau. C'est un organe non intelligent, qui répète automatiquement les signaux présenté à l'une de ses extrémités vers l'autre extrémité.
- **Le pont :** Au contraire d'un répéteur, un pont est un organe intelligent, il effectue le suivi des adresses MAC se trouvant de chacun de ces cotés et prend des décisions en fonction

de cette liste d'adresses correspond à une machine situé à l'opposé du pont. En générale, un pont permet de passer d'un réseau vers un autre réseau de même type, Mais il est possible d'avoir des ponts qui transforment la trame pour l'adapter au réseau raccordé.

- **Le concentrateur (Hub) :** Un concentrateur est un élément matériel possédant un certain nombre de ports. Il permet de concentrer le trafic en provenance de plusieurs hôte, et de régénérer le signale. L'orque une information arrive sur un hub, c'est- à- dire vers tous ces ports.
- **Le commutateur (switch) :** Un commutateur est similaire à un hub, il possède un certain nombre de ports sur lesquels plusieurs machines sont connectées. A la différance du hub, le Switch sait quels sont les ordinateurs qui sont autour de lui.

  Ainsi, s'il reçoit une trame pour l'ordinateur X , il ne l'envoie qu'à l'ordinateur X et pas aux autres.il commute(il branche) l'entrée des données vers la sortie ou est l'ordinateur concerné. C'est pour cela qu'on appelle ça un commutateur en français.
- **Le routeur :**Un routeur permet de relier de nombreux réseaux locaux de telle façon à permettre la circulation de données d'un réseau à un autre de façon optimale, c'est la raison pour laquelle le routeur est considéré comme étant un ordinateur à part entière.

  Il est capable d'examiner les paquets entrantes (donnés de couche 3), à choisir le meilleur chemin pour les transporter sur le réseau et à les commuter au port de sortie approprié.
- **La passerelle (gateway) :**

  Une passerelle permet de faire la liaison entre deux réseaux de type différent, servant notamment à assurer toutes les conversions de protocoles pour garantir l'échange entre ces deux réseaux. La passerelle est donc adaptée aux réseaux hétérogènes.

3.2 Le logiciel

Un réseau ne sert à rien sans une intelligence pour le faire fonctionner, c'est là le rôle des logiciel.

- **Les protocoles de réseau** sont des logiciels qui tournent à la fois sur les différentes stations et leurs cartes d'interfaces réseau. C'est le langage de communication entre machines.
- **Le système d'exploitation du réseau** (ou **NOS** pour Network Operating Système), Souvent nommé gestionnaire du réseau, est installé sur le ou les serveurs. Il comprend toutes les fonctions et tous les outils nécessaires à la gestion d'un réseau. Il fournit une

interface entre les applications de l'utilisateur et les fonctions du réseau auxquelles il fait appel par des demandes à travers la carte d'interface. Particulièrement l'accès à des supports de données communs et à des périphériques.

- **Les applications :** représentent l'ensemble des programmes exécutés sur les différentes stations pour exploiter et accéder au réseau : messagerie, navigation...etc.

4. Classification des réseaux

On peut classifier les réseaux selon deux critères : **la topologie** et **la taille.**

4.1 Selon la taille

La taille d'un réseau fait l'objet de la classification suivante :

- **LAN (Local area Network) :** appelé aussi réseau local, correspond par sa taille aux réseaux intra-entreprises. En règle générale, la distance du câblage de ce type de réseaux est de quelque certaines de mètres.
- **MAN (Métropolitain Area Network) :** appelé aussi réseau métropolitain, il couvre la superficie d'une ville ou d'une région, il peut être l'interconnexion de plusieurs réseaux locaux des différente entreprises pour le donner la possibilité de dialoguer avec l'extérieure.
- **WAN (Wide Area Network) :** appelé aussi réseau étendu, il est destiné, comme son nom l'indique, à transporter des donnés numériques sur des distances à l'échelle d'un payé, voire d'un continent ou de plusieurs contenants.

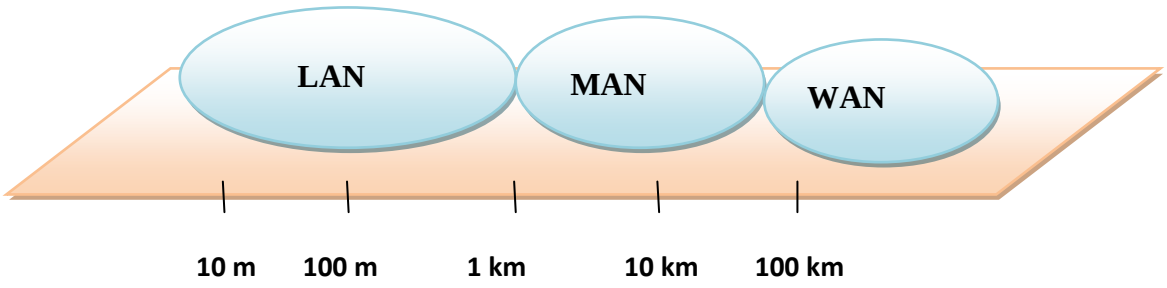


Figure II.1 Classification des réseaux

4.2 Selon la topologie

Par définition la topologie est l'organisation physique et logique d'un réseau l'organisation physique concerne la façon dont les machines sont connectées (BUS, Anneau, Etoile, Maillé, arboniscences,...). La topologie montre comment les informations circulent sur les réseaux (diffusion, point à point).

4.2.1 Les topologies physiques

Les différentes topologies physiques de base sont :

- La topologie en bus
- La topologie en étoile
- La topologie en anneaux

Ces dernières peuvent être combinées pour obtenir des topologies hybrides

- **La topologie en bus**

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet dans une topologie en bus, tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire d'un câble, généralement coaxiale. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

Cette topologie a pour avantage d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est excrément vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté.

- **La topologie en étoile (star)**

Dans une topologie en étoile, tous les composantes sont reliées à un même point centrale et l'information ne va de l'émetteur au récepteur qu'en transitant par ce point centrale.

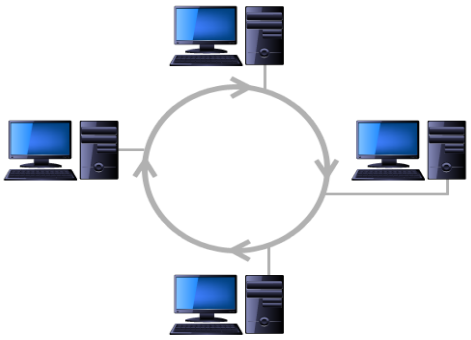
Ce point central peut être un Switch ou un hub, la gestion des liaisons de communications est alors différente selon le cas. On fait référence à ce que l'on appelle la topologie logique qu'on verra dans le point suivant :

Contrairement aux réseaux construites sur une topologie en bus, dans une étoile une panne ne touche qu'une seule branche sauf si c'est le point central qui est touché.

- **La topologie en anneau (Ring)**

Dans une topologie en anneau, le support relie tous les ordinateurs de manière à former un circuit en boucle. Il est cependant possible de réaliser un réseau bidirectionnel en utilisant deux anneaux.Le doublement de l'anneau donne lieu à deux possibilités : soit les transmissions s'effectuent dans le même sens sur les deux anneaux, soit elles s'effectuent au sens contraire.

Les réseaux en anneaux utilisent la technique de jeton. En effet un jeton circule autour de l'anneau. L'ordinateur qui le jeton émet des donnés qui font le tour de l'anneau.



L'lorsque les donnés reviennent, l'ordinateur qui les a envoyées les élimine du réseau .et passe le jeton à son voisin, et ainsi de suite…

Notons que la topologie en anneau est connue par une fiabilité assez médiocre qui lui a valu de nombreuses critiques, la rupture de l'anneau ou la défection d'un nœud actif rend le réseau inutilisable.

- **Les topologies hybrides**

Une topologie hybride est le résultat d'un mélange des différentes topologies de base, citons à titre d'exemple : un arbre, une intersection d'anneau, un maillage régulier, un maillage irrégulier, etc.

4.2.2. Les topologies logiques

Par symétrie, la topologie logique vient compléter la topologie physique. On y distingue alors deux catégories de réseaux :

Ceux au **mode diffusion** et ceux au **mode point à point**

- **En mode diffusion**

Ce mode consiste à partager un seul support de transmission. Chaque message envoyé par une machine sur le réseau est reçu par toutes les autres. Un champ adresse au sein du message précis le destinataire. A la réception cette adresse de destination et ignore le message. Si celle si ne la concerne pas .A tout moment une seul machine à besoin d'envoyer un message sur le support .Il faut donc qu'elle « écoute » au préalable si la voie est libre ; si ce n'est pas le cas elle attend selon un protocole spécifique à chaque architecture.

- **En mode point à point**

Dans mode point à pont le support physique (le câble) relie une paire d'équipements se quand deux élément non directement connecté entre eux veulent communiquer ils le font par l'intermédiaire des autres nœuds du réseau.

Remarque :

Une topologie physique en étoile peut bien correspondre à une topologie logique en bus si son nœud central est un hub. En effet le hub ne sait que diffuser l'information à tous ses ports sans exception, on retombe donc on retombe dans le chemin typique du bus.

5. Le mode de fonctionnement des réseaux [12]

La communication avec ou sans connexion sont les deux modes de connexions des réseaux ; sa mise en place se déroule entre eux est l'établissement de la connexion enter les deux entités communications.

5.1 Mode avec connexion

Le mode avec connexion est le fonctionnement bien connu du réseau téléphonique, sa mise en place se déroule en 3 phases distinctes :

1. L'établissement de la connexion : une connexion doit être explicitement établie par une requête de l'une des entités communicantes, l'accord de l'autre entité est indispensable pour que la communication ait lieu (découcher le téléphone).
2. Le transfert de données d'un point à l'autre.
3. La libération de la connexion.

Les avantages du mode avec connexion sont : la sécurisation du transport par l'identification claire de l'émetteur et du récepteur, la possibilité d'établir à l'avance des paramètres de qualité de services qui sont respectés lors de l'échange de données .Les défauts sont les lourdeurs de la mise en place de la connexion qui se révéler beaucoup trop onéreuse si l'on ne veut pas échanger que quelque octets ainsi que la difficulté à établir des communications multipoints.

5.2 Mode sans connexion

Le mode sans connexion na pas besoins de présence, à la fois et même temps des entités communicante distante. Il n'ya pas de négociation entre l'émetteur et le récepteur.

Les bloques de donnés appelée datagramme, sont mise sans vérifier à l'avance si l'équipement à atteindre, ainsi que les nœuds sont émis sans vérifier de l'avance si les équipements sont à atteindre, ainsi que les nœuds intermédiaire éventuelle, sont bien actifs. C'est alors aux équipements générant le réseau d'acheminer le message étape par étape et en assurant éventuellement sa temporisation jusqu'un ce que le destinataire soit actif.

Ce service est celui des courriers postaux classiques et suit le principe général suivant :

- Le client poste une lettre dans une boite aux lettres
- Chaque lettre porte le nom et l'adresse du destinataire

- Chaque client a une adresse propre et une boite au lettre
- Le contenu de l'information reste inconnu du prestataire de service
- Les supports du transport sont inconnus de l'utilisateur du service

6. l'architecture client serveur

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes contactent un serveur, une machine généralement très puissante en termes de capacité d'entrée-sortie, qui leur fournit des services.

Dans un environnement purement Client/serveur, les ordinateurs du réseau (les clients) ne peuvent voire que le serveur, c'est un des principaux atouts de ce modèle.

6.1 Fonctionnement d'un système client serveur

- Le client émet une requête vers le serveur grâce à son adresse et le port, qui désigne un service particulier du serveur
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine client et son port.

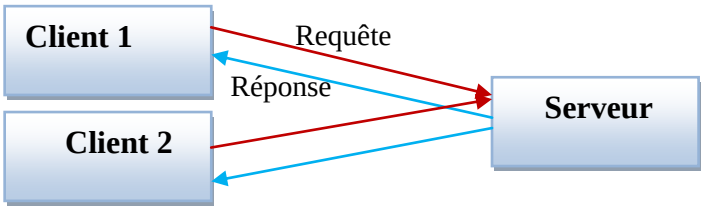


Figure II.2 Fonctionnement Architecture client serveur

6.2 Classification des architectures client/serveurs

6.2.1 Architecture client server à 2 niveaux

L'architecture à deux niveaux (appelées architecture 2-tiers). Caractérise les systèmes client/serveurs dans lesquels le client demande une ressource et le serveur la lui fournit directement. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir le service.

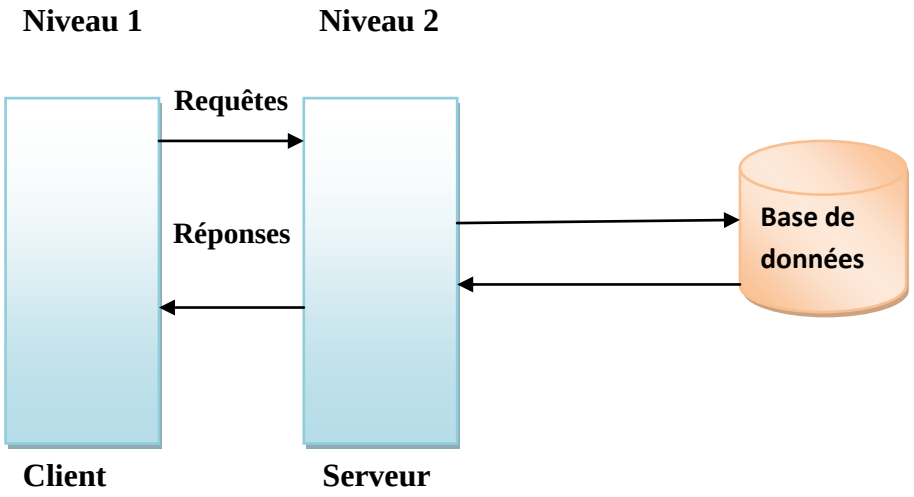


Figure II.3 Architecture client serveur à deux niveaux

6.2.2 Architecture client serveur à 3 niveaux

Dans l'architecture à 3 niveaux (appelées architecture 3-tiers), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre :

- **Le client :** le demandeur de ressources
- **Le serveur d'application** (appelé aussi **middleware**) : le serveur chargé de fournir la ressource mais faisant appel à un autre serveur.
- **Le serveur secondaire (**généralement un serveur de base de données), fournissant un service au premier serveur.

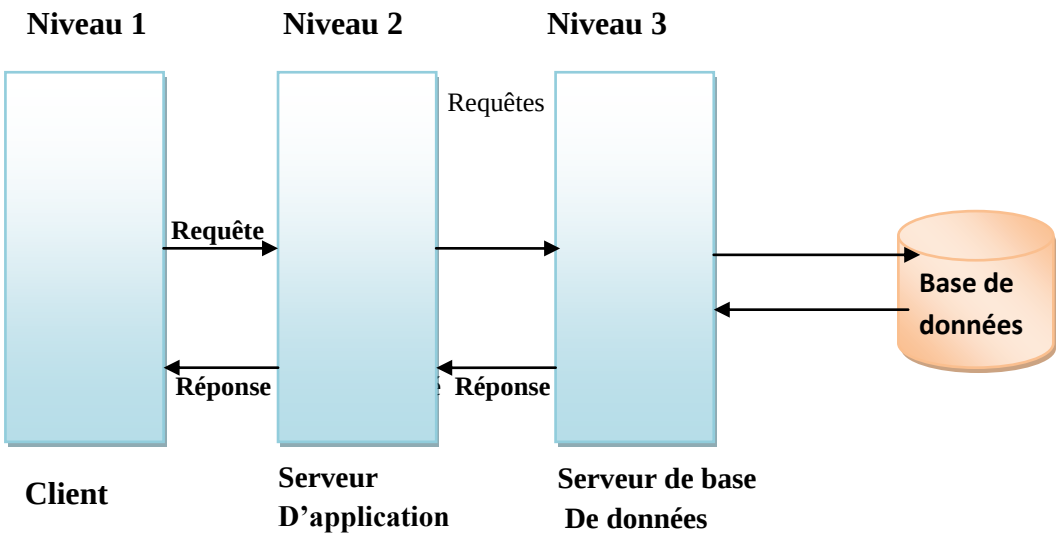


Figure II.4 Architecture client serveur à trois niveaux

7.1Les architectures protocolaires

Les règles du jeu à respecter pour transporter de l'information d'une extrémité à une autre du réseau s'appellent des **protocoles.** L'ensemble des protocoles nécessaire pour réaliser une communication constitue une **architecture protocolaire.** Celle-ci est connue aussi sous le nom d'architecture logicielle.

Deux grandes familles d'architectures logicielles se disputent actuellement le marché. La première provient de la normalisation de l'ISO (International Standardisation Organisation) .Que l'on appelle OSI (Open System Interconnexion).La deuxième est l'architecture **TCP/IP,** utilisé dans le réseau internet.

7.1'architecture OSI (open system Interconnexion)

Le modèle OSI est un modèle d'architecture des systèmes de communication. C'est le premier pas vers la standardisation des systèmes de communication, il permet d'interconnecter des systèmes ouverts, c'est-à-dire des systèmes ouverts à la communication avec d'autres systèmes hétérogènes.

7.1.1 Présentation des couches OSI

Le modèle de référence comporte une structure en sept couches. Les couches basses s'intéressent au transport de l'information, tandis que les couches hautes correspondent à leur traitement.

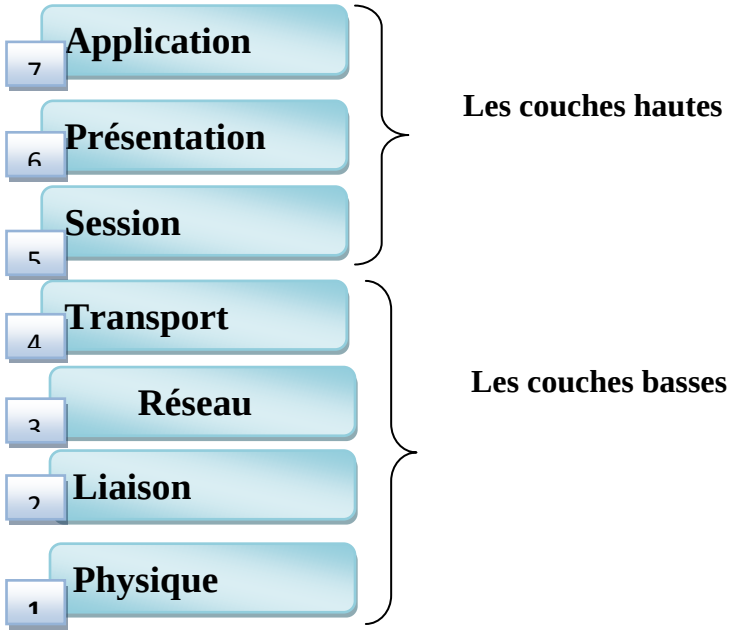


Figure II.5 Le modèle de référence OSI

- **Couche physique**

La couche physique assure la transmission des bits entre équipements distants. Elle spécifie les règles mécaniques, électriques, optiques ou autres, fonctionnelles ou procédurale liées aux circuits de données, Elle offre un moyen d'établir une connexion physique entre les équipements, de maintenir cette connexion durant les échanges et de la libérer en fin d'échanges.

- **Couche liaison de données**

La couche liaison de donnée a été introduite initialement pour pallier aux problèmes engendrés par les circuits de données (essentiellement les erreurs de transmission dues à l'imperfection des supports de communication).Le rôle principale de cette couche est donc de détecter et de corriger les erreurs de transmission.

- **Couche réseaux**

Cette couche assure toutes les fonctionnalités de relais et d'amélioration de services entre les entités du réseau, c'est-à-dire :l'adressage, le routage, le contrôle de flux, la détection et la correction d'erreurs nom résolues par la couche liaison de données.

- **Couche transport**

Elle découpe et segmente les données transmises par la couche (5) en entités plus petites et s'assure que les éléments arrivent correctement de l'autre coté .Elle détermine également quels types de services doivent être fournis à la couche session et donc aux utilisateurs. C'est elle qui gère la connexion d'un système A vers un système B de bout en bout de la communication.

- **Couche session**

Le rôle du niveau session est de fournir aux entités de présentation les moyens nécessaires à l'organisation et à la synchronisation de leur dialogue (identification des noms utilisateurs, mot de Passe, etc.) et les échanges des données.

- **Couche présentation**

La couche présentation assure la transparence du format des données à la couche 7.

- **Couche application**

La couche application donne au processus d'application le moyen d'accéder à l'environnement OSI et fournit tous les services directement utilisables par l'application, à savoir : des programmes de transfert de fichier, de soumission de travaux à distances, d'échange de courrier électronique, etc…

7.2L'architecture TCP-IP [8]

TCP-IP est une architecture réseau en 4 couches dans laquelle les protocoles **TCP** et **IP** jouent un rôle prédominant, car ils constituent l'implémentation la plus courante .Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

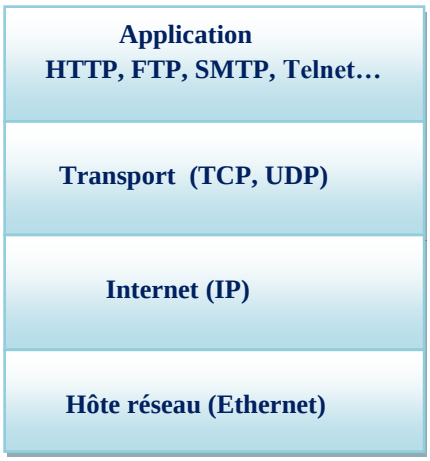


Figure II.6 La représentation en couches du modèle TCP/IP

7.2.1 Présentation des couches TCP/IP [11]

- **La couche hôte réseau**

Cette couche regroupe les couches physiques et liaison de données du modèle OSI. En effet, cette couche n'a pas vraiment été spécifiée ; sa seule fonction consiste dans l'émission et la réception des trames. Pratiquement, elle place les trames sur le réseau et les en extrait.

L'implémentation de cette dernière est laissée libre. De manière plus concrète, son implémentation est typique à la technologie utilisée sur le réseau local.Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte réseau.

- **La couche internet**

Cette couche est la plus importante de l'architecture. Elle réalise l'interconnexion des réseaux hétérogènes distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement des paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Le rôle le plus important de cette couche est l'acheminement des paquets, son point critique est **le routage.** C'est dans ce sens qu'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI.

Pour assurer les différentes fonctions de cette couche, des protocoles ont été mis en point dont le plus important est : **le protocole IP**

Le Protocol IP :

Principalement chargé de **l'adressage** et du **routage** des **paquets** entre hôtes et réseau. Il à pour but d'acheminer un paquet de données entre une station source et une station destinataire. Chaque paquet est une entité qui est absolument indépendante de toutes les autres. IP n'offre qu'un service de type remise de datagrammes, c'est-à-dire d'unités des données en mode nom connecté. Il ne s'occupe pas du contrôle de flux de données.

- **La couche transport**

So rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation .Officiellement, cette couche n'a que deux implémentation :Le protocole TCP (Transmission Control Protocol) et le Protocol UDP (User Datagramme Protocol).

Au niveau de la couche internet, les datagrammes sont routés d'une machine à une autre en fonction de l'adresse IP qui identifie le numéro de réseau. Lors de cette opération aucune destination n'est faite entre les services ou les utilisateurs qui émettent ou reçoivent des datagrammes, tous les datagrammes sont mélangés.

Les couches UDP et TCP ajoutent un mécanisme qui permet l'identification du service (niveau application).

En effet, il est indispensable de faire un tri entre les divers applications : plusieurs programme de plusieurs utilisateurs peuvent utiliser simultanément la même couche de transport et ne doit pas y avoir de confusion entre eux.D'où l'idée d'associer la destination à la fonction qu'elle remplie. Cette identification se fait à l'aide d'un entier positif que l'on nomme port. Associé à une adresse IP, il constitue ce qu'on appelle une socket (veut dire à peu prés connecteur en anglais).Une socket identifie pleinement le service qui est concerné sur une machine donnée.

Exemple de ports :

Port	Service application
21	FTP
23	TELNET
25	SMTP
53	DNS
80	HTTP

Remarque :

Les ports 0 à 1023 sont les ports reconnus (réservés).Ils sont de manière générale, réservés aux processus systèmes ou aux programme exécutés par des utilisateurs privés.

Le protocole TCP :

Transmission **C**ontrol **P**rotocol est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet.

A l'inverse, sur la machine destination, TCP remplace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial.TCP s'occupe également du contrôle de flux de la connexion.

Le protocole UDP :

Le protocole UDP est en revanche un protocole plus simple que TCP : il est nom fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conversation de l'ordre de remise des paquets.

Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages.

- **La couche application**

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est, en effet, aperçu avec l'usage que les logiciels réseaux n'utilisent que très rarement ces 2 couches. Le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.Elle offre une multitude de services pour l'utilisateur via ses différents protocoles tel que SMTP, TELNET, FTP, HTTP…

Quelques protocoles :

FTP : FTP est un protocole fiable et orienté connexion qui emploie TCP pour transférer des fichiers entre les systèmes qui supportent ce protocole. Le but principal du ftp est de transférer des fichiers à partir d'un ordinateur à un autre en copiant et/ou en déplaçant des fichiers des serveurs aux clients, et des clients vers les serveurs. Le protocole FTP est assigné au port 21 par défaut.

HTTP : Le protocole de transfert hypertexte (HTTP) fonctionne avec le World Wide Web, qui est la partie la plus utilisée et la plus importante d'Internet. Une des raisons principales de cette croissance extraordinaire est la facilité avec laquelle il permet l'accès à l'information.

SMTP : Les serveurs d'email communiquent entre eux en employant le *Simple Mail Transfer Protocol (SMTP)* pour envoyer et recevoir du courrier. Le protocole SMTP achemine des messages email dans le format Ascii en utilisant TCP. On l'utilise souvent en tant que protocole d'envoi de mail, rarement en tant que protocole de récupération d'email, car il est peu sécurisé.

POP3 : Le protocole POP (*Post Office Protocol* que l'on peut traduire par *protocole de bureau de poste* permet comme son nom l'indique d'aller récupérer son courrier sur un serveur distant (le serveur POP). Il est nécessaire pour les personnes n'étant pas connectées en permanence à Internet afin de pouvoir consulter les mails reçus hors connexion.

Conclusion

Nous avons présenté dans ce chapitre les concepts de base dans les réseaux, allant de la définition d'un réseau, ses équipements matériels et logiciel, jusqu'à la description des

architectures protocolaires OSI et TCP/IP. Nous avons terminé le chapitre par la définition de quelques protocoles les plus courants à savoir HTTP, FTP et SMTP. Dans le chapitre suivant, nous nous intéresserons à la sécurité dans les réseaux informatiques.

Chapitre III :

La Sécurité des réseaux informatiques

Introduction

Les systèmes informatiques ont pris ces dernières années une grande importance et leurs sécurité devient vitale pour la survie de l'entreprise et même des Etats ; les enjeux sont devenus de plus en plus important.La notion de risque liée à ces derniers devient une source d'inquiétude, il est donc formellement important pour les entreprises de traiter l'aspect de la sécurité réseau, contre tout ce qui constitue une menace à son égard.

Dans le présent chapitre, nous allons aborder la notion de sécurité des réseaux informatiques ; des enjeux de la sécurité du réseau ainsi que les menaces, vulnérabilités et des risques encourues.

1. Définition de la sécurité d'un réseau informatique :

La sécurité, c'est un ensemble de mesure permettant d'assurer la protection des biens et des valeurs**.** Quant à la sécurité d'un réseau informatique, c'est garantir la sécurité des informations et du réseau de l'entreprise**.[2] [17]**

Ces impératifs peuvent être définis à plusieurs niveaux :

- **Disponibilité :** assurer l'accès à l'information aux utilisateurs autorisés (empêcher l'utilisation non autorisée de ressources informatiques d'une façon générale).
- **Confidentialité :** les données ne doivent être visibles que des personnes habilitées pour.
- **Intégrité :**assurer l'exactitude et la complétude de l'information (empêcher la modification non autorisée de données).
- **Non répudiation :** on doit pouvoir certifier, quand un fichier a subi des modifications, et la personne qui l'a modifié.

Donc la sécurité d'un réseau informatique,c'est l'ensemble des mesures à appliquer afin de protéger les réseaux informatiques des attaques physiques ou bien logiques.

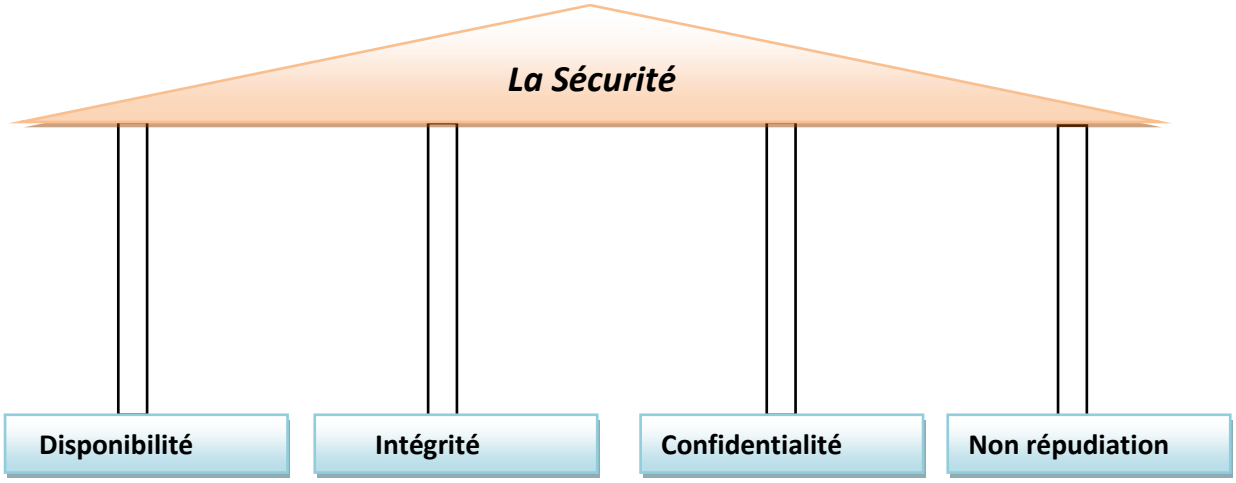


Figure III.1 Les fondements de la sécurité informatique

2. Les menaces sur les réseaux informatiques [3]

Une menace est une action ou bien un événement pouvant causer des dégâts réversibles ou bien irréversibles à un réseau informatique ; la menace peut être d'origine humaine volontaire ou bien involontaire, ou bien d'origine naturelle.Ces faits directes peuvent à leur tours engendrer d'autres conséquences plus grave à l'entreprise, à savoir la perte de sa clientèle ; perte financière ; poursuite judiciaire atteinte à la réputation.

On peut classer les menaces en deux catégories :

- Actes calculé ; malicieux ; volontaire
- Actes involontaire les accidents

2.1 Erreur et omission

Souvent d'origine humaine, en effet, ces menaces importantes touchent l'intégrité des données et des systèmes. N'importe quelle personne intervenant sur le système que ça soit (utilisateur, administrateur système, développeur…) contribue directement ou indirectement à ces dangers mettant en péril la sécurité des systèmes.Une erreur commise peut s'agir d'une menace ou plus encore elle peut mener à créé une vulnérabilité.

2.2 Fraudes et vol

Les fraudes et voles peuvent être causées par l'intérieur ou l'extérieur de l'entreprise, Il s'avère que la pluralité des menaces provient de l'intérieur par des utilisateurs ayant un accès privilégiés, en effet se sont les utilisateurs bien placé pour commettre des forfaits.

2.3 Sabotage causé par les employés

Ce sont les personnels les plus familiarisés avec les systèmes et les applications.Ils peuvent donc perpétrer des dommages, sabotage…Ce qui implique la nécessité de gérer et de contrôler de façon rigoureuses les comptes des utilisateurs surtout ce qui ont un accès privilégiés aux systèmes.

2.4 Les hackers

Le terme hacker ou encore cracker fait référence à la personne qui s'introduit sur les systèmes d'information sans autorisation pour. Afin de provoquer des dégradations dans les données ou les applications, ses actions peuvent s'effectuées de l'intérieur dans le cas ou il a peut obtenir un accès sur le réseau. Ou de l'extérieur de l'entreprise .Toutefois il n'est pas toujours facile de détecter sa présence sur les systèmes ni de connaitre ce qui la provoquer comme dégâts

2.5 Espionnage industriel ou commercial

C'est le fait de récupérer des données confidentielles de l'entreprise .dans le cas de concurrence économique ou industrielle. Cette menace n'implique en générale d'altération des données internes. Par contre elle peut avoir un impacte important sur les actifs sensibles de l'entreprise (donnés clients, brevet industrielle, cette menace vise les ordinateurs ou appareille portable particulièrement sensibles au vole, contenant des informations confidentiélles.des précautions d'utilisation et de protection devront être prise.

2.6 Les codes cachés

Les codes cachés peuvent conduire à l'introduction des objets malfaisants sur les stations de travail ou serveur informatique.une foie introduits, ils peuvent prendre possession de la place et corrompre la configuration de manière souvent irréversible dans la famille des codes cachés on distingue :

2.6.1 Le Virus :

Programme malveillant dont l'exécution est déclenchée lorsque le vecteur auquel il a été attaché clandestinement est activé, qui se recopie au sein d'autres programmes ou sur des zones systèmes lui servant à leur tour de moyen de propagation, et qui produit les actions malveillantes pour lesquelles il a été conçu.

2.6.2 Le ver (worms) :

Un ver est un programme qui se propage d'ordinateur à ordinateur via un réseau comme internet, ainsi contrairement à un virus, le ver n'a pas besoin d'un programme hôte pour assurer sa reproduction.son poids est très léger, ce qui lui permet de se propager à une vitesse impressionnante sur un réseau, et pouvant donc saturer ce dernier.

2.6.3 Chevaux de Troie (les trojans) :

Les trojans sont des programmes qui exécutent des opérations à l'insu de l'utilisateur afin d'ouvrir une porte dérobée (backdoor). Cette dernière permettra à un pirate de prendre le contrôle de la machine. en général, le trojan est caché dans un programme sain.

2.6.4 La bombe logique (soft bomb) :

Ce sont des programmes qui, à première vu semble inoffensif, activé soit à une date déterminée par son concepteur, soit lorsqu'une condition particulière se trouve vérifiée, ou un ensemble de conditions réunies, (un signal, une date), ou encore une action attendu d'un utilisateur et qui, dès lors, produit l'action malveillante pour laquelle il a été conçu.

2.6.5 Logiciel espion (spyware) :

Les logiciels espions, ou mouchards , sont des programme malveillant conçus pour surveiller les tâches que vous effectuez sur votre ordinateur et sur Internet, et pour transmettre ensuite ces renseignements à un tiers qui n'y aurait pas normalement accès. Ces programmes peuvent, entre autres choses, enregistrer les mots que vous tapez sur votre clavier, les mouvements de votre souris, les programmes que vous utilisez ou les sites que vous visitez sur Internet.

2.6.6 Le hijacker :

C'est un pirate de navigateur qui utilise les failles de sécurité d'internet explorer pour s'installer sur votre ordinateur.

2.6.7 Les hoax :

Un hoax (canulair) est un courrier électronique contenant une fausse information.et la diffusent à tout vos contactes.

2.6.8 Le spam :

Il s'agit, en général, de l'envoie massive et parfois répété, de courriers électronique non sollicité des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière.

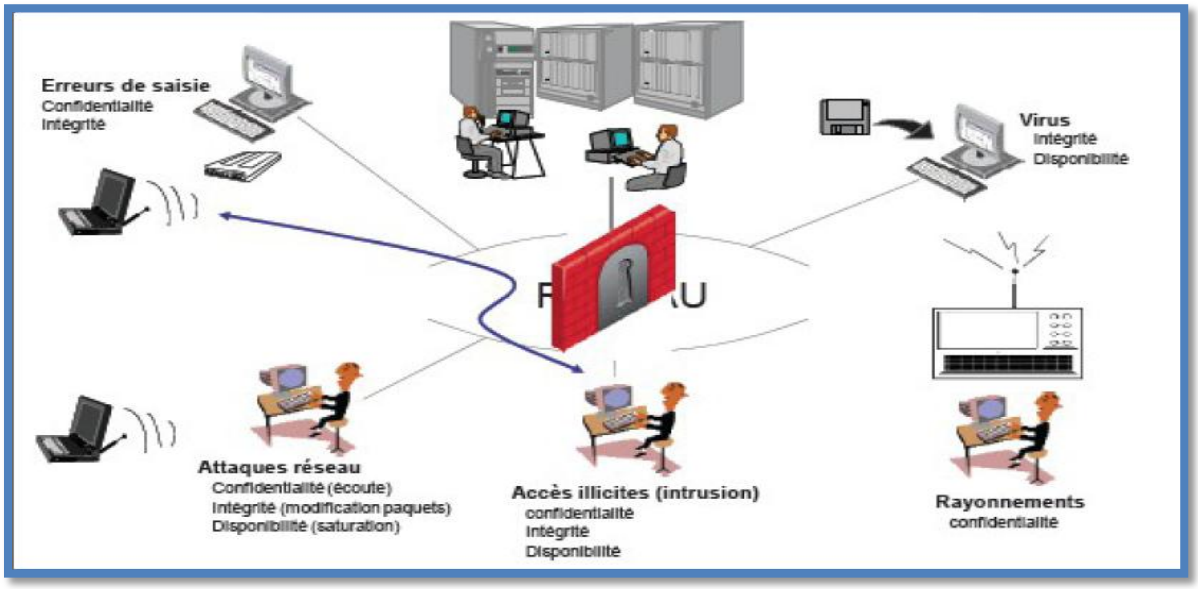


Figure III.2 Différents sources de menaces

3. Les vulnérabilités

La vulnérabilité est définie comme étant un niveau d'exposition face à une menace dans un certain contexte ; Dans le domaine de la sécurité informatique il existe trois familles de vulnérabilité

3.1 Vulnérabilité liés aux domaines physiques

- Manque de redondance et de ressource au niveau équipement
- Accès aux sales informatiques non sécurisé
- Absence ou mauvaise stratégie de sauvegarde de données

3.2 Vulnérabilité liés aux domaines organisationnels

- Manque de ressource humaine et personnelle qualifier communication
- Absence de contrôle périodiques document et procédures adaptés à l'entreprise
- Moyens adapté aux risques encourus
- Trop grande complexité fonctionnelle

3.3 Vulnérabilité liés aux domaines technologiques

- Failles nombreuses dans les services et applicatifs Web et les bases de données
- Pas de mise à jour du système d'exploitation et des collectifs
- Pas de contrôle suffisant sur les logiciels malveillants
- Récurrences des failles et absence de supervision des événements
- Mauvaise utilisation de la messagerie

4. La contre- mesure [13]

Ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique en prévention d'une menace (auquel cas il peut exister d'autre attaques sur la même vulnérabilité)

5. Les risques sur les réseaux informatiques [6]

Le risque est la possibilité qu'une chose critique apparaisse. Son évaluation permet d'établir des actions pour réduire et maintenir la menace à un niveau raisonnable et acceptable. Les risques peuvent être qualifiés selon leur origine (interne ou externe).Le risque dans le domaine de la sécurité informatique est calculé par la formule suivante :

Risque =menace * Vulnérabilité / contre-mesure

5.1 Les risques externes :

- **Attaque non ciblées :** toute entreprise est concerné par l'agression de virus ou d'attaques globales sur le réseau (dénis de service).
- **Attaques ciblées :** les risques physiques (vol ou destruction de matérielle) ou logique accès d'intrusion.

5.2 Les risques internes : ils sont plus difficiles à appréhender car ils concernent les ressources Internes de l'entreprise.

Il existe des facteurs aggravants de risque liés au métier de l'entreprise :

- **Les postes nomades** : ordinateur portable, assistance numérique de poche, téléphone évaluer (smart phone)
- Des infrastructures, services et applications mal protégée.
- Un plant de sauvegarde ou de secours informatique inexistant

5.3 L'impacte d'un risque

Il peut être exprimé par les conséquences ou les préjudices affectant un actif : atteint à l'intégrité, perte de disponibilité, atteint à l'image de marque, perte de chiffre d'affaires.

Les impactes peuvent être évalués selon les critères suivants :

- Financière (frés de remis en état ou de restauration, perte d'exploitation…)
- Juridique et légal
- Réputation et image de l'entreprise (par rapport à l'extérieure et au personnel)
- Expertise et savoir faire reconnus de l'entreprise

6. Définition d'une attaque

Une attaque est l'exploitation d'une faille d'un système à des fins non connues par l'exploitant du système et généralement préjudiciable. Une intrusion est consécutive à une attaque externe réussie, car avant de pénétrer dans le réseau cible il faut déployer certaines stratégies. On peut répartir les attaques en deux catégories :

6.1 Attaque passive

Une attaque passive constitue à écouter le trafic du réseau (ou de la machine) cible, afin de découvrir et de capturer les trames transitant pour y en déceler des informations particulières

Exemple : clé de cryptage, login et mot de passe …etc., et elle se réalise grâce à des outilles tel que les sniffer, les scanner.

6.2 Attaque active

Contrairement à une attaque passive, ici l'attaquant n'est plus en mode écoute. Consiste à s'introduire dans des équipements réseaux et de modifiées des données ou des messages, perturber le bon fonctionnement d'un réseau. A voir même contourner le dispositif de sécurité par divers méthodes.

7. Méthodologie d'une attaque

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma:

- ✓ **Identification de la cible :** cette étape est indispensable à toutes attaques organisées, elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'utilisation des bases Whois, l'interrogation des serveurs DNS,….
- ✓ **Le scanning :** l'objectif est de compléter les informations réunies sur une cible visées. Il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée (OS, versions des services, subnet, règles de firewall….). Il faut noter que certaines techniques de scans particulièrement agressives sont susceptibles de mettre à mal un réseau et entraîner la défaillance de certains systèmes.

- ✓ **L'exploitation :** Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau.

- ✓ **La progression :** Il est temps pour l'attaquant de réaliser ce pourquoi il a franchit les précédentes étapes. Le but ultime étant d'élever ses droits vers root (ou system) sur un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations, installation de backdoors, nettoyage des traces,…).

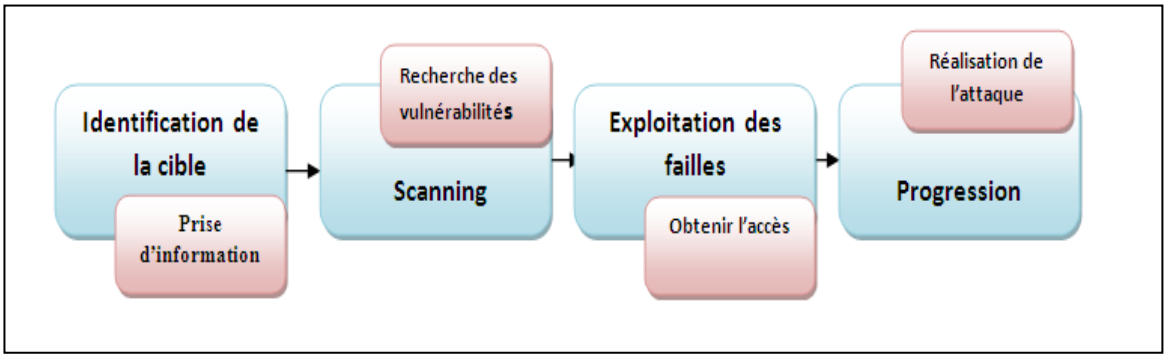


Figure III.3 Méthodologie d'une attaque

7.1 Type d'attaques les plus connus :

Les systèmes informatiques mettent en œuvre différentes composantes, allant de l'électricité pour alimenter les machines au logiciel exécuté via le système d'exploitation et utilisant le réseau.

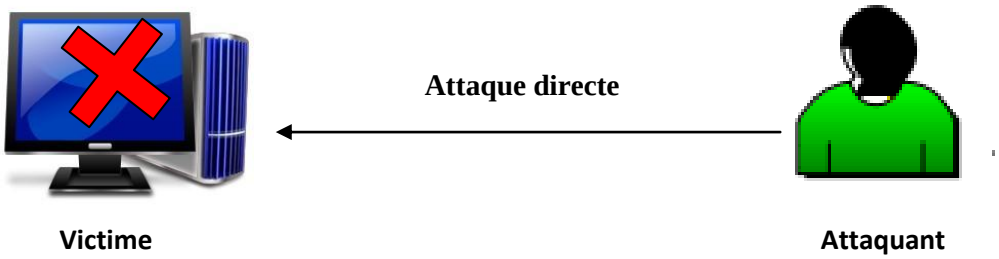
Les attaques peuvent intervenir à chaque maillon de cette chaîne, pour peu qu'il existe une vulnérabilité exploitable. Il existe un grand nombre, Néanmoins, la plupart d'entre elles ne sont que des variantes des quartes attaques réseaux les plus répondus aujourd'hui, et qui sont :

7.2 Les attaques réseaux

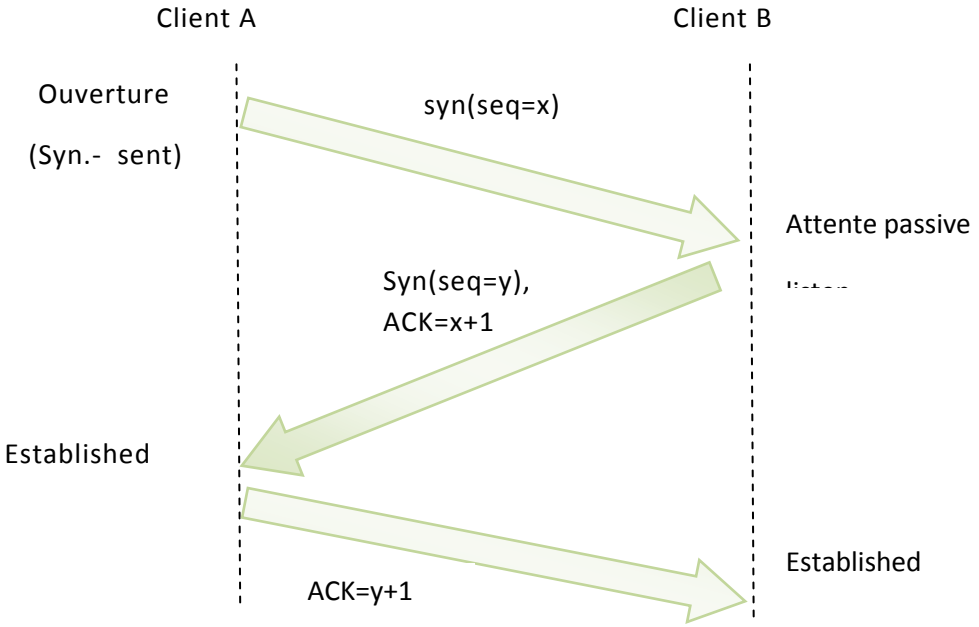
Nous avons choisie de se penché plus particulièrement aux attaques de surcharge réseaux, puisque l'une de ces attaques fait partie de notre champ d'étude, et le concept de ce type d'attaque et de rendre hors connexion le système d'information cible. Illustrons les principales attaques les plus répondu :

Attaques par dénis de service (DOS)

Ce type d'attaque consiste à saturer les ressources d'un système d'information de façon à l'empêcher de fonctionner correctement.Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur internet et éventuellement nuire à leur fonctionnement si leur activité repose sur un système d'information.



Cette technique d'attaque s'applique dans le cadre d'un protocole TCP (Transmission Control Protocol) et vise principalement à submerger le serveur cible d'une tonne de requêtes SYN (Synchronized), jusqu'à écroulement de ce dernier.



- **Attaques par réflexion (smurf)**

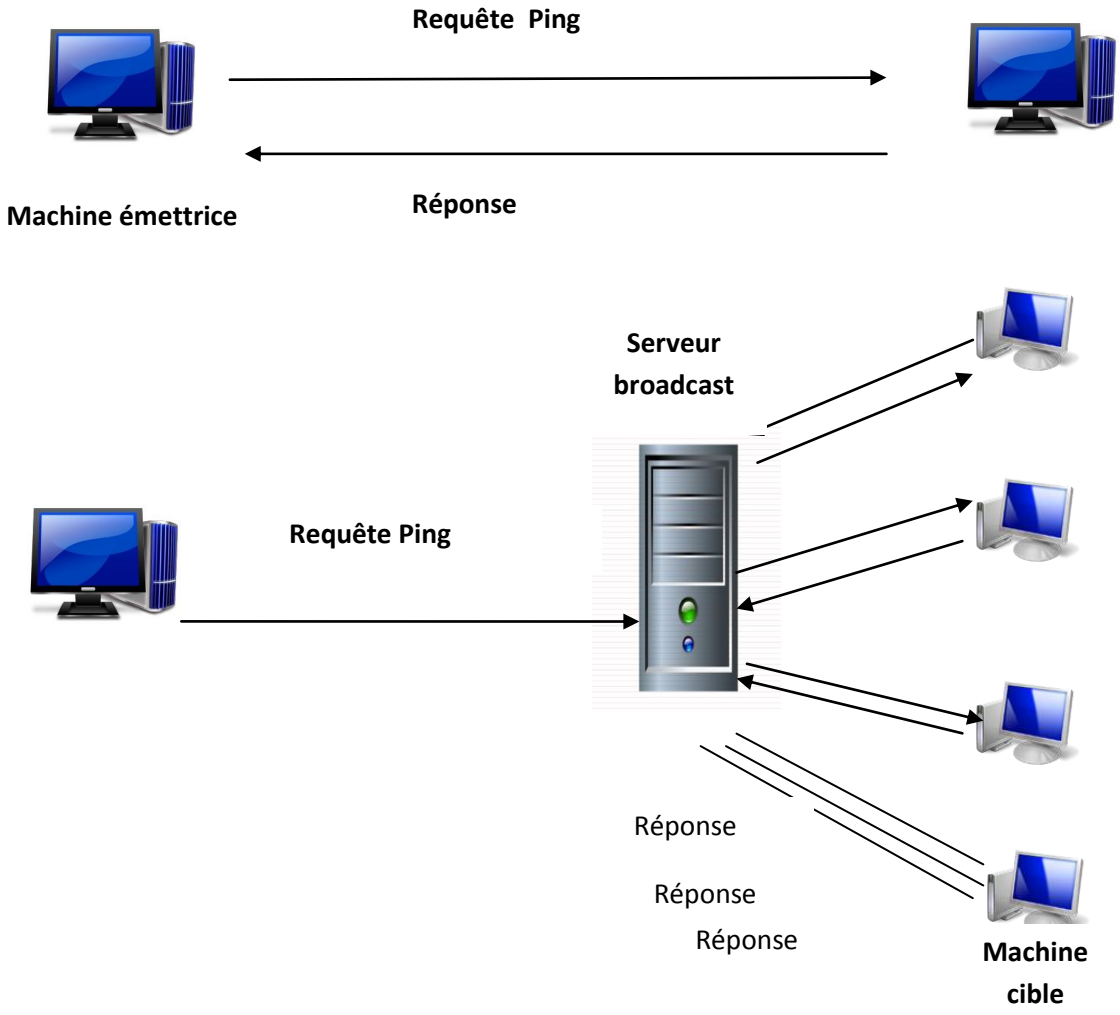
Cette méthode est basée sur l'utilisation de serveurs de diffusion **(broadcast)** pour paralyser un réseau. Le scénario de telle attaque est le suivant :

La machine attaquante envoie une requête **Ping** à un ou plusieurs serveurs de diffusion en falsifiant l'adresse IP source à laquelle le serveur doit théoriquement répondre en fournissant l'adresse IP de la machine cible.

Le serveur de diffusion répercute la requête sur l'ensemble du réseau, ensuite toute les machines du réseau envoient une réponse au serveur de diffusion.

Le serveur broadcast redirige les réponses vers la machine cible.

Ainsi, lorsque la machine attaquante adresse une requête à plusieurs serveurs de diffusion situés sur des réseaux différents, l'ensemble des réponses des ordinateurs des différents réseaux vont être routés sur la machine cible. Voir la figure ci-dessous.



- **Attaques par fragmentation (teardrop)**

Une attaque par fragmentation est une attaque réseau par saturation qui consiste à exploité le principe de fragmentation du protocole IP.

En effet, le protocole IP est prévu pour fragmenter les paquets de taille importante en plusieurs paquets IP possédant chacun un numéro de séquence et un numéro d'identification commun. A réception des données le destinataire réassemble les paquets grâce aux valeurs de décalage qu'ils contiennent.

Une des attaques les plus connues utilisant ces principes est le **teardrop,** son principe consiste à insérer des paquets fragmenté des informations de décalage erroné, ainsi lors de réassemblage il existe des vides ou des recoupements pouvant provoquer des instabilités du système.

7.3 Les attaques applicatives

Les attaques applicatives s'appuient principalement sur des vulnérabilités spécifiques aux applications utilisées.

- **Les scriptes :** Principalement web (ex. : Perl, PHP, ASP), ils s'exécutent sur un serveur et renvoient un résultat au client. Cependant, lorsqu'ils sont dynamiques (i.e. qu'ils utilisent des entrées saisies par un utilisateur), des failles peuvent apparaître si les entrées ne sont pas correctement contrôlées.

  L'exemple classique est l'exploitation de fichier à distance, telle que l'affichage du fichier mot de passe du système en remontant l'arborescence depuis le répertoire web.

- **Les injections SQL:** Tout comme les attaques de scripts, les injections SQL profitent de paramètres d'entrée non vérifiés. Comme leur nom l'indique, le but des injections SQL est d'injecter du code SQL dans une requête de base de données. Ainsi, il est possible de récupérer des informations se trouvant dans la base (exemple : des mots de passe) ou encore de détruire des données.

- **Les bogues :** Liés à un problème dans le code source, ils peuvent amener à l'exploitation de failles. Il n'est pas rare de voir l'exploitation d'une machine bloquée suite à une simple erreur de programmation. On ne peut toutefois rien faire contre ce type de problèmes, si ce n'est attendre un correctif de la part du développeur.

- **Les bufferoverflows :** Les buffer overflows, ou dépassement de la pile, sont une catégorie de bogue particulière.Issus d'une erreur de programmation, ils permettent l'exploitation d'un shellcode(3) à distance.

  Ce shellcode permettra à une personne mal intentionnée d'exécuter des commandes sur le système distant, pouvant aller jusqu'à sa destruction.

  L'erreur de programmation est souvent la même : la taille d'une entrée n'est pas vérifiée et l'entrée est directement copiée dans un buffer dont la taille est inférieure à la taille de l'entrée. On se retrouve donc en situation de débordement, et l'exploitant peut ainsi accéder à la mémoire.

8. Mécanisme de défense

La sécurité au sein d'une entreprise se repose sur plusieurs critères ; il y'as différentes procédures ou routines à suivre, différents outils à installer et a configurer qu'il soit de type hardware ou bien logiciel sans oublier les compagnes de sensibilisions, après voir cité les menaces nous allons aborder les moyens de défense.

8.1 La cryptographie

La cryptographie est une science mathématique qui concerne deux branches : **la cryptographi**e et **la cryptanalyse**.

La cryptographie traditionnelle est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible ; c'est ce que l'on appelle **le chiffrement**, qui, à partir d'un texte en clair, donne un texte chiffré ou cryptogramme. Inversement, le **déchiffrement**, est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Dans la cryptographie moderne, les transformations en question sont des fonctions mathématiques, appelées **algorithmes cryptographiques**, qui dépendent d'un paramètre appelé **clef**.

8.2 Encryptions, signature électronique et certificats

L'utilisation des techniques d'encryptions, de signature électronique et des certificats sont la base d'un commerce électronique sécurisé :

- **L'encryptions:**

Elle consiste à transformer les informations électroniques au moyen d'un algorithme mathématique afin de les rendre intelligibles, sauf pour celui qui possède le moyen (une clé) pour les décoder.

L'encryptions des informations qui transitent par le réseau est utilisée pour assurer la confidentialité, l'intégrité et l'authenticité des transactions et du courrier électronique.

Exemple :

Le logiciel d'encryptions gratuit Pretty good Privacy (PGP) est très largement employé pour protéger le courrier électronique.

- **La signature électronique :**

C'est un code digital qui valide l'identité des interlocuteurs d'une transaction électronique, associe une identité à une clé publique d'encryptions et fournit des informations de gestion complémentaire sur le certificat et le détenteur.

- **Le certificat :**

Document électronique (carte d'identité) émis par une autorité de certification. Il valide l'identité des interlocuteurs d'une transaction électronique, associe une identité à une clé public d'encryptions et fournit des informations de gestion complémentaires sur le certificat et le détenteur.

8.3 L'authentification et l'autorisation

Une personne peut être authentifiée par la combinaison d'une identification et d'un mot passe (code secret personnel).Le mot passe doit posséder certaines caractéristiques (non trivial, difficile à deviner, régulièrement modifié, secret, etc.…), Des outils logiciels ou hardware de génération de mot de passe existent. L'authentification précède généralement l'autorisation.

L'autorisation définit les ressources, services et informations que la personne identifiée peut utiliser et dans qu'elle mesure (par exemple consulter ou mettre à jour des données).

Les techniques d'encryptions et de certificats utilisés conjointement à celle des mots de passe ajoutant un très haut degré de sécurité dans le domaine de l'authentification.

8.4 Les fichiers historiques

Ces outils doivent être mis en ouvre pour garder une trace des événements comme par exemple : Quelle ont été les ressources utilisées ?

La consultation régulière des fichiers historiques constitués doit notamment permettre de vérifier les anomalies dans le trafic des transactions (par exemple les messages répétitifs en Provence peuvent être un signe d'essai d'intrusion).

8.5 Les copies de sauvegarde

Les copies de sauvegardes (back-up) créées régulièrement et stocker dans des endroits sécurités permettant de protéger les informations essentielles pour l'entreprise et permette également de redémarrer rapidement en cas de problème.

8.6 Antivirus

Sont des logiciels permettant de détecter et de supprimer les virus informatiques sur n'importe quel type de stockage (disque dure, disquette, CD-ROM etc.).Pour être efficace ce type de logiciel demande des mises à jour très fréquentes au coure desquelles il mémorise les nouvelles formes de virus en circulation.

8.7 Anti-spam

Les logiciels anti-spam peuvent aider à mieux gérer son logiciel d'email, à faire le tri automatiquement entre vos mails et le spam, voire à effacer bon nombres de spam avant même qu'ils arrivent dans vos boites.

8.8 Le firewall

Un pare-feu (firewall en anglais) est un système physique (matériel) ou logique (logiciel) servant d'interface entre un ou plusieurs réseaux afin de contrôler et éventuellement bloquer la circulation des paquets de données.

8-9 Les IDS

Il s'agit d'un équipement permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de se prémunir contre d'éventuelles attaques.

Conclusion

La sécurité a 100% n'existe pas ; la sécurité est un travail qui se maintient au quotidien avec la mise en place d'une politique de sécurité adaptée au domaine à protéger, ainsi que la formation des personnes au risques et aux dangers de l'ignorance informatique (la mise à jour des systèmes d'exploitations,des anti-virus, l'ouverture d'un mail spam …..) peut limiter, voire éliminer les risques encourus à l'utilisation d'un système informatique.

Suite à ce chapitre qui a fait le tour des principes de bases relatifs à la sécurité informatique et aux menaces et vulnérabilités qui s'y reportent, ainsi qu'aux différents mécanismes de défense connus à ce jour ; nous avons voulu nous pencher de plus près dans, le prochain chapitre, sur l'un de ses derniers, à savoir la détection d'intrusions.

Chapitre IV :

Les Systèmes de détection d'intrusions

Introduction

Le cout de la mise en place d'une politique de sécurité au niveau des entreprises est assez élevée, ce qui pousse les administrateurs réseaux à utiliser des moyens peu onéreux parmi ceux-ci on trouve les Systèmes de détection d'intrusions (IDS) qui constitue une bonne alternative pour mieux protéger le réseau informatique, mais aussi avec un bon rapport qualité-prix.

Avant d'entamer le domaine de détection d'intrusion, nous allons vous présenter la notion de détection d'intrusion et illustrer par la suite les différentes sortes d'IDS, chacun intervenant à un niveau différent. Nous étudierons ensuite leurs mode de fonctionnement, c'est-à dire les modes de détection utilisés et les réponses apportées par les IDS.

1. Terminologie d'un système de détection d'intrusion

2. Qu'est ce que la détection d'intrusion ?

L'intrusion peut être définie comme n'importe quel ensemble d'actions qui essaye de compromettre, l'intégrité, la confidentialité ou l'accessibilité d'une ressource. Les différentes formes d'intrusion peuvent être regroupées en deux classes :

- **Intrusion connues :** Ces intrusions sont des attaques bien définies, qui généralement exploitent des failles connues des systèmes cibles.
- **Intrusion non connus (anomalies) :** ces intrusions sont considérées comme des déviations du profile normal d'un système. Elles sont détectées dès qui il est observé un comportement anormal du système.

Maintenant, que nous avons éclaircie le terme intrusion on passe au concept de **La détection d'intrusion** qui consiste à analyser les informations collectées par un mécanisme d'audit de sécurité à la recherche d'éventuelle attaques.

3. Définition d'un système de détection d'intrusion [5]

Un **systèmede détection d'intrusion** ou IDS s'agit d'un équipement matériel ou bien logiciel permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion (volontaire ou non) et éventuellement de réagir à cette tentative.

Certains termes sont souvent employés quand on parle d'IDS, comme :

- **Faux positif** : une alerte provenant d'un IDS, mais qui ne correspond pas à une attaque réelle.
- **Faux négatif** : une intrusion réelle qui n'a pas été détectée par l'IDS.

4. Description d'un système de détection d'intrusion

Un système de détection d'intrusion à un niveau très macroscopique, peut être décrit comme un détecteur .Ce détecteur est un moteur d'analyse qui reçoit des données de trois sortes de ressources .L'analyse de ces données génère une décision d'évaluation de la probabilité que ces actions peuvent être comme des symptômes d'intrusion. Ces donnés sont :

- Des informations de configuration relatives à l'état actuel du système ;
- Des informations à long terme relative à la technique utilisé pour détecter les intrusions par exemple une base de connaissance d'attaque ;
- Des systèmes d'information venant du système à protéger qui à partir des informations d'audit décrivant les événements qui apparaissent dans le système.

5. Caractéristiques d'un système de détection d'intrusion [15]

- **La distribution:** un grand nombre d'attaques réseaux se caractérisent par des comportements anormaux à différents éléments du réseau (serveur, routeur,…). Il est donc très important de distribuer les fonctions de détection à plusieurs entités qui surveillent différents points du réseau ;
- **L'autonomie:** des échanges excessifs d'informations entre les entités distribuées peuvent congestionner le réseau. Il serait donc plus judicieux de laisser l'entité, surveillant un élément réseau, effectuer une analyse locale et détecter les comportements intrusifs locaux. Ainsi, les entités distribuées doivent être autonomes ;
- **La délégation :** La dynamicité des réseaux nécessite de pouvoir modifier, à n'importe quel moment, les fonctions de détection d'intrusions pour les adapter aux changements se produisant dans le réseau surveillé. Cela est possible grâce au modèle de délégation. Les tâches déléguées sont envoyées aux entités autonomes. Chaque entité aura à exécuter sa propre tâche. Lorsque de nouvelles tâches doivent être ajoutées, ceci est fait dynamiquement ;

- **La communication et coopération** : la complexité des attaques coordonnées ne facilite pas leur détection par une seule entité. En effet, chaque entité n'ayant qu'une vue locale restreinte du réseau, il lui est très difficile de détecter ce type d'attaques. La détection de ce genre d'attaques, nécessite une corrélation des différentes analyses effectuées à différents points du réseau.
  Les différentes entités doivent alors se communiquer leurs analyses et coopérer afin de détecter efficacement les attaques coordonnées.
- **La réactivité :** l'objectif majeur de la détection d'intrusions est de réagir rapidement lorsqu'une attaque se produit afin de limiter les dommages qui peuvent être causés.
- **L'adaptabilité:** les politiques de sécurité d'une entreprise peuvent changer. Dans ce cas, l'administrateur doit changer et/ou rajouter de nouvelles politiques afin de modifier et réadapter les tâches de détection d'intrusions. Le système de détection d'intrusions doit alors s'adapter à ces changements.

6. L'architecture générale d'un IDS :

L'architecture d'un IDS se traduit par trois niveau bien distinct dont

- ✓ **Niveau 1:** collecte de données
- ✓ **Niveau 2** : analyse des données collectées
- ✓ **Niveau 3** : système de prise de décision

Un IDS possède quatre fonctions principales : l'analyse, la journalisation, la gestion et l'action.

- ✓ **Analyse :** Analyse des journaux du système pour identifier des intentions dans la masse de données recueillie par l'IDS. Il ya deux méthodes d'analyse : une basée sur les signatures d'attaque, et l'autre sur la détection d'anomalies.
- ✓ **Journalisation :** Enregistrement des événements dans un fichier de log.
- ✓ **Gestion :** Les IDS doivent êtres administrés de manière permanente. On peut assimiler un IDS à une caméra de sécurité.
- ✓ **Action :** Alerter l'administrateur quand une attaque dangereuse est détectée.

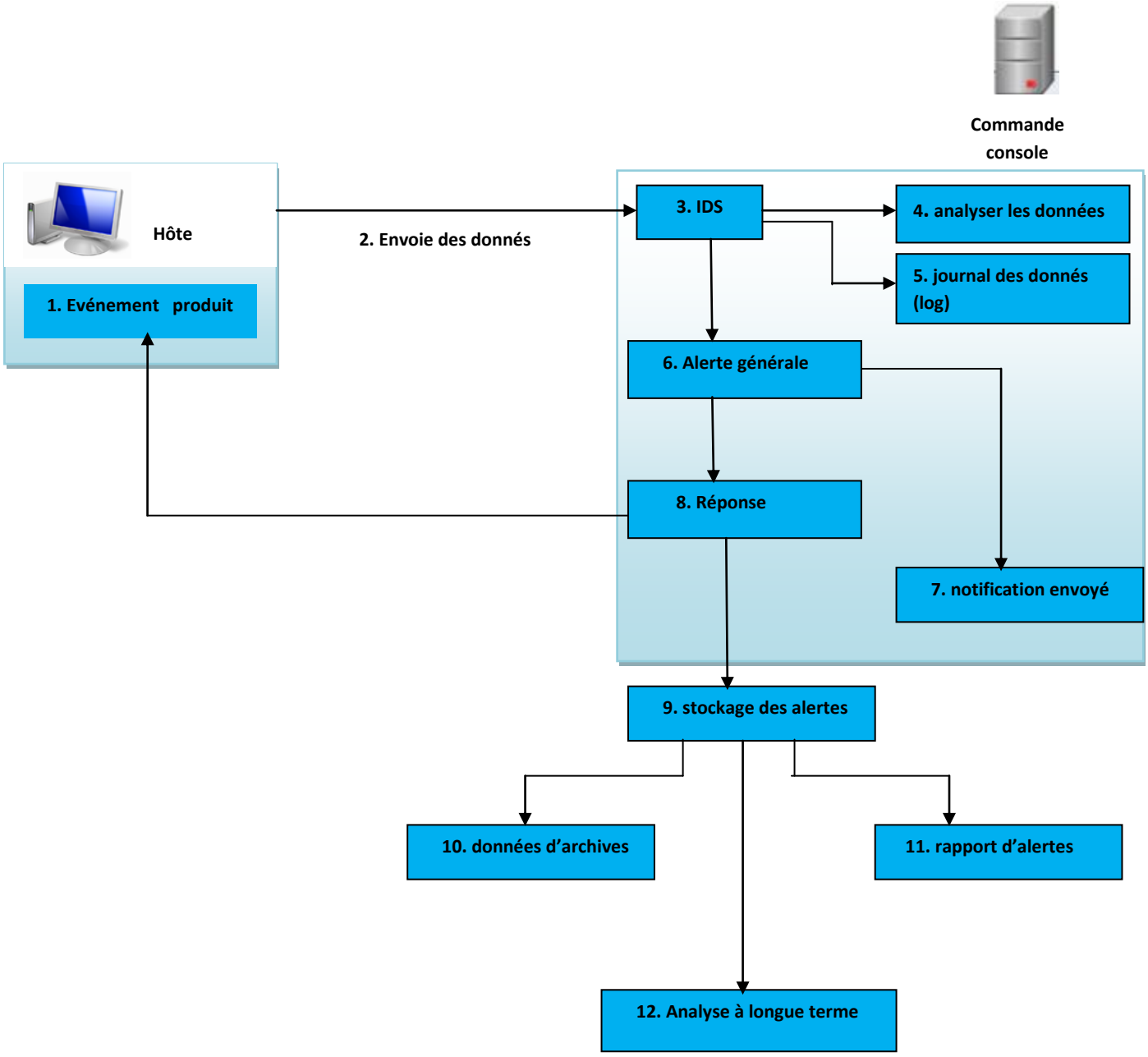


Figure IV.1 Architecture générale d'un IDS

7. Classification des systèmes de détection d'intrusion [15]

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

- ✓ La méthode de détection.
- ✓ Le comportement de l'IDS après la détection.

- ✓ La source des données.
- ✓ La fréquence d'utilisation.
- ✓ Architecture

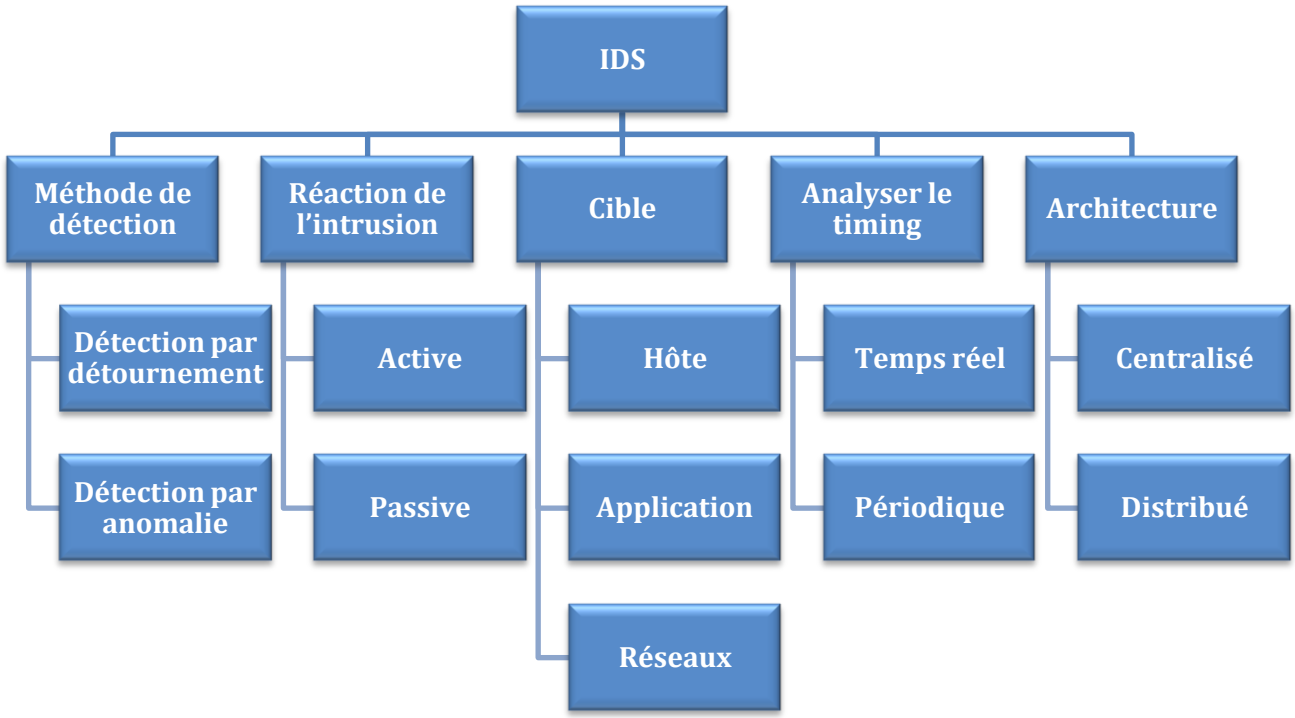


Figure IV.2 Taxonomie des systèmes de détection d'intrusions

8. Principe de fonctionnement des IDS [7]

Pour bien gérer un système de détection d'intrusions, il est important de comprendre comment celui-ci fonctionne :

- ✓ Comment reconnaître/définir une intrusion?
- ✓ Comment une intrusion est-elle détectée par un tel système ?
- ✓ Quels critères différencient un flux contenant une attaque d'un flux normal ?

Ces questions nous ont amené à étudier le fonctionnement interne des IDS.

Il existe plusieurs méthodes permettant de détecter une intrusion :

8.1 Approche par scénario ou par signature :

Consiste à détecter des signatures d'attaques connues dans les paquets circulant sur le réseau.Cette technique s'appuie sur la connaissance des techniques utilisées par les attaquants pour déduire des scénarios typiques. Elle ne tient pas compte des actions passées de

l'utilisateur et utilise des signatures d'attaques existantes (ensemble de caractéristiques permettant d'identifier une activité intrusive : une chaîne alphanumérique, une taille de paquet inhabituelle, une trame formatée de manière suspecte, …).

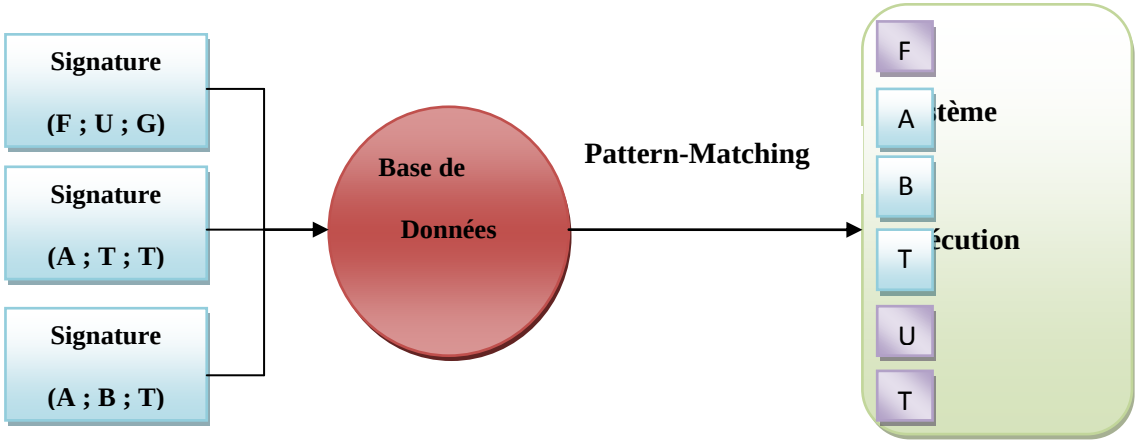


Figure IV.3 : Approche par scénario ou par signature

Cette technique se base sur :

- ✓ **La recherche de motifs (pattern matching) :**

C'est la méthode la plus connue et la plus facile à comprendre. Elle se base sur la recherche de motifs (chaînes de caractères ou suite d'octets) au sein du flux de données.L'IDS comporte une base de signatures où chaque signature contient les protocoles et ports utilisés par une attaque spécifique ainsi que le motif qui permettra de reconnaître les paquets suspects.

De manière analogue, cette technique est également utilisée dans les anti-virus. En effet un anti-virus ne peut reconnaître un virus que si ce dernier est reconnu dans sa base de signatures virale, d'où la mise à jour régulière des anti-virus.

- ✓ **Recherche de motifs dynamiques**

Le principe de cette méthode est le même que précédemment mais les signatures des attaques évoluent dynamiquement. L'IDS est de ce fait doté de fonctionnalités d'adaptation et d'apprentissage.

- ✓ **Analyse de protocoles**

Cette méthode se base sur une vérification de la conformité des flux, ainsi que sur l'observation des champs et paramètres suspects dans les paquets. L'analyse protocolaire est souvent implémentée par un ensemble de préprocesseurs (programmes ou plug-in), où chaque

préprocesseur est chargé d'analyser un protocole particulier (FTP, HTTP, ICMP, ...). Du fait de la présence de tous ces préprocesseurs, les performances dans un tel system en voient fortement dégradées (occupation du processeur).

L'intérêt fort de l'analyse protocolaire est qu'elle permet de détecter des attaques inconnues, contrairement au pattern matching qui doit connaître l'attaque pour pouvoir la détecter.

- ✓ **Analyse heuristique et détection d'anomalies**

Le but de cette méthode est, par une analyse intelligente, de détecter une activité suspecte ou toute autre anomalie (une action qui viole la politique de sécurité définie dans l'IDS). Par exemple une analyse heuristique permet de générer une alarme quand le nombre de pings vers un réseau ou hôte est très élevé ou incessant (Ping de la mort).

8.2 Approche comportementale ou par Anomalie

Consiste quant à elle, à détecter une activité suspecte dans le comportement de l'utilisateur**.**

Remarque : Cesdeux techniques, aussi différentes soient-elles, peuvent être combinées au sein d'un même système afin d'accroître la sécurité.

Cette technique consiste à détecter une intrusion en fonction du comportement passé de l'utilisateur. Il faut préalablement dresser un profil utilisateur à partir de ses habitudes et déclencher une alerte lorsque des événements hors profil se produisent. Cette technique peut être appliquée non seulement à des utilisateurs mais aussi à des applications et services.

Plusieurs métriques (paramètres) sont possibles : la charge CPU, le volume de données échangées, le temps de connexion sur des ressources, la répartition statistique des protocoles et applications utilisés, les heures de connexion, ...

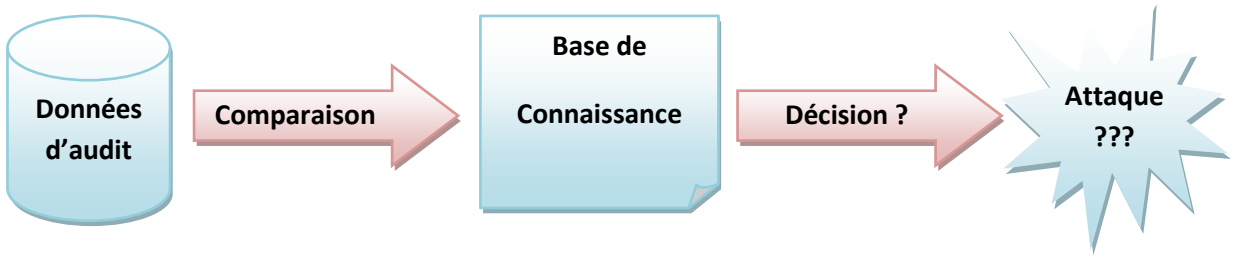


Figure IV.4 : Approche comportementale

8.3 Approche probabiliste

On prévoit quelle est la probabilité d'avoir un évènement après un autre.

Exemple : quelqu'un qui se connecte à un site : forte probable que la demande de connexion soit suivi de GET http://www.google.fr HTTP/1.0 Et on peut supposer que ce sera suivi de 8 TP/1.1 200 OK Si ce n'est pas ça la plupart du temps, on peut avoir un doute…

8.4 Approche statistique

Effectue des tests sur d'autres éléments concernant l'utilisateur

- Le taux d'occupation de la mémoire
- L'utilisation des processeurs
- La valeur de la charge réseau
- Le nombre d'accès à l'Intranet par jour

9. Comment mesurer l'efficacité d'un système détection d'intrusion ?

L'efficacité d'un système de détection d'intrusion est déterminée par les mesures suivantes :

- **Exactitude :** Le système de détection d'intrusion n'est pas exact s'il considère les actions légitimes des utilisateurs atypique ou intrusive.
- **Performance :** La performance d'un système de détection d'intrusion est mesurée par le taux de traitement des traces d'audits, Si la performance d'un système de détection est pauvre, donc la détection en temps réel n'est pas possible.
- **Perfection :** Un système de détection d'intrusion est imparfait s'il n'arrive pas à détecter une attaque.
- **Tolérance aux pannes :** Un système de détection doit être résistant aux attaques, en particulier dans le cas de déni de services.
- **Opportunité :** Un système de détection d'intrusions doit exécuter et propager son analyse d'une manière prompte pour permettre une réaction rapide dans le cas d'existence d'une attaque.

10. Les différents types d'IDS

Comme nous l'avons vu, les attaques utilisées par les pirates sont très variées. Certaines utilisent des failles réseaux et d'autres des failles de programmation. Nous pouvons donc

facilement comprendre que la détection d'intrusions doit se faire à plusieurs niveaux. Ainsi, on peut justifier l'existence de plusieurs types d'IDS/IPS.

Pour répondre à des problématiques précises selon les occurrences d'utilisations de ces dernières et les fonctions qu'ils doivent remplir, ci-dessous nous allons citer les catégories des IDS et nous détaillons leur caractéristique principale :

- ✓ Les systèmes de détection d'intrusions réseau(NIDS).
- ✓ Les systèmes de détection d'intrusions de type hôte(HIDS).
- ✓ Les systèmes de détection d'intrusions hybride.
- ✓ Les systèmes de détection d'intrusions et prévention réseau (NIPS).
- ✓ Les systèmes de détection d'intrusion et prévention de type hôte(HIPS).

10.1 Les systèmes de détection d'intrusions réseau (NIDS)

Les NIDS sont des IDS dédiés aux réseaux. Ils comportent généralement une sonde (machine par exemple) qui "écoute" sur le segment de réseau à surveiller, un capteur et un moteur qui réalise l'analyse du trafic afin de détecter les intrusions en temps réel. Un NIDS écoute donc tout le trafic réseau, puis l'analyse et génère des alertes si des paquets semblent dangereux.

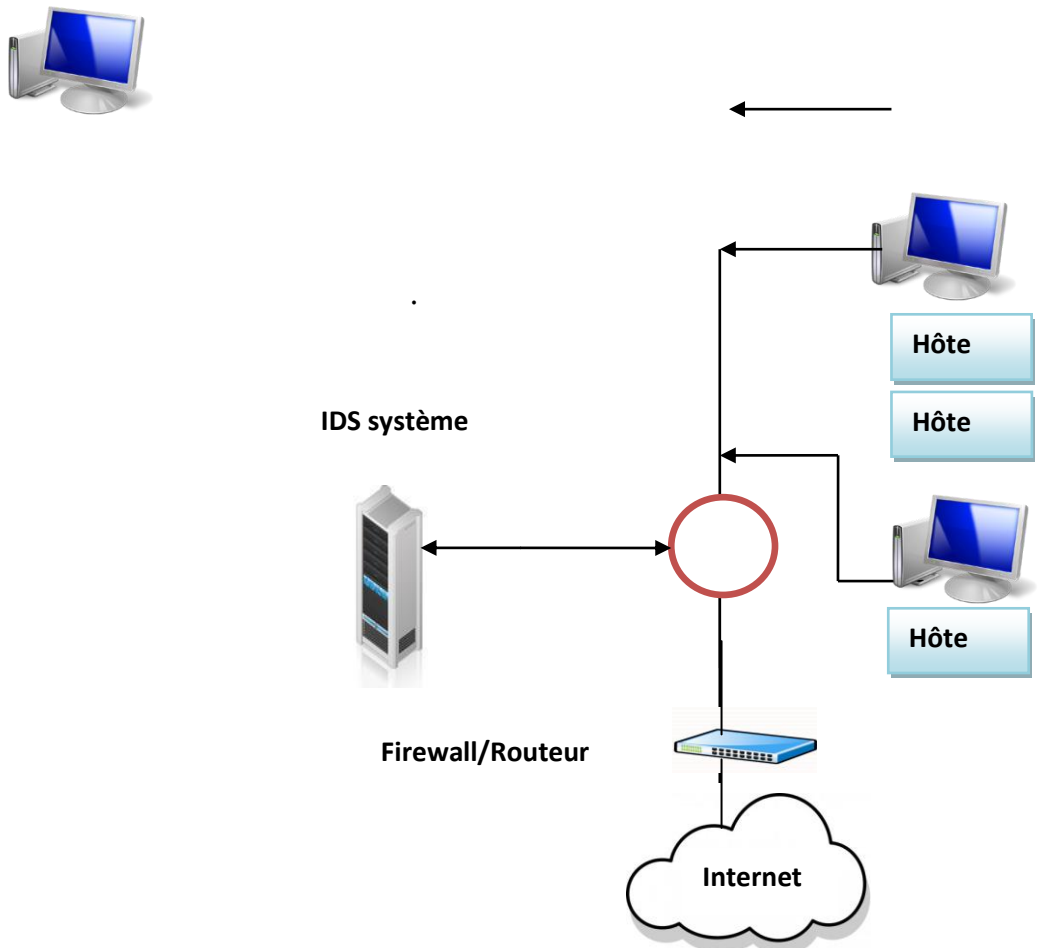


Figure IV.5 : Modèle d'un NIDS

10.2 Les systèmes de détection d'intrusion de type hôte (HIDS)

Un HIDS se base sur une unique machine, n'analysant cette fois plus le trafic réseau ; mais l'activité se passant sur cette machine. Il analyse en temps réel les flux relatifs à une machine ainsi que les journaux.

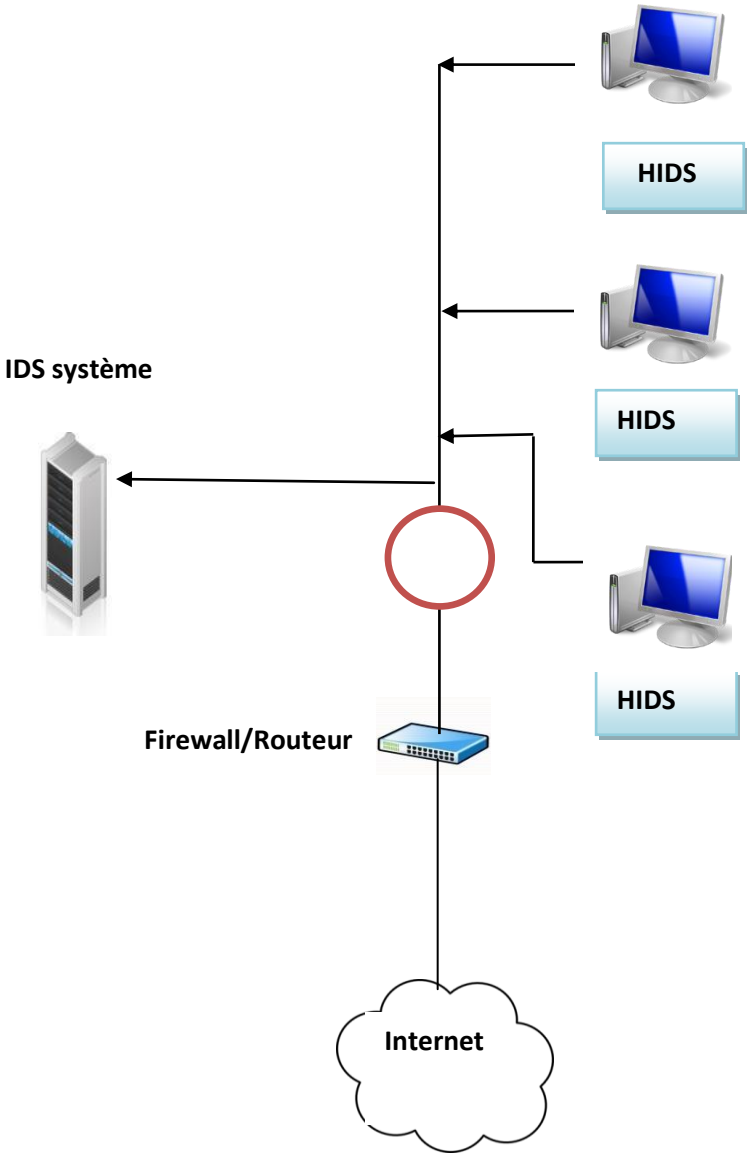


Figure IV.6 : Modèle d'un HIDS

Ci-joint un tableau comparatifs des différents avantages et inconvénients relatifs aux NIDS et HIDS :

Comparaison entre NIDS/HIDS :

NIDS	HIDS
Large portée	Portée limitée spécifique à l'hôte dont lequel l'IDS est installé
Examine l'entête des paquets plus leurs contenus	N'analyse pas les entête des paquets ni leur contenu
Réponse en temps réel	Répond après une détection d'intrusion
Ne dépend pas de l'hôte	Dépend de l'hôte
Dépend de la bande passante	Indépendant de la bande passante
Pas de surcharge	surcharge
Ralenti le réseau quand il ya des clients IDS installés	Ralenti les hôtes sur les quelles l'IDS est installé
Détecte les attaques réseau une fois le flux analysé	Détecte l'attaque au niveau hôte avant quelle ne se propage au réseau
Il n'est pas conseiller pour les réseaux encrypté et les Switch réseaux	Il est bien approprié pour l'environnement crypté avec des Switch
Il n'est pas performant pour détecter des attaques complexes	Outil puissants pour la détection des attaques dés qu'il possède une base de données
Taux de détection de faux positif élevé	Taux de détection de faux positif minimum
Faible cout pour l'installation	Besoin d'être compléter avec d'autre équipements physiques
Très performant pour détecter les attaques de l'externe	Performent pour détecter les attaques internes

10.3 Les systèmes de détection hybrides

Généralement utilisés dans un environnement décentralisé, ils permettent de réunir lesinformations de diverses sondes placées sur le réseau. Leur appellation « hybride » provient du fait qu'ils sont capables de réunir aussi bien des informations provenant d'un système HIDS qu'un NIDS pour une visualisation centralisée des attaques.

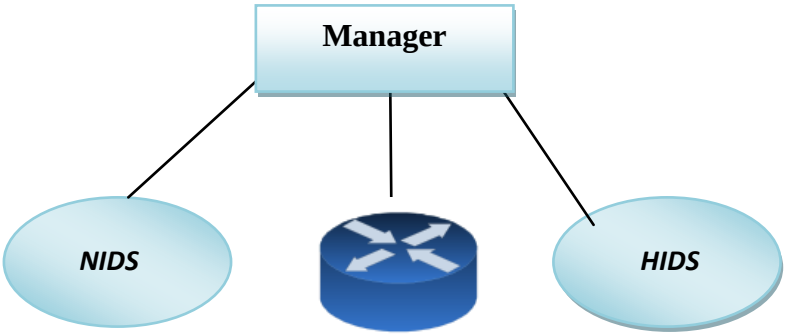


Figure IV.7 : Système de détection hybride

11. Les systèmes de prévention d'intrusion (IPS) [19]

Les IPS ont pour fonction principale d'empêcher toute activité suspecte détectée au sein d'un système : ils sont capables de prévenir une attaque avant qu'elle atteigne sa destination.Contrairement aux IDS, les IPS sont des outils aux fonctions « actives », qui, en plus de détecter une intrusion, tente de la bloquer.

On peut classer les IPS en deux groupes suivants leurs domaines d'utilisation :

11.1 Les systèmes de prévention d'intrusion réseau : Network IPS dédiés aux réseaux.

Ils ont les mêmes fonctions que les IDS classiques, sauf qu'ils ont la capacité d'anticiper une attaque.

11.2 Les systèmes de prévention d'intrusion hôte : Host IPS, plus connu sous l'appellation de systèmes de prévention d'intrusions.

11.3 Les systèmes de prévention d'intrusion karnel (KIPS) : spécifiques aux hôtes. Ils supervisent l'intégralité des activités sur la machine où elle est déployée.L'utilisation d'un détecteur d'intrusions au niveau noyau peut s'avérer parfois nécessairepour sécuriser une station.

12. Choix d'emplacement d'un IDS

L'IDS peut se placer à différent endroits stratégiques du réseau, tout dépend ce que l'en veut surveiller, et quelles informations que l'on veut. Mais il existe des positions que l'on peut qualifier de standard, par exemple il serait intéressant de placer des IDS :

Emplacement 1 :

1. **Dans la zone à protégé (démilitarisée) :** pour observer les attaques contre les systèmes publics.

Emplacement 2 :

2. Devant le pare-feu : Mais sa serai très probablement un gaspillage de ressources de le placer ici, c'est le meilleur endroit pour analyser les attaques externes contre l'entreprise.

Emplacement 3 :

3. **Dans le réseau privé :** pour voire les intrusions vers ou depuis internet.
4. **Derrière le pare-feu :** pour une possibilité de détection de signes parmi tout le trafic entrant et sortant.

Chacun de ces positionnements a ces avantages et inconvénients. Le plus important est de bien identifier ce que l'on veut protéger et ce qui est susceptible d'être attaqué.

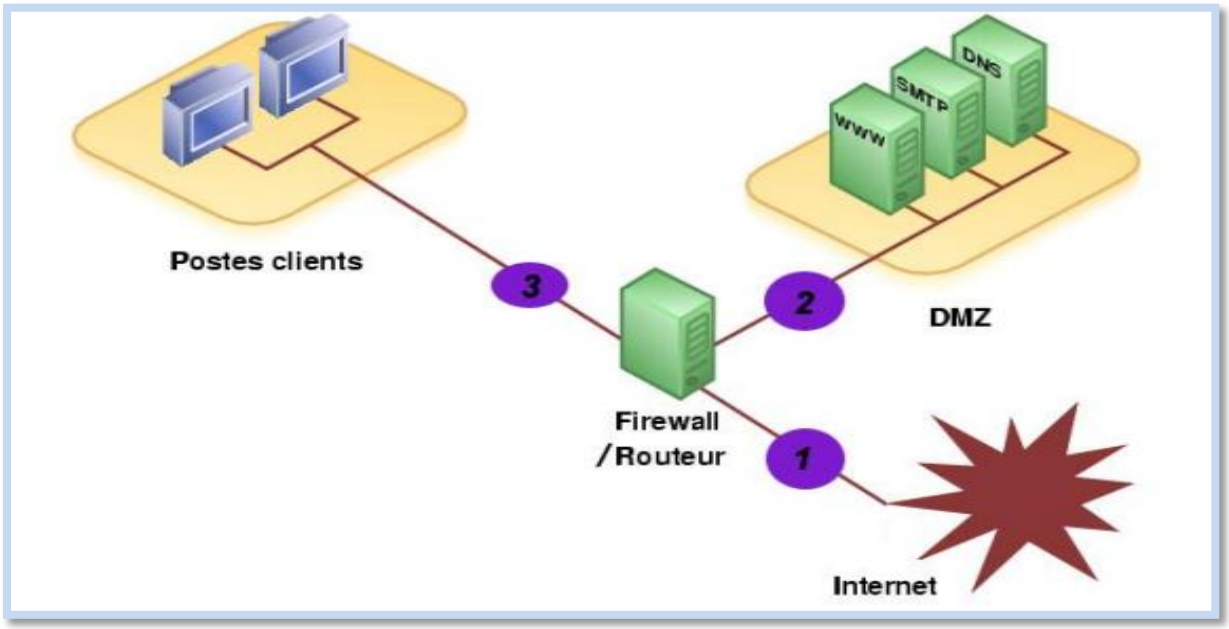


Figure IV.8 : Choix d'emplacement d'un IDS

Conclusion

A travers ce chapitre, nous avons abordé en détail les systèmes de détection d'intrusions. Nous avons présenté toutes les notions et concepts nous permettant de passer un une étude concrète sur ces derniers.

Le dernier chapitre explore l'étude et la simulation d'attaques sous un environnement de détection d'intrusion Suricata .

Chapitre V :

Simulationd'attaquesur des ressources protégées dans un environnement Suricata

Introduction

Le présent chapitre présente la simulation d'une attaque type « ForceBrute » sur un serveur de messagerie dans un réseau virtuel configuré pour détecter les intrusions en se basant sur l'IDS Suricata.

On s'efforcera d'expliquer le choix de cet outil comme solution au problème étudié, Comment simuler une attaque en tenant compte comme cible d'attaque le serveur de messagerie (SMTP, POP3). En outre, nous allons éclaircir les détails de déploiement.

1. Description de l'environnement de développement

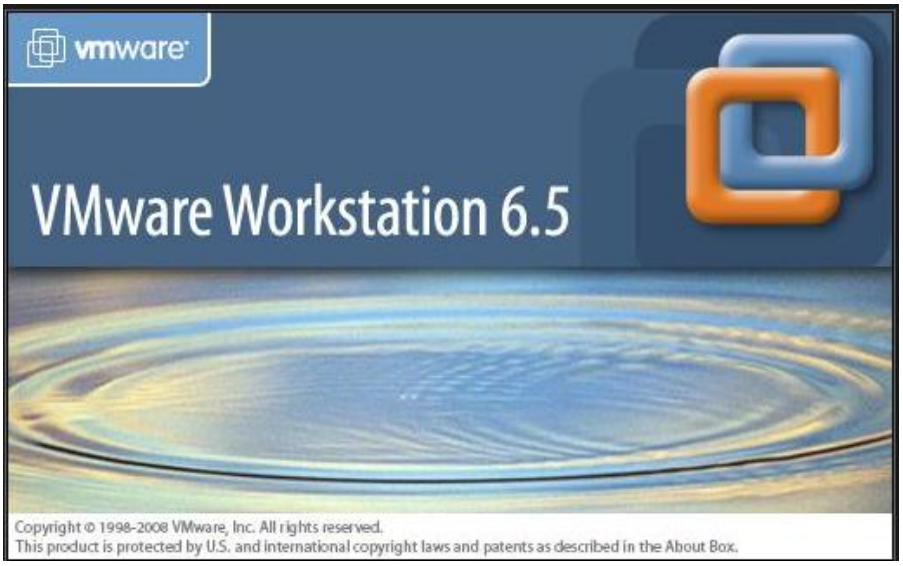
1.1 Qu'est-ce que la virtualisation?

La virtualisation fait appel à un logiciel pour simuler l'existence du matériel et créer un système informatique virtuel. Ce modèle permet aux entreprises d'exécuter plusieurs systèmes virtuels et plusieurs systèmes d'exploitation sur un seul et même serveur physique .Il se traduit ainsi par des économies d'échelle et des gains d'efficience.

Dans le cadre de notre travail, nous faisons appel **VMware** Workstation.

1.2 Présentation du VMware Workstation

Vmware Workstation est une solution professionnelle de virtualisation qui permet de faire tourner plusieurs systèmes d'exploitation momentanément sur la même machine physique, sans avoir besoin de partitionner les disques.Vmware fonctionne comme un pont entre la machine réelle et la machine virtuelle pour tous les types de ressources matérielles, y compris les disques durs, les périphérique USB et CD-ROM, tous les pilotes de périphérique sont installés par la machine hôte.



Il permet aux administrateurs réseaux et systèmes de vérifier, tester et implémenter des environnements client/ serveur ou autres.

1.3 Installation de VMware Workstation

L'installation est VMware est une installation wizard simple et facile à suivre. Les différentes étapes et les étapes de la création des machines virtuelles nécessaires seront décrites en annexe.

2. Configuration de l'environnement de simulation

2.1 Création des machines virtuelles et leur configuration

Maintenant que l'installation de VMware Workstation est terminée et la création des machines virtuelles l'est aussi, nous pouvons à présent passer à la seconde étape qui est la configuration de notre réseau.

Ce dernier comprend trois machines virtuelles :

- **VM1(Serveur)** ⟶ dédié à un serveur (serveur de messagerie hmail serveur SMTP, POP3)
- **VM2 (Suricata)** ⟶ dédié IDS/IPS suricata (Système de détection et de prévention d'intrusions)
- **VM3(Externe)** ⟶ dédié à une machine (client externe**)**

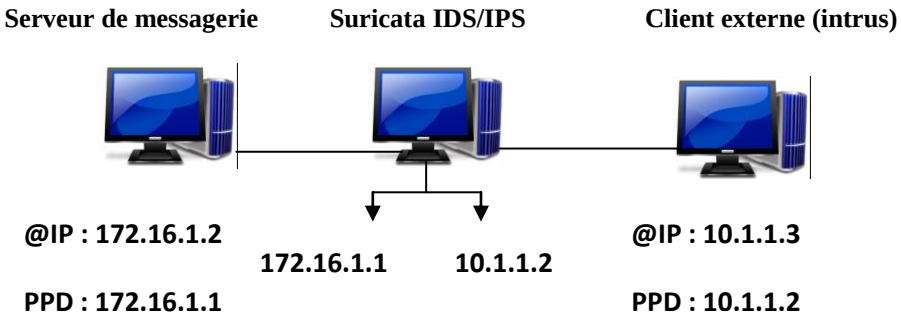
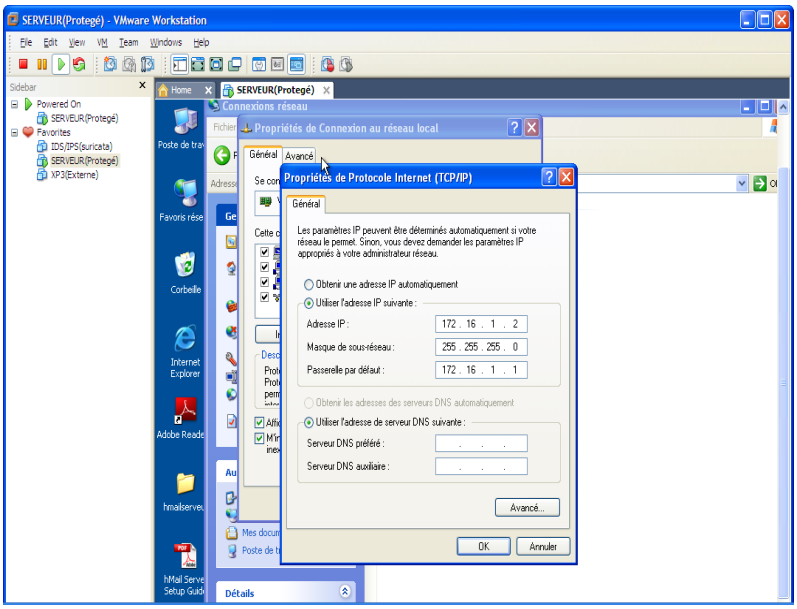


Figure V.1 Configuration d'adressage réseau

Configuration des adresses IP :

Cliquer sur favoris réseau, puis sur propriétés de Protocol Internet (TCP/IP) comme illustré dans la figure suivante :



Nous allons attribuer des adresses IP et passerelles pour chaque machine comme illustré dans la **figure V.1**

Tester la connectivité des VM en effectuant des pingsentre les machines.

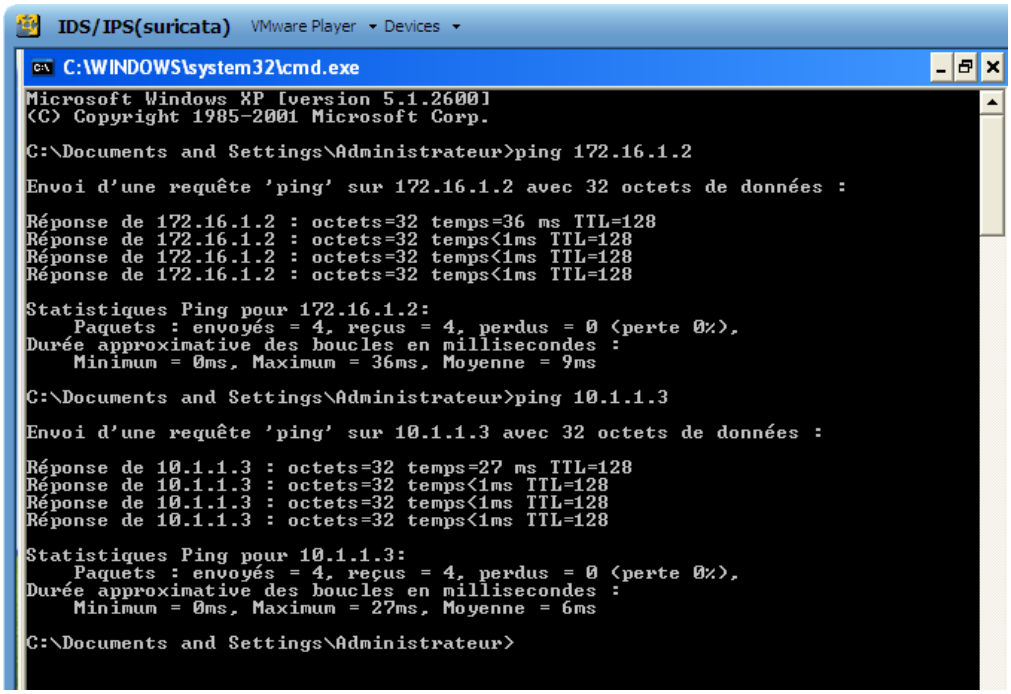


Figure V.2 : teste de la connectivité réseau

Maintenant que nous avons bien configuré notre réseau, nous allons passer à l'installation des outils nécessaire pour la simulation.

2.2 Hmail serveur (machine1)

2.2.1 Présentation de Hmail Serveur [25]

Hmail serveur comme son nom l'indique est un serveur de courrier électronique gratuit. Il prend en charge les protocoles de messagerie communs (IMAP, SMTP et POP3) et peut être facilement intégrée avec de nombreux client de messagerie existants.Il travaille avec une base de données (MySQL ou Microsoft SQL), pour les mails ainsi que certaines données liées à sa configuration.

Son utilité est qu'il permet de gérer les mails d'un **Nom de domaine** enregistré, comme il supporte également les domaines virtuels en local.

2.2.3 Fonctionnement d'un système de messagerie

En effet, l'envoi et la réception des messages électroniques sur un réseau se fait à travers des protocoles, et avant de renter en détail dans la description de ces protocoles il est important de connaitre les différentes phases qui se succèdent entre l'envoi d'un mail par l'émetteur et sa réception par le destinataire. Voir figure V.3

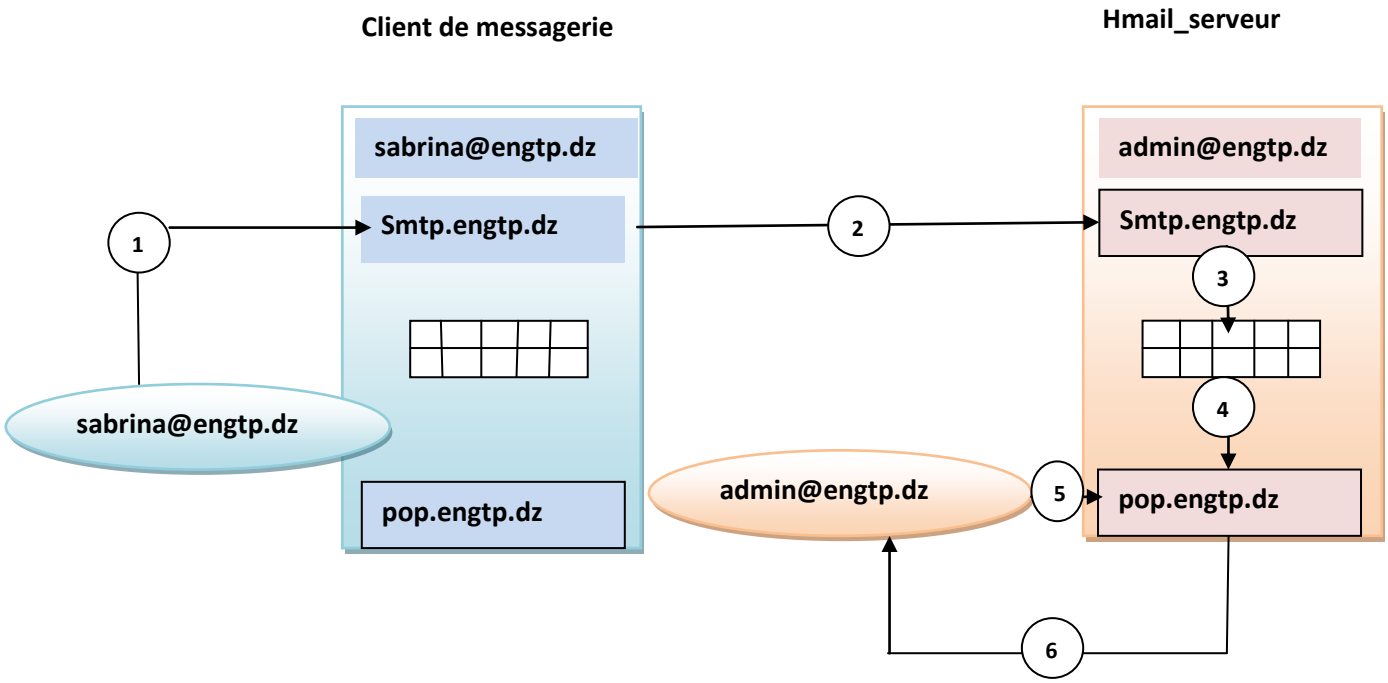


Figure V.3 : Fonctionnement d'un système de messagerie

2.2.4 **Configuration de Hmail Serveur**(voir annexe)

Cela nous permet d'envoyer des mailes sur un réseau local, voire même de les relayer vers internet, très utile simple et rapide. Et pour mieux concrétiser l'envoie d'un mail à partir du client de messagerie vers hmailserveur, nous avons testé un envoi d'un mail à partir des comptes que nous avons créés précédemment :

- ✓ Compte expéditeur : sabrina@engtp.dz
- ✓ Compte destinataire : admin@engtp.dz

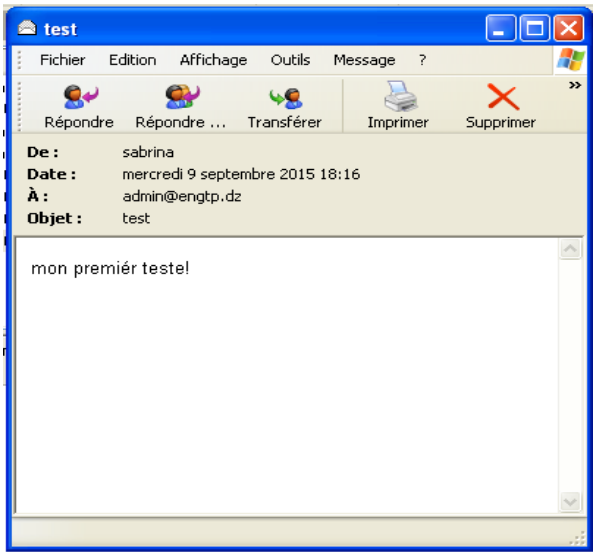


Figure V.4 : teste d'envoie d'un mail

2.3 Client de messagerie Outlook express (VM2) :

2.3.1 Présentation

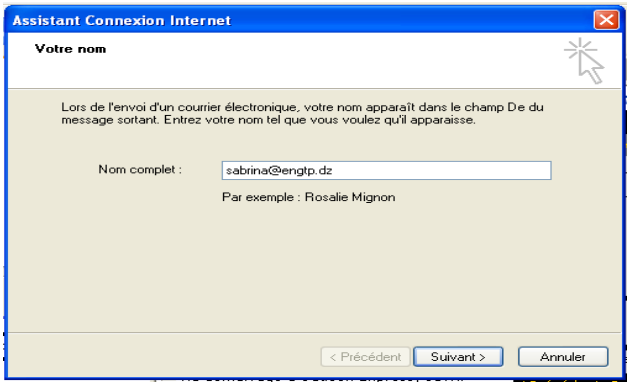
Outlook express est un programme de messagerie développé par Microsoft qui nous permet de stocker, gérer, et surtout d'envoyer et recevoir des e-mails.

2.3.2Configuration

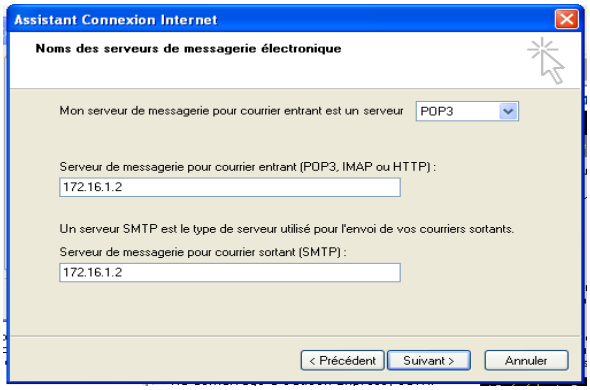
Pour configurer notre client mail, il suffit d'indiquer ces informations dans les paramètres du compte mail créé au préalable pour recevoir nos mails locaux.

Les valeurs suivantes sont en rapport avec l'exemple développé dans la partie précédente.

1. Saisir l'adresse de messagerie : **sabrina@engtp.dz**



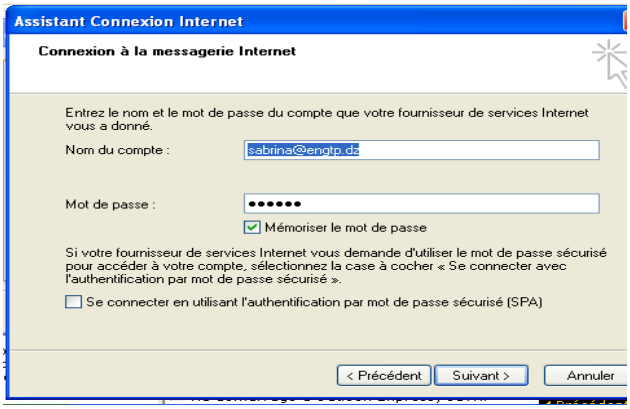
2. on indique l'adresse du serveur (son nom)



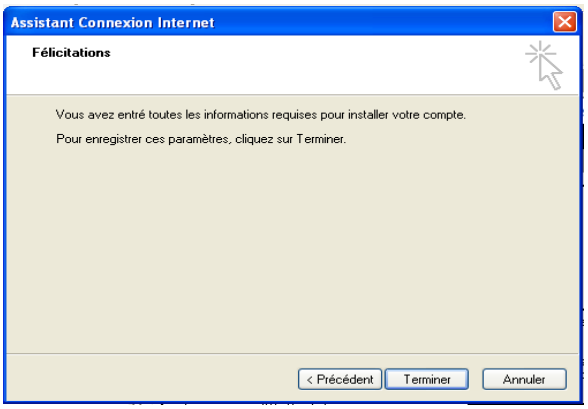
3. enregistrement du nom et du mot de passe :

Mot de passe **: 123456**

Nom du compte : **sabrina@engtp.dz**



4. fin de la création de nouveau compte on clique sur **terminer**



2.4IDS suricata (VM3)

2.4.1 Historique

Suricata est un IDS/IPS développé par l'Open Information Security Foundation (OISF) qui est une association à but non lucratif qui a été fondée pour porter le projet. Développer depuis zéro sous l'impulsion de Victor julien qui reste le développeur principal et leader du projet .Il appartient à la même famille d'IDS/IPS que SNORT (aussi IDS/IPS) dont il a repris le langage de signatures.

Avec un développement commencé en 2008, Suricata à une base de code récente et a pris la partie d'utiliser de nouvelles idées et de nouvelle technologies, notamment d'adresser les

problématiques de performance face à l'accroissement des débits, l'accélération matérielle, le multithreading qui fut l'axe fort du développement de suricata**.**

2.4.2 Fonctionnement de Suricata

Suricata a différents modes de fonctionnement. S'il peut être configuré en tant que dispositif de prévention d'intrusion IPS en s'appuyant sur Netfilter ou ipfw (sous FreeBSD),il supporte aussi de nombreux modes de capture en mode IDS qui vont de pcap,le standard de facto, au support des cartes d'acquisitions.

2.4.3 Installation et configuration Suricata [14]

Pour débuter nous devons installer les outils de compilations, et les dépendances de Suricata nous détaillons les prérequis nécessaires à son installation :

a- Installation de cygwin
c-Installation de WinPcap
d-Téléchargement de Wpdpack
e-Configuration des variables d'environnement
f-Compilation de LIBYaml
g-Compilation de suricata
h-Configuration de suricata
I-Configuration standard de suricata.yaml

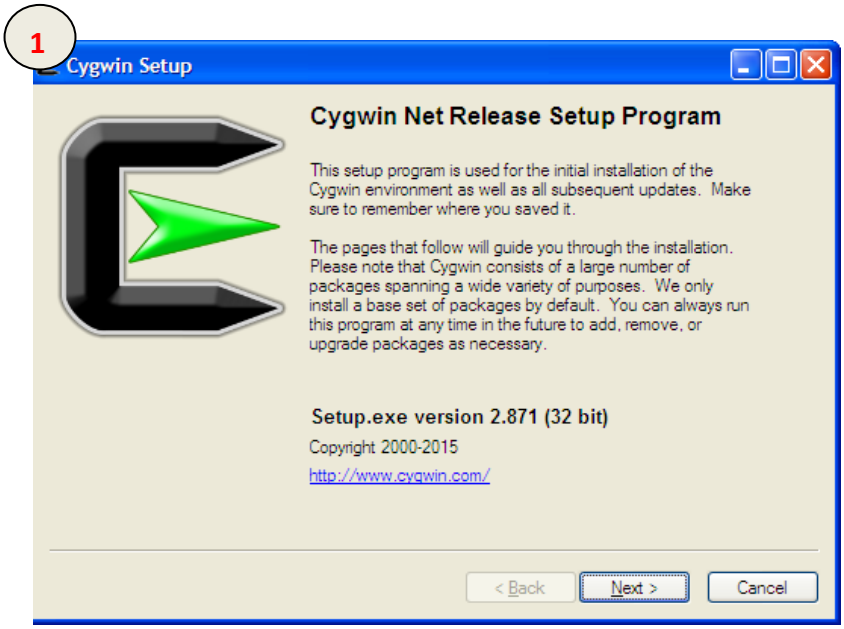
2.4.4 Prérequis suricata

a-Installation de cygwin

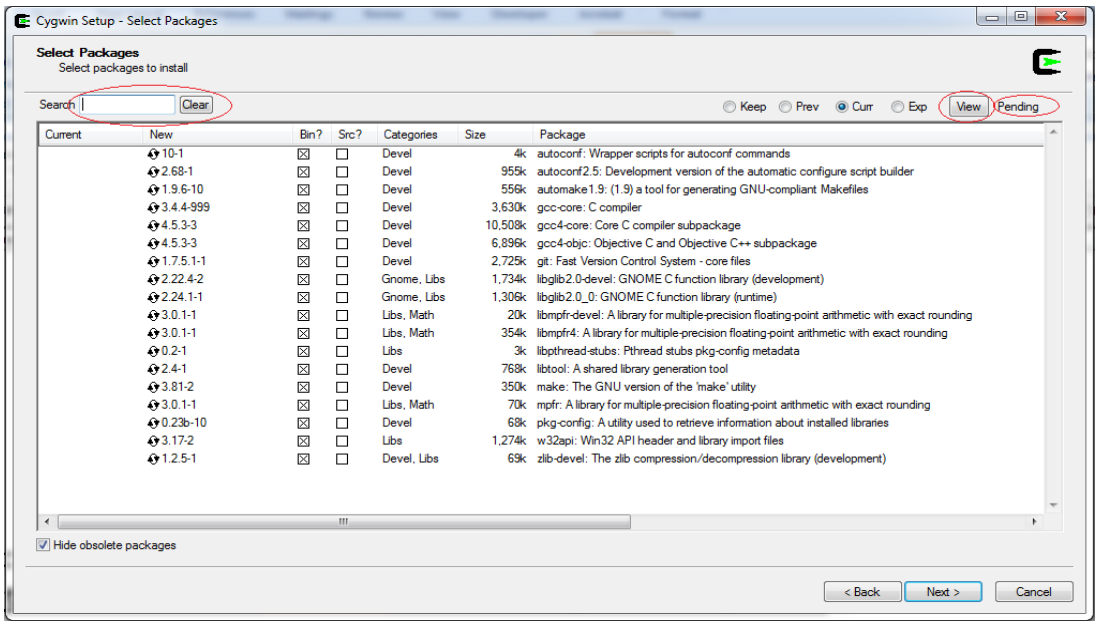
Cygwin est une collection de logiciels libres qui permet d'émuler un environnement Unix sous Windows, rendant possible l'exécution de ces logiciels après une simple compilation. Il permet ainsi de réaliser les tâches suivantes :

- Ouvrir une console (type bash) accessible d'un simple raccourci sur votre bureau ;
- Reproduire les fonctions Unix "classiques" ls, cp, cat, gcc, pwd... ;
- Compiler et exécuter des programmes développés pour Unix.

b- Téléchargement et installation de cygwin[21]



Arrivé à cette étape on sélectionne et on installe les packages suivants : w32api, mpfr, pthreads, gcc-core, gcc4-core, make, zlib , autoconf , automake , libtool , glib , pkg-config ,pkg-config, git



c- Installation de WinPcap:[22]

WinPcap est une bibliothèque pour la surveillance de trafic réseau, nécessaire pour utiliser un nombre croissant de programmes et d'utilitaires de surveillance réseau. Gratuit, WinPcap contient notamment un pack de pilotes utilisant l'interface NDIS afin de capturer les paquets en transit, directement depuis la carte réseau de l'ordinateur. Un composant indispensable pour faire fonctionner bon nombre de logiciels de maintenance réseau: outils de balayage de port, détecteurs d'intrusions, sniffeurs, …

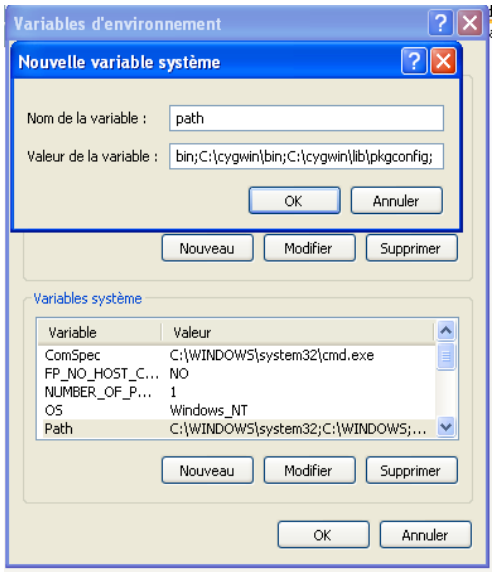
d- Téléchargement de Wpdpack

On télécharge Wpdpack et on le décompresse, ensuite suivre les instructions suivantes :

1- Copier le contenu de **Wpdpack\lib** dans**cygwin\lib**
2- Copier toutes les entêtes de **Wpdpack\include** dans**cygwin\usr\include**
3- Renommer le répertoire **libwpcap** en **libpcap** dans le répertoire **cygwin\lib**

e- configuration des variables d'environement :

1. Cliquez sur Démarrer -> Panneau de configuration -> Système -> Avancé.
2. Cliquez sur Variables d'environnement, puis, sous Variables système, recherchez la valeur **PATH** et cliquez dessus.
3. Dans la fenêtre d'édition, modifiez **PATH** en ajoutant l'emplacement suivant :***C:\cygwin\bin;C:\cygwin\lib\pkgconfig;***
4. Fermez la fenêtre.



f-La bibliothèque LibYaml [23]

C'est quoi LIBYaml ?

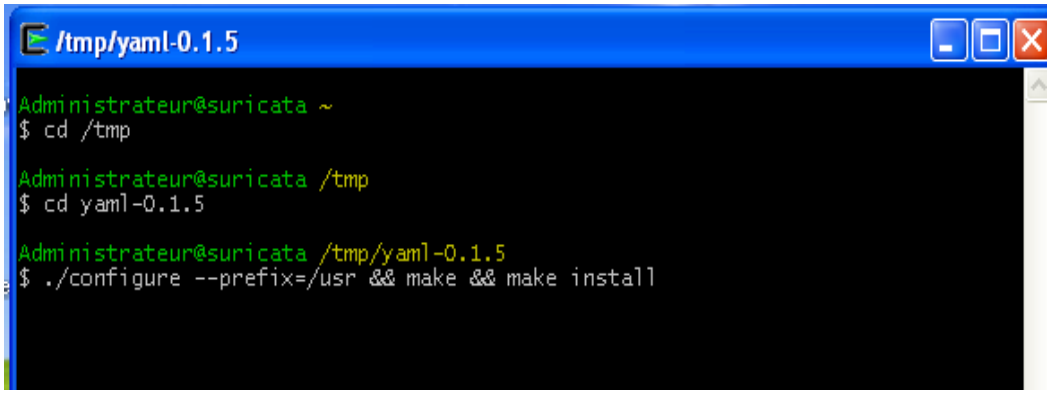
LIBYaml est une bibliothèque de routines pour la manipulation de données formatées au format YAML qui est un format de représentation de données à l'instar de XML.

Une fois la bibliothèqueLibYaml téléchargé on la décompresse au niveau du répertoire :

C:\cygwin\tmp

- Compilation de LibYaml :

```
Cd /tmp/yaml-0.5.1
. /configure –prefix=/usr&& make && make install
```



g. Compilation de suricata :

Pour l'installation de suricata deux solutions s'offrent à nous : **[24]**

- Installez la version suricata en cours de développement (version encours de production) à partir du GIT
- Installez la dernière version stable de suricata à partir du site officiel (ce deuxième point est notre choix)

Suivre les étapes suivantes :

Ouvrire la console cygwin:

a) wget http://www.openinfosecfoundation.org/download/suricata-1.2.1.tar.gz

b) tar –zxf suricata-1.2.1.tar.gz

c) cd suricata-1.2.1

d) dos2unix.exe libhtp/configure.ac && dos2unix.exe libhtp/htp.pc.in && dos2unix.exe libhtp/Makefile.am

e) libtoolize -c &&autoreconf -fv --install && ./configure && make

h- Configuration de suricata

La Configuration du fichier suricata.yaml ; modifier les variables suivantes en respectant le répertoire d'installation:

```
default-log-dir: C:\Suricata\log
……
- file:
enabled: yes
filename: C:\Suricata\suricata.log
……
default-rule-path: C:\Suricata\rules\
……
classification-file: C:\Suricata\classification.config
……
reference-config-file:  C:\Suricata\reference.config
```

i-Configuration standard de suricata.yaml

Tous les paramètres à régler de suricata se trouvent dans le fichier **suricata.yaml** situé dans le répertoire « **c:\suricata** ».Dans ce fichier, une quantité importante d'information est fournie en commentaire **« #»**pour permettre à l'utilisateur de connaitre l'utilité de chaque section de chaque variable et être capable de faire une configuration correcte.

Nous allons maintenant décrire les sections les plus importantes du fichier **suricata.yaml,** à savoir la configuration des règles :

Voici une partie de l'écran **suricata.yaml** :

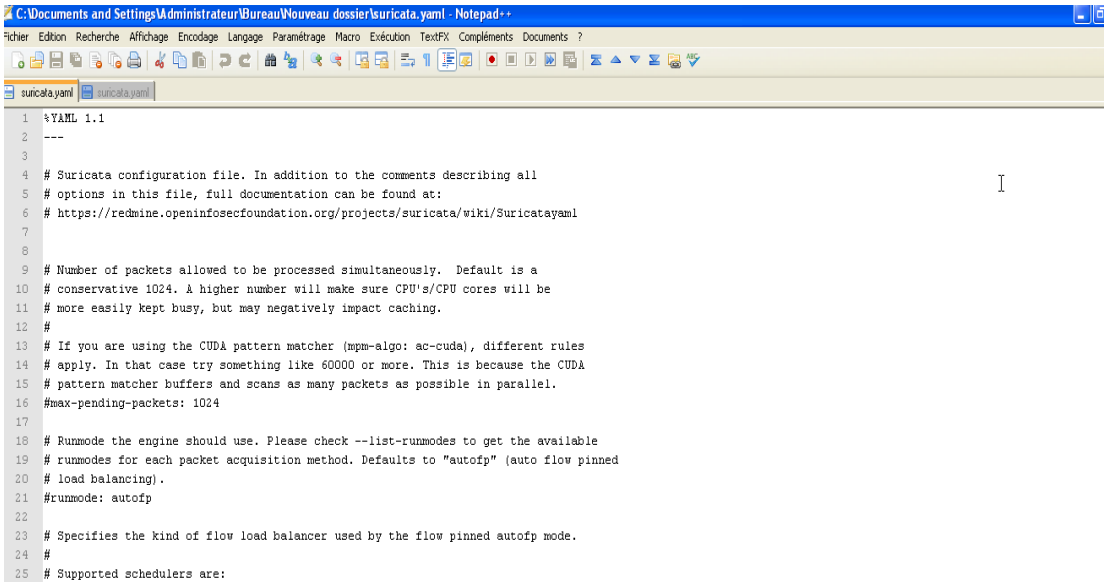


Figure V.5 : capture de suricata.yaml

2.4.5 Ecriture de règles de suricata : [18]

En effet, suricata implémente un langage de signature entier, décrit comme étant un ensemble de règles simple, léger flexible et assez puissant à correspondre sur les violations de politique et les comportements malveillants. Mais aussi de détecter de nombreuses anomalies dans le trafic qu'il inspecte.

Il ya un nombre d'indications simple à se souvenir en développant des règles suricata.

Le premier est que les règles de suricata doivent être complètement contenues sur une seule ligne, l'analyseur de règle de suricata ne sait pas comment traiter des règles sur plusieurs lignes.

Les règles suricata sont divisées en deux sections logiques qui sont :

- **L'entête de la règle**
- **Les options de la règle.**

La première : contient comme informations l'action de la règle, le Protocol, les adresse IP source et destination et les masques réseau, et les ports source et destination.

La seconde : contient les messages d'alerte et les informations sur la partie du paquet qui doivent être inspectées pour déterminer si l'action de la règle doit être acceptée.

Dans ce qui suit, nous décrirons la signification des proprietés de chaque section comme ce ci :

a) **L'entête de la règle :**

L'action :

C'est une partie qui nous informe quoi faire quand suricata trouve un paquet qui correspond aux critères de la règle. En résume quatre actions disponible par défaut dans suricata .

- **Alerte:** décrit l'action à effectué, en voici une courte description des options
- **Passer :** cela peut être comparé à «**accepter** » c'est-à-dire que si le paquet correspond à une règle définit, il va être accepté à travers.
- **Drop :** ici le paquet ne sera pas traité au plus loin de la chaine, ignoré, il sera silencieusement supprimé de la pile réseau.
- **Rejeter :** Il agit de la même manière que drop, le paquet sera retiré de la pile et bloquer.

L**e protocole :**

Utilisé pour la transmission des données, suricata on considère quatre : **IP, TCP, UDP, ICMP… etc**

IP source et destination et ports :

- **IP source :$HOME_NET :** indique l'adresse de l'interface réseau qui écoute le trafic
- **IP destination : $EXTERNAL_NET :** indique l'dresse du réseau externe à écouter.

Les ports :

Se sont les interfaces d'entrée/sortie sur lesquelles il faudra vérifier les paquets.

Exemple : http c'est le port 80 ; SMTP : 25 ; POP : 110

Opérateur de direction :

La flèche située entre l'IP et le port indique la direction du flux de paquet qui applique la règle. Presque chaque signature à une flèche vers la droite ce qui signifie que seule les paquets avec le même sens peuvent égaler.

b) Les options de la règle :

Msg :affiche un message dans les alertes et journalise les paquets.

Nocase :correspond à la procédure de chaîne de contenu sans sensibilité aux différences majuscules/minuscules.

Sid : signature ID (identifiant de signature) c'est une valeur unique utilisé pour identifier une règle parmi d'autre et autoriser des notes de version pour chaque règle (REV).

Gid (ID du groupe) : est un mot clé identifiantutilisé pour donner les différents groupes de signatures comme (dans un Sid), suricata utilise le gid 1 par défaut.

Classtype : utilisé pour donner des informations sur la classification des règles et des alertes, il se compose d'un nom court, un nom long et une priorité, il peut dire par exemple si une règle est simplement informatif ou si c'est un hack, pour chaque classtype classification. Config à une priorité qui sera utilisé dans la règle

Priorité : Le mot-clé de la priorité est livré avec une valeur numérique obligatoirequi peut aller de 1 à 4 sont les plus souvent utilisé, les signatures avec une priorité plus élevé sera examiner en premier, la plus haute priorité c'est 1.

En voila un exemple de règle :

```
Alert icmp any any       10.1.1.3/24 any (msg "PING VERS; serveur de messagerie"; isdataat: 2; Sid: 1699
```

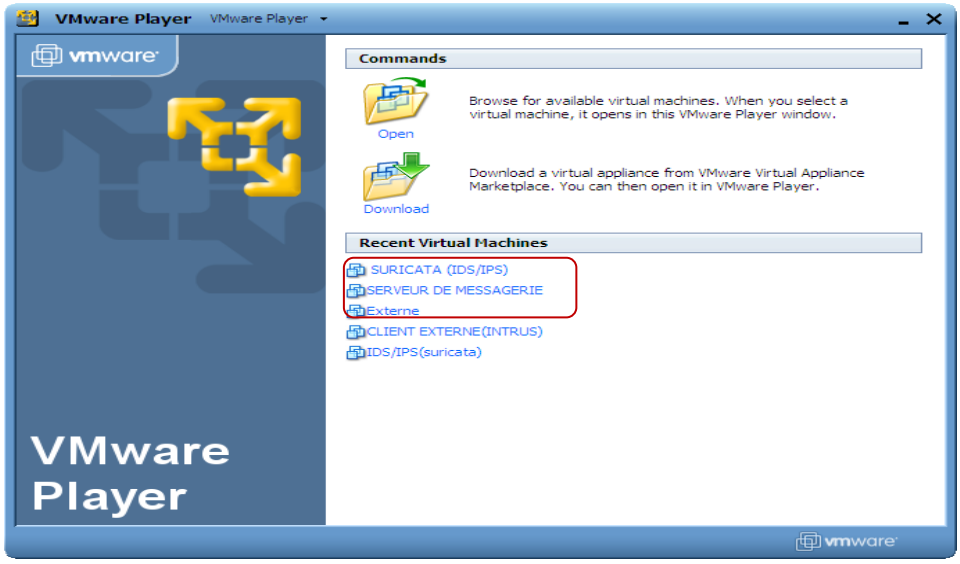
3. Simulation d'attaque

Dans cette partie nous allons tester et exploité notre environnement précédemment installé et configuré et cela en mettant en ouvre une attaque nommé Force Brute, dont l'objectif principal est celui de tester plusieurs mot de passe pour usurper un compte de messagerie ; le système de détection d'intrusion va surveiller et analyser le flux du réseau et nous produire un rapport sur les activités suspect du réseau.

Lancement de l'environnement de simulation :

On commence par lancer VMware Player sur laquelle nous avons crée précédemment les trois machines de testes :

- Serveur de messagerie (machine 1)
- Client de messagerie outlook (machine2)
- IDS/IPS suricata (machine 3)

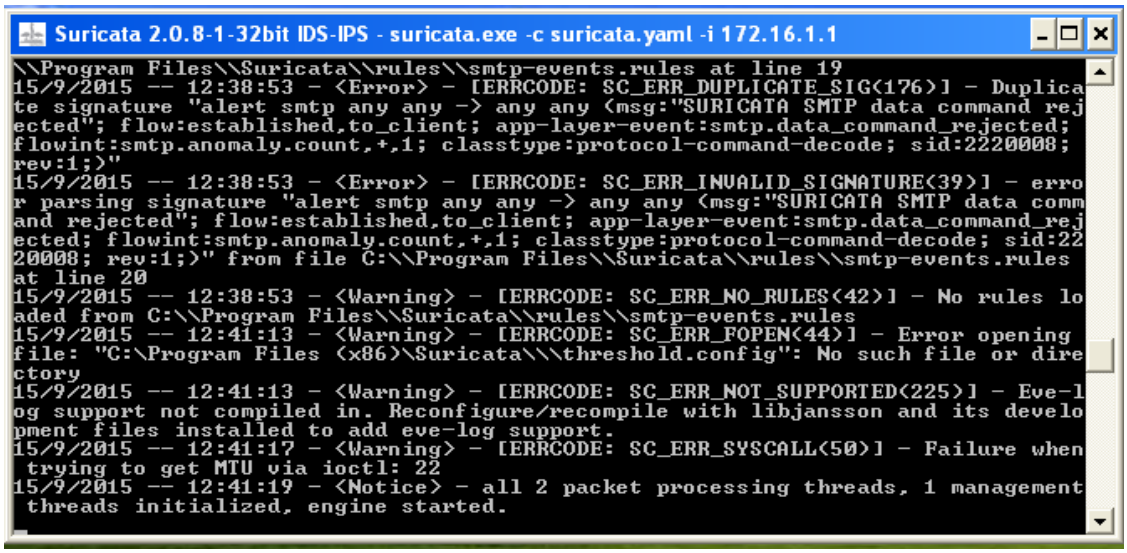


Pour lancer les machines de teste, il suffit de s'authentifier.

Sur la (machine 3), on lance suricata IDS/IPS et s'assurer que l'engin démarre correctement

Comme le montre l'image ci-dessous :

```
suricata.exe -c suricata.yaml –i 172.16.1.1
```



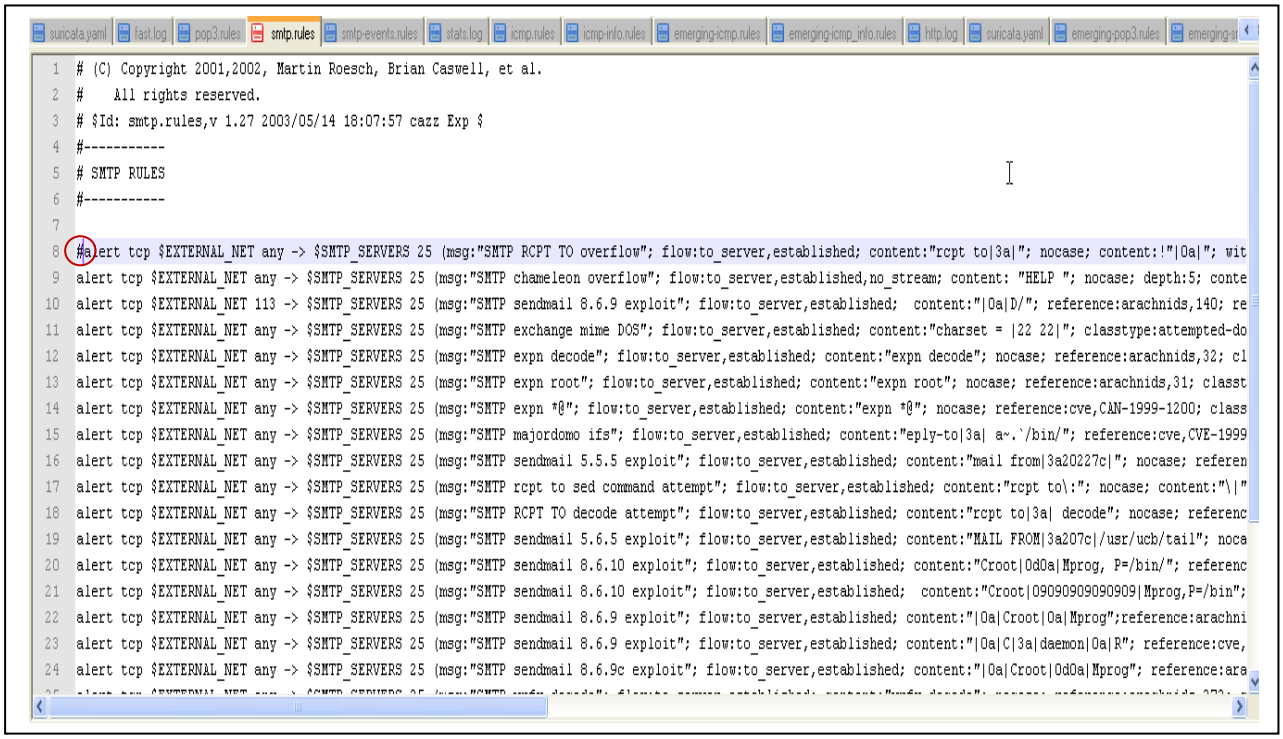
3.1 Simulation d'attaque du serveur hmail

Cas I : Envoi d'un mail via SMTP

Dans ce cas –là on doit rédiger nous même les rules dans le fichier **SMTP.rules** et **POP3.rules**

Et activer ou désactiver les rules donnée dans ce fichier en enlevant le **«#»** ou bien le remettre

- En voici une prise d'écran du fichier **SMTP.rules**



L'attaque :

L'attaque informatique passe par quatre étapes qu'on a vu dans le chapitre « «sécurité »

3.1.1La phase 1-Identification de la cible :

Consiste a se fixer un objectif à atteindre et dans notre cas c'est l'attaque du serveur de messagerie GTP ; l'objectif est de disposer des crédentités du compte administrateur du serveur de messagerie; donc on commence a prospecter sur internet, à discuter avec les employer de GTP et cela dans le but de récolté une masse d'information à exploiter ; une fois cette étape terminé » au passe à la phase deux

3.1.2La phase 2-Le sanning :

Cette étape et celle du scanning, et pour ce faire nous avons utilisé un logiciel de scan connu par les administrateurs réseau à savoir le Nmap ;

Scanner externe de port :

Nmapest un excellent outil d'exploration réseau et scanneur de ports /sécurité dont la syntaxe est la suivante :

Nmap [type de scans…] [options] {spécification des cibles}.

Nmap existe aussi en mode graphique sous le nom « zenmap Gui »**Nmap** permet d'éviter certaines attaques et aussi de connaitre quels services tournent sur une machine, étant un logicielle très complet et évolutif il est la référence dans le domaine du scanning.

A partir du réseau externe client **externe (intrus)** on va essayer de scanner les ports du serveur de messagerie à l'aide de **Nmap**comme l'image le montre ci-dessous :

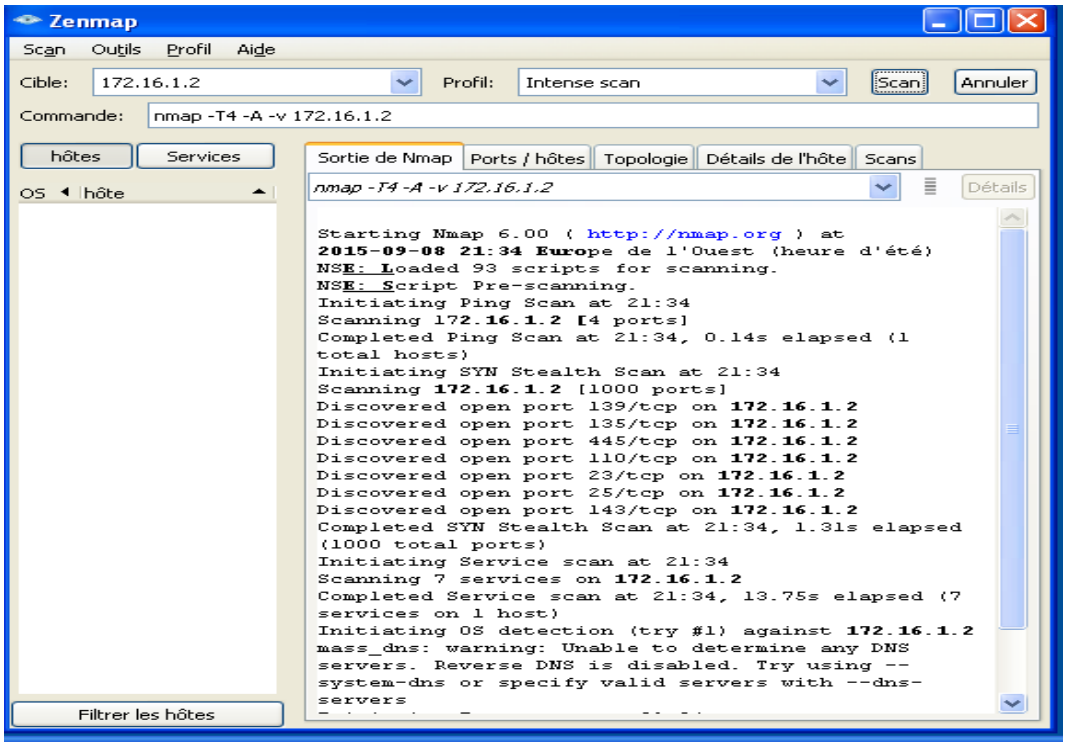


Figure V.6: Scan de ports de serveur de messagerie

C'est à partir de ce scanne qu'on récolte les informations relatives au adresse Ip au port ouvert.

3.1.3Phase 3 –l'exploitation:

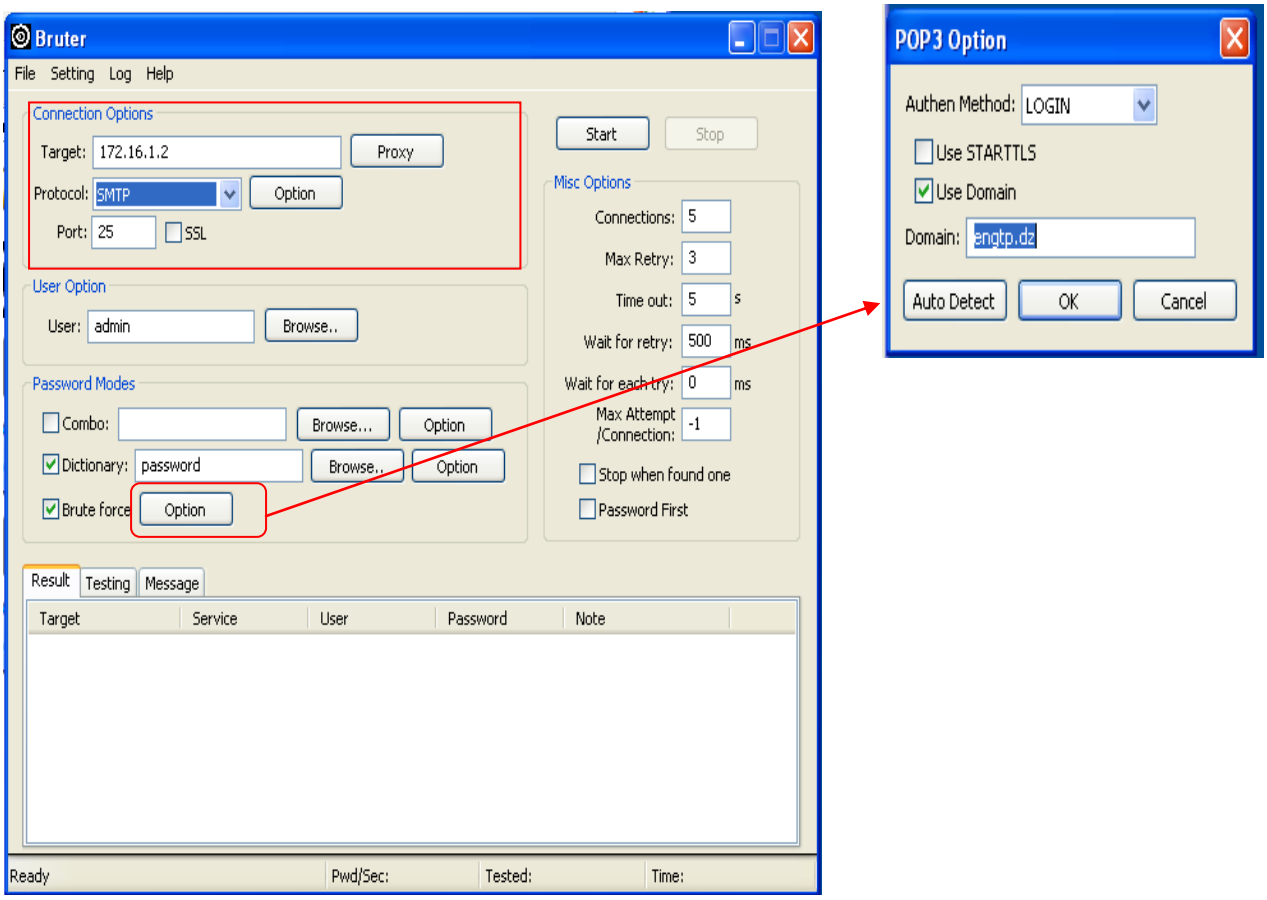
C'est la partie consacré à l'exploitation des failles découverte et dans ce cas on va se servir d'un logiciel Bruter ; l'attaque qu'on va essayer de mettre en œuvre une attaque de type Force Brute.

4. Définition de l'attaque force brute :

Il s'agit d'une méthode de craquage de mot de passes utilisée en cryptanalyse qui consiste à tester une à une toutes les combinaisons possibles jusqu'à trouver le bon. mais pour pouvoir tester suricata on a déployé un logiciel qui permet de faire un balayage réseau sur réseau sur certains périmètre choisi dans notre cas on parle d'un serveur de messagerie (hmail_serveur) par exemple : Nmap

Par la suite, suricata sera capable de détecter ces scan et d'envoyer immédiatement un message d'alerte qui va nos alerter de la tentative ou l'attaque subie par le réseau.

-Utilitaire de force brute : [26] [1]



Bruter génère et essaye tous les combinaisons possibles alphabétique, numérique, caractères spéciaux…. Jusqu'à ce qu'il trouve le bon mot de passe.

On renseigne l'adresse IP du serveur de messagerie comme cible d'attaque; le Protocol SMTP ; pour la messagerie

Et dans les options de Bruter on a choisi l'authentification mode [LOGIN] et on renseigne le domaine dans notre cas « engtp.dz ».

5. La Détection d'intrusion avec L'IDS suricata :

Au niveau de suricata l'administrateur réseau sera alerté par les messages suivant suite au lancement du scan

Serveur de messagerie (DMZ) : détection de la tentative de scan de port par suricata

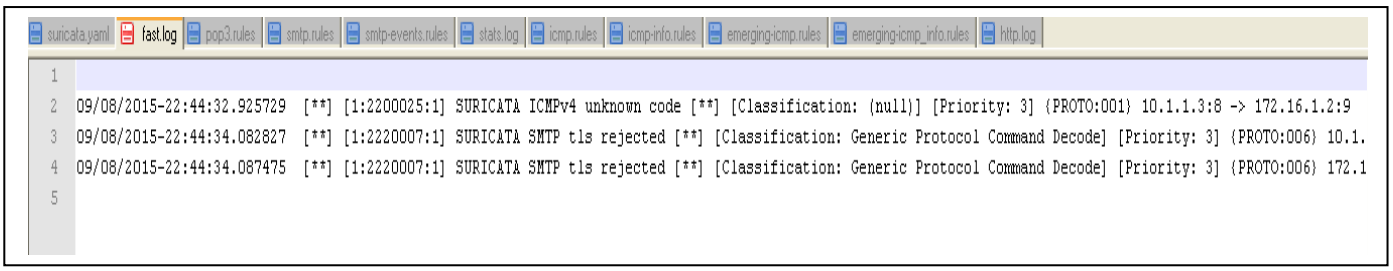


Figure V.7: la journalisation des alertes dans le fichier fast.log

Voici quelque explications du message généré et enregistrer sur le fichier

fast.log :09/08/2015-22 :44 :32 : date et heure du scan

09/08/2015-22 :44 :32.925729 [**] [1 :2200025 :1] suricata ICMPv4 unknown code [**] [classification : (null)] [Priority : 3] {PROTO : 001} 10.1.1.3 :8 -> 172.16.1.2 :9

09/08/2015-22 :44 : date et heure
[1:2200025 :1] : 1 : le gid, 2200025 :le sid,1 : la revision.
ICMPv4 PING, unknoun code [**] [classification : (null)] :
Protocole : ICMPv4
Menace classé comme activité inconnue
{PROTO: 001)}10.1.1.3 IP source (intrus) -> 172.16.1.2 IP (cible)

Toujours sur la machine VM 3

qui représente l'intrus (machine externe au réseau) sur laquelle on a déjà installé **brutforcer**.On va lancerbruteforcer et on simule l'attaque comme montré ci-dessous :

Dans le fichier fast.log, on peut remarquer :

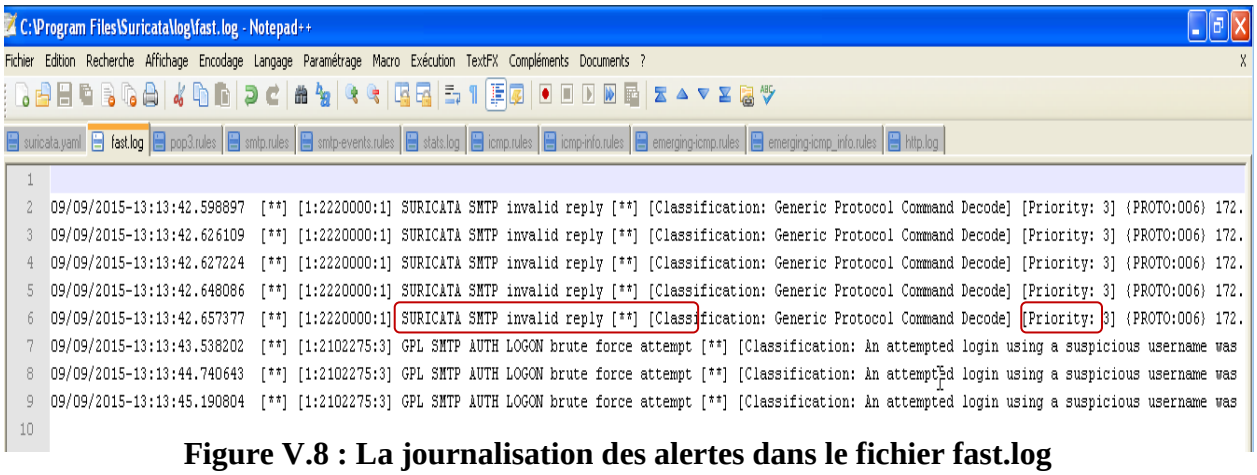


Figure V.8 : La journalisation des alertes dans le fichier fast.log

Pour plus de détailles sur le message généré et enregistré sur le fichier **fast.log** de la détection de cette attaque, voici quelques explications :

Ici le message nous indique :

Cette alerte a étéconfiguré au niveau du fichier emerging-smtp.rules en respectant la syntaxe voir la page

09/09/2015-13:13:44.740643 [**] [1:2102275:3] GPL SMTP AUTH LOGON brute force attempt [**] [classification: An attempted login using a suspicious username was detected] [Priority: 2] {PROTO: 006} 10.1.1.3:1108 —> 172.16.1.2:25

09/09/2015-13 :13 :44. : La date et l'heur.
Le protocole d'envoi SMTP : tentative de connexion de force.
[**] [Classification: An attempted login using a suspicioususernamewasdetected]: une tentative de connexion en utilisant un nom d'utilisateur suspect a été détectée.
La gravité de la menace : classé priorité 2
(PROTO : 006) IP source 10.1.1.3 —> IP cible 172.16.1.2
IP source 10.1.1.3 : machine (intrus) d'où provient le message malicieux.
IP cible 172.16.1.2 : machine du serveur hmail.

A cet étape, l'administrateur réseau est informé qu'un scan du réseau a été émis de l'extérieur et maintenant il y'a une tentative pour forcer le mot de passe de la messagerie du compte administrateur et en analysant le fichier de journalisation ; donc comme mesure de sécurité on bloque cet adresse IP qui lance cet attaque de l'extérieur et le problème est réglé.

Dans notre cas on ne peut passer à la phase quatre qui est celle de la progression car on a été bloqué par l'IDS Suricata.

Conclusion

Dans ce chapitre nous avons vu un aspect de la sécurité des réseaux informatiquesqui est la détection d'intrusion et cela en installant et configurant l'IDS SURICATA dans un environement Windows ,toute la difficulté dans la sécurité informatique réside dans la complexité de ce domaine .

Suricata est un système developpé par la communauté Open source donc dédier à l'environement Unix ;En algerie GTP est utilisé sur des plateforme Windows ,comme la plus part des entreprises ;donc on a essayé de deployer cet utilitaire dans un environement virtuel Windows et une fois l'environement installé ,on a simulé une attaque force brut pour testé notre configuration ;d'autres attaques peuvent etre testé telque ddos ,http attack ;trojian attaque ….. ;durant cet étude on a été initié à la sécurité informatique et on a aquis une bonnemaitrise de la configuration des IDS.

Conclusion générale

Le projet qui nous a été confié est de maitriser la configuration du système de détection d'intrusion Suricata de bien le configurer dans l'optique de protéger des ressources importantes se trouvant au niveau du serveur en l'occurrence le serveur de messagerie contre d'éventuelles attaques provenant de l'extérieur. Nous avons illustré ceci par une attaque de type force brut dans laquelle nous avons vu comment Suricata fonctionne pour intercepter un flux suspect et le bloquer.

Le développement de ce projet nous a permis de nous initier au domaine des réseaux et d'avoir une idée plus claire sur les applications du domaine de la sécurité informatique, plus particulièrement à l'IDS \ IPS suricata.Cependant, nous avons rencontré de nombreux problèmes au cours de l'élaboration de ce travail, principalement lors de l'installation desuricata ainsi que le nombre important des paquets complémentaires qu'il faut installer et bien configurer.

En perspective, nous proposons d'exposer le système à d'autres attaques (…..) pour confirmer la robustesse de la protection. Aussi nous proposons d'améliorer les performances de notre IDS\IPS à travers l'exploitation des fichiers logs générées par suricata en alertant l'administrateur réseau à chaque tentative d'intrusion de haut niveau par un mail ou un sms.

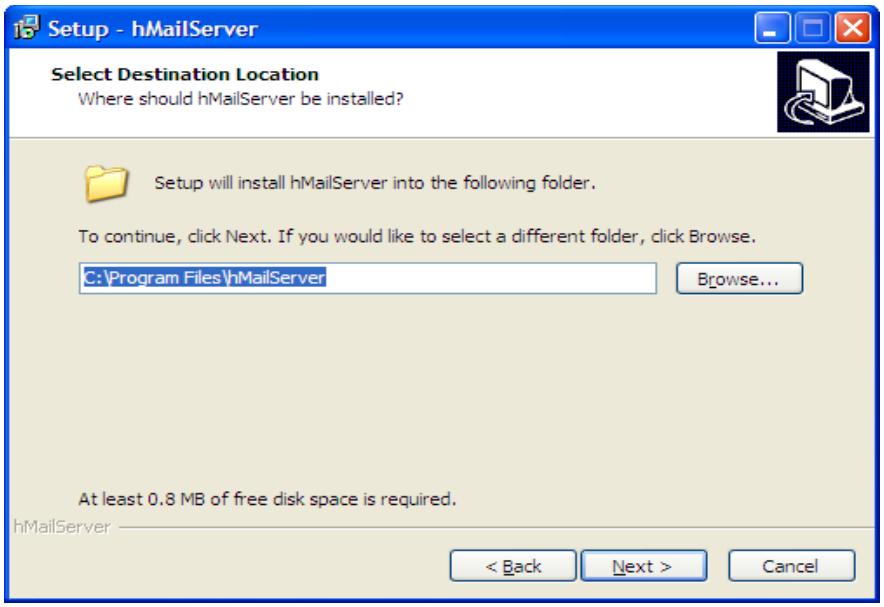
Il faut bien signaler que ce projet est une excellente initiation à la vie professionnelle car il offre un aperçu de ce que sera le travail au sein d'une équipe de sécurité informatique .Il a donc été une expérience enrichissante aussi bien sur le plan théorique que pratique.

A la fin de ce mémoire, nous souhaitons que nous soyons parvenues à accomplir la tâche qui nous été confiée, et espérons que ce travail puisse servir et contribuer à des développements futurs dans ce domaine.

Annexe A : Installation de hmail server

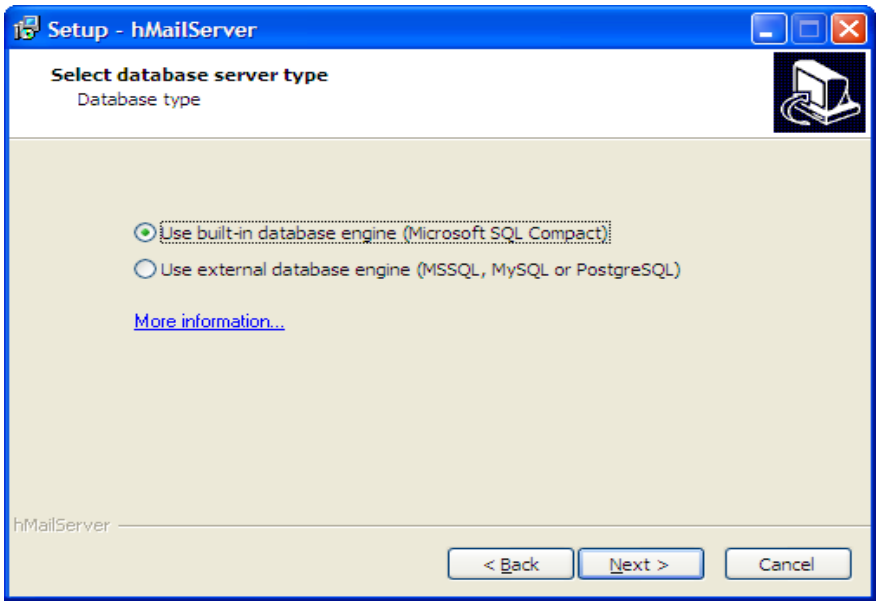
Installation de hmail serveur :

1. Sélectionner le dossier de destination sur lequel hmail Server doit être installé.

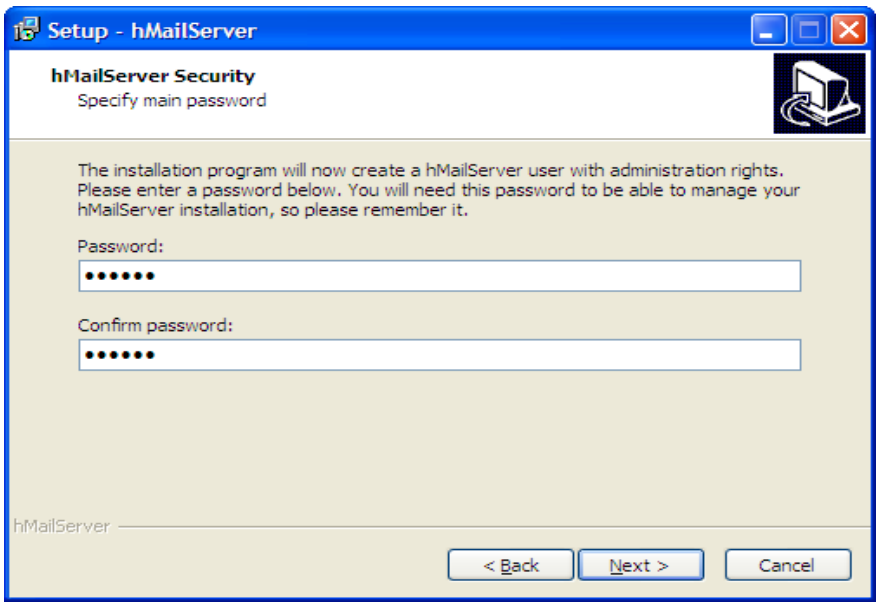


2. Un détail à prendre en considération est le choix du serveur de base de données :

Il est recommandé de laisser le 1er choix comme proposé par le setup, cela permet d'utiliser la base de données incluse dans le serveur et qui la rend indépendante de toute autre base, et si on veut utiliser un autre serveur de base de données, il faut prendre le 2eme choix.



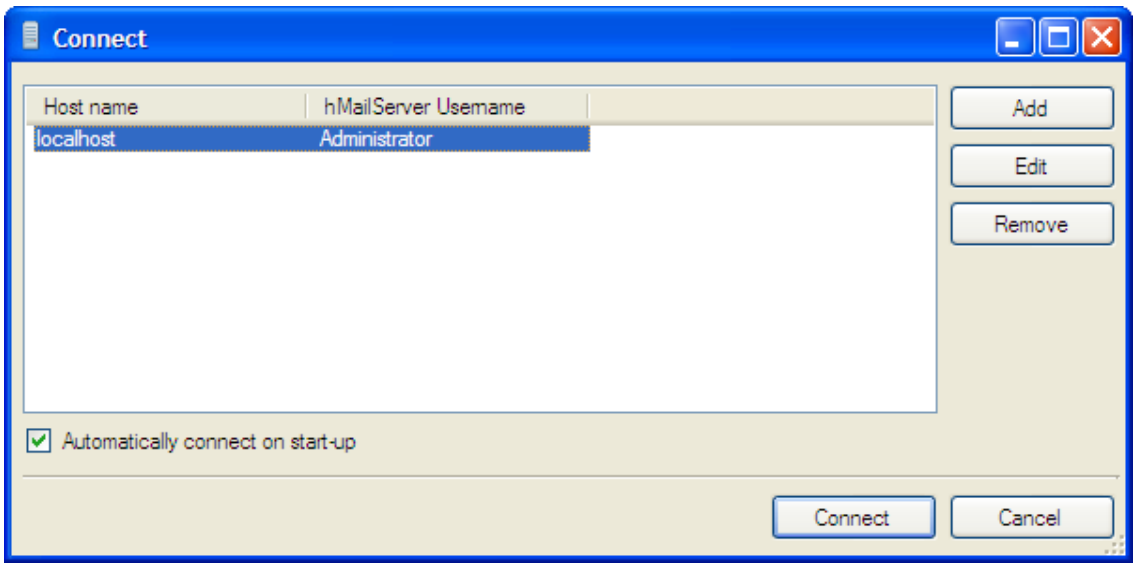
3. Il faut pour sécuriser la configuration, créer un mot de passe pour l'administrateur.



Une fois l'installation terminée, on va lancer le Serveur de mail en tant que service. Celui-ci démarrera automatiquement en même temps que l'ordinateur et la session.

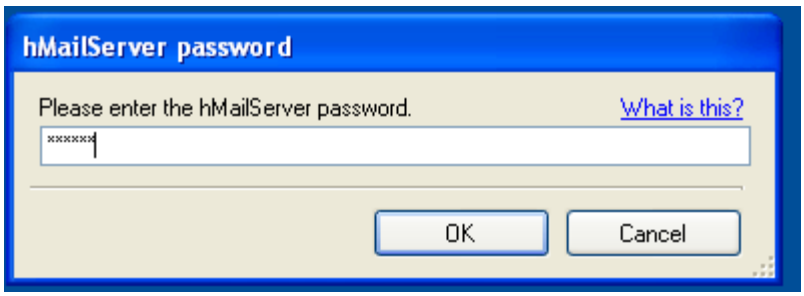
Pour se connecter la première fois au panneau d'administration de hMailServer, cette fenêtre va permettre de sélectionner l'utilisateur qui est par défaut "Administrator".

Pour se connecter la première fois au panneau d'administration de hmailServer, cette fenêtre va permettre de sélectionner l'utilisateur qui est par défaut "Administrator"



La possibilité de se connecter automatiquement au serveur est de cocher la case: Connexion automatique au démarrage.

4. Le mot de passe que vous avez saisi lors de l'installation est maintenant demandé.

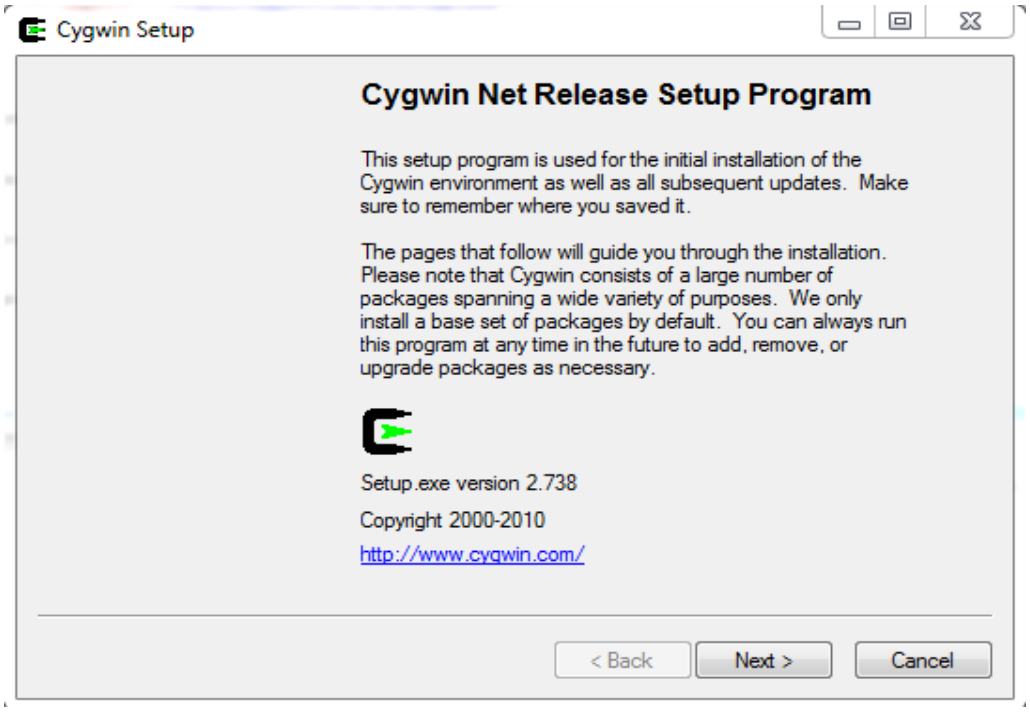


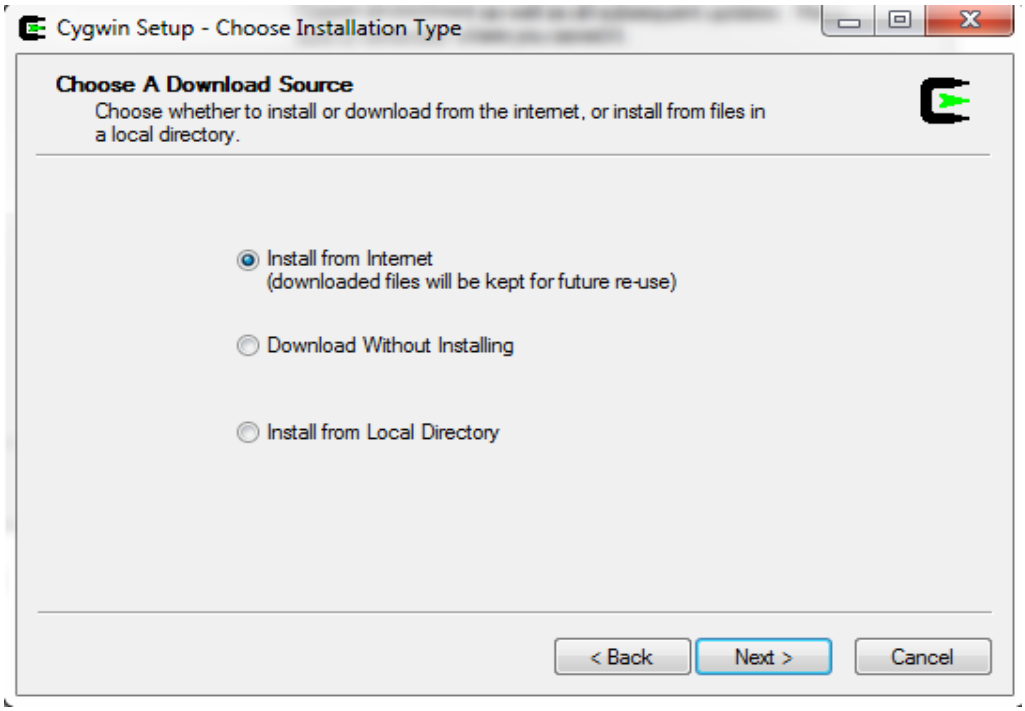
Annexe B : Installation de Cygwin

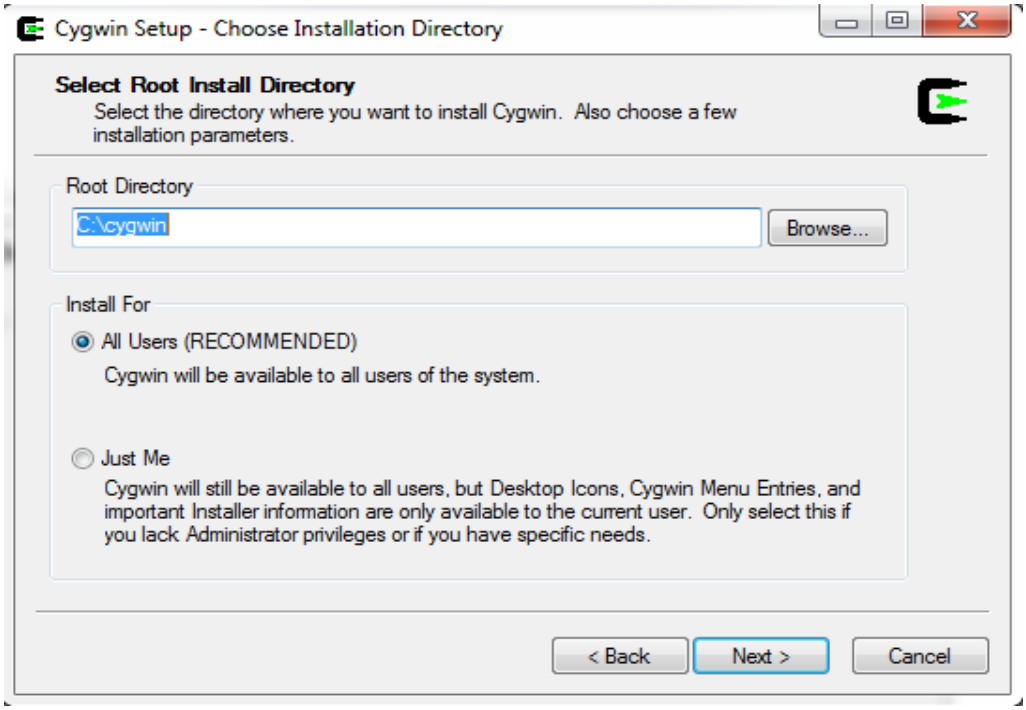
Installation de cygwin :

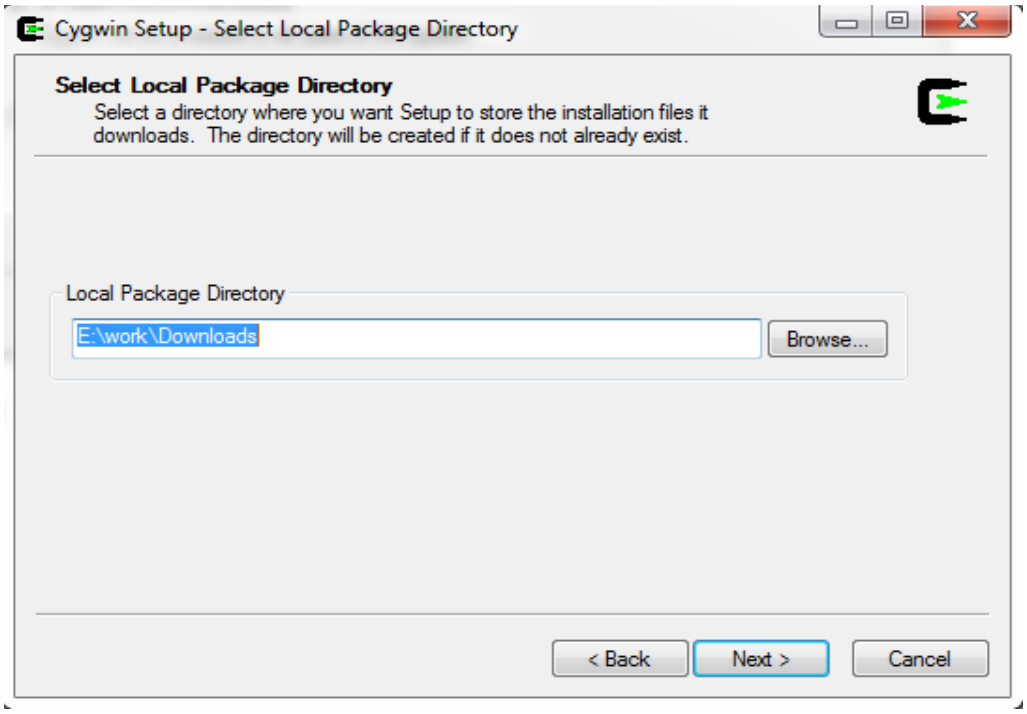
Phase 1 :

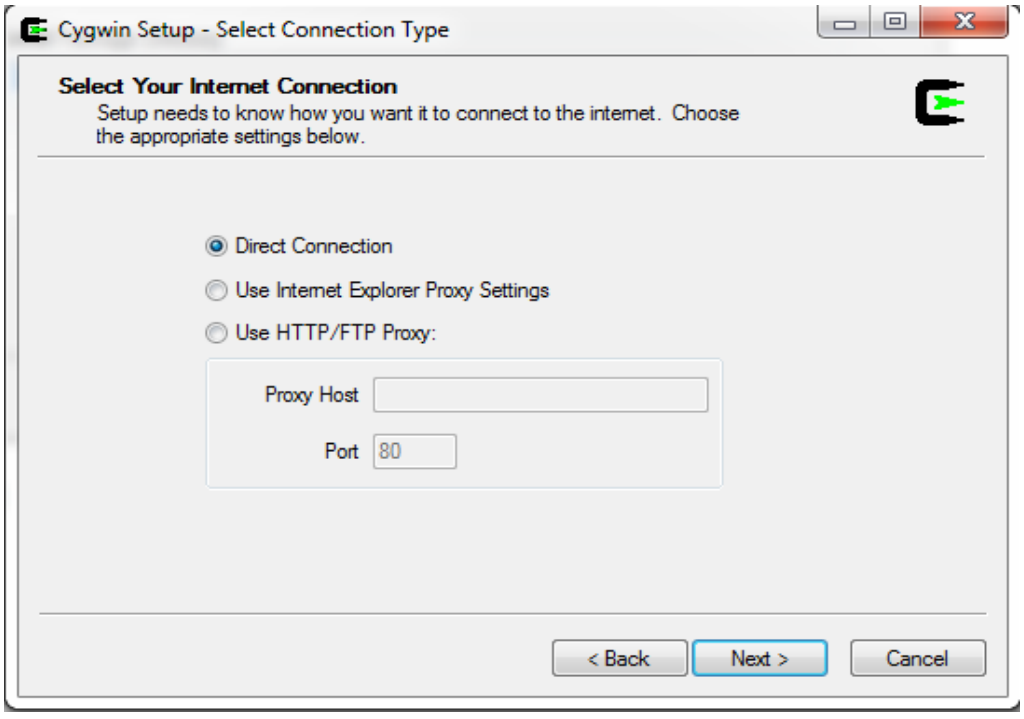
Dans cette étape on va juste cliquer sur Next et OK



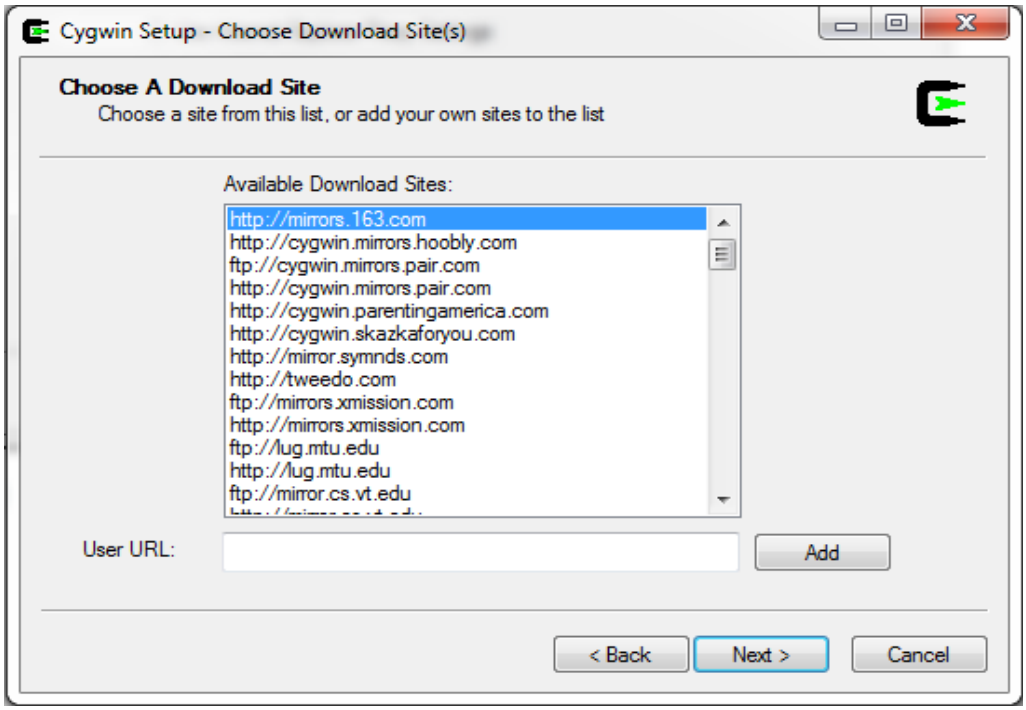

Cygwin Setup - Choose Installation Type
Choose A Download Source
Choose whether to install or download from the internet, or install from files in a local directory.
Install from Internet
(downloaded files will be kept for future re-use)
Download Without Installing
Install from Local Directory
< Back
Next >
Cancel


Cygwin Setup - Choose Installation Directory
Select Root Install Directory
Select the directory where you want to install Cygwin. Also choose a few installation parameters.
Root Directory
C:\cygwin
Browse...
Install For
All Users (RECOMMENDED)
Cygwin will be available to all users of the system.
Just Me
Cygwin will still be available to all users, but Desktop Icons, Cygwin Menu Entries, and important Installer information are only available to the current user. Only select this if you lack Administrator privileges or if you have specific needs.
< Back
Next >
Cancel

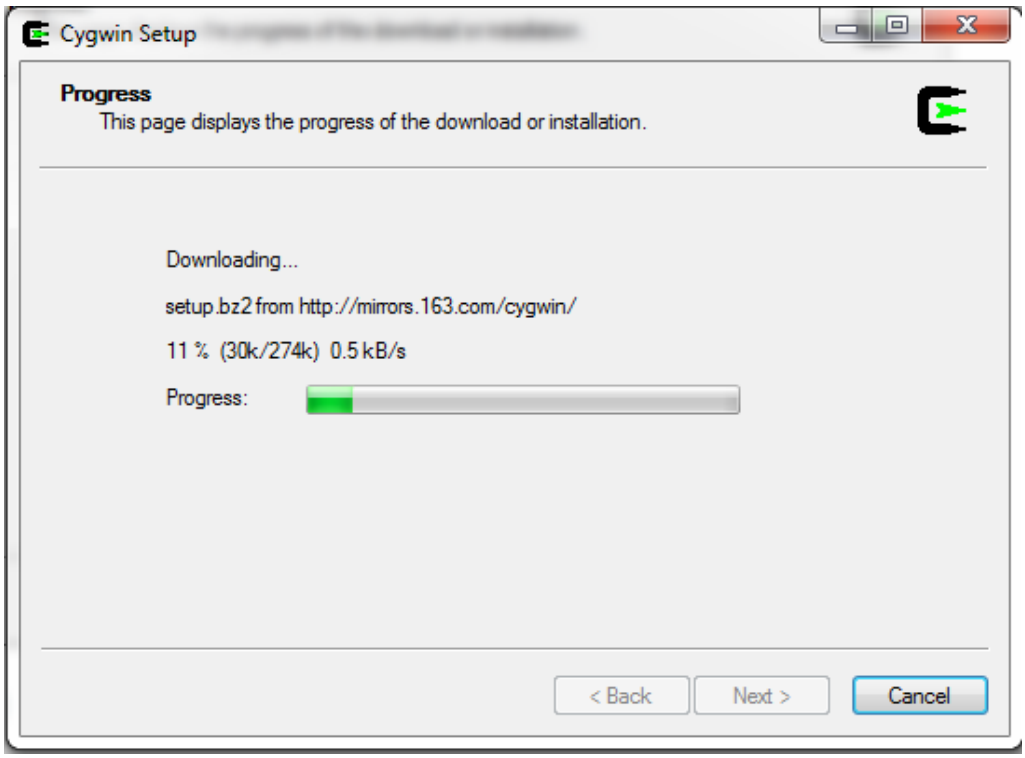


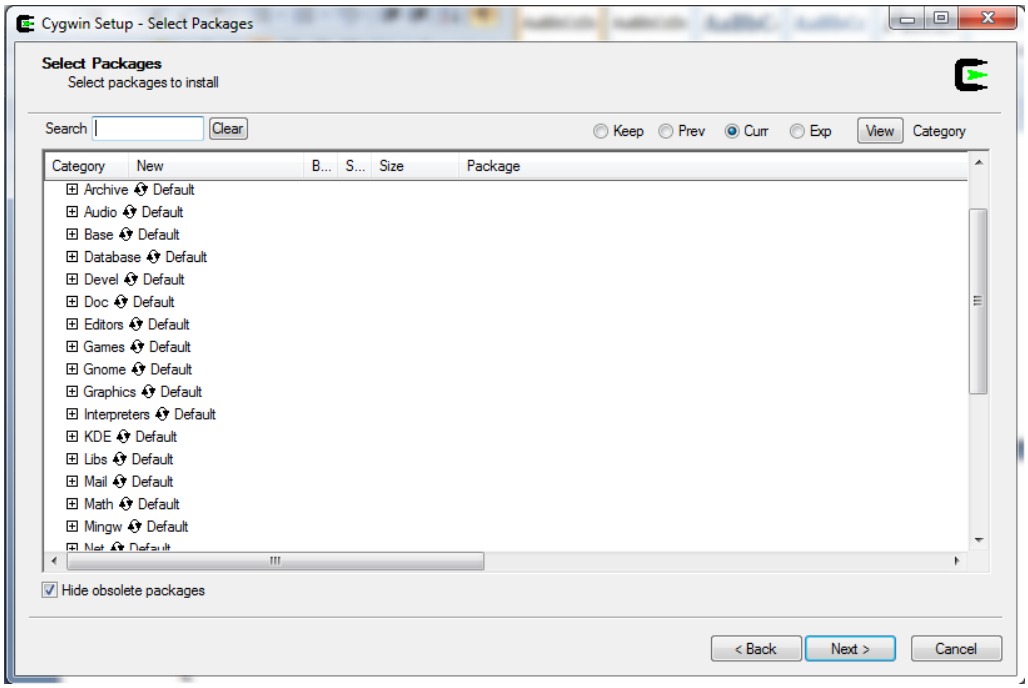


Arriver à cette étape, on sélection le site de téléchargement.

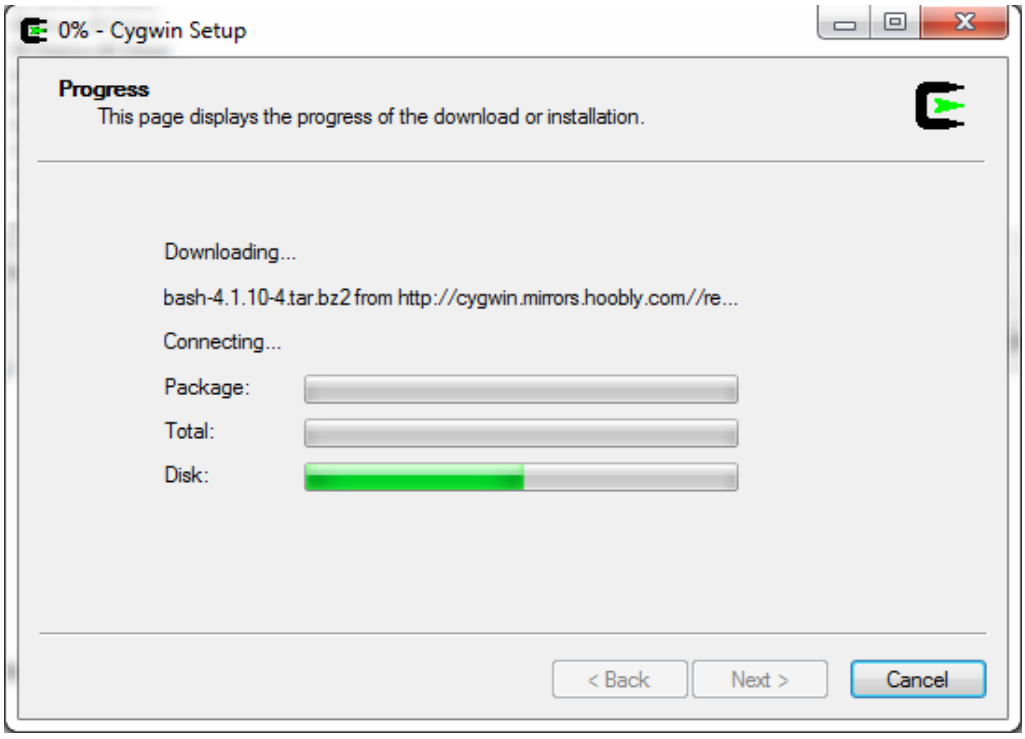


Vous allez voir une barre de progression comme ce ci

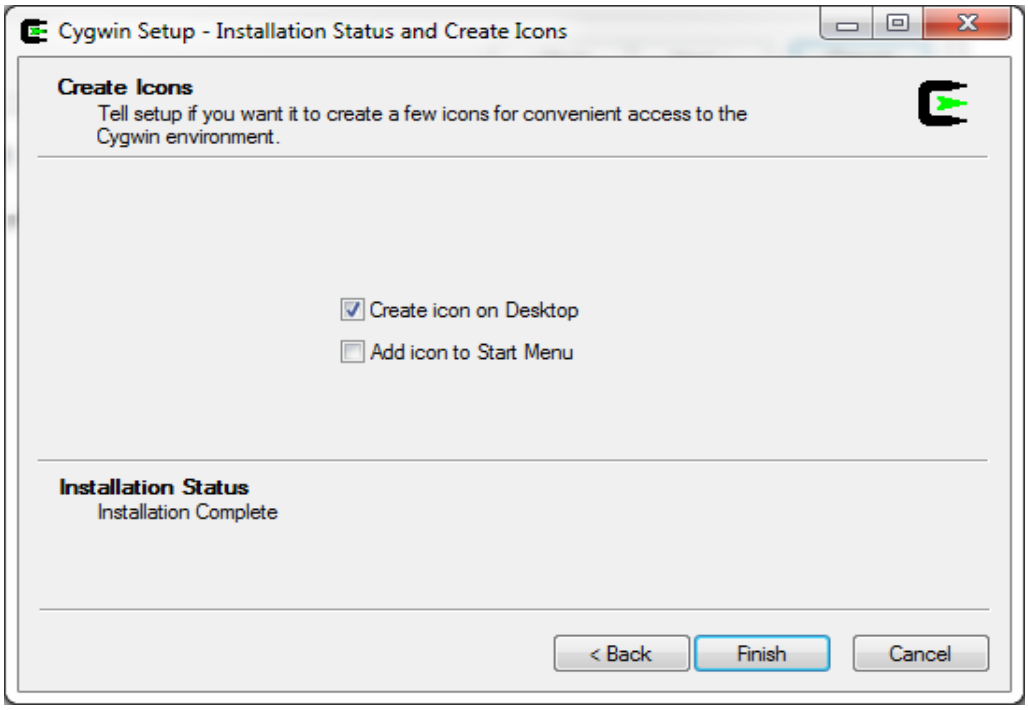




Cygwin va commencer le téléchargement et l'installation des paquets nécessaires.



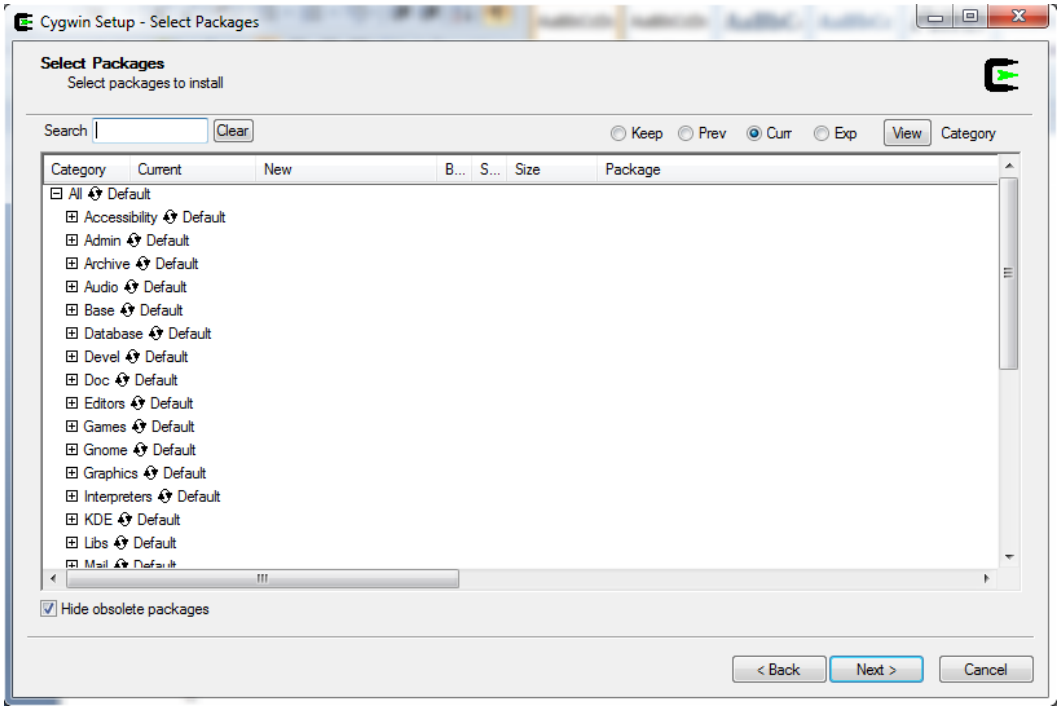
Cela va prendre environs 10-15 minutes, juste après on clique sur finish.



Phase 2 :

Installation des packages :

On retourne vers l'exécutable setup.exe et on clique sur Next jusqu'à arriver à cette étape :

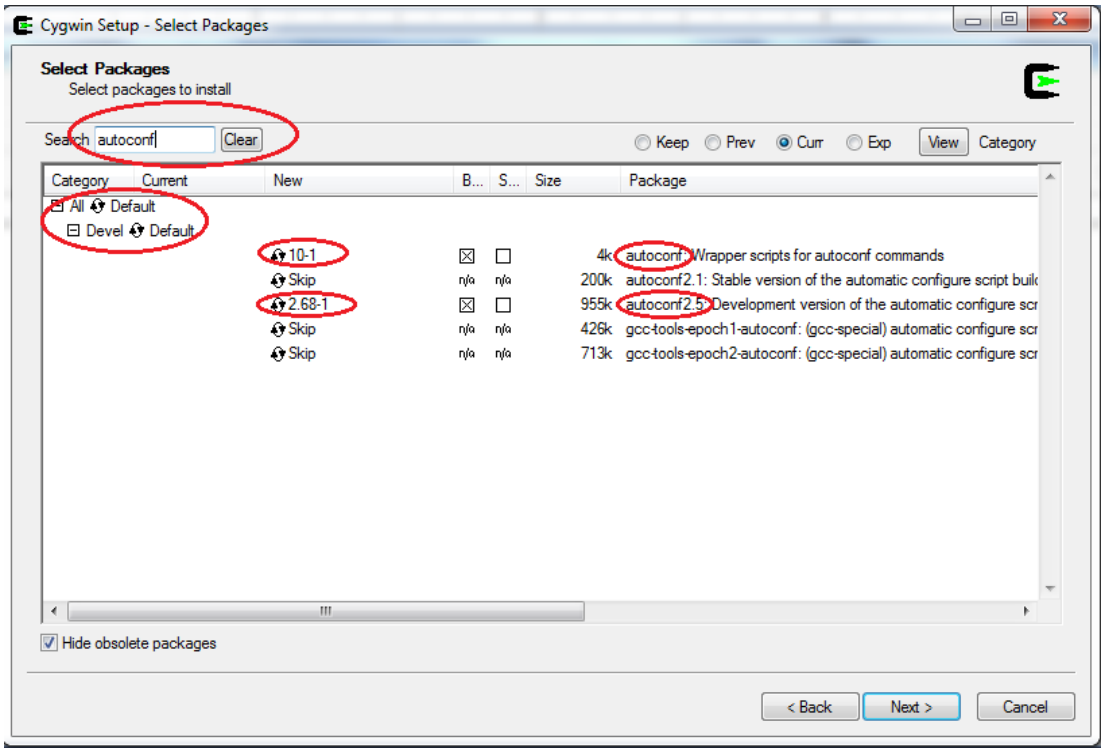


On installe les packages suivant comme c'est monté ci-dessous :

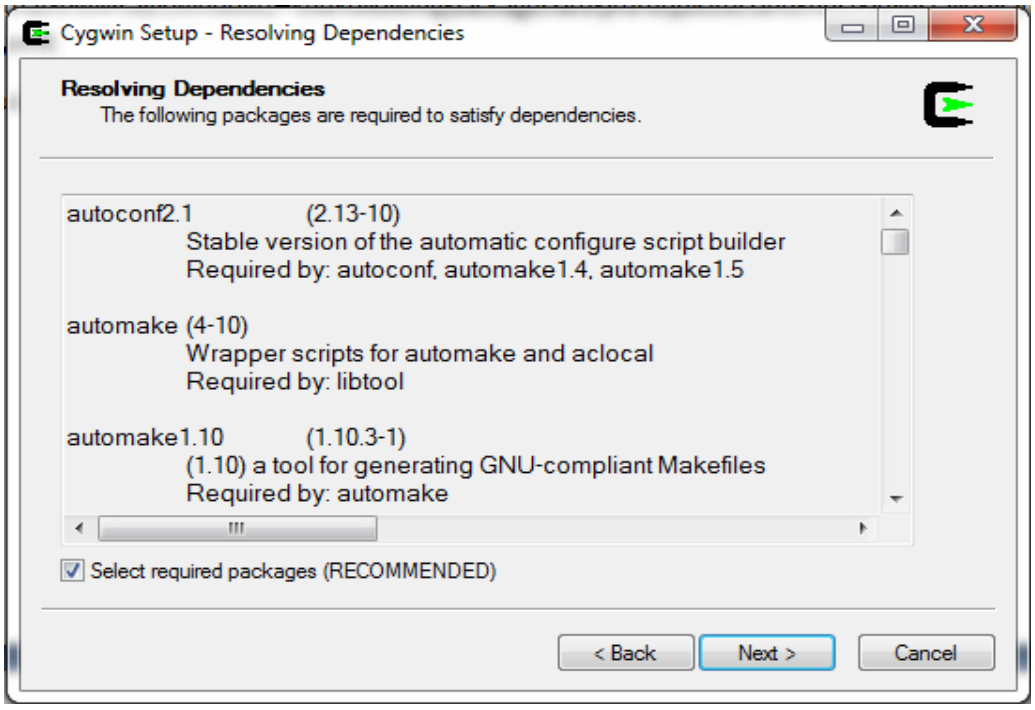
w32api, mpfr, pthreads, gcc-core, gcc4-core, make,

zlib ,autoconf , automake , libtool , glib , pkg-config ,

pkg-config, git

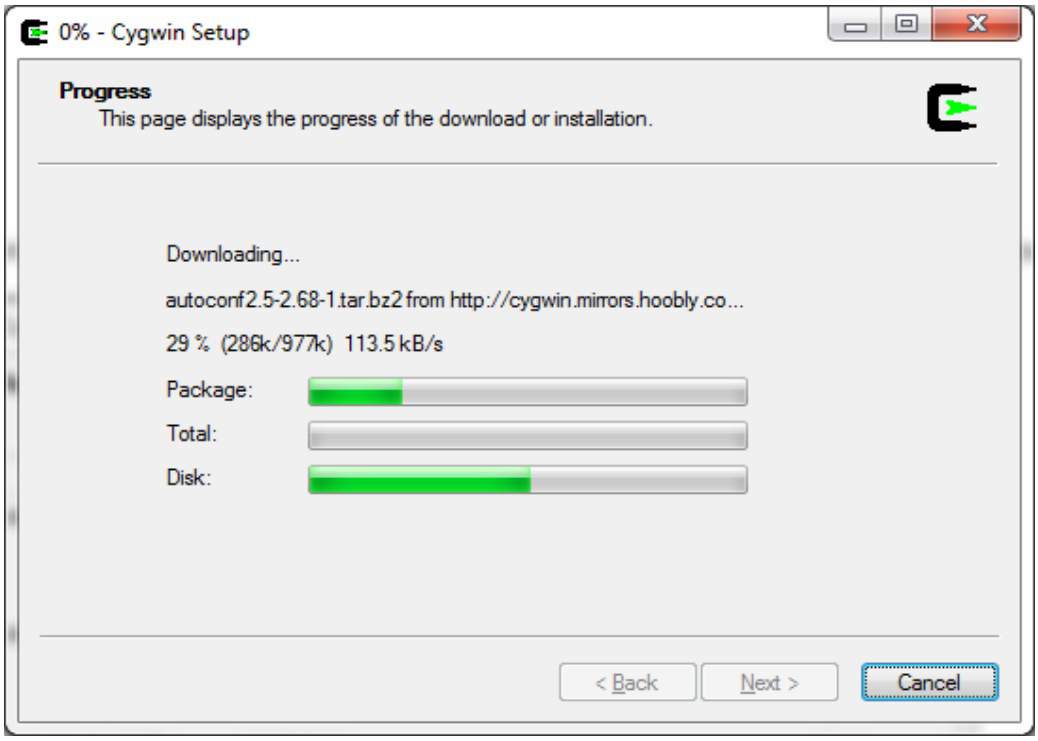


Puis on clique sur Next en étant sure que « select required packages » est bien sélectionner

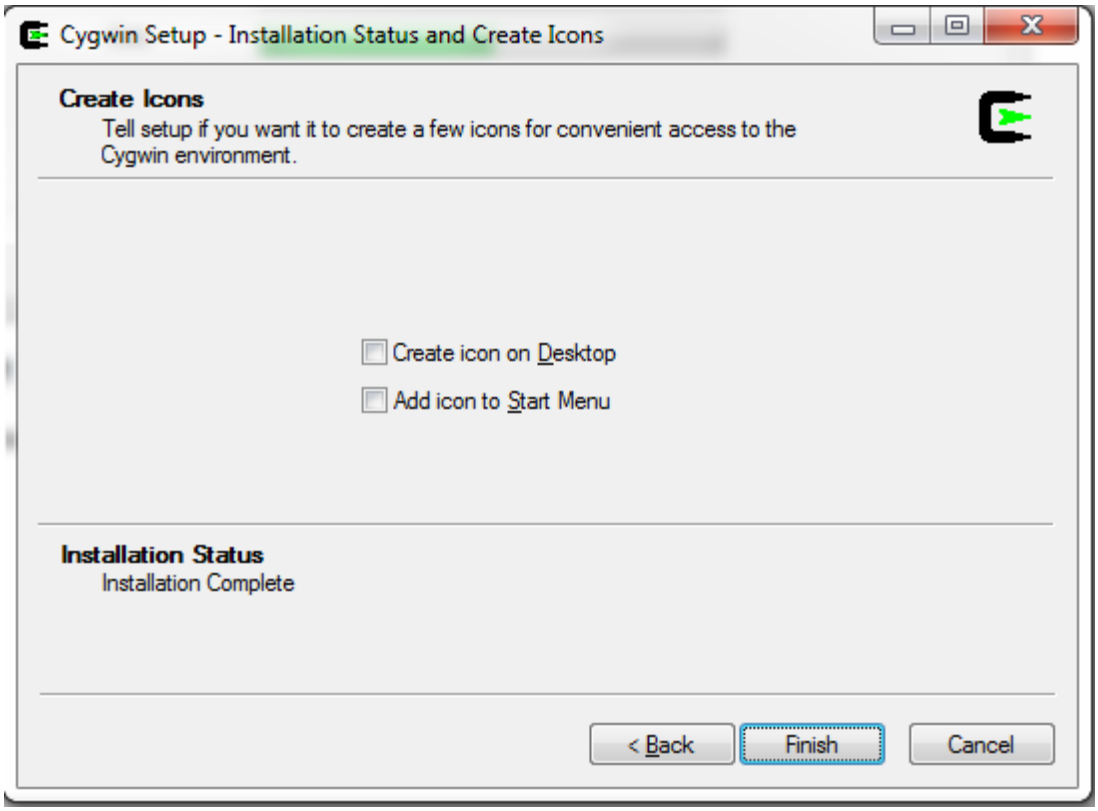


.

C’est à ce moment là que les packages qu’on à sélectionner commence leur installation



Cela va prendre 5 minutes, puis on clique sur finish



Glossaire

Ce glossaire se veut simple, il a pour but de présenter des définitions succinctes des termes

Apparus dans ce document.

Administrateur réseau : Personne responsable de la planification, la configuration et la gestion de fonctionnement journalier du réseau. L'administrateur réseau est aussi appelée administrateur système.

Attaque : Exploitation d'une ou plusieurs vulnérabilités à l'aide d'une méthode d'attaque avec une opportunité donnée.

Backdoor : Est un petit bout de code introduit en générale par un pirate informatique pour pouvoir ouvrir un accès dérobé sur un système informatique et ainsi prendre le contrôle de celui-ci quand il le désire.

Balayage de ports : Technique qui consiste à envoyer des paquets de données sur les différents ports d'une machine distante, puis en déduire les états (la disponibilité) de ces ports en fonction de la réponse retournée, si elle existe.

Broadcast : est un serveur capable de dupliquer un message et de l'envoyer à tout les machines présentes sur le même réseau.

Confidentialité : Propriété des éléments essentiels de n'être accessible qu'à l'utilisateur autorisé.

Déni of service : Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.

Disponibilité : Propriété d'accessibilité au moment voulu des éléments essentiels par les utilisateurs autorisés.

Exploitation : Prendre le contrôle d'un ou plusieurs hôtes, pour ce faire les pirates utilisent souvent de nombreux outils de développés par les plus brillants d'entre eux, ou tirent profit des outils d'évaluations aux vulnérabilités proposé prioritairement aux administrateurs systèmes.

Fichier log : Fichier contenant les informations de connexion sur un serveur, il liste tout les requêtes aux clients, c'est à partir de ce document que l'on étudie les statistiques de fréquentation d'un site, il existe en plusieurs format, le format standard et le format étendu.

Hoax (canular) : un courrier électronique propageant une fausse information et incitant le destinataire à diffuser la fausse nouvelle à tous ses proches ou collègues.

Intégrité : Propriété d'exactitude et de complétude des éléments essentiels.

Intrusion : l'intrusion est le fait, pour une personne ou un objet, de pénétrer dans un espace (physique, logique, relationnel) définit ou sa présence n'est pas souhaitée.

ISO : (Internet Standard Organisation) Organisation nom gouvernementale de standardisation crée en 1946 et installé a Genève. Elle regroupe les principaux organismes de normalisation d'une centaine de payes, comme l'Afnor pour la France.

IDMEF : Est de définir les formats de données et les procédures d'échange pour le partage des informations d'intérêt pour détection d'intrusion des systémes et de réponse et les systèmes de gestion qui pourrait avoir besoin d'interagir avec eux.

Libpcap : Fournis les paquets de capture et de filtrage des moteurs de beaucoup open source et les outilles de réseaux commerciaux, y compris les analyseurs de protocole (de renifleur de paquets, contrôleurs de réseau, système de détection d'intrusion réseau.

Menace : Est une cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation.

NDIS : est une norme qui définit la communication entre un adaptateur de réseau (le pilote qui le gère) et les pilotes de protocole (par exemple TCP \ IP) , le but principale d'un NDIS est d'agir comme un wrapper qui permet aux pilotes de protocole d'envoyer et de recevoir des paquets sur un réseau (LAN ou WAN) .

Pattern matching : autrement dit, filtrage par motif est la vérification de la présence de constituant d'un motif par un programme informatique, ou parfois par un matérielle spécialisé .Par contraste avec la reconnaissance de forme, les motifs sont complètement spécifier.

Ping : est un outil exploitant le protocole ICMP, permettant de tester les connexions sur un réseau en envoyant un paquet et en attendant la réponse.

Port : Point d'entrée et de sortie logique par lequel les services d'une machine peuvent être

Accessible. Et réciproquement, une machine peut émettre des données depuis ce port.

Politique de sécurité d'un système d'information : Ensemble, formalisé dans un document, applicable des éléments stratégiques, des directives procédures, codes de conduite, règles organisationnelle et techniques, ayant pour objectif la protection du (des) systèmes d'informations de l'organisme. [PSSI]

POP : Est un protocole qui permet de récupérer les courriers électroniques situé sur un serveur

De messagerie électronique, actuellement c'est la version 3 qui est utilisé, et le service POP écoute sur le port 110 d'un serveur.

Protocole : Ensemble de règle et de procédures à respecter permettant à des équipements informatiques d'échangé des informations d'un type donné.

Risque : La probabilité d'occurrence d'une menace se transformant en événement réelle entrainant une perte consécutive à sa réalisation.

Serveur : Un programme applicatif acceptant des connexions dans le but de traiter des requêtes en délivrant une réponse.

Serveur SMTP : est un service qui écoute sur le port **25**, son principale objectif est de router les mails à partir de l'adresse du destinataire.

SMTP : Signifie **S**imple **M**essage **T**ransfert **P**rotocole, ce protocole est utilisé pour transféré les messages électroniques sur les réseaux.

Socket : Point de communication par lequel un processus donné pourra émettre et recevoir

Des données. Il est représenté par une adresse IP et un port.

Système d'information : Ensemble des circuits d'information dans une entreprise. Il peut comprendre une ou plusieurs bases de données, des traitements informatisés ou nom, des règles décision, etc.

Vulnérabilité : Caractéristique d'une entité qui peut constituer une faiblesse ou une faille à l'égard de la sécurité des systèmes d'information.

Bibliographie

[01]« Sécurité informatique Ethical Hacking **»** ;[Sébastien Baudru; Robert Crosfert;FranckEbel; Jérôme Hennecart; Sébastien Lasson Marion ; David Puche;2010]

[02]«Tous sur la sécurité informatique » ;[*Jean-philippe* Bay,FrancoisPillou ; 2013]

[03]« Sécurité informatique Principes et méthode » ; **[**Laurent Bloch ; Christophe Wolfhugel ; 2007]

[04] « Les bases du hacking » [Patrick Engebretson ; 2013]

[05]« Les systèmes de détection d'intrusions informatiques (IDS) » [Thierry Evangelista ; 2004]

[06] « Sécurité informatique, Risque, Stratégie et solution » [Didier Godart ; 2005]

[07] « Sécurité réseau avec Snort et les IDS » [Christopher Greg; Sébastien Naméche ; 2004]

[08] « Architecture TCP/IP » ; Technique de l'ingénieur ; [GuyPujolle ;1997]

[09] « Les Réseaux » ; [Guy Pujolle ; Eyrolle 2008]

[10] « Hacking ; Sécurité et testes d'intrusion » [David Kennedy ; 2013]

[11] « Coures d'introduction à TCP/IP **» ; [**François Laissus **;** 2009**]**

[12]« Réseau sécurisé à 200% » [Andrew Lockhart ; 2004]

[13]« Gestion des risques en sécurité de l'information » ; [Anne Lupfer ; 2010]

[14] « Windows installation guide for suricata IDS\IPS**» [**Peter Manev; 2012]

[15] « Détection d'intrusion de réseau » [Stephen Northeutt ; Judy Novak ; 2007]

[16] « Tous sur les systèmes d'informations **» [**Jean-François Pillou **;**2013**]**

[17] « Réseau informatique, les bases essentielles **» ;[** Jaques Poirier **;]**

[18] « Snort user's manual » [Martin Roesch; 1998]

[19]« Detecting and Preventing Unauthorized Outbound Traffic **» [**Brian Wippich; 2007]

WEBGRAPHIE :

[20] http://www.laissus.fr/cours/cours.html

[21] http://cygwin.com/

[22]http://www.wincap.org/

[23] http://pyyaml.org/download /libyaml/yaml-0.1.4.tar.gz