EPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
FACULTE DE GENIE ELECTRIQUE ET INFORMATIQUE
DEPARTEMENT D'INFOMATIQUE

Memoir de fin etude

Présenté par :

Boudedja Lynda

Kherkhour Mustapha

Réalisation d'un IDS Comportementale

Diriger par : M^me^ Heddaoui Rebiha

Année Universitaire : 2014/2015

Sommaire

Chapitre I

Chapitre II

Chapitre III

Chapitre IV

Introduction Générales

Introduction

Du fait de la démocratisation des moyens de connexion à l'Internet due à une pratique des prix de plus en plus attractifs par les différents fournisseurs d'accès, et d'une couverture géographique de plus en plus importante, le nombre d'internautes utilisant des connexions de type haut débit ne cesse de croître. Avec ces types de connexion, les internautes restent en ligne longtemps, ce qui les expose davantage à la convoitise de personnes mal intentionnées qui voient en eux des ressources à utiliser afin, par exemple, d'augmenter leur notoriété dans le monde des pirates. En effet, un pirate peut prendre le contrôle d'un tel poste afin d'attaquer une institution de l'Etat ou un acteur de l'Internet connu, tel qu'un portail ou un site de vente en ligne.

Les entreprises et les particuliers se voient donc confrontés de façon quotidienne à des vers, des virus, des attaques de tous types ou des tentatives d'intrusions.

En effet, l'évolution rapide des technologies et du parc informatique des entreprises fait que la question de la sécurité se pose de façon récurrente. Par exemple, l'apparition des réseaux sans fils (**Wifi**) a introduit de nouveaux types de vulnérabilités. Il en va de même lorsque nous ajoutons un nouveau poste dans un réseau d'entreprise. Si sa configuration n'est pas faite de façon correcte, ceci peut permettre des intrusions dans une partie du réseau. La sécurisation d'un réseau n'est pas simple à réaliser. Le réseau est constitué d'un ensemble de systèmes hétérogènes. De nombreux services, qui ne cessent d'évoluer, sont disponibles. Les personnes en charge de la sécurité telles que les administrateurs réseau, ont à leur disposition toute une panoplie d'outils :

- Des logiciels spécialisés dans la protection tels antivirus, firewall…etc.
- Des technologies dédiées permettant le cryptage des données.
- Des outils de surveillance, des journaux de traces et des logiciels de détection d'intrusion **IDS**.

Au cours de notre travaille on essayera de détaillée au mieux l'utilité de cette puissance outils ces avantages et ces inconvenant, leur types et leur méthode de fonctionnement. Vers la fin on réalisera un de ces types de system de détection d'intrusion.

Chapitre I
Introduction au réseaux et a la sécurité informatique

Partie I : [1]

I-1 Introduction aux réseaux :

I-1-1 Définition de réseaux :

Un réseau est un ensemble de machine, qui peut être géographiquement dispersé mais interconnecter entre eux via une liaison, afin d'offrir aux utilisateurs de meilleur gestion de ressources et un accès plus facile et plus simple rapide et efficaces.

I-1-2 Classification des réseaux

I-1-2-1 Classification selon l'étendue

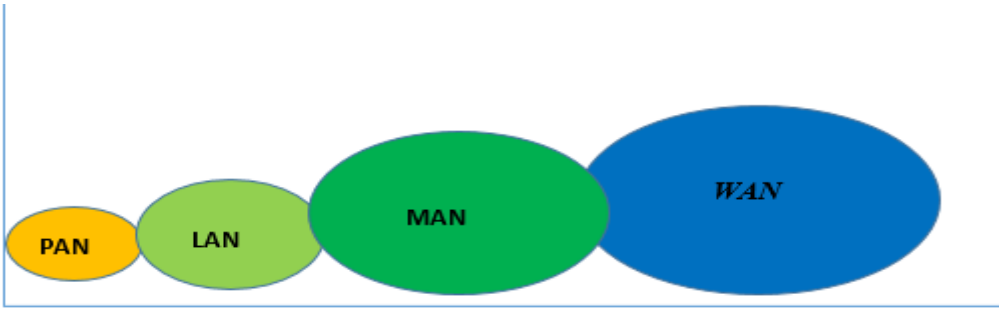


Figure I-1 : L'étendue des différents réseaux [1]

- **PAN :** (Personal Area Network) un réseau personnel qui interconnecte des équipements situés à quelque mètre (une dizaine de mètre)
  - Bluetooth
  - Infrarouge …
- **LAN :** (Local Area Network) un réseau informatique qui est limité géographiquement. On parle de LAN lorsque des distances concernées sont de l'ordre de quelque dizaine de mètre à une centaine de mètres, les LAN peuvent être vue comme un moyen pour partager une connexion internet, travailler sur un même serveur ou échanger des messages de donnée.
  - Ethernet
  - Tolkin Ring
  - WIFI

- **MAN :** (Metropolitan Area Network) Désigne un réseau habituellement dans les grande campus et villes. Nous pouvons imaginer une interconnexion de plusieurs réseaux locaux (LAN) situé dans un espace 1Km à quelque Kilomètre

    - ATM
    - FDDI
    - WMAX (sans fil)

- **WAN** : (Wide Area Network) Un réseau informatique couvrant une grande zone géographique (pays, continent, ou la planète tout entière).

    - Internet

I-1-3 Le modèle TCP/IP :

Le modèle TCP/IP nous permets la gestion des connections et le contrôle des flux, dont le processus entre deux ordinateurs client et serveur en se basant sur le model TCP/IP fonction selon le three way handshake comme suite :

Le client envoi une demande de synchronisation avec le serveur qui contient un nombre qui sert a Controller les données et assurer qu'il n'y a pas de perte, une fois la demande est reçue le revoit un accuser de réception avec le numéro de trame qu'il attend et il demande aussi une synchronisation avec le client, à son tour le client lui envoie une accusée de réception avec le numéro de la trame qu'il attend une fois ces trois message sont envoyé la connections est établie, le serveur va transférer des données et chaque message qui n'est pas acquitté va être retransmis. Pour fermer une session le client envoi en message fin vers le serveur et à son tour il va l'acquitté et il demande aussi la fin de session et il l'acquitte à son tour.

Figure I-2 : Ouverture et fermeture d'une session TCP

I-1-3-3 Les couches du modèle TCP/IP :

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches

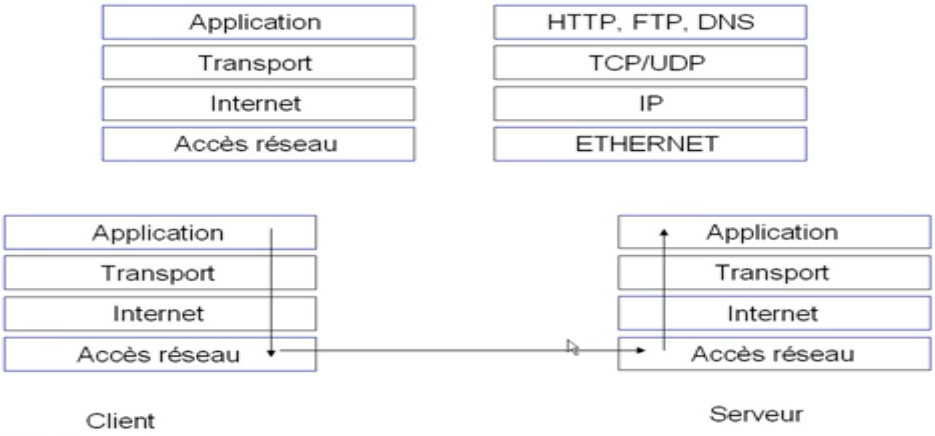


Figure I-3 : Architecture TCP/IP [1]

La couche application :

Cette couche se situe au sommet de modèle a quatre couche. La plupart des applications et des utilitaires fonctions au niveau de cette couche qui leur sert à accéder à la fonctionnalité de réseau TCP/IP. Voici quelque application qui opère au niveau de la couche application : HTTP, FTP, SMTP, Telnet, DNS.

La couche transport :

Cette permettre à des entités paires de soutenir une conversation. Officiellement, cette couche n'a que deux implémentations : le protocole TCP et le protocole UDP.TCP est un protocole fiable, dans cette couche une entête doit insérer essentiellement le port source et le port destination qui est un numéro qui identifie l'application sur l'ordinateur.

La couche internet :

Dans cette couche qu'on trouve le protocole IP (Internet Protocole) qui rajoute une entête sur deux champs, adresse IP source qui est l'adresse de l'émetteur et l'adresse IP destination qui est l'adresse de récepteur, son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination.

La couche réseau :

En fait, cette couche n'a pas vraiment été spécifiée la seule contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau.

L'implémentation de cette couche est laissée libre. Par exemple, beaucoup de réseaux locaux utilisent Ethernet, Ethernet est une implémentation de la couche hôte réseau.

I-1-4 Encapsulation :

Quand une trame est envoyée sur réseau elle passe par les quatre couche du protocole TCP/IP et à chaque couche une entête est rajouté on appel ce processus l'encapsulation voici un exemple ou on demande une connexion a un site web.

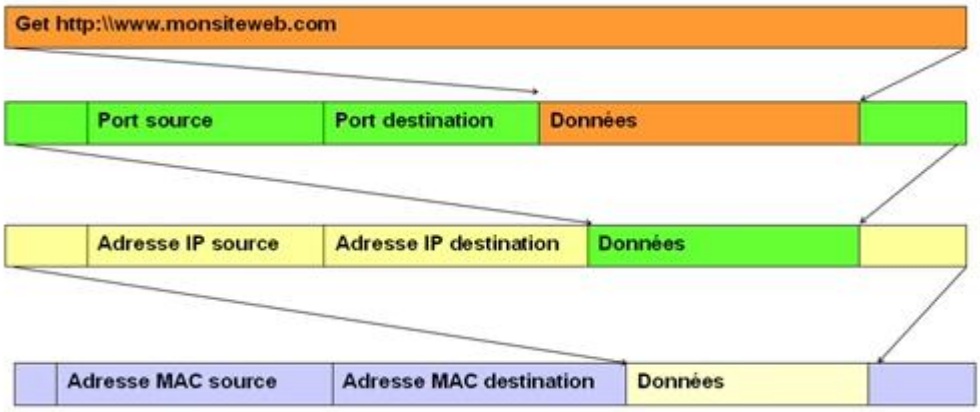


Figure I-4 : Encapsulation [1]

I-1-5 Le protocole UDP :

Le protocole (User Data gram Protocole) est un protocole de transport non orienté connexion qui n'assure pas le contrôle de transfert de donnée il envoie en continue sans se préoccupée ces les donnée envoyer sont arrivé à destination ou pas, généralement utiliser entre serveur afin d'éviter de surcharger le réseau.

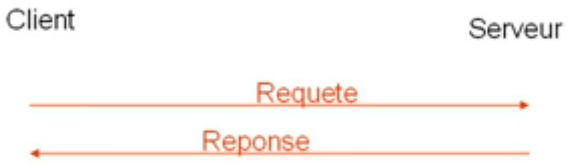


Figure I-5: Protocol UDP [1]

Conclusion :

Vue les grand avantage qu'offre les réseaux facilité d'installation, meilleur gestion, efficacité, meilleur rendement…etc. toute les entreprise on fait recours a ces reaux ce qui a pousser les chercheurs à chercher des moyens pour sécuriser ces dernier vue leur large utilisation.

I-2 Introduction :

La sécurité de l'information consiste à la sécuriser contre toute tentative d'accès non autorisé, divulgation ou destruction. Pour la plupart des organisations l'information est une ressource critique qu'il faut protéger puisque si elle tombe entre de mauvaise main l'organisation fait face à un grand danger.

I-2-1 Généralité sur la sécurité d'informatique :

Dans cette section on passera en revue les éléments essentiels de la sécurité informatique, la force des éléments du triangle (Sécurité, Fonctionnalité, Stabilité), les terminologies essentielles.

I-2-2 Internet current crime IC3[1]: [2]

Sur le graphique, on observe que, dans l'année 2005, il y avait 231 493 plaintes de la criminalité, alors que dans l'année 2009, les plaintes considérablement augmenté pour atteindre 336 655. Par rapport à 2009, internet crim dans l'année 2011 a diminué d'une certain mesure

Figure I.1 : le nombre de crime commis par année **[2]**

I-2-3 Rapport d'investigation de violation de donnée : [2]

Reporter par « Verizon Businesse »[2], le rapport classifie les types de violation et donne leur pourcentage, on constate que la plus part des violations de donnée sont due au piratage (hacking)

[1]**Internet current crime IC3** : C'est un partenariat entre le bureau Fédéral d'investigation (FBI), le NW3C (nation white collar center), et le bureau de l'assistance judiciaire(BJA),

[2] **Verizon Businesse** : une entreprise américaine de télécommunications, présente sur le marché des services mobiles

donc afin de nous protéger contre la violation de donnée on doit commencer par sécuriser notre réseau de manière a ce qui ne soit pas pirater

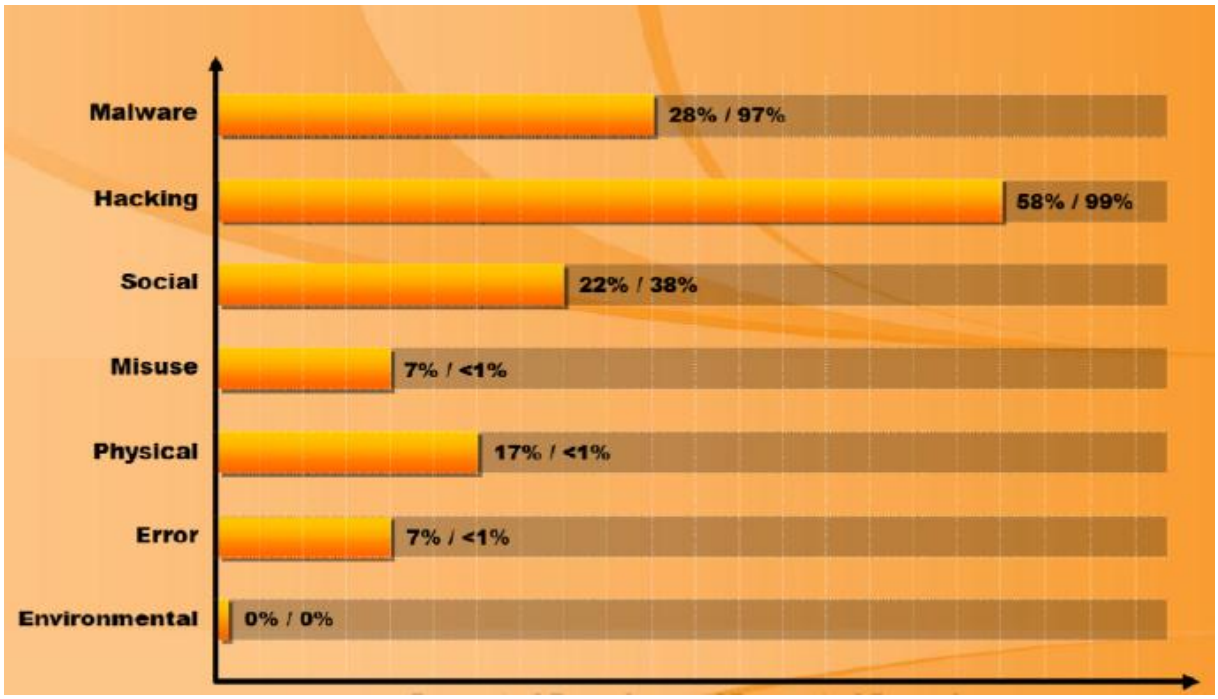


Figure I.2 : Rapport d'investigation de violation de donnée **[2]**

I-2-4 Terminologie essentiel : [2]

Hack value :

C'est le but qui pousse un hacker a pirater et comme ça peut être un bute purement légale comme pour teste la sécurité d'un réseau, application ou système d'information ou pour la célébrité, l'argent, l'humiliation, divulgation de secret…etc.

Exploit:

Définie l'ensemble des étapes qu'un pirate informatique suit a fin de pirater ou violer la sécurité d'un système IT, en exploitant les vulnérabilités découverte sur l'hôte de la cible.

Vulnérabilité :

C'est une faiblesse dans la conception, ou une erreur qui peut mener a un compromis imprévue dans le système de sécurité, il peut être vue comme un trou qui peut être exploité par l'attaquant pour s'introduire dans le système cible.

Targect of evaluation:

C'est un ensemble de produit qui sert a évalué notre système de sécurité, ce type d'évaluation aide a montré les vulnérabilités qui peuvent être exploité par le pirate.

Zero-day attaque :

Dans ce type d'attaque, le pirate exploite les nouvelles vulnérabilités des applications avant que les développeur trouve une solution et développe un patch pour remédier a cette vulnérabilité.

I-2-6 Elément essentiel d'un système de sécurité : [2]

La sécurité de l'information est définie par « le bien être de l'information et de l'infrastructure dans la possibilité de vols, modification ou perturbation de l'information, et que les services assurent au minimum ». Les éléments essentiels d'un système de sécurité sont : Confidentialité, intégrité, non répudiation, authenticité et la disponibilité.

Confidentialité : c'est l'assurance que les informations seront accessibles seulement aux personnes autorisé à avoir accès.

Intégrité : c'est l'assurance que les informations restent telle qu'elles sont et ne subissent aucune modification non autorisé.

Disponibilité : La disponibilité est l'assurance que les systèmes responsables de la prestation, le stockage et le traitement des informations sont accessibles en cas de besoin par les utilisateurs autorisés.

Authentification : réfère aux caractéristiques d'une communication, un document ou n'importe quelle donnée est d'assuré que ces donnée sont authentique a l'original et non modifie ou falsifié. Son rôle principal est d'assuré que l'utilisateur est celui qui prétend être que les messages sont authentiques.

Non répudiation : C'est l'assurance que si un utilisateur fait une tache ou envoie un message il ne peut pas nier l'authenticité de leur signature

Figure I.3 : Elément essentiel d'un système de sécurité **[2]**

I-2-7 Qui sont les pirates :

Sont des individus très intelligent qui ont d'excellente compétence en informatique, qui peuvent crée et profité des vulnérabilités des system ou des réseaux afin de s'introduire sans autorisation et réaliser leur action malveillante, un pirate peut être motivé de plusieurs manière :

- Pour certain est un hobby (passe-temps) pour voir jusqu'à quelle point il peut aller.
- Pour acquérir plus de connaissance et d'expérience ou juste pour faire des choses illégales.
- Avec des buts tracés a l'avance comme volé des informations critiques, numéro de la carte du crédit, mot du passe…etc.

I-2-7-$_1$ classe de pirate :

Il existe exactement 8 types de pirate informatique qui sont :

- **Black hats :** sont des gens avec de large connaissance et des compétences extraordinaires avec des but malveillant. Aussi connue sous le nom de crackers, ils utilisent leur compétence pour découvrir les failles des system de défense, ils attaquent généralement au site gouvernementaux.
- **White hats :** sont des gens qui possède de large compétence qu'ils utilisent seulement pour des fin défensive, connue sous le nom de d'analyste de sécurité. La plupart des organisations possède un analyste pour protéger leur system d'information.
- **Gray Hats :** sont les individus qui travaillent dans les deux cas le défensive et l'offensive, ils mélangent entre le black hats et le white hats comme il peut aider des hackers a découvrir les faille d'un system de sécurité il peut aussi aider un développeur à sécuriser un produit.

- **Suicide hackers :** c'est des individus qui piratent pour une cause qui défend et ils s'en fichent complètement des conséquences ils sont tels que les kamikaze qui s'explose et sacrifie leur vie pour une cause qui crois être juste.
- **Script kiddies :** ce sont des pirate non qualifie qui compromettent des systèmes en utilisant des utilitaires développé par des vrais hackers ils utilisent de petit programme pour réaliser leur attaque, sont intéressé beaucoup plus par la quantité que par la qualité d'attaque.
- **Spy hackers :** sont des employés des organisations qui sont recruté pour pénétrer les system des adversaires et récupérer leur donnée classé secret.
- **Cyber terroriste :** sont des groupes organiser et former par des organisation terroriste motivé par une cause politique, religieuse…etc. c'est le type le plus dangereux par ce que ils peuvent pas seulement pirater un site web mais une zone toute entière.
- **State sponsored hackers :** sont les employés du gouvernement qui pénètre et endommage les systèmes d'information des autres pays et récupéré des informations classé top secret.

Figure I.4 : Le type de hackers [2]

I-2-7 Hacking phases : [2]

Afin de pirater une cible, un pirate réalise sa tache sur déférente étapes qui commence par la connaissance et finit par l'effacement de traces on passera en revue ces phases et on va essayer d'expliquer le but de chaque étapes.

Phase 01 : La reconnaissance

C'est la phase préparatoire ou un pirate doit ramasser le plus possible d'informations sur sa cible, cette phase permet au pirate de mettre en place une stratégie d'attaque ce qui risque de prendre un peu de temps parce qu'il doit recourir a déférentes techniques qui lui permettent d'avoir des informations sur la cible tel que :

- **Social engineering :** profiter des défaillances humaines par des hackers qui peuvent manipuler une cible pour leur soutirer des informations sensibles.
- **Dumpster diving :** c'est le processus de surveillance des poubelles de l'entreprise cible pour récupérer des informations critique et secrète qu'on ne peut pas se procurer ailleurs.

- **Type de reconnaissance :** Il existe deux types de reconnaissance Active et passive

  - **Reconnaissance passive :** le pirate ne montre pas sa présence il se contente que d'écouter ce qu'il se passe au seine de la cible on utilisant déférentes technique de reconnaissance.
  - **Reconnaissance active :** dans ce type de reconnaissance le pirate interagit directement avec la cible ou ils utilisent les déférents utilitaires afin de détecter une vulnérabilité qui peut exploiter.

Phase 02: Le Scanning

Certain experts ne font pas la différence entre l'étape de reconnaissance et scanning seulement que les deux étapes sont légèrement déférente. Après la reconnaissance le pirate s'appuie sur les informations rassemblé pour identifier les faiblesses et les vulnérabilités du réseau ou le pirate recours a des utilitaires pour accomplir cette tâche tel que :

- **Trace route :** qui peut nous procurer un mappage du réseau, parfeu utilis é et l'emplacement des machine, router…etc.
- **Scanner de port :** tel que Nmap qui peut nous aider a détection des ports ouverts et des services en cours d'exécution.

La solution dans ce cas est d'éteindre tous les portes inutiles ou d'utiliser un filtre pour Controller le trafic qui circule.

Phase 03: Gain d'accées

C'est l'étape la plus importante ou le pirate est sur le point d'accéder au système cible qui se fait par niveau, en premier lieu le pirate commence par gagner l'accès au niveau le plus bas de la cible et escalader les niveaux en suite jusqu'à ce que il gagne un contrôle complet.

Phase 04: Maintien d'accée

Une fois que le pirate réussi à avoir le contrôle de la cible le pirate choisi entre rester au profile bas et continué a hacker la machine sans que la cible se rend compte a l'aide d'une porte dérobé (torjan) ou de se servir de la cible et exploiter ces ressource ou d'utiliser comme machine intermédiaire pour hacker une autre cible.

- **Cheval detroie (torjan) :** utiliser pour transférer des donnée sensible de puis la machine cible ver le pirate tel que mot de passe, nom d'utilisateur, numéro de carte de crédit…etc. La solution pour ce genre de menace est de déployer des IDS (système de détection d'Intrus) ou des honeypots.

Phase 05: Clearing tracks (effacer les trace)

Après être introduit dans la cible le pirate essaye d'effacer toute trace de sa présence pour déférente raison que ce soit pour éviter qu'on le découvre ou il risque une peine de prison ou pour cacher et continue a hacker la cible.

- **Toolkits :** sont des utilitaires qui servent à cacher la présence du pirate
- **Sténographie :** est l'art de dissimulation des objets, son but est de faire passer un message dans un autre message sans que la cible se rend compte, comme la technique de LSB pour les images.
- **Tunneling :** plusieurs protocoles s'exécute sur un système, le tunneling consiste a isolé un protocole et l'utiliser les bits insignifiant des entêtes des paquets et les remplacer par les donnée volé tels que le mot de passe, nom d'utilisateur…etc.

I-2-8 motivations, les buts et objectifs des attaques de sécurité :

Attaque = Motive (but) + Méthode + Vulnérabilité

Les Attaquants ont généralement des motifs ou des objectifs ou des objectifs derrière les attaques de sécurité qui peuvent être pour :

- perturber le travail continu et l'objectif d'une organisation.

- Vol de précieuses informations.

- À titre de curiosité.

-Se venger sur l'organisation cible

I-2-9 Les attaques de sécurité :

Le pirate peut effectuer son attaque sous plusieurs formes et on ne peut jamais prédire le chemin que l'attaquant peut entreprendre lors d'une attaque afin d'arriver a ces but malveillant

Par ce qu'il existe déférentes manières d'attaquer et les compétences des pirate sont déférentes donc chacun a une manière de procéder et c'est pour cela qu'on devrait couvrir toute des brèches dans notre système de sécurité. La figure suivante montre les déférentes menaces auxquelles doit faire l'entreprise.

Figure I.5 : déférente menace pour un système d'information **[2]**

I-2-10$_{-1}$ Différents types d'attaques [3]

I-2-10$_{-1-1}$ Les attaques par protocole

- ✓ **IP spoofing :** L'« usurpation d'adresse IP » est une technique remplace l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.

Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une *mascarade* de l'adresse IP au niveau des paquets émis.

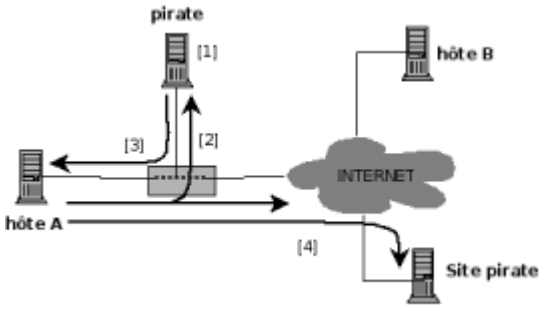


Figure I.6 DNS spoofing [3]

- ✓ **Le DOS :**

Les attaques par déni de service ont pour seul but d'empêcher le bon fonctionnement d'un système et non de récupérer des informations. Elles utilisent les faiblesse de l'architecture d'un réseau. Il est ainsi possible d'envoyer des paquets de taille anormalement importante. Le système victime reçoit des paquets IP qu'il ne peut gérer et fini par stopper tous les services (saturation mémoire).

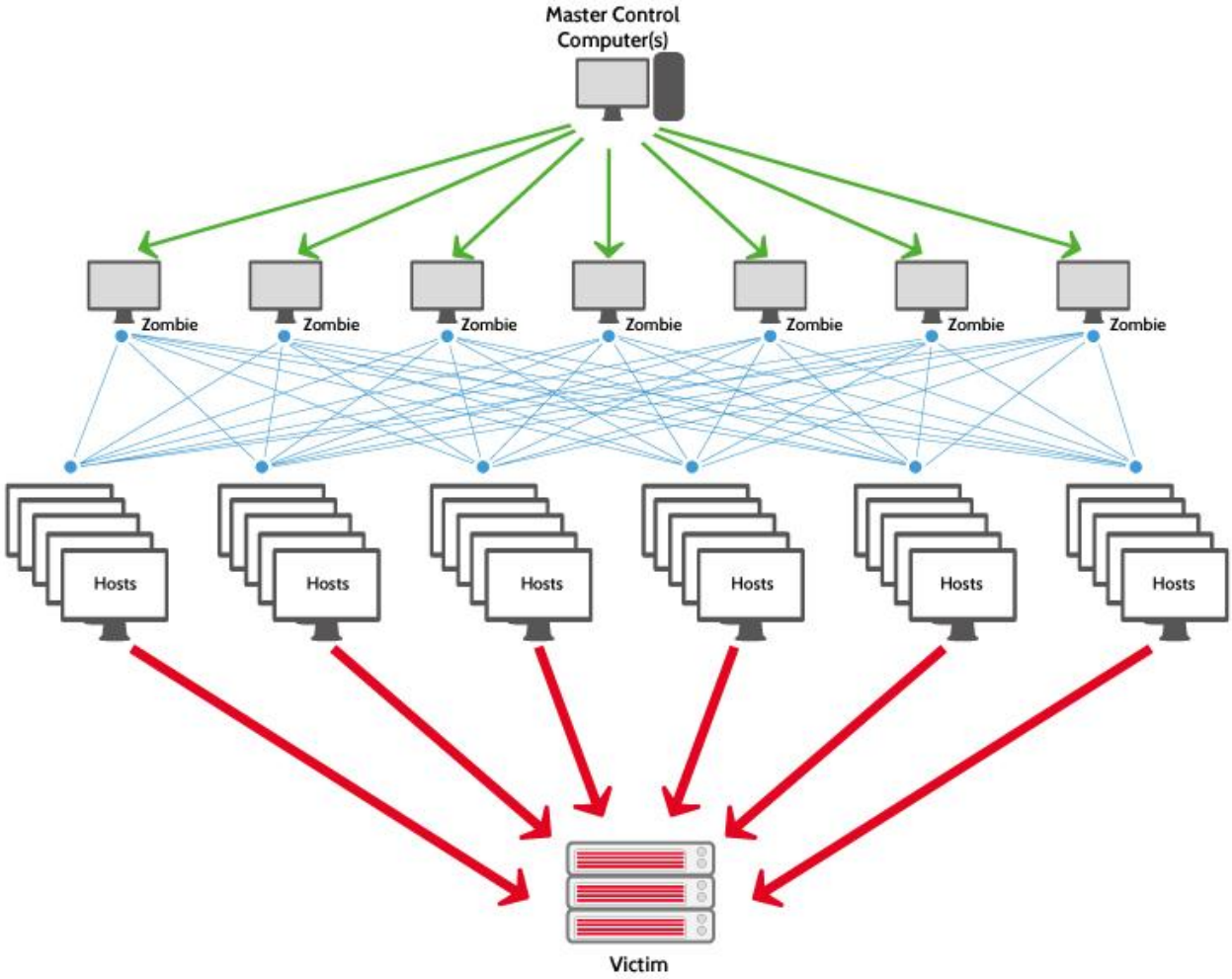


Figure I.7 Dos [4]

- ***Une technique de déni de service : le smurf***

Cette attaque est organisée car elle utilise une liste de serveurs broadcast récupérée à l'avance par un scanner. Cette liste contient les serveurs broadcast qui permettent de router vers le plus grand nombre de machine, et qui sont les plus rapides. Par exemple, une machine A décidé d'attaquer une machine B : la machine A envoie un ping à un serveur broadcast en falsifiant son adresse IP, l'adresse IP falsifiée est celle de la machine B, le serveur broadcast adressera le ping à son réseau et il y aura autant de réponses, qu'il y a de machines, renvoyées à la machine

- ✓ **Le Sniffing**

Correspond à l'écoute passive par surveillance des paquets IP qui transitent sur un réseau. L'un des but final est de récolter illégalement des mots de passe. Les logiciels, qui permettent d'analyser le trafic sont très utilisés à des fins de gestion de réseau ; ils sont disponibles généralement avec divers systèmes d'exploitation, ou en freeware sur le réseau. Ils s'exécutent sur n'importe quel PC en sniffant et en analysant les données en transit sur les lignes, pour en extraire les mots de passe transmis par l'utilisateur lors de sa demande de connexion.

Cette écoute passive de données en transit peut conduire à des intrusions illicites.

Figure I.8 Sniffing [4]

- ✓ **Attaque par le protocole RIP**

Ce protocole peut être utilisé pour détourner des communications : l'imposteur se fait passer pour l'émetteur autorisé, envoie de fausses informations de routage aux passerelles et aux destinataires, qui utiliseront l'adresse IP donnée par le paquet RIP de l'imposteur pour transmettre des données à destination de l'émetteur, qui est en fait le récepteur.

- ✓ **Attaque par requêtes ARP**

Une requête ARP peut être diffusé jusqu'à ce qu'une machine se reconnaissant, et renvoie son adresse ethernet. Mais si une requête ARP est émise avec une adresse IP inexistante, on peut générer des tempêtes de diffusion (broadcast storm), ce qui provoque la saturation de la bande passante, et rend indisponible le réseau(effondrement du réseau, déni de service) .

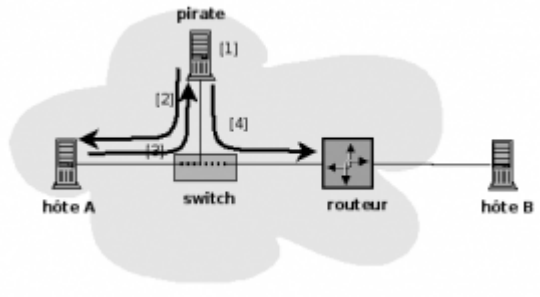


Figure I.9 .Attaque d'un switch avec des messages Arp [3]

- ✓ **Attaque ICMP**

Le protocole ICMP contrôle l'acheminement des paquets de données IP, et si un problème de transmission est détecté par un routeur, celui-ci informe l'émetteur du paquet en lui envoyant un paquet ICMP.

Par exemple, des faux messages ICMP peuvent être générer pour surcharger le réseau, le rendre inutilisable, et entraîner certains dénis de service.

Autres exemples :

- paralyser le réseau en rédigeant des paquets IP vers une fausse destination
- augmenter la charge des systèmes en faisant traiter un grand nombre de messages ICMP
- empêcher un émetteur d'envoyer des données, en exploitant la facilité offerte par ICMP pour contrôler le flux d'émission des paquets. Cela provoque des conséquences sur le trafic supporté par le réseau et atteinte aux performances du réseau.

- ✓ **Attaque par fragmentation**

Le protocole Internet autorise la fragmentation de paquets de trop grande taille pour adapter la taille aux capacités de transfert du réseau. Seul le premier segment d'un paquet IP fragmenté contient le numéro de port TCP, les autres segments du paquet ne contenant pas de numéro de port TCP et ne peuvent pas être filtrés par le firewall, ainsi ils peuvent pénétrer un environnement à priori protégé.

- ✓ **Attaque par tromperie UDP**

Le protocole UDP n'effectue pas de contrôle (contrôle de flux, contrôle d'erreur et contrôle d'identification) lors de transfert de données entre 2 correspondants. N'importe qui peut donc

utiliser une adresse IP d'une machine autorisée à se connecter à un système, et le pénétrer. Ces vols de sessions UDP peuvent avoir lieu sans quel' serveur s'en rende compte.

- ✓ **Attaque par inondation de messages**

Submerger la boîte aux lettres d'un utilisateur par un grand nombre de mails entraîne des dénis de service.

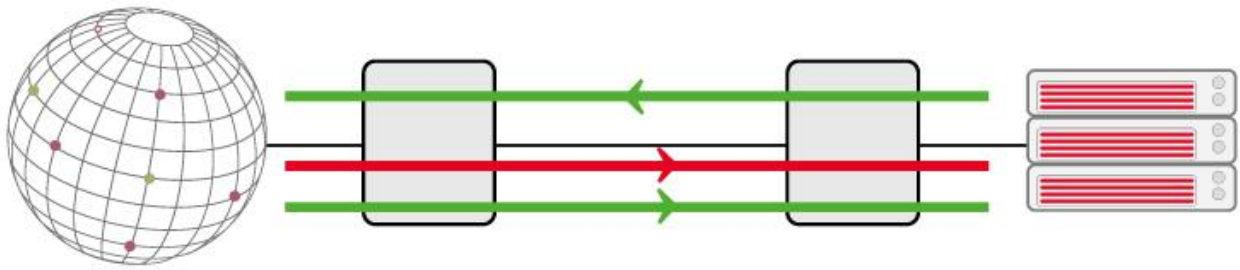


Figure I.10 .Innondation de MSG[5]

- ✓ **Attaque par débordement de tampon (buffer overflow)**

Cette attaque vise les systèmes informatiques en exploitant leurs caractéristiques internes de fonctionnement, notamment celles de leur système d'exploitation, et non celles liées aux protocoles qu'ils supportent.

Par exemple, l'attaquant fait subir des dépassements de capacités de certaines zones tampon entraînant des dysfonctionnements graves pouvant entraîner l'arrêt des systèmes.

Par exemple, le port 80 n'étant pas filtré par le pare-feu, un débordement de la mémoire tampon du serveur web via une longue requête HTTP est possible, et elle peut contenir un bout de code trafiqué qui sera exécuté par le serveur. Celui-ci écoutera le trafic et exécutera les commandes transmises par le hacker.

I-2-10$_{\text{-1-2}}$ Les attaques virales

Il existe principalement quatre types de menaces distinctes :

- ✓ **Virus** : Se reproduisent en infectant le corps de programmes hôtes
- ✓ **Vers** : Le vers se duplique et se propage à travers le réseau, par courrier électronique par exemple.
- ✓ **Chevaux de Troie** : Exécutent des tâches malignes en se cachant dans un programme

sain. Il peut par exemple voler des mots de passe, copier des données, ou exécuter toute autre action nuisible.

Trappes (portes dérobées) : Permet à un utilisateur externe de prendre le contrôle d'une application par des moyens détournés.

I-2-11 Outils de sécurité : [4]

Le système de sécurité d'une entreprise se construit à l'aide de nombreux outils complémentaires et techniques existant sur le marché. Un seul ne suffit pas: la sécurité est assurée par une utilisation correcte d'un ensemble d'outils à choisir, paramétrer et/ou développer en fonction de l'objectif de sécurité fixé.

I-2-11-1Encryption, signature électronique et certificats :

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

- **l'encryption:** elle consiste à transformer les informations électroniques au moyen d'un algorithme mathématique afin de les rendre inintelligibles, sauf pour celui qui possède le moyen (une clé) de les décoder. L'encryption des informations qui transitent par le réseau est utilisée pour assurer la confidentialité, l'intégrité et l'authenticité des transactions et du courrier électronique. Il existe deux types de cryptage :
  - **Cryptage Symétrique :** le même clé utiliser pour le cryptage est utiliser pour le décryptage tes le que le ***AES, DES, 3DES****…etc*.
  - **Cryptage Asymétrique :** Ce type utilise de clé une qui est public qui est connue par tout le monde est une autre privé, tous se qui est Crypter par la clé public du destinataire ne peut être décrypté qu'avec la clé privé du destinataire. Voice queqle exemple de cryptage asymétrique : *RSA, DSA, DH, El Gamal…etc.*

- **la signature électronique:** c'est un code digital (une réduction du document électronique à envoyer) qui, associé aux techniques d'encryption, garantit l'identité de la personne qui émet le message et assure la non-répudiation et l'intégrité de l'envoi.
- **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 publique d'encryption et fournit des informations de gestion complémentaires sur le certificat et le détenteur.

I-2-11-2 L'authentification et l'autorisation

Une personne peut être authentifiée par la combinaison d'une identification et d'un mot de passe (code secret personnel). Le mot de passe doit posséder certaines caractéristiques: non trivial, difficile à deviner, régulièrement modifié, secret, etc. Des outils logiciels ou hardware de génération de mots 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 quelle mesure (par exemple consulter ou mettre à jour des données).

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

I-2-11-3 Le firewall

Le firewall est un ensemble informatique du réseau d'entreprise comprenant du matériel hardware (un ou des routers, un ou des serveurs) et des logiciels (à paramétrer ou à développer). Son objectif est de protéger le réseau interne contre les accès et actions non autorisés en provenance de l'extérieur, en contrôlant le trafic entrant. Le firewall peut également contrôler le trafic sortant.

Le firewall est localisé entre le réseau externe et le réseau interne. Pour être efficace, le firewall doit être le seul point d'entrée-sortie du réseau interne (pas de modem sur un serveur ou pc pour accéder à l'extérieur sans passer par le firewall) et surtout doit être correctement configuré et géré en fonction des objectifs spécifiques de sécurité. Sans ces précautions, un firewall ne remplit pas son rôle et est complètement inutile.

Le firewall est un élément de la sécurité, il ne couvre pas tous les risques (par exemple le firewall n'assure pas la confidentialité des informations, n'authentifie pas l'origine des informations, ne vérifie pas l'intégrité des informations, ne protège pas contre les attaques internes).

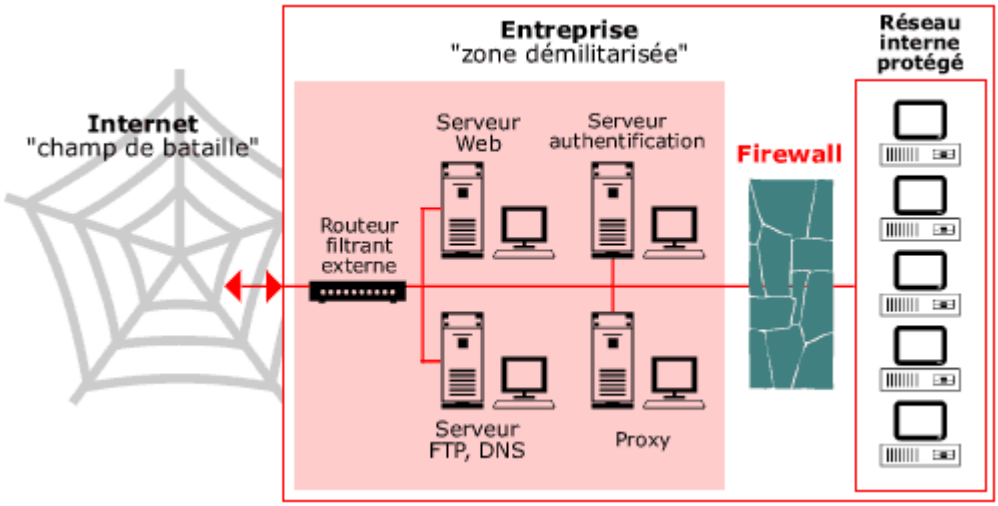


Figure I.11 : placement d'un firewall au sein d'une entreprise **[6]**

Il existe plusieurs types de techniques de firewall:

- **la technique de filtrage des paquets**: chaque paquet d'information entrant ou sortant est accepté ou rejeté selon des règles établies par l'utilisateur;
- **la technique des serveurs proxy** qui empêchent l'extérieur de connaître les adresses internes du réseau d'entreprise;
- **la technique des passerelles** qui fournissent des systèmes de sécurité pour établir des connexions TCP/IP entre l'extérieur et l'intérieur ou pour certains services comme FTP et Telnet.

I-2-11-4 Les fichiers historiques

Des outils de traçabilité (logging) doivent être mis en oeuvre pour garder une trace des événements, comme par exemple:

- qui est venu, quand, quelle a été la durée de la transaction?
- qu'a-t-on consulté ou modifié?

- quelles 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 provenance d'une même adresse extérieure et rejetés par le firewall peuvent être un signe d'essai d'intrusion).

I-2-11-5 Les copies de sauvegarde

Les copies de sauvegarde (back-up) créées régulièrement et stockées dans des endroits sécurisés permettent de protéger les informations essentielles pour l'entreprise et permettent également de redémarrer rapidement en cas de problème.

I-2-11-6 Réseau Privé Virtuel

Le VPN (Virtual Private Network) est un service disponible chez les fournisseurs de services Internet (ISP) qui permet d'établir des connexions sécurisées privées (un réseau privé) sur un réseau public comme l'Internet. Le VPN est réalisé avec les techniques d'encryptions et d'authentification, en assurant la qualité de services requise. Le VPN permet l'économie de connexions directes coûteuses entre les différentes implantations de l'entreprise, l'accès Internet lui servant à la fois pour la consultation classique de sites web et pour son réseau privé.

Voici un exemple de VPN:

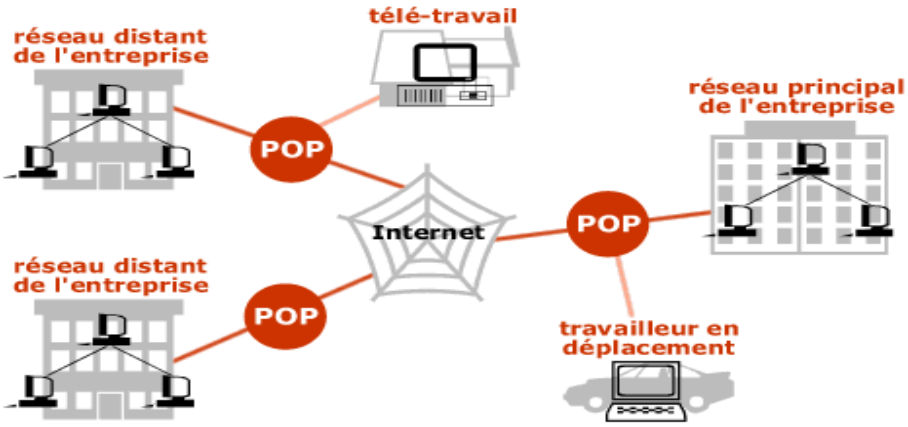


Figure I.12: liaison VPN entre déférent siège d'une entreprise. **[6]**

I-2-11-7 LES IDS

IDS signifie Intrusion Detection Système. Il s'agit d'un équipement permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion et éventuellement de réagir à cette tentative.

Conclusion :

Nous avons constaté dans ce chapitre, que la sécurité réseau est un point primordial. Les administrateurs déploient des solutions de sécurité efficaces, capables de protéger le réseau de l'entreprise. Dans ce contexte, les IDS constituent une bonne alternative pour mieux protéger le réseau informatique.

Dans le chapitre II, aborder les systèmes de détection d'intrusion de maniérer plus détaillé et nous discuterons des déférente approche des IDS et de leur fonctionnement.

Chapitre II
Les system de détection d’intrusion

II.1. Introduction :

Nous avons présenté au Chapitre I les réseaux de manière générale et les menaces qui menace ces dernier ainsi que les mécanismes de défense contre ces attaques, quoi que certain attaque passe inaperçue face a ces mécanismes, le système de détection d'intrusions tente de déceler les attaques qui passent inaperçues à travers les mécanismes de sécurité. Un IDS a pour fonction d'analyser en temps réel ou différé le trafic réseau et de détecter les différentes attaques lancées contre le réseau de l'entreprise.

Après la courte introduction des systèmes de détection d'intrusions présentée au Chapitre I, dans ce chapitre, nous détaillons les qualités requises d'un IDS, son utilité , le critère de choix et un état de l'art des approches proposées dans la littérature.

11.2. Système de détection d'intrusions [1] :

Les IDS, ou systèmes de détection d'intrusions, sont des systèmes software ou hardware conçus afin de pouvoir automatiser le monitoring d'événements survenant dans un réseau ou sur une machine particulière, et de pouvoir signaler à l'administrateur système, toute trace d'activité anormale sur ce dernier ou sur la machine surveillée. L'IDS est un système de détection passif. L'administrateur décidera ou non de bloquer cette activité.

Ces systèmes de surveillance du réseau sont devenus pratiquement indispensables dû à l'incessant accroissement en nombre et en dangerosité des attaques réseaux depuis quelques années.

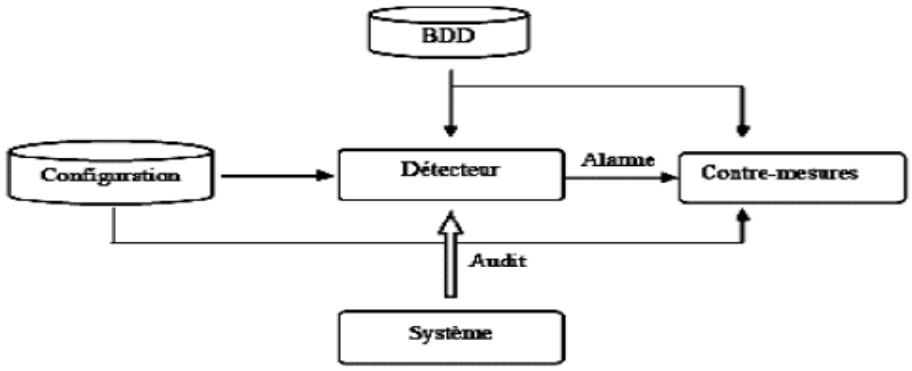


Figure II.1 : Modèle simplifié d'un système de détection d'intrusions **[3]**

Le détecteur analyse trois types d'informations : les informations de long terme relatives aux techniques utilisées dans la détection (Base de données de signatures), les informations de configuration qui déterminent l'état courant du système, et les informations d'audit qui décrivent les événements survenus dans le système.

11.3. Fichier historique : [5]

Fichier historique permet d'enregistrer tout ou une partie des actions effectuées sur le système. L'analyse de ses informations permet de détecter d'éventuelles intrusions. Les systèmes d'exploitation génèrent des fichiers historiques, certaines applications aussi. Les différents évènements du système sont enregistrés dans un journal, qui devra être analysé fréquemment, voire en permanence. Sur les réseaux, il est indispensable de disposer d'une base de temps commune pour estampiller les évènements.

Voici les types d'informations à collecter sur les systèmes pour permettre la détection d'intrusions : On y trouve les informations sur les accès au système (qui a accédé, quand et comment), les informations sur l'usage fait du système (utilisation du processeur, de la mémoire ou des entrées/sorties) et les informations sur l'usage fait des fichiers. Le fichier historique doit également permettre d'obtenir des informations relatives à chaque application (le lancement ou l'arrêt des différents modules, les variables d'entrée et de sortie et lesdifférentes commandes exécutées), Les informations sur les violations éventuelles de la sécurité (tentatives de commandes non autorisées) ainsi que les informations statistiques sur le système seront elles aussi nécessaires.

Notons que ces nombreuses informations occupent beaucoup de place et sont très longues à analyser. Ces informations devront être, au moins pour un temps, stockées quelque part avant d'être analysées par le système de détection d'intrusions.

11.4. Caractéristiques d'un système de détection d'intrusions [5]

Pour une détection d'intrusions efficace, il est très important de considérer certaines caractéristiques :

- 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.

11.5. Emplacement d'un système de détection d'intrusions [6]

Le placement des IDS va dépendre de la politique de sécurité menée. Mais il serait intéressant de placer des IDS :

- dans la zone démilitarisée (attaques contre les systèmes publics),
- dans le (ou les) réseau privé (intrusions vers ou depuis le réseau interne),
- sur la patte extérieure du firewall (détection de signes d'attaques parmi tout le trafic entrant et sortant, avant que n'importe quelle protection intervienne).

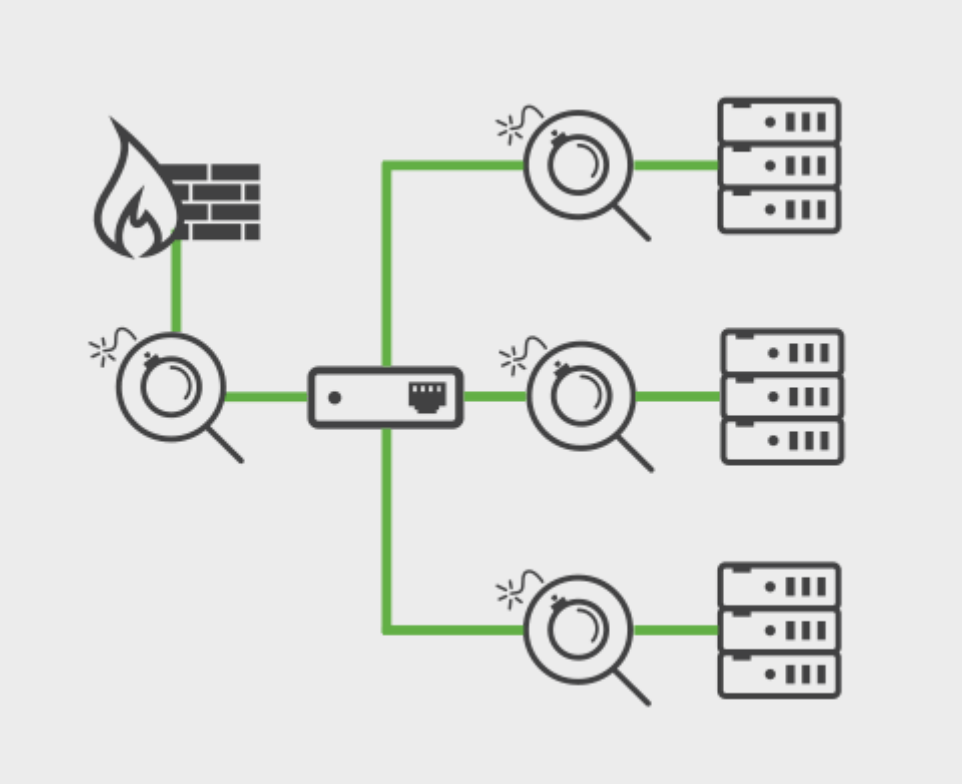


Figure II.2 placement d'un IDS[11]

11.6. Classification des systèmes de détection d'intrusions : Les IDS peuvent être classés selon différents critères qui ne sont pas mutuellement exclusif, et ils sont :

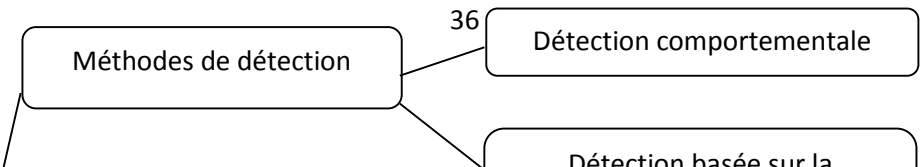
a) Méthode de détection utilisée.

b) Mode de fonctionnement des mécanismes de détections.

c) Sources de données à analyser.

d) Réponse aux attaques

e) Fréquence d'utilisation.



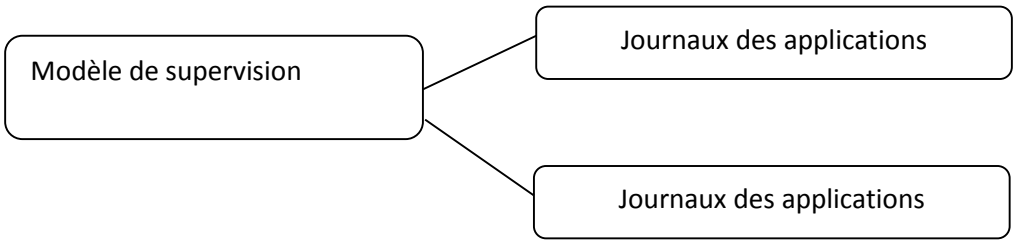


Figure II.3 : classification des systèmes de détection d'intrusions [9]

11.6.1 Méthodes de détection : [7]

Nous classons les IDS en deux grandes catégories de principe de détection d'intrusion :

11. 6.1 .$_1$ 1 Approche par scénario

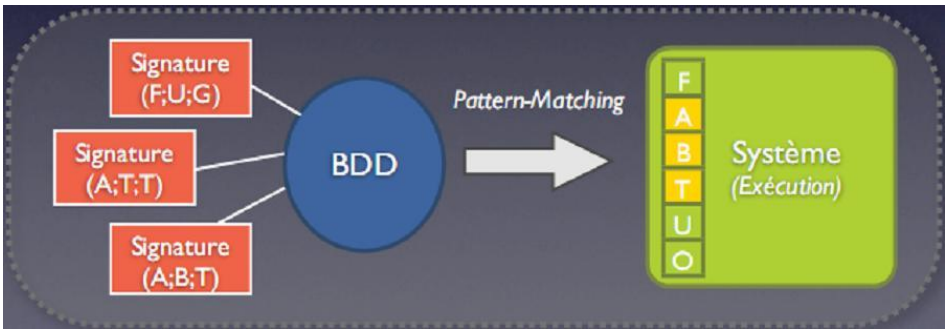


Figure II.4 approche par scénario [10]

Les systèmes à base de signatures qui consistent à rechercher dans l'activité de l'élément surveillé les signatures (empreintes) d'attaques répertoriées et donc connues. Ce principe de détection d'intrusion est réactif et pose plusieurs contraintes, en effet il ne détecte que les attaques répertoriées dont il possède l'empreinte. De ce fait il nécessite des mises à jour fréquentes. Ce principe de détection implique aussi que les pirates peuvent contourner celui-ci en maquillant leurs attaques, il modifie en fait la signature connue par les IDS et de ce fait l'attaque devient invisible par l'IDS.

Il existe différentes méthodes pour repérer les attaques :

- ANALYSE DE MOTIF :

  la plus simple et la plus couramment utilisée pour détecter une intrusion. Une base de connaissance contient toutes les chaînes alphanumériques caractéristiques d'une intrusion.

- RECHERCHES GENERIQUES :

Adaptée pour les virus. On regarde dans le code exécutable les commandes qui sont potentiellement dangereuses. Par exemple, une commande DOS non référencée est détectée, des émissions de mails, des instructions liées à des attaques connues.

- CONTRÔLE D'INTEGRITE :

  Effectue une photo de tous les fichiers d'un système et génère une alerte en cas d'altération de l'un des fichiers. MD-5 est le plus fréquemment utilisé mais les spécialistes recommandent maintenant le SHA-256 et SHS on signe les hash et on les mets dans un coffre fort (stocké sur un periphérique externe en lecture seule physique) Et on compare périodiquement les nouveaux hash au hash signés. Aujourd'hui l'exemple le plus connu utilisant cette approche est l'IDS SNORT.

11. 6.1 .1 Approche comportementale

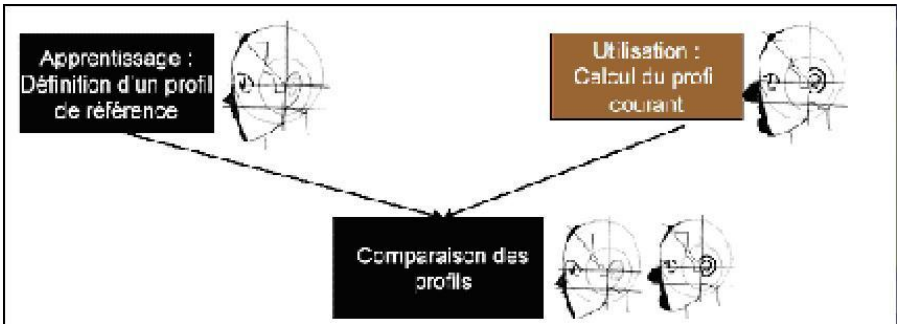


Figure II.5 approche comportementale[10]

Les systèmes à approche comportementale consistent à détecter les différentes anomalies sur le réseau. C'est l'administrateur qui définira le fonctionnement "normal" des éléments surveillés, il y a donc une phase d'apprentissage pour fixer ce niveau. Par la suite l'IDS sera en mesure de signaler à l'administrateur toute situation qui divergera du niveau de fonctionnement de référence. Le fonctionnement de référence peut être élaboré par différentes analyses statistiques de l'élément à surveiller. Ce système de détection présente un avantage par rapport au précèdent : il détecte les nouveaux types d'attaques. Cependant il faudra faire parfois des ajustements afin que le fonctionnement de référence corresponde au mieux à l'activité normale des utilisateurs et ainsi réduire les fausses alertes qui en découleraient.

Il existe différentes techniques pour repérer les attaques :

❖ **APPROCHE PROBABILISTE :**

On prévoit quelle est la probabilité d'avoir un évènement après un autre. Ex : quelqu'un qui se connecte à un site : forte proba que la demande de connexion soit suivi de GET OK Si ce n'est pas ça la plupart du temps, on peut avoir un doute…

- **Avantage**:
  - ✓ Construction du profil simple et dynamique
  - ✓ Réduction de faux positifs
- **Inconvénient**:
  - ✓ Risque de déformation progressive du profil par des attaques Répétées

❖ **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

✓ **Avantage**:

- ✓ Permet de détecter des attaques inconnues
- ✓ Habitudes des utilisateurs apprises automatiquement

✓ **Inconvénients**:

- ✓ Complexité en termes de maintenance
- ✓ beaucoup de faux-positifs

❖ **IMMUNOLOGIE (en cours d'étude) :**

Construit un modèle de comportement normal des service (et non des utilisateurs) Il faut observer un service suffisamment longtemps dans de bonnes conditions pour construire un modèle de comportement complet.

11.6.1.3 Comparaison entre les deux approches :

Scénarios	Comportements
Spécification complexe des scénarios	Taille des automates générés
Pas de faux positifs	Phase critique d'entraînement
Aucune prise en compte des nouvelles attaques	Prise en compte des nouvelles attaques
Mise à jour rapide	Mise à jour délicate (phase d'entraînement)
Protection facile à contourner	Faux positifs nombreux
Prise en compte incomplète des environnements parallèles	

Figure II.6 Tableau de comparaison entre l'approche comportementale et l'approche par scénario [9]

11.6.1.4 Approche comportementale ou approche par scénarios ? [9]

Nous avons constaté, que chacune de ces deux approches présente des avantages et des inconvénients. Il semble donc indispensable d'hybrider l'approche comportementale avec l'approche par scénarios de manière à profiter des avantages de l'une et de l'autre.

Les modèles comportementaux sont de plus en plus intégrés à des IDS initialement basés sur une bibliothèque de signatures. En effet, certains éditeurs ont déjà fait le choix de compléter leur base de signature, par un modèle comportemental basique permettant de signaler des événements non identifiables.

11.6.2 Réponses:

Lors de la détection d'une attaque, un système de détection d'intrusions, peut adopter plusieurs comportements. Les IDS peuvent émettre des réponses actives qui influent directement sur la source d'attaque, par exemple un IDS peut réagir en réparamétrant un par-feu, pour mettre en place des règles de blocage temporaire de certains flux réseau anormaux, comme ils peuvent se restreindre à des réponses passives en diffusant une alerte identifiant l'attaque détectée. Une liste des réponses actives et passives est présentée dans le tableau.

Dans la pratique, peu d'administrateur de sécurité envisage concrètement de mettre en place, des contres mesure automatique (réponse active). Il laisse au lecteur le soin de deviner la dénomination d'une réponse active, après détection d'une attaque.

Réponse passive	Réponse active
Ernettre un rapport Générer une alarme Activer un archivage plus dét?jllé Activer un archivage à distance **Créer des fichiers** de sauvegarde	Bloquer le compte d'un utilisateur Suspendre des processus malveillants **Terminer une session** Bloquer une adresse **IP** Arrêter la **machine** **Déconnecter la machine** du réseau Mettre hors service les ports et les services attutuées Avertir l'utilisateur **TraCer l'origine de la connexion** **Forcer** une nouvelle authentification Restreindre le activités d'un utilisateur

Figure II.7 Tableau Réponses aux attaques des systèmes de détection d'intrusions **[9]**

11.6.3 Sources de données à analyser :

La source des données a analyser est une caractéristique essentiel des IDS et un critére important pour leur classification.

Les données proviennent : soit de fichier générer par le système d'exploitation et on parle alors d'IDS système (les HIDS :hot Intrusion detection Sytem) , soit de fichier générer par des application , soit encore l'information obtenus en écoutant le trafic sur le réseau et on parle alors d'IDS réseau (les NIDS :Network Intrusion Detection System)

11.6.4 NIDS (Network Based Intrusion Detection System) :[8]

L'IDS réseau ou Network based IDS (NIDS) surveille comme son nom l'indique le trafic réseau. Il se place sur un segment réseau et "écoute" le trafic. Ce trafic sera ensuite analysé afin de détecter les signatures d'attaques ou les différences avec le fonctionnement de référence. On notera une contrainte à ce système, en effet le cryptage du trafic sur les réseaux commutés rend de plus en plus difficile l‘ "écoute" et donc l'analyse du segment réseau à analyser, car le contenu

des paquets est crypté. De plus, un trafic en constante augmentation sur les réseaux contraint les NIDS à être de plus en plus performants pour analyser le trafic en temps réel. Enfin, avec sa ou ses cartes d'interface réseau en mode promiscuous (permet à celle-ci d'accepter tous les paquets qu'elle reçoit, même si ceux-ci ne lui sont pas adressés.), qui n'ont donc pas d'adresses IP, ni de pile de protocole attaché, il peut écouter tout le trafic qui arrive à l'interface en restant invisible.

- **Placement de la sonde sur le réseau**

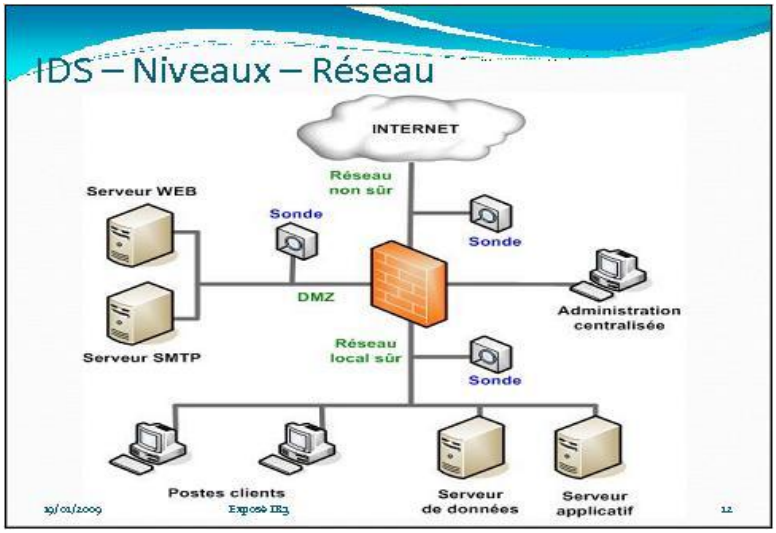


Figure II.8 Emplacement d'un Network IDS[11]

On peut placer les NIDS à différents endroits sur le réseau, mais bien sûr la politique de sécurité menée définira leur emplacement.

- On peut les mettre par exemple dans la zone démilitarisée ou DMZ afin de contrer les attaques contre les systèmes publics.
- On peut les mettre aussi derrière un firewall donnant accès à l'extérieur du réseau (Internet) afin de détecter des signes d'attaque parmi le trafic entrant/sortant du réseau.

Prendre l'option de mettre l'IDS derrière le firewall permet de réduire les paquets à analyser par celui-ci; le firewall bloque le plus "gros " du trafic et décongestionne par ce fait l'IDS et le travail de l'administrateur. Les logs se trouvent sinon trop "parasités" et rendent difficile la détection de vrai risque.

Derrière le firewall, il y a deux positions possible pour la sonde:

- En coupure

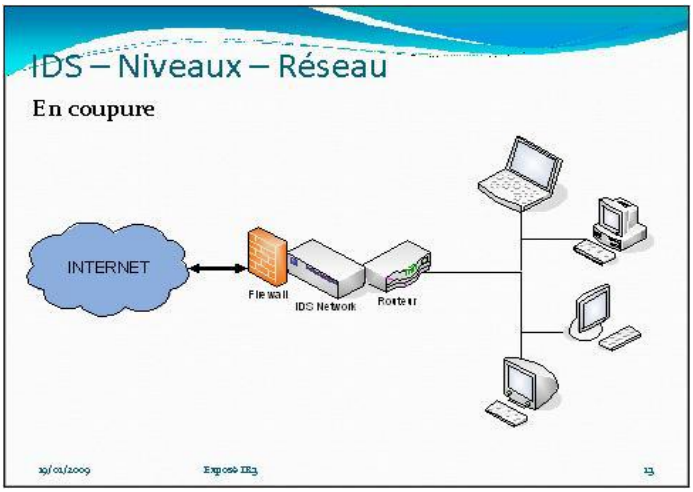


Figure II.9 Placement d'un IDS en coupure. [11]

Ici il a une faiblesse d'architecture, si la sonde tombe (par exemple à cause d'une attaque de dénis de service) c'est tout le réseau qui tombe.

- En recopie de port

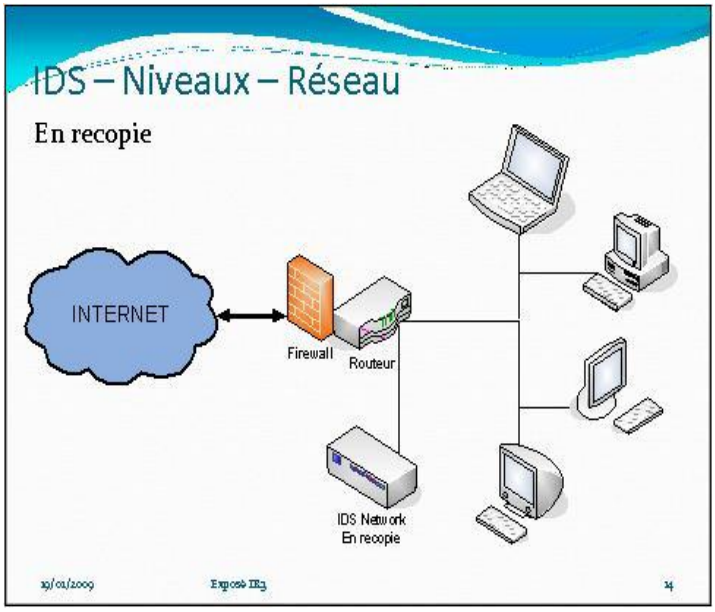


Figure II.10 Placement d'un IDS en recopie. [11]

Ici la sonde analyse aussi bien le réseau que en mode coupure sauf que si elle tombe due à une attaque cela ne pose aucun problème à l'architecture réseau. Et la sonde étant passive cette solution est la meilleure

11.6.5 HIDS (Host Based Intrusion Detection System)

L'IDS Systèmes ou Host Based IDS (HIDS) surveille le trafic sur une seule machine. Il analyse les journaux systèmes, les appels systèmes et enfin vérifie l'intégrité des systèmes de fichiers. Les HIDS sont de part leur principe de fonctionnement dépendant du système sur lequel ils sont installés. Ce système peut s'appuyer ou non sur le système propre au système d'exploitation pour en vérifier l'intégrité et générer des alertes. Il peut aussi capturer les paquets réseaux entrant/sortant de l'hôte pour y déceler des signaux d'intrusions (Déni de Services, Backdoors, chevaux de Troie, tentatives d'accès non autorisés, exécution de codes malicieux, attaques par débordement de buffers…). Il permet:

- Détection de compromission de fichiers (contrôle d'intégrité)
- Analyse de la base de registre (windows) ou des LKMs (Linux)
- Analyse et corrélation de logs en provenance de firewalls hétérogènes
- Analyse des flux cryptés (ce que ne peut réaliser un NIDS !)

L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent êtres levées.

Par nature, ces IDS sont limités et ne peuvent détecter les attaques provenant des couches réseaux.

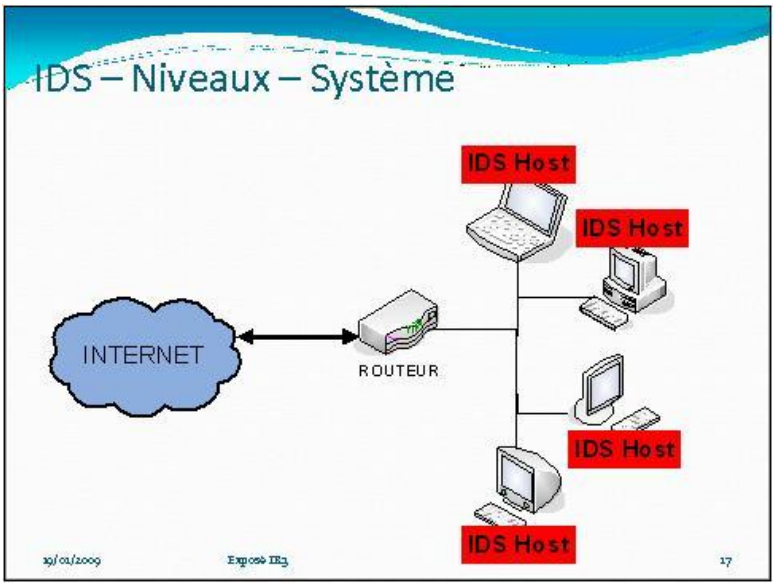


Figure II.11 Placement d'un HIDS. [11]

Récapitulatif

- Network based IDS (NIDS)
  - ✓ Positif:

    - N’affecte pas les performances du réseau
    - N’est pas visible

  - ✓ Négatif:

    - Faible devant les attaques de dénis de services
    - Un point unique de défaillance

- Host Based IDS (HIDS)
  - ✓ Positif:

    - Surveille les intrusions qui s'appliquent uniquement à l'hôte

  - ✓ Négatif:

    - Utilise la ressource du système
    - Besoin de HIDS spécifique pour des système spécifique

11.6.6 Détection d'Intrusion basée sur une application

Les IDS basés sur les applications sont un sous-groupe des IDS hôtes.
Ils contrôlent l'interaction entre un utilisateur et un programme en ajoutant des fichiers de log afin de fournir de plus amples informations sur les activités d’une application particulière. Puisque vous opérez entre un utilisateur et un programme, il est facile de filtrer tout comportement notable. Un ABIDS se situe au niveau de la communication entre un utilisateur et l’application surveillée.

L’avantage de cet IDS est qu’il lui est possible de détecter et d’empêcher des commandes particulières dont l'utilisateur pourrait se servir avec le programme et de

surveiller chaque transaction entre l'utilisateur et l'application. De plus, les données sont décodées dans un contexte connu, leur analyse est donc plus fine et précise.
Par contre, du fait que cet IDS n'agit pas au niveau du noyau, la sécurité assurée est plus faible, notamment en ce qui concerne les attaques de type "Cheval de Troie". De plus, les fichiers de log générés par ce type d'IDS sont des cibles faciles pour les attaquants et ne sont pas aussi sûrs, par exemple, que les traces d'audit du système.
Ce type d'IDS est utile pour surveiller l'activité d'une application très sensible, mais son utilisation s'effectue en général en association avec un HIDS. Il faudra dans ce cas contrôler le taux d'utilisation CPU des IDS afin de ne pas compromettre les performances de la machine.

Voici un exemple de mise en place d'un IDS RealSecure avec des IDS hôtes et réseaux connectés à une console de management centrale (sur le schéma, les HIDS sont appelés RealSecure Server Sensor et les NIDS RealSecure Network Sensor).

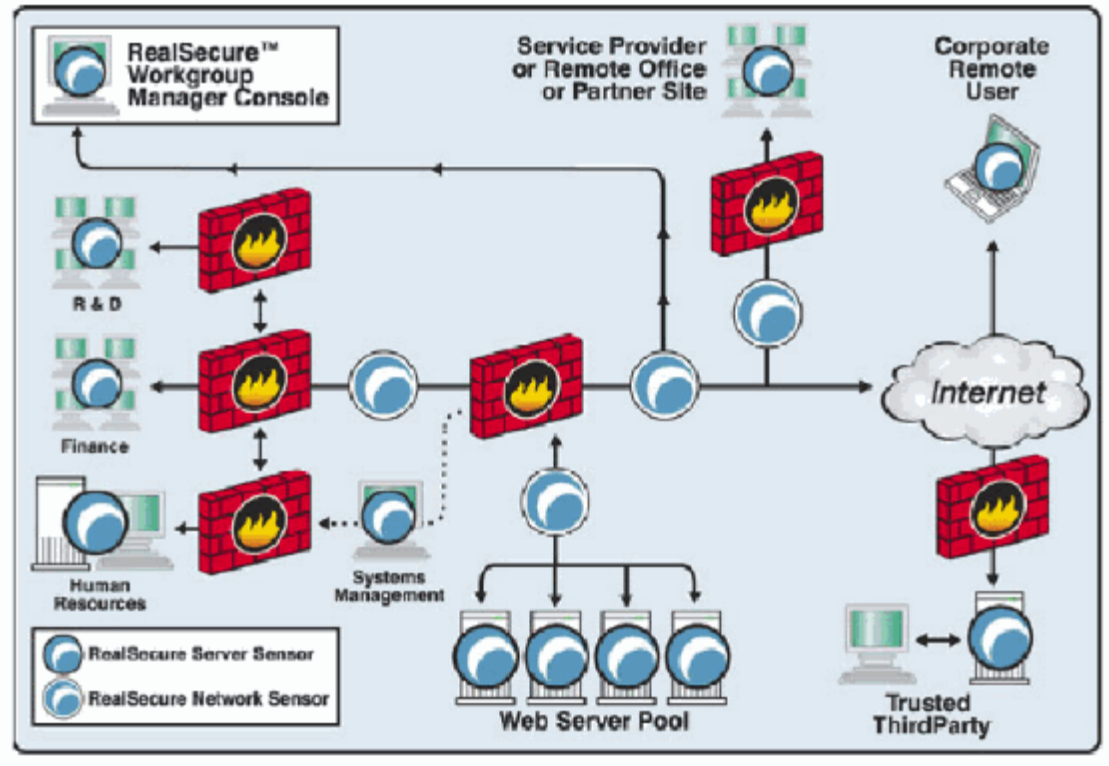


Figure II.12 Placement d'un IDS en coupure. Exemple d'architecture HIDS/NIDS

11.6.7 IDS hydrides *(NIDS+HIDS) :*

Les IDS hybrides rassemblent les caractéristiques de plusieurs IDS différents. En pratique, on ne retrouve que la combinaison de NIDS et HIDS. Ils permettent, en un seul outil, de surveiller le réseaux et les terminaux. Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces sondes remontent alors les alertes à une machine qui va centraliser le tout, et agréger/lier les informations d'origines multiples.

11.6.8 Paradigme de détection [22]

Un IDS, peut tenter d'identifier des attaques en s'appuyant sur : des informations relatives aux transitions ayant lieu dans le système (l'exécution de certains programmes, de certaines séquences d'instructions, l'arrivée de certains paquets réseau, etc.) ou bien en étudiant l'état de certaines parties du système (par exemple, l'intégrité des programmes stockés, les privilèges des utilisateurs, etc.). Durant ces deux types d'inspection, l'IDS récupère les informations en interrogeant directement le système ou en écoutant passivement les événements.

11.6.9. Mode de supervision

Une autre caractéristique des systèmes de détection d'intrusions, c'est leur fréquence d'utilisation :

- ***Périodique :*** certains systèmes de détection d'intrusions, analysent périodiquement les fichiers d'audit à la recherche d'une éventuelle intrusion ou anomalie passée. Cela peut être suffisant dans des contextes peu sensibles, par exemple du fait qu'un ***HIDS*** analyse des fichiers traces transmis seulement toutes les heures.

- ***Continue :*** la plupart des systèmes de détection d'intrusions récents, effectuent leur analyse des fichiers d'audit ou des paquets réseau de manière continue, afin de proposer une détection en quasi temps réel. Cela est nécessaire dans des contextes sensibles (confidentialité). C'est toutefois coûteux en temps de calcul car il faut analyser à la volée tout ce qui se passe sur le système.

11.7. Méthodes de classification et d'IA pour la détection d'intrusions

Plusieurs algorithmes de classification et d'IA, peuvent être utiles dans la détection d'intrusions. Ces algorithmes génèrent des classificateurs, sous forme d'arbre de décision, de règles ou de réseau de neurones, etc. Une application dans la détection d'intrusions serait d'appliquer ces algorithmes à une quantité suffisante de données d'audit normales ou anormales, pour générer un classificateur capable d'étiqueter comme appartenant à la catégorie normale ou anormale de nouvelles données d'audit. Parmi ces techniques de classification, nous citons :

11.7.1. Réseaux bayésiens naïfs

La méthode de classification Bayésienne applique un modèle probabiliste pour l'apprentissage. Ce type de classification utilise des modèles graphiques largement utilisés pour représenter et traiter l'information incertaine. Il représente une forme très simple des réseaux Bayesiens. Le nœud racine représente le nœud non observée, et les noeuds feuilles correspondent aux attributs observes, avec l'hypothèse forte de l'indépendance entre les noeuds fils (feuille) dans le cadre de leur parent (figure 5.3).

Figure II .12: Réseau Bayésien naïf.[9]

11.7.3. Réseaux de neurones

Les réseaux de neurones formels sont à l'origine une tentative de modélisation mathématique du cerveau humain. Les premiers travaux datent de 1943 et sont l'oeuvre de MM. *Mac Culloch et Pitts*. Ils présentent un modèle assez simple pour les neurones et explorent les possibilités de ce modèle.

L'idée principale des réseaux de neurones "modernes" est la suivante :

On se donne une unité simple, un neurone, qui est capable de réaliser quelques calculs élémentaires. On relie ensuite entre elles un nombre important de ces unités et on essaye de déterminer la puissance de calcul du réseau ainsi obtenu. Il est important de noter que ces neurones manipulent des données numériques et non pas symboliques.

11.8. Les systèmes de détection d'intrusions actuels [6]

Le premier système de détection d'intrusions a été proposé en 1980 par *James ANDERSON*. Il en existe maintenant beaucoup d'autres, commerciaux ou non. La majorité de ses systèmes se basent sur les deux approches, comportementale et par scénarios.

Stefan AXELSSON donne un modèle d'architecture de base pour un système de détection d'intrusions : un module s'occupe de la collecte d'informations d'audit, ces données étant stockées quelque part, un module de traitement des données qui interagit avec ces données de l'audit et les données en cours de traitement, ainsi qu'avec les données de référence (signatures, profils) et de configuration entrées par l'administrateur du système de sécurité. En cas de détection, le module de traitement remonte une alarme vers l'administrateur du système de sécurité ou vers un module. Une réponse sera ensuite apportée sur le système surveillé par l'entité alertée. Les imperfections de ce type de systèmes monolithiques et même des systèmes de détection d'intrusions en général sont à prendre en compte. *stefano MARTINO* souligne que si un certain nombre de techniques ont été développées jusque là, pour les systèmes de détection d'intrusions, la plupart analysent des évènements au niveau local et se contentent de remonter une alarme sans agir. Ils détectent de plus, les activités dangereuses d'un utilisateur sans se préoccuper du code dangereux.

11.9. Imperfection des systèmes de détections d'intrusions

Les systèmes de détections d'intrusions de nos jours présentent quelques imperfections, dans la plupart des cas, ces systèmes sont faits d'un seul bloc ou module qui se charge de toute

l'analyse. Ces systèmes monolithiques exigent beaucoup de données d'audit, de ce fait ils utilisent beaucoup de ressources de la machine surveillée. L'aspect monolithique pose également des problèmes de mise à jour et constitue un point d'attaque unique pour ceux qui veulent s'introduire dans le système d'informations. D'autres imperfections plus générales sont relevables dans les systèmes de détection d'intrusions actuels :

- Même en implémentant les deux types d'approches, certaines attaques sont indécelables et les systèmes de détection sont eux-mêmes attaquables. Les approches comportementale et par scénarios ont elle-même leurs limites.
- Les groupes de travail sur ce sujet sont relativement fermés et il n'y a pas de méthodologie générique de construction. Aucun standard n'a pour l'instant vu le jour dans ce domaine. Des groupes y travaillent, notamment au sein de la DARPA et de l'IETF.
- Les mises à jour de profils, de signatures d'attaques ou de façon de spécifier des règles sont généralement difficiles. De plus, les systèmes de détection d'intrusions demandent de plus en plus de compétence à celui qui administre le système de sécurité.
- Les systèmes de détection, sont généralement écrits pour un seul environnement et ne s'adapte pas au système surveillé, alors que les systèmes d'informations sont la plupart du temps, hétérogènes et utilisés de plusieurs façons différentes.
- Aucune donnée n'a été pour l'instant publiée, pour quantifier la performance d'un système de détection d'intrusions. De plus, pour tester ces systèmes, les attaques sont de plus en plus difficiles à simuler.

Concclusion :

Le principe de rendre compte après coup d’une intrusion, a vite évolué pour chercher des IDS capables de réagir en temps réel. Le constat des dégâts ne suffisait plus : il fallait réagir et pouvoir bloquer les trafics douteux détectés. Ces techniques de réponse impliquèrent les IDS.

Chapitre III
Base KDD, Classification, Algorithme K-means

Introduction :

A fin de réaliser un IDS par scénario basé signature nous allons introduire dans ce chapitre les notions BASE KDD, Classification et Algorithme K-mans que on utilisera lors de la réalisation

III.1 Description de la base KDD :

La base KDD est représenter sous un format texte ou chaque ligne représente une connexion qui caractériser avec ces 41 attribue (type de connexion, durée de la connexion, protocole utiliser…etc.) et chaque ligne représente comme normal ou une attaque. Ces données sont fournies par la DARPA.

III.1.1 Attaques de la base KDD :

La base KDD recense 38 attaques possibles qui peuvent être regroupé en quatre catégories.

- **Denial-Of-Service(DOS) :**

Ce type d'attaque est très simple à mettre en œuvrer, le but de cette attaque est très simple, c'est de compromettre le fonctionnement et la disponibilité des ressources d'une organisation en temps normal.

- **Attaque de type User to Root Attaks(U2R) :**

L'attaquant essaye d'avoir les droits d'accès afin d'accéder au système.

- **Reconnaissance-Probing :**

Généralement c'est la première étape des attaques, elle consiste à rassembler des informations sur la cible pour bien organiser son attaque.

- **Attaque de type Remote to User**

L'attaquant essaye d'exploiter les vulnérabilités de le la cible afin d'avoir un accès distant a la machine.

DOS	Probing	R2L	U2R
Apache2	Ipsweep	Ftp_write	Buffer_overflow
Back	Mscan	Guess_passwd	Httptunnel
Land	Nmap	Imap	Loadmodule
Mailbomb	Portsweep	Multihop	Xterm
Neptune	Saint	Named	Perl
Pod	Satan	Phf	Ps
Processtable		Dict	Rootkit
Smurf		Snmpguess	
Teardrop		Spy	
Udpstorm		Sqlattack	
		Warezclient	
		Warezmaster	
		Xlock	
		Xsnoop	
		Guest	

Figure-III.1 : Type d'attaque[9]

III.1.2 La KDD contient deux types de bases de connexions : [5]

- **Base d'apprentissage KDD**
  - Enregistrement :
  - 41 attributs + nom de classe pour apprendre
  - Fichiers au format texte
  - ~5 millions de connexions (10% (494000) utilisées)
  - -4 classes d'attaques + trafic normal

- Probing : scan de port (nmap, satan …)

-DoS : déni de Service (syn flooding, smurf …)

- U2R : acquisition des privilèges d'un super utilisateur (buffer overflow)

-R2L : accès illégitime à partir d'une machine distante(password guessing)

-Normal : trafic légitime

- **Base de test KDD**

  - Enregistrement :
  - 41 attributs + nom de classe pour vérifier
  - ~ 311000 connexions
  - 4 classes d'attaques enrichies + trafic normal
  - Probing : scan de port (mscan, saint)
  - -DoS : déni de Service (apache2, …)
  - -U2R : acquisition des privilèges d'un super utilisateur (sqlattack…)
  - R2L : accès illégitime à partir d'une machine distante (snmpguess, snmpgetattack…)
  - Normal : trafic légitime

III.1.3 Attributs:

Ils caractérisent chaque connexion d de la base KDD, qui est détaillé dans le tableau ci-dessous

	Attributs basiques
A1	durée de la connexion (nb de secondes)
A2	type du protocole, ex. tcp, udp, etc.
A3	service réseau (destination) ex. http, telnet
A4	statut de la connexion (normal ou erreur)
A5	nb de données (en octets) de la source vers la destination
A6	nb de données (en octets) de la destination vers la source
A7	1 si la connexion est de/vers le même hôte/port; 0 autrement
A8	nb de fragements "erronnés"
A9	nb de paquets urgents
	Attributs relatifs au contenu
A10	nb d'indicateurs "hot"
A11	nb d'essais login ratés
A12	1 si succès du login ; 0 autrement
A13	nb de conditions de "compromis"
A14	1 si la racine shell est obtenu; 0 autrement
A15	1 si la commande on a la commande "racine su" ; 0 autrement
A16	nb d'accès à la "racine"
A17	nb de créations d'opérations de fichiers
A18	nb de shell prompts
A19	nb d'opérations sur les fichiers de contrôle d'accès
A20	nb de commandes outbound dans une session ftp
A21	1 si le login appartient à la liste "hot" ; 0 autrement
A22	1 si le login est login "invité" ; 0 autrement
	Attributs basés sur le temps utilisant des fenêtres de temps de deux secondes
A23	nb de connex. pour le *même hôte*
A24	nb de connex. pour le *même service*
A25	% de connex. pour le *même hôte* ayant l'erreur "SYN"
A26	% de connex. pour le *même service* ayant l'erreur "SYN"
A27	% de connex. pour le *même hôte* ayant l'erreur "REJ"
A28	% de connex. pour le *même service* ayant l'erreur "REJ"
A29	% de connex. pour le *même hôte* utilisant le *même service*
A30	% de connex. pour le *même hôte* utilisant *différents services*
A31	% de connex. pour le *même service* utilisant *différents hosts*
	Attributs basés sur le temps utilisant des fenêtres de temps de 100 connex.
A32	nb de connex. pour le *même hôte*
A33	nb de connex. pour le *même hôte* utilisant le *même service*
A34	% de connex. pour le *même hôte* utilisant le *même service*
A35	% de connex. pour le *même hôte* utilisant *différents services*
A36	% de connex. pour le *même hôte* ayant le port src
A37	% de connex. pour le *même hôte* et le *même service* utilisant *différents hosts*
A38	% de connex. pour le *même hôte* ayant l'erreur "SYN"
A39	% de connex. pour le *même hôte* et le *même service* ayant l'erreur "SYN"
A40	% de connex. pour le *même hôte* ayant l'erreur "REJ"
A41	% de connex. pour le *même hôte* et le *même service* ayant l'erreur "REJ"

Tableau III.2 : Liste des attributs **[9]**

III.2.1 **Classification :**

La classification c'est construire une collection d'objets Similaires au sein d'un même groupe et dissimilaires quand ils appartiennent à des groupes différents. Les algorithmes de classification non supervisées sont souvent utilisés pour étudier des données pour lesquelles peu d'information sont disponible.

III.2.1.$_1$ **Classification supervisée :**

C'est l'ensemble des techniques qui visent à deviner l'appartenance d'un individu à une classe en s'aidant uniquement des valeurs qu'il prend. Elle construire un modèle représentatif d'un certain nombre de données organisées en classes (ensemble) que l'on appelle généralement le corpus d'apprentissage - puis d'utiliser ce modèle afin de classer de nouvelles données, c'est à dire de prédire leur classe au vu de leurs caractéristiques (appelées paramètres ou features). La construction du modèle relève de l'apprentissage automatique supervisé, l'ensemble des exemples constituant le corpus d'apprentissage étant annotés, c'est à dire qu'ils portent le label de leur classe donné a priori.

La plupart des algorithmes d'apprentissage supervisés tentent de trouver un **modèle** (une fonction mathématique) qui explique le lien entre des données d'entrée et les classes de sortie. Ces jeux d'exemples sont donc utilisés par l'algorithme.

I existe de nombreuses méthodes d'apprentissage supervisé :

- Méthode des k plus proches voisins**.**
- Réseau de neurones**.**
- Arbre de décision**.**
- Classification naïve bayesienne**.**

La méthode directe de la classification supervisée k plus proches voisins.

III.2.1.2 K plus proches voisins (k-ppv) :

La méthode des plus proches voisins (noté parfois k-PPV ou k-NN pour (k-Nearest-Neighbor) consiste à déterminer pour chaque nouvel individu que l'on veut classer, la liste des plus proches voisins parmi les individus déjà classés. L'individu est affecté à la classe qui contient le plus d'individus parmi ces plus proches voisins. Cette méthode nécessite de choisir une distance, la plus classique est la distance euclidienne et le nombre de voisins à prendre en compte.

Cette méthode supervisée est souvent performante, cependant, le temps de prédiction est très long, car il nécessite le calcul de la distance avec tous les exemples, mais il existe des heuristiques pour réduire le nombre d'exemples à prendre en compte.

III.2.1.3 Affectation par la méthode bayésienne :

Un classificateur probabiliste linéaire simple basée sur le théorème de Bayes qui suppose que les descripteurs (attributs) qui décrivent les objets de l'ensemble d'apprentissage sont indépendants.

L'approche bayésienne a pour but de minimiser la probabilité d'erreur de classification, C'est-à-dire la probabilité jointe qu'une observation x soit en provenance d'une classe Ci et soit classée dans une autre.

III.2.1.4 Analyse discriminante :

Les méthodes d'analyse discriminante ont été largement étudiées; la littérature à ce sujet est très abondante.

Le but de ces méthodes est de produire des décisions concernant l'appartenance ou non d'un objet à une classe en utilisant des fonctions discriminantes appelées également *fonctions de décisions.* Suivant les formes des classes, on peut trouver différents types de discrimination: discrimination linéaire et discrimination quadratique.

III.2.1.5 Les réseaux de neurones :

Les réseaux de neurones sont à l'origine d'une tentative de modélisation mathématique du cerveau humain.

Le principe général des méthodes utilisant les réseaux de neurones consiste à modifier (ou ajuster) les paramètres comme, par exemple, le s poids et les seuils par des algorithmes itératifs afin d'obtenir des réponses correctes.

III.2.1.6 Arbre de décision :

Un arbre de décision est une structure simple récursive permettant d'exprimer un processus de classification séquentiel au cours duquel une correspondance est établie entre un objet décrit par un ensemble de caractéristiques (attributs), et un ensemble de classes disjointes. Chaque feuille de l'arbre dénote une classe et chaque nœud intérieur un test portant sur un ou plusieurs attributs, produisant un sous-arbre de décision pour chaque résultat possible

du test.

III.2.2 **Classification non supervisée :**

III.2.2.$_1$**Définition :**

L'objectif de ces méthodes est de regrouper les individus en un nombre restreint de classes homogènes sans connaissances à priori.

L'apprentissage non supervisé consiste à inférer des connaissances sur des classes sur la seule base des échantillons d'apprentissage, et sans savoir *a priori* à quelles classes ils appartiennent.

On distingue aussi les approches de classification non hiérarchiques et les méthodes de classification hiérarchiques.

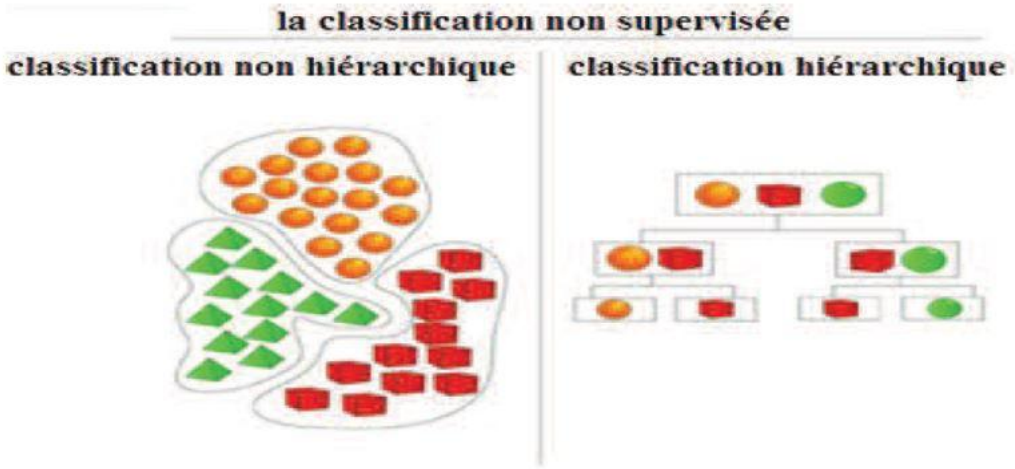


Figure I-1 : les deux types de clustering hiérarchique/non hiérarchique.**[8]**

III.2.1.2 Méthodes non hiérarchiques :

C'est une méthode très répondues est très connue parmi les Algorithme qui repose sur cette méthode on trouve el K-Means, le principe de fonctionnement de cette méthode est très simple elle **consiste à** Regrouper n individus en k classes de telle sorte que les individus d'une même classe soient le plus semblables possible et que les classes soient bien séparées

III.3.1Définition :

L'algorithme k-means mis au point par McQueen en 1967, un des plus simples Algorithmes d'apprentissage non supervisé, appelée algorithme des centres mobiles , il attribue chaque point dans un cluster dont le centre (centroïde) est le plus Proche. Le centre est la moyenne de tous les points dans le cluster, ses coordonnées Sont la moyenne arithmétique pour chaque dimension séparément de tous les Points Dans le cluster c'est à dire chaque cluster est représentée par son centre de gravité.

III.3.2 Exemples d'applications :

· **Marketing:** segmentation du marché en découvrant des groupes de clients Distincts à partir de bases de données d'achats.

· **Environnement:** identification des zones terrestres similaires (en termes D'utilisation) dans une base de données d'observation de la terre.

· **Assurance:** identification de groupes d'assurés distincts associés à un nombre Important de déclarations.

· **Planification de villes:** identification de groupes d'habitations suivant le type d'habitation, valeur, localisation geographiques, ….

III.3.3 L'algorithme des centres mobiles :

L'objectif de la méthode est de partitionner en différentes classes des individus pour lesquels on dispose de mesures. On représente les individus comme des points de l'espace ayant pour coordonnes ces mesures. On cherche à regrouper autant que possible les individus les plus semblables (du point de vue des mesures que l'on possède) tout en séparant les classes le mieux possible les unes des autres. Ici encore (comme dans le cas de la classification hiérarchique ascendante) on choisit de procéder de /ac.n automatique, c'est-à-dire qu'on ne cherche pas à utiliser l'expertise que l'on aurait des individus pour trouver des regroupements avec ce que l'on connait les concernant mais plutôt un moyen de /aire apparaître, uniquement à partir des mesures, des ressemblances et des différences a priori peu visibles. Cette idée, travailler automatiquement, à l'aide de l'ordinateur et en aveugle, est appelée apprentissage non supervise.

La méthode des centres mobiles s'applique lorsque l'on sait à l'avance combien de classes on veut obtenir. Appelons k ce nombre de classes. L'algorithme est le suivant :

Etape 0 : Pour initialiser l'algorithme, on tire au hasard k individus appartenant à la population, C^0_1, C^0_2, ..., C^0_k : ce sont les k centres initiaux. On notera que l'indice numérote les différents centres et l'exposant indique qu'il s'agit des k centres initiaux. On choisit aussi une distance entre individus.

On va ensuite répéter un grand nombre de fois les deux étapes suivantes :

Etape 1 : Constitution de classes : On repartit l'ensemble des individus en k classes Γ^0_1, Γ^0_2 ..., Γ^0_k en regroupant autour de chaque centre C^0_i pour i = 1..., n l'ensemble des individus qui sont plus proches du centre C^0_ique des autres centres C^0_j pour $j \neq i$ (au sens de la distance choisie).

Etape 2 : Calcul des nouveaux centres : On détermine les centres de gravite G_1, G_2, ..., G_k des k classes ainsi obtenues et on désigne ces points comme les nouveaux centres $C^1_1 = G_1$, $C^1_2 = G_2$ ...., $C^1_k = G_k$

Répétition des étapes 1 et 2 : on répète ces deux étapes jusqu'à la stabilisation de l'algorithme, c'est- à-dire jusqu'à ce que le découpage en classes obtenu ne soit (presque) plus modifie par une itération supplémentaire.

Le schéma ci-dessous illustre la méthode (à noter qu'en pratique, bien sûr, on ne fait pas ces calculs "à la main" mais à l'aide d'un logiciel d'analyse de données). Dans cette figure la distance choisie est la distance euclidienne : en effet, pour repartir les points du nuage en deux groupes, ceux qui sont les plus proches d'un point C^0_1 et ceux qui sont les plus proches d'un autre point C^0_2 au sens de la distance euclidienne, il suffit de tracer la médiatrice du segment [C^0_1, C^0_2].

Mais est-on sûr que cet algorithme conduit bien à une partition meilleure que celle dont on est parti, c'est-à-dire celle qui était issue du tirage aratoire initial de k centres ? Pour répondre à cette question, il faudrait préciser ce que l'on entend par meilleure. Nous allons pour cela introduire la notion d'inertie d'un nuage de points.

Algorithme K-means

Donnée : k le nombre maximum de classe désiré.

Début

(1) Choisir k individus au hasard (comme centre des classes initiales)

(2) Affecter chaque individu au centre le plus proche

(3) Recalculer le centre de chacune de ces classes

(4) Répéter l'étape (2) et (3) jusqu'à stabilité des centres

(5) Editer la partition obtenue

Fin

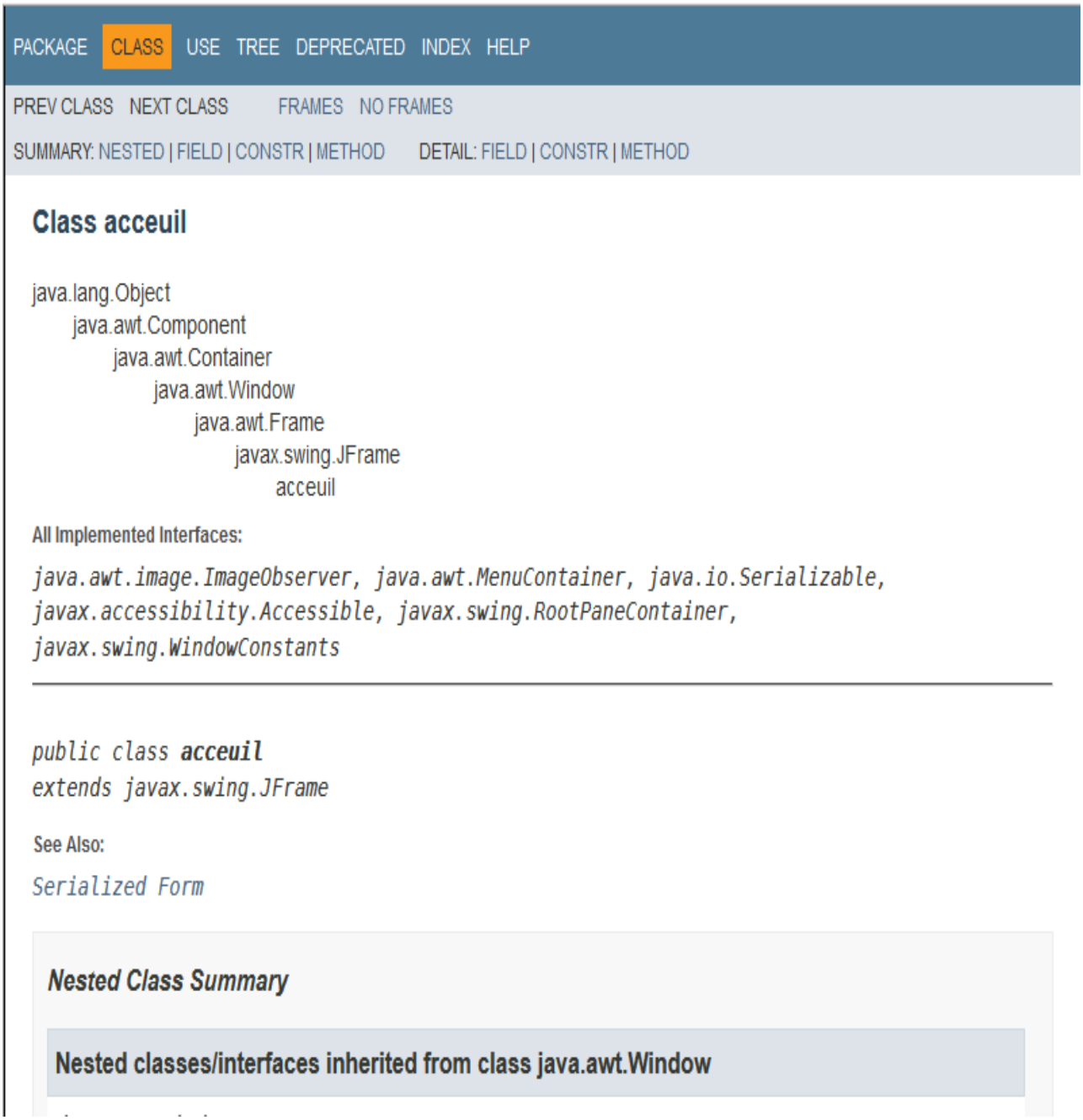
Conclusion

Les risques d'intrusion sont une réalité et cela n'arrive pas qu'aux autres. Il faut donc songer à sécuriser son réseau à l'aide d'outils de détection des intrusions et de prévention des intrusions.

Les IDS sont des systèmes de détection d'intrusion qui, avec la bonne configuration, peut être utilisé comme système de prévention des intrusions. Cette solution a prouvé son efficacité et ne cesse d'évoluer afin de déjouer les nouveaux types d'attaques.

Réalisation

III. Réalisation :



PACKAGE CLASS USE TREE DEPRECATED INDEX HELP

PREV CLASS NEXT CLASS FRAMES NO FRAMES

SUMMARY: NESTED | FIELD | CONSTR | METHOD DETAIL: FIELD | CONSTR | METHOD

Class acceuil

java.lang.Object
  java.awt.Component
    java.awt.Container
      java.awt.Window
        java.awt.Frame
          javax.swing.JFrame
            acceuil

All Implemented Interfaces:

java.awt.image.ImageObserver, java.awt.MenuContainer, java.io.Serializable, javax.accessibility.Accessible, javax.swing.RootPaneContainer, javax.swing.WindowConstants

---

public class ***acceuil***
extends javax.swing.JFrame

See Also:

Serialized Form

Nested Class Summary

Nested classes/interfaces inherited from class java.awt.Window

Field Summary

Fields

Modifier and Type	Field and Description
`float[][]`	`tab_cente_gravité`
`float[][]`	`tab_conn`
`float[][]`	`tab_conn_2`

Fields inherited from class javax.swing.JFrame

`EXIT_ON_CLOSE`

Fields inherited from class java.awt.Frame

`CROSSHAIR_CURSOR, DEFAULT_CURSOR, E_RESIZE_CURSOR, HAND_CURSOR, ICONIFIED, MAXIMIZED_BOTH, MAXIMIZED_HORIZ, MAXIMIZED_VERT, MOVE_CURSOR, N_RESIZE_CURSOR, NE_RESIZE_CURSOR, NORMAL, NW_RESIZE_CURSOR, S_RESIZE_CURSOR, SE_RESIZE_CURSOR, SW_RESIZE_CURSOR, TEXT_CURSOR, W_RESIZE_CURSOR, WAIT_CURSOR`

Fields inherited from class java.awt.Component

`BOTTOM_ALIGNMENT, CENTER_ALIGNMENT, LEFT_ALIGNMENT, RIGHT_ALIGNMENT, TOP_ALIGNMENT`

Fields inherited from interface javax.swing.WindowConstants

`DISPOSE_ON_CLOSE, DO_NOTHING_ON_CLOSE, HIDE_ON_CLOSE`

Fields inherited from interface java.awt.image.ImageObserver

`ABORT, ALLBITS, ERROR, FRAMEBITS, HEIGHT, PROPERTIES, SOMEBITS, WIDTH`

Constructor Summary

Constructors

Constructor and Description
`acceuil()`

Method Summary

All Methods | **Static Methods** | **Instance Methods** | **Concrete Methods**

Modifier and Type	Method and Description
`void`	`affich_tab_centre()` methode utiliser pour afficher le tableay de connection
`void`	`affich_tab_conn()` cette methode eest utiliser pour afficher le tableaux qui contien les valeur extraite une fois extraite et stockée dans un tableaux.
`void`	`ajout_ligne_tab(int num_ligne, java.lang.String lig)` cette pethode prend en entré le num-ligne et un String du quelle on vas extraire les valeur float contenue dans cette ligne et le stoquée en suite dans un tableau a la laigne avec l'index num_ligne.

float	***distance_conn_classe**(int ligne_conn, int num_classe)* La methode a pour but de calculer la distance entre une connection est une classe en utilisant la methode de la distance euclidienne.
java.lang.String	***extr_ele**(java.lang.String ss, int i)* cette mecthode a pour but d'extraire les valeur d'un String en utilisant l'index des vergules qui separe c'es variable en suite untiliser la methode "substring" de la classe String pour extraire ce qui est contenue entre ces vergules et avancée en suite jusqu'a extraire toutes les valeur de cette ligne.
void	***init_classe_dis_conn2**()* Utiliser pour calculer la distance entre la classe a tester et l'ensemble des classe pour trouver la classe la plus proche
void	***init_tab_centre_gravité**()* cette pethode est utiliser pour affectué pour chaque connection une classe a fin de inatialiser les calcule
java.lang.Boolean	***ligne_normal**(java.lang.String ss)* cette methodea pour but de determiner lla fin d'une ligne de la base KDD si elle setermine avec la chaine de caractère "normal" donc c'est une connection normal autrement c'est une attaque.
static void	***main**(java.lang.String[] args)*
java.lang.String	***modif_ele**(java.lang.String ele)* Si on extrait une valeur qui n'est pas float comme par exemple le type de la connection 'tcp, udp, icmp...etc' dans ce cas on leur effectue des valeur fixe pour chaque type de connection par exemple: if ((ele.equals("tcp")) || (ele.equals("icmp")) || (ele.equals("udp"))...etc ele = "1.00";

boolean	***reclasser_conn_i_2**(int num_ligne_conn)* calculede la classe pla plus proche de la connection a analyser
boolean	***reclasser_conn_i**(int num_ligne_conn)* cette methode a pour but de prendre une connection et luis changer de classe de puis une classe sourche vers la classe destinaltion et calculer en suite les nouveau centre de graviter de ces deux classe
void	***reclasser_conn**()* la methode fait appel a une aune autre methode qui reclasse une connection et lui change de classe vers une classe plus proche. elle parours toute les connection en fesant appel a cette methode.
int	***recup_nbr_ligne_normal**(java.io.File fichier)* avec cette péthode on peut recuperer le nobre de ligne " connection" normale de notre ficher a fin de donnée une demention a norte tableau qui contiendre en suite les valeur contenue dans ce fichier texte pour en suite effectué le traitement.

Methods inherited from class javax.swing.JFrame

getAccessibleContext, getContentPane, getDefaultCloseOperation, getGlassPane, getGraphics, getJMenuBar, getLayeredPane, getRootPane, getTransferHandler, isDefaultLookAndFeelDecorated, remove, repaint, setContentPane, setDefaultCloseOperation, setDefaultLookAndFeelDecorated, setGlassPane, setIconImage, setJMenuBar, setLayeredPane, setLayout, setTransferHandler, update

Figure IV.1 Documentation de l'application en se basant sur la méthode API java

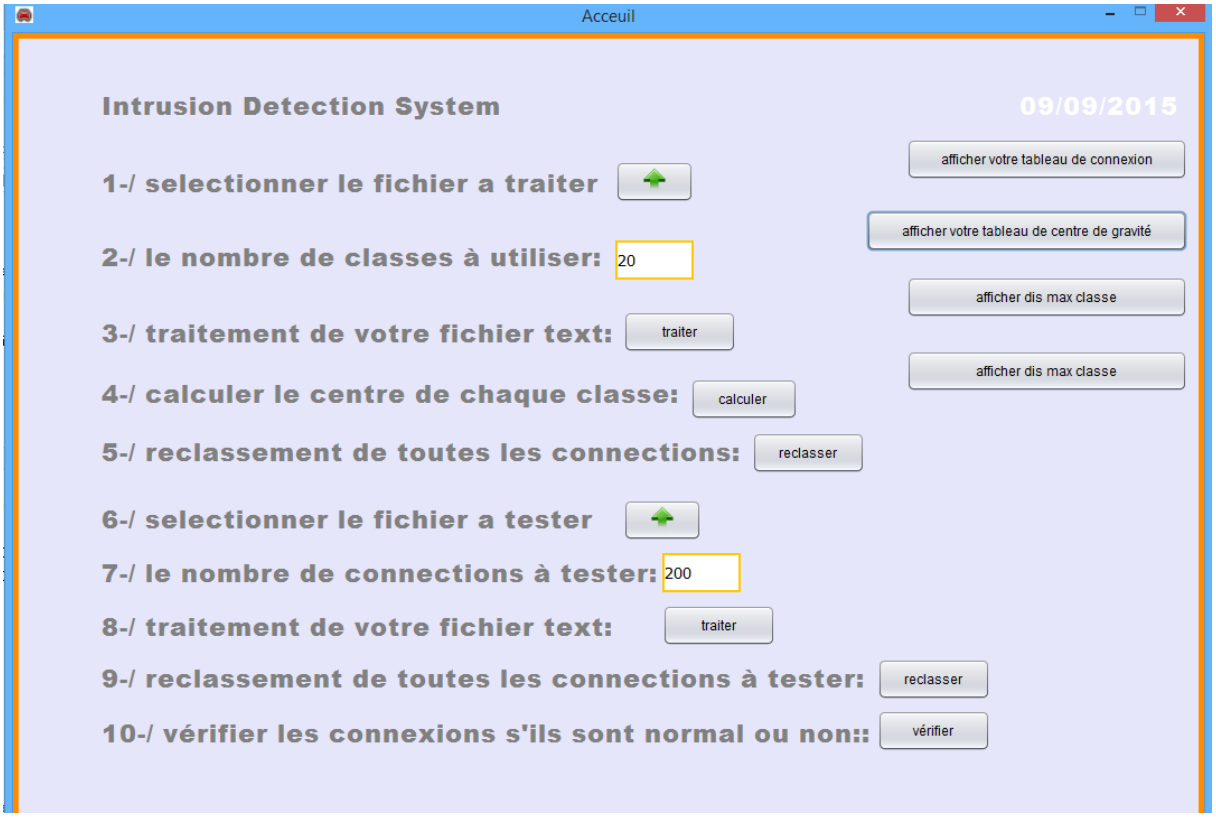


Figure IV.2 Interface d'accueille de l'application

1- Charger la base KDDD
2- Initialiser le nombre de classe pour l'algorithme K-means
3- Charger la Base KDD dans un tableau
4- Calcul du centre de gravité de chaque classe
5- Reclassement des connexions jusqu'à la stabilité de K-means

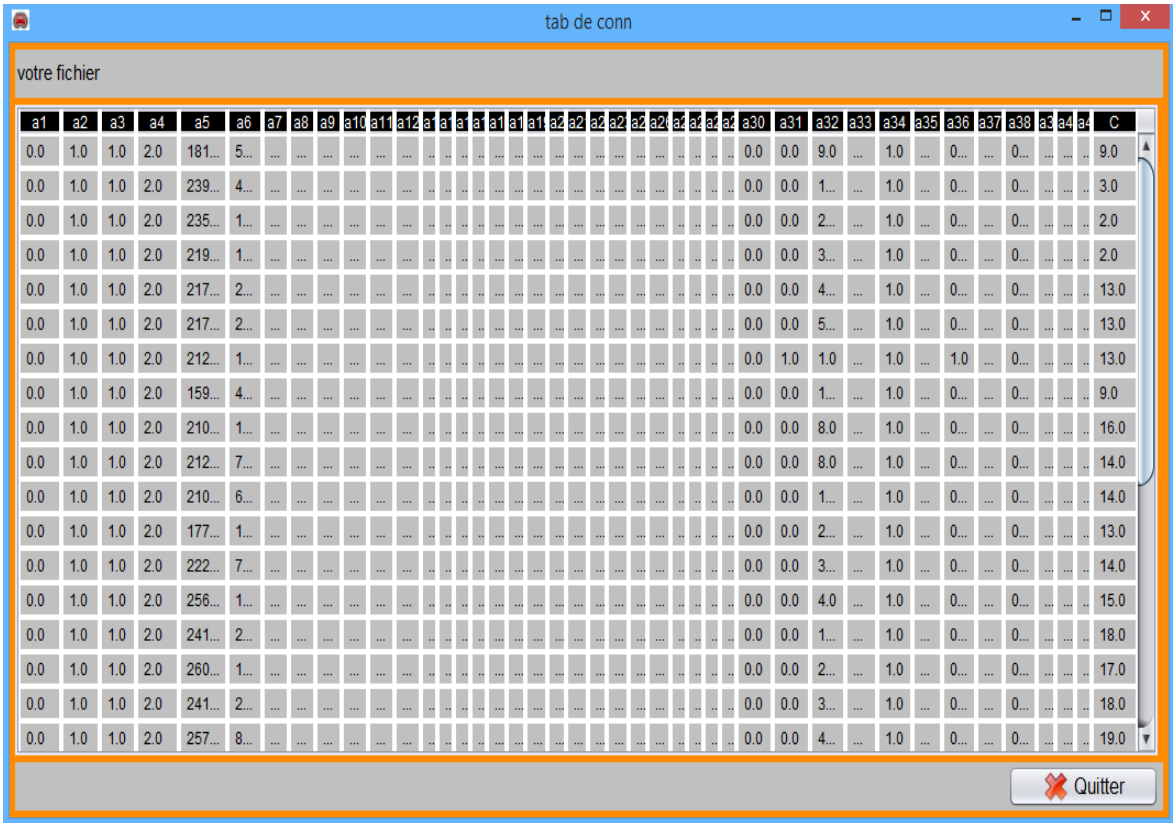


Figure IV.3 Tableaux qui contient les valeurs extraite du fichier texte

Le tableau contient l'ensemble des connexion avec la dernière colonne qui représente la classe a qui elle appartient.

votre tableau de centre de classe:

a1	a2	a3	a4	a5	a6	a7	a8	a9	a10	a11	a12	a13	a14	a15	a16	a17	a18	a19	a20	a21	a22	a23	a24	a25	a26	a27	a28	a29	a30	a31	a32	a33	a34	a35	a36	a37	a38	a39	a40	a41	nbr_ap	C
0.0	4.182...	0...	0...	0...	0...	8...	..	..	..	6...	4...	..	0...	0...	4...	0...	0...	0...	0...	0...	3...	0...	0...	0...	0...	7...	0...	6...	0....	6....	..	..	..	..	..	...	...	0...	0.198...	2....	1472.0	1.0
0.00112...	0.003...	0...	0...	1...	1...	0...	..	..	..	0.0	0...	..	0...	1...	0...	0...	0...	0...	0...	0...	0...	0...	0...	0...	4...	0...	3...	0...	3....	5....	..	..	..	..	..	...	...	0...	0.0	0.0	892.0	2.0
0.0	0.011...	0...	0...	0.0	0.0	0.0	..	..	..	0...	0...	..	9...	0...	0...	0...	0.0	0...	0.0	0...	0...	0...	0...	0...	5...	0...	0...	2...	8...	0.0	0....	..	..	..	..	..	...	...	0...	0.0	0.0	1113.0	3.0
0.02027...	0.023...	0...	5...	0...	0...	0...	..	..	..	0...	0...	..	0...	0...	0...	0...	0.0	0...	0...	0...	0...	0...	0...	1...	0...	5...	7...	1...	7...	0....	0....	..	..	..	..	..	...	...	0.0	0.002...	0....	1382.0	4.0
0.06972...	0.008...	9...	0.0	0.0	0...	9...	..	..	..	0...	9...	..	0...	0...	9...	0...	0.0	0...	0...	0...	0...	1...	2...	0...	9...	7...	2...	0.0	0...	9....	0.0	..	..	..	..	..	...	...	0.0	0.085...	0....	1091.0	5.0
1.11061...	1.488...	0...	0...	0...	3...	0.0	..	..	..	0...	0...	..	0...	0...	0.0	0...	5...	0...	0...	0...	0...	8...	5...	0...	0...	0...	0...	0...	0...	0....	..	..	..	..	..	...	...	0...	0.466...	1....	1764.0	6.0
3.46895	0.0	0.0	2...	0.0	2...	0...	..	..	..	2...	0.0	..	0.0	0.0	0.0	2...	0...	0...	2...	2...	0.0	0...	0...	0...	1...	0...	0...	0...	1....	1....	..	..	..	..	..	...	...	0...	423.5...	56...	677.0	7.0
0.0	0.002...	0...	0.0	0...	1...	0...	..	..	..	0...	0.0	..	0.0	0...	0...	0...	1...	3...	2...	0...	2...	0...	5...	0...	0...	0...	0...	0...	0...	0....	..	..	..	..	..	...	...	2...	0.525...	0.0	1351.0	8.0
0.00486...	0.001...	4...	0...	1...	0...	5...	..	..	..	0.0	0.0	..	0...	0...	0...	1...	1...	0...	0.0	0...	0.0	0...	0...	1...	0.0	0...	0.0	0.0	0.0	0.0	..	..	..	..	..	...	...	0.0	0.0	0....	1028.0	9.0
4.40446...	0.0	0.0	3...	1...	4...	0.0	..	..	..	0.0	0.0	..	4...	0...	0...	8...	1...	0...	0.0	0...	0.0	0...	0...	0...	0...	2...	0.0	0.0	0.0	0.0	..	..	..	..	..	...	...	0.0	0.0	4....	694.0	10.0
3.52944...	9.666...	0...	1...	5...	0...	0...	..	..	..	0...	0.0	..	0...	0...	0...	0...	0.0	0...	0...	0...	0.0	0...	0...	0...	0...	0...	0...	0...	0.0	0.0	..	..	..	..	..	...	...	0...	3.529...	5....	851.0	11.0
0.02509...	0.317...	0...	0...	0...	0...	0...	..	..	..	6...	0...	..	0...	3...	9...	0...	6...	0...	1...	6...	0...	0...	0...	0...	0...	0...	0...	0...	0...	0....	0.0	..	..	..	..	..	...	...	0...	0.001...	0....	1600.0	12.0
0.00325...	1.614...	1...	0...	0...	0...	0...	..	..	..	2...	0...	..	0...	0...	0.0	0...	0...	0...	4...	0...	1...	0...	8...	0...	0...	0...	0.0	0.0	0.0	0....	..	..	..	..	..	...	...	6...	4.842...	0....	1240.0	13.0
2.77888...	1.089...	0...	0...	0...	0...	0...	..	..	..	0...	0...	..	0.0	0.0	0.0	0...	0.0	1...	0...	1...	0...	1...	0...	0...	0.0	0...	0.0	0.0	0....	0....	..	..	..	..	..	...	...	0.0	0.002...	7....	1001.0	14.0
0.18681...	0.003...	0...	0...	2...	7...	5...	..	..	..	0...	1...	..	0...	2...	0.0	0...	0...	0...	0.0	0...	0...	0...	0...	0...	0...	0...	0...	0.0	0...	0....	0....	..	..	..	..	..	...	...	1...	0.812...	0....	1387.0	15.0
0.00237...	0.003...	0...	0...	0...	0.0	0.0	..	..	..	0...	4...	..	0.0	0...	0...	7...	0...	0...	0...	0...	0...	0...	0...	0...	0...	7...	1...	0...	0...	0....	1....	..	..	..	..	..	...	...	7...	3.306...	0....	1264.0	16.0
0.00407...	0.005...	0...	0...	0...	0.0	8...	..	..	..	1...	0.0	..	0...	0.0	1...	0...	1...	0...	8...	0...	0...	8...	0.0	0...	2...	0...	0...	0...	2....	1....	..	..	..	..	..	...	...	0...	0.002...	0....	1231.0	17.0
0.00560...	0.273...	0...	0.0	6...	0...	0...	..	..	..	0...	0.0	..	0.0	8...	0...	0...	0...	2...	0...	0...	1...	0...	0.0	0...	0...	0...	0...	1...	7....	0....	..	..	..	..	..	...	...	0...	0.002...	0....	1535.0	18.0
1.68354...	0.691...	0.0	0.0	0...	0...	7...	..	..	..	0...	0...	..	0...	0...	0...	6...	0...	0...	0...	0...	0.0	0...	0...	0...	0...	0...	1...	0...	0....	3....	..	..	..	..	..	...	...	0...	0.139...	0....	1325.0	19.0
0.0	0.0	0.0	0...	0...	0...	0...	..	..	..	0...	0...	..	7...	0.0	0.0	0...	0...	0...	0...	2...	0...	0...	6...	0...	0...	0...	7...	0.0	7....	0....	..	..	..	..	..	...	...	0...	0.042...	0.0	1333.0	20.0

Figure IV.4 : Tableau qui contient le centre de gravité de chaque classe

Pour chaque classe un cenyre de gravité est calculée et stoquée en suite dans un tableau avec la colonne 42 qui contient le nombre de connexion dans chaque classe

la connexion: 10 est une attaque
la connexion: 11 est une connexion normale
la connexion: 12 est une attaque
la connexion: 13 est une attaque
la connexion: 14 est une attaque
la connexion: 15 est une attaque

Figure IV.5 Résultat du test

La figure démontre le résultat obtenue du test avec le numéro de la connexion et son type Attaque ou normal

Conclusion Générale

Conclusion Générale

Le système d'information d'une entreprise peut être vital à son fonctionnement. Il est donc nécessaire d'assurer sa protection, afin de lutter contre les menaces qui pèsent sur l'intégrité, la confidentialité et la disponibilité des ressources.

La malveillance informatique est souvent à l'origine de ces menaces, qu'il s'agisse de vol d'information ou de sabotage, n'importe qui pouvant s'improviser pirate informatique avec des outils adaptés.

Beaucoup de compétences sont nécessaires pour assurer une sécurité optimale, mais il est impossible de garantir la sécurité de l'information à 100%. Malgré tout, il existe des moyens efficaces pour faire face à ces agressions.

C'est pour cela qu'il est utile de bien savoir gérer les ressources disponibles et comprendre les risques liés à la sécurité informatique, pour pouvoir construire une politique de sécurité adaptée aux besoins de la structure à protéger. La mise en place d'un dispositif de sécurité efficace ne doit cependant jamais dispenser d'une veille régulière au bon fonctionnement du système.

Référence Bibliographique

[1] Memoir 3eme Année license kherkhour Mustapha "Active directory"

[2] CEH v8 chapitre 1- introduction to ethical hacking

[3] Cyrille Duret, Nathalie Gaillard « les attaque réseau et les moyen de s'en protéger » DESS IIR option Réseaux

[4] « http://www.awt.be/web/sec/index.aspx?page=sec,fr,fic,045,004 » Rédigé par Agence Wallonne

[5] Mdme Heddaoui Rebiha mémoire de magister

[6] « http://lehmann.free.fr/RapportMain/node10.html »

[7] « http://www.w3.org/1999/xhtml»

[8] « http://igm.univ-mlv.fr/~dr/XPOSE2009/Sonde_de_securite_IDS_IPS/IDS.html »

Figure

[1] Memoir kherkhour Mustapha "Active directory"

[2] CEH v8 chapitre 1- introduction to ethical hacking

[3] « http://www.aldeid.com »

[4] « www. projet.piratage.free.fr/techniques.html »

[5] www.OVH.com

[6] « http://www.awt.be/web/sec/index.aspx?page=sec,fr,fic,045,004 » Rédigé par Agence Wallonne

[7] N. Ben Amor, S. Benferhat et Z. Elouedi, « Réseaux bayésiens naïfs et arbres de décision dans les systèmes de détection d'intrusions ».

[8] Melle Oumiloud Horiya Melle Mokeddem Asma memoir licence Classification non supervisée : Application de k-means

[9] Mdme Heddaoui Rebiha mémoire de magister

[10] « http://www.w3.org/1999/xhtml »

[11] « http://igm.univ-mlv.fr/~dr/XPOSE2009/Sonde_de_securite_IDS_IPS/IDS.html »

[12] « https://www.alienvault.com/solutions/intrusion-detection-system »