République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Bejaïa
Faculté des Sciences Exactes - Département Informatique

Mémoire de fin de Cycle
En vue de l'obtention du titre de Master Professionnel en Informatique
Option : Administration et Sécurité des Réseaux Informatiques

Thème :

Politiques de sécurité

& systèmes de protection contre les intrusions

Réalisé par :

- **M^r^. Atmani Abdelfetah**
- **M^r^. Benkaid Djebar**

Jury:

President	M^r^	U.A/MIRA Bejaia
Promoteur	M^r^ A.Sider (maître assistant)	U.A/MIRA Bejaia
Examinateur	M^r^	U.A/MIRA Bejaia

Promotion 2011

Remercîments

Nos sincères remercîments à Dieu le tout puissant pour la volantè, la santé et la patience qu'il nous a donné afin de réaliser ce mémoire.

Nous tenons à exprimer nos vifs remercîments à nos familles pour leur appui continu et inconditionnel durant tout notre cursus d'études.

Nous tenons à exprimer aussi nos remercîment à notre promoteur M$^{r.}$A.SIDER pour ces judicieux conseils et sa confiance.

Nous voudrions également témoigner notre reconnaissance à tous nos enseignants du département informatique.

Qu'il nous soit permis d'exprimer ici nos vifs remercîments à ceux qui ont accepté de juger notre travail.

Et dans le souci de n'oublier personne, que tous ceux qui de près ou de loin ont contribué à la réalisation de ce mémoire trouvant ici toute notre gratitude et notre sympathie.

Dédicaces

Je dédie ce modeste travail à toutes les personnes que je chérie le plus :

À mes chers parents que j'adore et qui me soutiennent toujours.

À mes chers frères et sœurs : Nabil, Atmane, Hakim, lynda,

meriem ,asma, et soumia

À mes chères neveux et nièces : Naoufel, Sara,et Yasmine.

À ma tante Hdjila que j'aime beaucoup.

À mon binôme Djebar qui a participé à l'élaboration de ce travail à qui je souhaite une grande réussite

.

.

ABDELFETAH

Dédicaces

Je dèdie ce modeste travail à mes chères parent qui me soutiennent toujours durant les dûres épreuves que ça soit personnelles ou professionnelles.

À mes chers frères et sœurs : Yazid, Nassima, Nadia et Kawtar

À mes chères neveux et nièces : Zohir, Abdelghani, Amine,

Ayoub,Larbi,Abd Raouf et Imane.

À tous mes amis et amies surtout : Azouz, Salim,Sofiane,Nabil,naim,laucif,

Toufik, Mourad et mohand,et Karima.

À mon binôme Abdelfetah (alias Farid) à qui je

souhaite une grande réussite.

DJEBAR

Table des matières

Table des figures

Table des tableaux

Introduction générale

Face aux nouvelles technologies de l'information et de la communication, apparue avec l'avènement des réseaux et d'internet, et surtout des systèmes distribués ont malheureusement contribué à faire évoluer de manière considérable les menaces informatiques. Face à cette situation la sécurité informatique est devenu un défi majeur, et les travaux dans cet axe de recherche sont de plus en plus nombreux.

Les risques auxquels sont confrontées les entreprises et les organisations aujourd'hui sont tels que la sécurité informatique prend une place de plus en plus prépondérante et vitale au sein des institutions privées et publiques. Il ne s'agit plus de considérer la sécurité comme un luxe réservé aux grandes organisations ou entreprises car il n'est pas rare d'assister de nos jours à des prises d'otages de petits systèmes ou réseaux afin de s'en servir comme relais pour réaliser des attaques de grandes envergures sur de gros systèmes ou réseaux.

Au même moment, le niveau de connaissance requis pour devenir pirate ne cesse de diminuer en raison de la reproduction d'outils et de logiciels malfaisants (malwares) disponibles gratuitement sur le web. Vue cette situation inquiétante, pour survivre et poursuivre, avec un minimum de sécurité leurs activités, les entreprises et les organisations doivent adopter et mettre en œuvre des politiques de sécurité. Ces dernières sont en fait des ensembles cohérents et compatibles de mesures de sécurité qui visent à protéger les systèmes d'informations des entreprises des attaques et d'incidents de toutes sortes, ou d'en réduire autant que possible les impacts.

Toutefois, il arrive parfois que des incidents de types intrusions ou attaques surviennent malgré toutes les mesures et politiques de sécurité mises en place. Ces incidents qui sont de plus en plus nombreux peuvent provenir de l'intérieur comme de l'extérieur des réseaux des entreprises ou des organisations. Face à cette situation, de nouveaux systèmes de surveillance (les systèmes de détection d'intrusion ou IDS), et de protection (les systèmes de prévention d'intrusion ou IPS), sont développés depuis quelques années par les éditeurs de solutions de sécurité. Ces dernières années, les systèmes de détection d'intrusion sont devenus très largement déployés dans les systèmes d'information, et ils ont gagné une place importante dans la conception de la politique de sécurité. Ils sont généralement utilisés pour surveiller l'accès et le flux d'information, dans le but de déterminer tout comportement malicieux, que ce soit de l'intérieur ou l'extérieur de système d'information, et rendre cette information

disponible aux administrateurs de la sécurité. En option, les systèmes de détection d'intrusion peuvent réagir contre ces comportements malicieux et prendre des contre-mesures.

Notre travail consiste savoir comment mettre en place ces mesures et solutions de sécurité efficacement afin de réellement protéger les systèmes d'information. Dans ce contexte, la mise en application d'une politique de sécurité constitue le meilleur moyen d'atteindre les objectifs de la sécurité informatique.

Et l'étude de la détection d'intrusion nous permettra de mieux comprendre les systèmes de détection et comment se protéger efficacement face à ces intrusions et de voir comment ils arrivent à renforcer la sécurité en fermant les trous de sécurité laissés par les mesures classiques de sécurité.

Dans ce cadre, nous avons commencé par une introduction générale au domaine de la sécurité informatique d'une façon générale dont nous avons évoqué les diffèrent principes, menaces et solutions en matière de sécurité informatique. La seconde partie présente les politiques et modèles de sécurité, où nous avons mis en évidence la nécessité pour les organisations d'aller vers une vision plus large de la sécurité de leurs systèmes d'informations à travers les politiques de sécurité et la démarche à suivre.

La troisième partie consistera à présenter les différents types et principe de fonctionnement des systèmes de détection d'intrusions. Et nous terminerons par une mise en place d'un IDS **Snort** qu'est un projet Open Source de détection d'intrusion sur le réseau open-source fonctionnant sur les systèmes Windows et Linux où nous allons voir les étapes d'installation et de configuration.

I. Introduction à la sécurité informatique

I.1 Principes de la sécurité

Pour des soucis d'efficacité et de rentabilité, une entreprise communique aujourd'hui avec ses filiales, ses partenaires et va jusqu'à offrir des services aux particuliers, ce qui induit une ouverture massive à l'information. Par l'ouverture des réseaux, la sécurité devient un facteur décisif du bon fonctionnement de l'entreprise ou de l'organisme.

Il reste qu'une entreprise ou un organisme possède certaines informations qui ne doivent être divulguées qu'à un certain nombre de personnes ou qui ne doivent pas être modifiées ou encore qui doivent être disponibles de manière transparente à l'utilisateur. Ces informations feront l'objet d'une attaque si et seulement si des menaces existent et si le système abritant ces informations est vulnérable.

Par conséquent on appelle **sécurité de l'information**, l'état de protection, face aux risques identifiés, qui résulte de l'ensemble des mesures générales et particulières prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée, où :

- **La confidentialité :** est le caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service.
- **L'intégrité :** de l'information traitée garantit que celle-ci n'est modifiée que par un acte volontaire et légitime.
- **La disponibilité :** est l'aptitude d'un système d'accéder à l'information dans des conditions définies d'horaires, de délais et de performances.

De façon générale, la sécurité informatique peut être définie par l'ensemble des moyens matériels, logiciels et humains mis en œuvre pour minimiser les vulnérabilités d'un système d'information, et le protéger contre les menaces accidentelles ou intentionnelles, provenant de l'intérieur ou de l'extérieur de l'entreprise.

Du point de vue organisationnel, nous pouvons découper le domaine de la sécurité informatique de la façon suivante :

- **La sécurité logicielle :** gère la sécurité au niveau logiciel du système d'information (par exemple : l'intégration des protections logicielles comme l'antivirus).
- **La sécurité du personnel** : comprend la formation et la sensibilisation des personnes utilisant ou travaillant avec le système d'information.

- **La sécurité physique :** regroupe la politique d'accès aux bâtiments, la politique d'accès aux matériels informatiques, et les règles de sécurité pour la protection des équipements réseaux.
- **La sécurité procédurale** : définit les procédures et les règles d'utilisation du système d'information.
- **La sécurité réseau** : s'occupe de l'architecture physique et logique du réseau, la politique d'accès aux différents services, la gestion des flux d'informations sur les réseaux, et surtout les points de contrôle et de surveillance du réseau.
- La veille technologique souvent oubliée permet d'évaluer la sécurité au cours du temps afin de maintenir un niveau suffisant de protection du système d'information.

I.2 Terminologie de la sécurité informatique

La sécurité informatique utilise un vocabulaire bien défini que nous utilisons dans ce mémoire. Il est nécessaire de définir certains termes :

- **Les vulnérabilités :** ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.
- **Les attaques (exploits):** elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.
- **Les contre-mesures :** ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique (auquel cas il peut exister d'autres attaques sur la même vulnérabilité).
- **Les menaces :** ce sont des adversaires déterminés capables de monter une attaque exploitant une vulnérabilité.

I.3 Services et mécanismes de sécurité

De façon générale, les mécanismes de sécurité permettent de mettre en œuvre des services de sécurité. Ces services peuvent être la confidentialité (des données ou du flux de données), l'authentification (d'une entité ou de l'origine des données), le contrôle d'accès, l'intégrité ou encore la non répudiation (avec preuve de l'origine ou preuve de la remise). Les mécanismes peuvent être le chiffrement, l'authentification, l'intégrité, la signature numérique, et d'autres encore.

I.3.1 Les services de sécurité

Le célèbre modèle en couches OSI (Open Systems Inter connection) est décrit dans la norme multi parties ISO 7498, intitulée "Interconnexion des Systèmes Ouverts - Modèle de référence de base". Dans la partie intitulée "Architecture de sécurité", se trouvent des définitions et des concepts de base de la sécurité.

Les principaux besoins de sécurité que peut avoir l'émetteur d'un message sont les suivants :

- ✓ A1: le message ne doit être connu que de son destinataire.
- ✓ A2: le message doit parvenir au bon destinataire.
- ✓ A3: le message reçu doit être identique au message émis.
- ✓ A4: le destinataire ne doit pas pouvoir nier avoir reçu le message.

Et les besoins du destinataire peuvent être :

- ✓ B1: le message ne doit être connu que de lui (et de l'émetteur).
- ✓ B2: l'émetteur du message doit être connu avec certitude.
- ✓ B3: le message reçu doit être identique au message émis.
- ✓ B4: l'émetteur ne doit pas pouvoir nier avoir émis le message.

Les besoins A1 et B1 sont identiques. Ils sont satisfaits par la mise en œuvre d'un service de

confidentialité, définie dans la norme 7498-2 comme la "propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés".

Les besoins A2 et B2 sont symétriques. Chaque entité doit s'assurer de l'identité de l'autre, ce qui implique de mettre en œuvre un service d'authentification, défini comme la "confirmation qu'une entité homologue d'une association est bien l'entité déclarée", et même, dans le cas du destinataire, un service d'authentification de l'origine des données, ou "confirmation que la source des données est telle que déclarée".

Les besoins A3 et B3 sont identiques. L'égalité entre le message émis et le message transmis est assurée par un service d'intégrité (des données), qui est la "propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée".

Enfin, les besoins A4 et B4 sont symétriques. Le service correspondant est le non répudiation, qui empêche la répudiation, c'est-à-dire "le fait, pour une des entités impliquées dans la communication, de nier avoir participé aux échanges, totalement ou en partie". Dans un cas il

s'agira de non répudiation avec preuve de l'origine, dans l'autre de non répudiation avec preuve de la remise [1].

A tout cela s'ajoute le service de contrôle d'accès, ou "précaution prise contre l'utilisation non autorisée d'une ressource", et qui peut s'appliquer à divers types d'accès (utilisation de ressources de communication, lecture, écriture ou suppression d'une ressource d'information, exécution d'une ressource de traitement).

Parfois, la simple observation du flux de données fournit de l'information à un ennemi. C'est ce qu'on appelle l'analyse de trafic, qui permet de détecter la présence, l'absence, la quantité, la direction, ou la fréquence de telles ou telles données, qu'elles soient compréhensibles ou non. On peut alors renforcer la confidentialité des données en assurant également la confidentialité du flux de données, c'est-à-dire un "service de confidentialité fournissant une protection contre l'analyse de trafic". La confidentialité, tout comme l'intégrité, peut être sélective par champ, c'est-à-dire ne s'appliquer qu'à une partie des champs contenus dans le message transmis.

I.3.2 Les mécanismes de sécurité

Les différents services de sécurité décrits précédemment sont mis en œuvre grâce à des mécanismes, dont la plupart sont de nature cryptographique. La cryptographie est la "discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée".

Afin d'assurer la confidentialité des données et/ou du flux de données, on fait appel à un mécanisme de chiffrement, qui est la "transformation cryptographique de données produisant un cryptogramme", unité de données dont "le contenu sémantique n'est pas compréhensible".

L'opération inverse du chiffrement est le déchiffrement. Lorsqu'il est effectué de bout en bout, le chiffrement a lieu "à l'intérieur ou au niveau du système extrémité source, le déchiffrement correspondant ne se produisant qu'à l'intérieur, ou au niveau du système extrémité de destination".

S'il n'est effectué qu'à chaque liaison du système (dans quel cas les données sont en clair à l'intérieur des entités relais), il s'agit de chiffrement de liaison. La confidentialité du flux de données exige en outre un mécanisme de bourrage de trafic, consistant à produire des

"instances de communications parasites, des unités de données parasites et/ou des données parasites dans des unités de données". Cet échange continu de données, transportant ou non de l'information, permet d'éviter qu'un tiers ne sache quand deux entités sont entrées en communication.

Le service d'authentification (d'entité homologue) est fourni par un mécanisme d'échange d'authentification, "destiné à garantir l'identité d'une entité par échange d'informations".

(Typiquement, cet échange est constitué d'un nombre choisi au hasard envoyé par l'entité qui souhaite authentifier l'autre, et d'une réponse de cette dernière obtenue en appliquant un mécanisme cryptographique à ce nombre et à un secret connu d'elle seule).

L'authentification de l'origine des données peut être obtenue grâce à un mécanisme de signature numérique. Il s'agit de "données ajoutées à une unité de données permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple)". Le même terme désigne aussi la transformation cryptographique qui produit ces données. Pour produire une signature, il faut une information privée, c'est-à dire connue du seul signataire. Pour la vérifier, il suffit d'une information publique. Il doit cependant être matériellement impossible de déduire l'information privée de l'information publique correspondante.

L'intégrité des données est assurée par un mécanisme du même nom. Un tel mécanisme peut consister à produire une valeur de contrôle cryptographique, à partir des données à protéger et d'un secret partagé par les entités en communication. Dans ce cas, la vérification par le destinataire consiste à recalculer cette valeur et à la comparer avec celle reçue. Si elles sont égales, il y a présomption d'intégrité. Mais on peut également utiliser un mécanisme de signature numérique qui, en plus de l'origine des données, garantit également leur intégrité.

Par ailleurs, il peut être nécessaire de recourir en outre à des mécanismes visant à éviter le rejoue (répétition frauduleuse de tout ou partie des données), tels que la numérotation, l'horodatage ou le chaînage cryptographique des données.

Pour obtenir la non répudiation avec preuve de l'origine, on peut utiliser un mécanisme de signature numérique. En effet, la caractéristique essentielle de ce mécanisme est que la signature ne peut être produite qu'en utilisant l'information privée du signataire. On peut donc, en vérifiant la signature, prouver à tout moment à une tierce partie (par exemple un juge

ou un arbitre) que seul le détenteur unique de l'information privée peut avoir produit la signature. Il est cependant possible d'utiliser aussi des mécanismes de chiffrement ou d'intégrité.

Les mécanismes de contrôle d'accès peuvent utiliser des éléments variés tels que l'identité authentifiée de l'entité, une information sur cette entité, une liste de droits d'accès, des "étiquettes" de sécurité spécifiant des niveaux de sensibilité, etc. La politique de contrôle d'accès choisie peut être de type discrétionnaire (l'utilisateur définit les droits d'accès aux informations dont il a la responsabilité) ou de type par mandat (l'autorisation d'accès dépend des droits du demandeur, du niveau de sensibilité des informations et d'attributs spécifiques).

Le contrôle de routage permet d'acheminer l'information à travers des sous réseaux, liaisons ou relais considérés comme sûrs. Il peut, soit spécifier explicitement les chemins autorisés, soit tenir compte du niveau de sensibilité des informations dans le choix des chemins utilisés [2].

I.4 Les menaces en matière de sécurité informatique

Les risques potentiels sur le fonctionnement conforme des réseaux, des systèmes et des infrastructures sont de types variés qui vont de la panne ordinaire à la malveillance technique en passant par la maladresse humaine.

I.4.1 Étude des risques

Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés. L'ensemble des solutions retenues doit être Les coûts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi. Organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque. On obtient ainsi la liste de ce qui doit être protégé.

Il faut cependant prendre conscience que les principaux risques restent : « câble arraché », « Coupure secteur », « crash disque », « mauvais profil utilisateur », « test du dernier CD Bonux »…

Voici quelques éléments pouvant servir de base à une étude de risque:

- ✓ Quelle est la valeur des équipements, des logiciels et surtout des informations ?
- ✓ Quel est le coût et le délai de remplacement ?
- ✓ Faire une analyse de vulnérabilité des informations contenues sur les ordinateurs en réseau (programmes d'analyse des paquets, logs…).

- ✓ Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société ?

Les progrès technologiques ne profitent malheureusement pas qu'aux utilisateurs légaux ; ils sont aussi mis à contribution pour améliorer les techniques de violation des politiques de sécurité. Les techniques d'attaques ont connu une évolution remarquable au cours de ces vingt (20) dernières années, les outils permettant d'attaquer les systèmes d'informations sont devenus bien plus puissants et plus facile à utiliser. Cette facilité d'utilisation a abaissé le niveau de connaissances techniques nécessaires pour lancer une attaque, augmentant en conséquence de façon exponentielle le nombre d'assaillants potentiels [3].

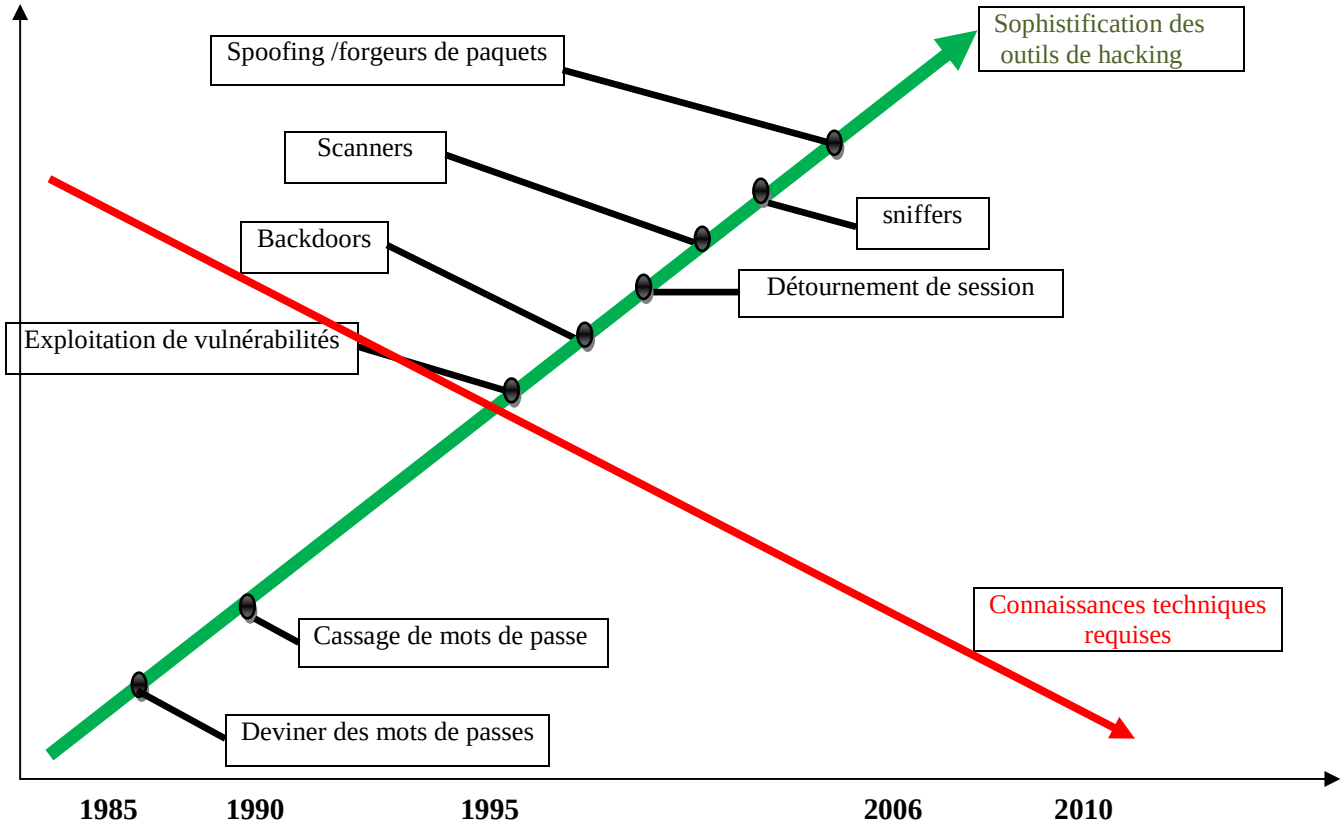

Figure I.1 : Rapport entre sophistication des outils et niveau de connaissance requis

Dans cette partie de notre document, nous allons tenter de catégoriser les dangers ou les risques auxquels sont exposés les systèmes d'information en deux grandes catégories que nous décortiquerons successivement en profondeur. Il s'agira de voir dans un premier temps les dangers que l'on appelle parfois aussi risques ou attaques informatiques en général et dans un deuxième temps nous parlerons du cas spécial des intrusions.

I.4.2 Les attaques informatiques

Une attaque informatique est l'exploitation d'une faille d'un système (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur Internet des attaques ont lieu en permanence. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (appelées bot nets) par des virus, des chevaux de Troie, des vers et autres, à l'insu de leur propriétaire. Les motivations des attaques peuvent être de différentes sortes :

- ✓ Obtenir un accès au système ;
- ✓ Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- ✓ Glaner des informations personnelles sur un utilisateur ;
- ✓ Récupérer des données bancaires ;
- ✓ S'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- ✓ Troubler le bon fonctionnement d'un service ;
- ✓ Utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- ✓ Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

Les systèmes informatiques mettent en œuvre différentes composantes, allant de l'électricité pour alimenter les machines au logiciel exécuté via le système d'exploitation et utilisant le réseau. Les attaques peuvent intervenir à chaque maillon de cette chaîne, pour peu qu'il existe une vulnérabilité exploitable. Le schéma ci-dessous rappelle très sommairement les différents niveaux pour lesquels un risque en matière de sécurité existe :

Il y a d'abord les attaques qui visent l'accès physique et l'environnement du système d'information. Il s'agit des cas où l'attaquant a accès aux locaux et éventuellement même aux machines. Il s'agit souvent des événements comme :

- ✓ Les coupures de l'électricité ;
- ✓ L'extinction manuelle des ordinateurs ou des serveurs ;
- ✓ Le vandalisme ;
- ✓ L'ouverture des boîtiers des ordinateurs et le vol des disques durs ou d'autres composants ;
- ✓ L'écoute directe du trafic sur le réseau c'est-à-dire en se branchant directement sur backbone ou sur un core-Switch (commutateur principal) par exemple.

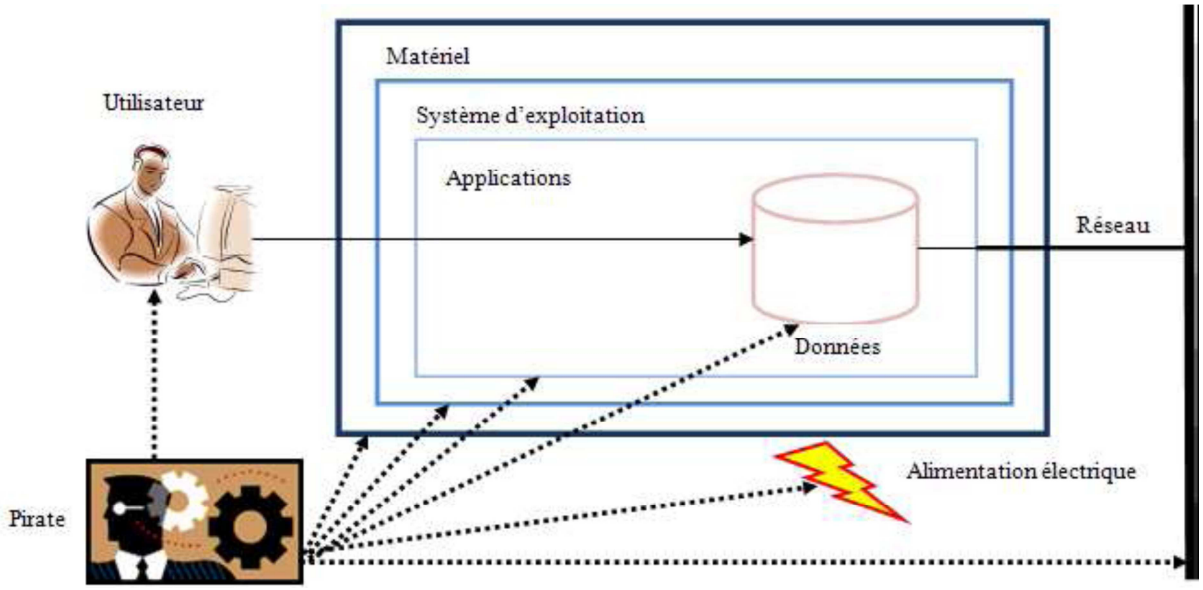

Figure I-2 : Les niveaux de vulnérabilité d'un système informatique

Ces attaques que l'on pourrait qualifié de basiques étaient surtout à la mode quand l'informatique était encore à ses débuts. C'est-à-dire l'ère de l'informatique centralisée.

Après les attaques visant les accès physiques et l'environnement, il y a celles utilisant les interceptions des communications comme :

- ✓ L'usurpation de ressources ou des paramètres d'identité (mots de passe, adresses IP, adresses MAC) ;
- ✓ Le détournement ou altération de messages (Man In the Middle, Brute Force attack etc.);
- ✓ Le vol de session (session hijacking), l'ARP poisoning, l'écoute réseau, le balayage de ports etc.

Ensuite, il y a les attaques de type déni de service. Il s'agit des attaques visant à perturber le bon fonctionnement d'un service du système d'exploitation ou d'une application. On distingue habituellement les types de déni de service suivant :

- ✓ Exploitation de faiblesses des protocoles TCP/IP ;
- ✓ Exploitation de vulnérabilité des logiciels serveurs.

Parmi les techniques utilisées pour réaliser ce type d'attaque, on peut citer les attaques par réflexion, les attaques « Ping de la mort » (ping of death), les attaques par fragmentation, les attaques Land, les attaques SYN etc.… [4].

I.4.3 Le cas spécial des intrusions

Une intrusion est une forme particulière d'attaque informatique car la plupart des autres attaques servent souvent à préparer ou à rendre les cibles plus vulnérables afin de faciliter la réalisation des intrusions.

Les intrusions sont souvent effectuées dans les contextes d'espionnage industriel ou politique.

Par exemple au tout début du mois d'octobre 2008 selon la rédaction du «Journal du Net», des pirates ont pu s'introduire dans le système informatique d'un fabricant sud-coréen de missiles et dérober des données. Selon le premier rapport de l'administration de la sécurité nationale du pays, le National Security Research Institute, les cyber-attaquants sont parvenus à installer un programme malveillant sur le réseau de l'industriel LIGNex1 Hyundai Heavy Industries.

Pour pouvoir mettre en œuvre un exploit (il s'agit du terme technique signifiant exploiter une vulnérabilité), la première étape du hacker consiste à récupérer le maximum d'informations sur l'architecture du réseau et sur les systèmes d'exploitations et applications fonctionnant sur celui-ci [2].

L'obtention d'informations sur l'adressage du réseau visé, généralement qualifiée de prise d'empreinte, est souvent le préalable à toute attaque. Elle consiste à rassembler le maximum d'informations concernant les infrastructures de communication du réseau cible :

- ✓ Adressage IP ;
- ✓ Noms de domaine ;
- ✓ Protocoles de réseau ;
- ✓ Services activés ;
- ✓ Architecture des serveurs ;
- ✓ Etc.……

En connaissant l'adresse IP publique d'une des machines du réseau ou bien tout simplement le nom de domaine de l'organisation, un pirate est potentiellement capable de connaître l'adressage du réseau tout entier, c'est-à-dire la plage d'adresses IP publiques appartenant à l'organisation visée et son découpage en sous-réseaux. Pour cela il suffit de consulter les bases publiques d'attribution des adresses IP et des noms de domaine.

Lorsque la topologie du réseau est connue par le pirate, il peut le scanner (le terme balayer est également utilisé), c'est-à-dire déterminer à l'aide d'un outil logiciel (appelé scanné ou

scanneur en français) quelles sont les adresses IP actives sur le réseau, les ports ouverts correspondant à des services accessibles, et le système d'exploitation utilisé par ces serveurs.

L'un des outils les plus connus pour scanner un réseau est Nmap **(**Network Mapper), reconnu par de nombreux administrateurs réseaux comme un outil indispensable à la sécurisation d'un réseau. Cet outil agit en envoyant des paquets TCP et/ou UDP à un ensemble de machines sur un réseau (déterminé par une adresse réseau et un masque), puis il analyse les réponses. Selon l'allure des paquets TCP reçus, il lui est possible de déterminer le système d'exploitation distant pour chaque machine scannée.

Lorsque le balayage du réseau est terminé, il suffit au pirate d'examiner les rapports des outils utilisés pour connaître les adresses IP des machines connectées au réseau et les ports ouverts sur celles-ci. Les numéros de port ouverts sur les machines peuvent lui donner des informations sur le type de service ouvert et donc l'inviter à interroger le service afin d'obtenir des informations supplémentaires sur les versions des principales applications serveurs (Apache par exemple) dans les informations dites de « bannière ».

Après avoir établi l'inventaire du parc logiciel et éventuellement matériel, il reste au pirate à déterminer si des failles existent. Lorsque le pirate a dressé une cartographie des ressources et des machines présentes sur le réseau, il est en mesure de préparer son intrusion. Pour pouvoir s'introduire dans le réseau, le pirate a besoin d'accéder à des comptes valides sur les machines qu'il a recensées. Pour ce faire, plusieurs méthodes sont utilisées par les pirates :

- ✓ L'ingénierie sociale. Ceci est généralement fait en se faisant passer pour l'administrateur réseau ;
- ✓ La consultation de l'annuaire ou bien des services de messagerie ou de partage de fichiers, permettant de trouver des noms d'utilisateurs valides ;
- ✓ L'exploitation des vulnérabilités des commandes R* de Berkeley ;
- ✓ Les attaques par force brute (brute force cracking).

Lorsque le pirate a obtenu un ou plusieurs accès sur le réseau en se « logeant » sur un ou plusieurs comptes peu protégés, celui-ci va chercher à augmenter ses privilèges en obtenant un accès root (en français super utilisateur), on parle ainsi d'extension de privilèges.

Dès qu'un accès root a été obtenu sur une machine, l'attaquant a la possibilité d'examiner le réseau à la recherche d'informations supplémentaires. Il lui est ainsi possible d'installer un sniffeur (en anglais sniffer), c'est-à-dire un logiciel capable d'écouter (le terme renifler, ou en

anglais sniffing, est également employé) le trafic réseau en provenance ou à destination des machines situées sur le même brin. Grâce à cette technique, le pirate peut espérer récupérer les couples identifiants/mots de passe lui permettant d'accéder à des comptes possédant des privilèges étendus sur d'autres machines du réseau (par exemple l'accès au compte d'un administrateur) afin d'être à même de contrôler une plus grande partie du réseau. Les serveurs NIS présents sur un réseau sont également des cibles de choix pour les pirates car ils regorgent d'informations sur le réseau et ses utilisateurs.

Grâce aux étapes précédentes, le pirate a pu dresser une cartographie complète du réseau, des machines s'y trouvant, de leurs failles et possède un accès root sur au moins l'une d'entre-elles.

Une fois la cartographie du système établie, le hacker est en mesure de mettre en application des exploits relatifs aux versions des applications qu'il a recensées. Un premier accès à une machine lui permettra d'étendre son action afin de récupérer d'autres informations, et éventuellement d'étendre ses privilèges sur la machine.

Lorsqu'un pirate a réussi à infiltrer un réseau d'entreprise et à compromettre une machine, il peut arriver qu'il souhaite pouvoir revenir. Pour ce faire celui-ci va installer une application afin de créer artificiellement une faille de sécurité, on parle alors de porte dérobée (en anglais backdoor, le terme trappe est parfois également employé).

Lorsque l'intrus a obtenu un niveau de maîtrise suffisant sur le réseau, il lui reste à effacer les traces de son passage en supprimant les fichiers qu'il a créés et en nettoyant les fichiers de logs des machines dans lesquelles il s'est introduit, c'est-à-dire en supprimant les lignes d'activité concernant ses actions.

Par ailleurs, il existe des logiciels, appelés « kits racine » (en anglais « rootkits ») permettant de remplacer les outils d'administration du système par des versions modifiées afin de masquer la présence du pirate sur le système. En effet, si l'administrateur se connecte en même temps que le pirate, il est susceptible de remarquer les services que le pirate a lancé ou tout simplement qu'une autre personne que lui est connectée simultanément. L'objectif d'un rootkit est donc de tromper l'administrateur en lui masquant la réalité [5].

S'il s'agit d'un pirate expérimenté, la dernière étape consiste à effacer ses traces, afin d'éviter tout soupçon de la part de l'administrateur du réseau compromis et de telle manière à pouvoir

garder le plus longtemps possible le contrôle des machines compromises. Le schéma suivant récapitule la méthodologie complète :

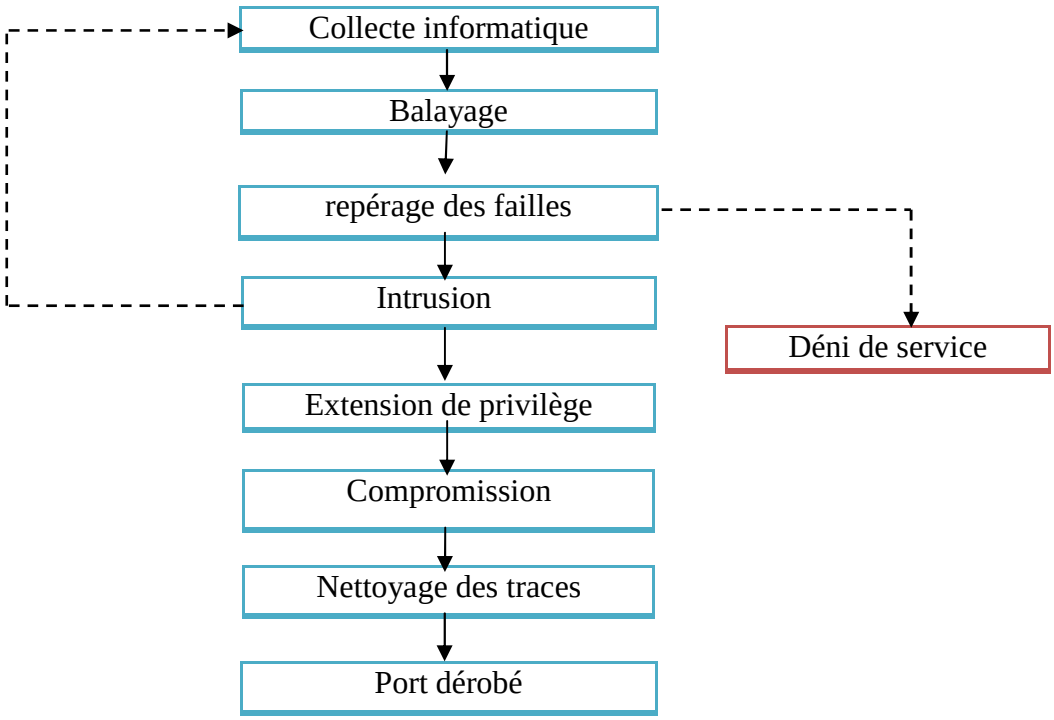

Figure I-3 : Etapes de réalisation d'une intrusion informatique

Une autre caractéristique des attaquants est leur contrôle unidirectionnel ou bidirectionnel sur les communications, du fait de la nature asymétrique de celles-ci. En effet, la plupart des canaux de transmissions sur Internet ou sur tout autre réseau hétérogène sont unidirectionnels et empruntent des chemins différents suivant les règles de routage. Ainsi, de nombreux protocoles de sécurité sont également unidirectionnels et il faut établir plusieurs canaux pour permettre un échange en "duplex". Ces canaux qui sont au nombre de 2 minimums, sont la plupart du temps gérés de façon totalement indépendante par les protocoles de sécurité. C'est le cas pour SSL/TLS mais également pour IPSec dont les associations de sécurité sont unidirectionnelles et indépendantes, chacune définissant son propre jeu de clés, algorithmes, etc.… [3].

I.5 Quelques solutions en matière de sécurité

Actuellement, toute une série d'outils et de techniques permettent à un administrateur de sécuriser facilement son réseau et les machines qui le composent. Chacune de ces techniques se base sur des principes fondamentalement différents, mais celles-ci ont un but commun :

Permettre une connexion entre Internet (réseau non sécurisé) et le réseau de l'entreprise concernée, en assurant la sécurité des équipements et des informations disponibles sur ce réseau, tout en tenant compte des contraintes de plus en plus présentes, telles que les interconnexions de réseaux, les besoins de « contacts électroniques » pour le personnel (mails, transferts de fichiers, accès Web, etc.), les systèmes d'informations complexes, et autres.

Nous allons citer et expliquer brièvement quelques outils de sécurité courants, pour nous permettre par la suite de distinguer entre les systèmes de détection d'intrusions (IDS), l'objectif de ce travail, et les Firewalls, à cause de la confusion qui peut exister entre eux.

I.5.1 Les Firewalls

Le mot Firewall (Pare-feu) signifie qu'on instaure une série de protections en un point particulier entre deux entités connectées, en l'occurrence entre Internet et le réseau interne d'une entreprise. En pratique, le Firewall consiste en une architecture, plutôt qu'un matériel ou un logiciel précis. Cette architecture intègre alors une série de composants matériels et logiciels, qui tentent précisément d'assurer le niveau de sécurité requis.

L'architecture la plus utilisée actuellement est basée sur une « Zone démilitarisée », communément appelée DMZ. Elle consiste à placer un réseau intermédiaire entre l'accès Internet et le réseau interne. Cette DMZ sera isolée, aussi bien vis-à-vis de l'Internet que du réseau local, par des systèmes de filtrage (filtres de paquets entrant et sortant). Ensuite, les éventuels serveurs nécessaires à l'entreprise devant continuer à être accessibles de l'extérieur seront connectés directement sur cette DMZ, de manière à les séparer du réseau interne. Par exemple, on pourra y trouver un serveur Web, un serveur DNS, un serveur de mails, un serveur FTP, etc.… Dans le cas où l'un de ces serveurs serait compromis, le filtrage entre la DMZ et le réseau interne doit être capable d'assurer une protection suffisante au réseau interne.

Bien évidemment, cette architecture doit être adaptée plus précisément à la structure d'une entreprise précise, et éventuellement intégrer des composants supplémentaires, tels que des Proxys (machine intermédiaire entre les ordinateurs d'un réseau local et le Web) et autres dispositifs [2].

I.5.2 Les filtres de paquets

Un filtre de paquet, tout comme son nom l'indique, permet de filtrer les paquets circulant sur un réseau.

Plus précisément, on peut même dire que le filtrage s'effectue sur les paquets traversant une interface réseau. Celui-ci fonctionne en analysant le contenu de ces paquets, principalement en observant les valeurs de certains champs des en-têtes des protocoles IP, ICMP, UDP et TCP. Cela permet par exemple d'interdire des paquets provenant d'une source précise, étant destinés à une destination précise, des paquets réceptionnés sur une interface précise, des paquets avec des ports sources ou cibles précis, d'intégrer des contraintes d'heures éventuelles d'après l'horaire d'une entreprise, etc.

Au niveau de la configuration, on fait établir une série de règles de filtrage qui reflète la politique de sécurité de l'entreprise. Les paquets ne satisfaisant pas aux règles de filtrage seront alors bloqués (supprimés), et peuvent entraîner éventuellement la génération d'un message d'erreur (via un protocole comme ICMP).

I.5.3 Audit

L'audit sert à conserver des traces des opérations susceptibles de mettre en cause la sécurité, de façon à analyser, après coup ou en temps réel, si des malveillances ont lieu ou ont eu lieu et quels sont les moyens et les méthodes utilisés, de façon à punir les coupables et à corriger les vulnérabilités. Il faut donc enregistrer toutes les opérations liées à la sécurité, que ces opérations soient réussies ou qu'elles aient échouées (empêchées par les mécanismes de contrôle d'accès). Les principales opérations à surveiller sont :

- ✓ La connexion et la déconnexion des utilisateurs ;
- ✓ La création, modification, destruction des informations de sécurité (droits d'accès, mots de passe, etc.) ;
- ✓ Les changements de privilèges.

Les journaux d'audit doivent être indestructibles (sauf par les administrateurs de l'audit). Ils doivent porter sur tous les utilisateurs (y compris les administrateurs et les responsables de la sécurité) et contenir un maximum d'informations utiles (date et heure, identité de l'utilisateur, type d'opération, référence de l'information, etc.). Bien évidemment, l'administrateur de l'audit doit être indépendant des administrateurs du système surveillé, et il est souhaitable que le système surveillé ne puisse pas accéder au système d'audit.

Les journaux d'audit sont en particulier l'une des sources d'informations des systèmes de détection d'intrusion.

I.5.4 Les scanners et les outils relatifs à la sécurité

Etant donné que les hackers (pirates informatique) trouvent de plus en plus les outils nécessaires à la réalisation de leurs attaques, les entreprises travaillant dans le domaine de la sécurité ont petit à petit commencé à proposer leurs propres outils de vérification de vulnérabilités. C'est ainsi qu'on commence à avoir apparaître toute une série de scanners, qui offrent de nombreuses possibilités. Il est primordial à l'heure actuelle d'effectuer de nombreux tests de sécurité réguliers, car ces tests permettent de mettre en avance des modifications dans l'architecture et dans la configuration du réseau et des machines qui le composent [6]. Ces outils sont décomposés en toute une série de catégories, dont notamment :

- ✓ Les scanners de vulnérabilités.
- ✓ Les scanners orientés réseaux.
- ✓ Les scanners orientés hosts (machines).
- ✓ Les sniffers.
- ✓ Les vérificateurs de mots de passe.

I.5.5 ANTIVIRUS

Principale cause de désagrément en entreprise, les virus peuvent être combattus à plusieurs niveaux.

La plupart des antivirus sont basés sur l'analyse de signature des fichiers, la base des signatures doit donc être très régulièrement mise à jour sur le site de l'éditeur (des procédures automatiques sont généralement possibles).

Deux modes de protection :

- ✓ Généralisation de l'antivirus sur toutes les machines, il faut absolument prévoir une mise à jour automatique de tous les postes via le réseau.
- ✓ Mise en place d'un antivirus sur les points d'entrée/sortie de données du réseau après avoir parfaitement identifiés tous ces points. La rigueur de tout le personnel pour les procédures doit être acquise.

I.5.6 Les systèmes de détection d'intrusions

Un IDS a pour fonction d'analyser en temps réel ou différé les évènements en provenance des différents systèmes à travers le réseau, de détecter et de prévenir les attaques. Les IDS ont donc un rôle d'alarme (la comparaison avec une alarme anti-vol placée dans le hall d'une maison, qui détecte des mouvements ou des ouvertures de portes, correspond d'ailleurs assez bien). Les buts sont nombreux :

- ✓ Collecter des informations sur les intrusions ;
- ✓ Gestion centralisée des alertes ;
- ✓ Effectuer un premier diagnostic sur la nature de l'attaque permettant une réponse rapide et efficace ;
- ✓ Réagir activement à l'attaque pour la ralentir ou la stopper.

Malheureusement, on se rend bien compte aujourd'hui que malgré toutes les mesures et stratégies de sécurité qu'on peut mettre en place, les systèmes d'informations restent néanmoins vulnérables à certaines attaques ciblées ou à des intrusions. C'est pourquoi depuis quelques années, les experts de la sécurité parlent de plus en plus d'un nouveau concept à savoir la détection d'intrusion. L'étude de la détection d'intrusion nous permettra de mieux comprendre les systèmes de détection et de prévention d'intrusions et de voir comment ils arrivent à renforcer la sécurité en fermant les trous de sécurité laissés par les mesures classiques de sécurité, c'est ce que nous allons voir en détail dans la suite de notre travail.

II Les politiques de sécurité des systèmes d'information

II.1. Introduction

L'objet de la sécurité peut se définir comme une contribution à la préservation des forces, des moyens organisationnels, humains, financiers, technologiques et informationnels, dont s'est dotée une organisation pour la réalisation de ses objectifs.

Dans un système informatique, l'autorisation a pour but de ne permettre que les actions légitimes, c'est-à-dire à empêcher qu'un utilisateur puisse exécuter des opérations qui ne devraient pas lui être permises. Pour définir quelles sont les opérations autorisées et celles qui sont interdites, il faut établir une politique de sécurité.

Le standard européen des ITSEC (Information Technology Security Evaluation Criteria) définit une politique de sécurité comme étant " l'ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique " [7].

Une politique de sécurité doit prendre en considération les règlements qui doivent être appliqués ainsi que les menaces éventuelles dues à l'utilisation du système informatique.
Cette dernière comportera la motivation et la formation du personnel, la mise en place de mesures ainsi que par l'optimisation des solutions, consiste donc à concevoir une conduite générale de protection, d'organisation de la défense (démarche proactive) et d'élaboration de plans de réaction (démarche réactive).

Pour construire une politique de sécurité il faut :

- ✓ D'une part, définir un ensemble de propriétés de sécurité qui doivent être satisfaites par le système. Par exemple "une information classifiée ne doit pas être transmise à un utilisateur non habilité à la connaître" ;
- ✓ D'autre part, établir un schéma d'autorisation, qui présente les règles permettant de modifier l'état de protection du système. Par exemple "le propriétaire d'une information peut accorder un droit d'accès pour cette information à n'importe quel utilisateur".

II.1.1 Composantes d'une politique de sécurité

Depuis le début des années 2000, la prise en compte par les organisations des problèmes liés à la sécurité informatique s'est généralisée au moins dans les grandes structures. La sécurité est

de moins en moins une approche de technologies hétérogènes de sécurité. Elle est dorénavant appréhendée et traitée, comme un processus continu. Cette vision « processus » met en avant la dimension managériale de la sécurité qui vise à l'optimisation et la rationalisation des investissements, tout en assurant la continuité et l'efficacité des solutions de sécurité dans le temps [8].

Politiques de contrôle d'accès	Gestion des identités, des profils des utilisateurs, des permissions, des droits, etc.
Politique de protection	Prévention des intrusions et malveillances, Gestion des vulnérabilités, dissuasion, etc.
Politique de réaction	Gestion des crises, des sinistres, des plans de continuité, de reprise, de modification, d'intervention, de poursuite, etc.
Politique de suivi	Audit, évaluation, optimisation, contrôle, surveillance, etc.
Politique d'assurance	Politique de sensibilisation.

Tableau II-1 : Les différentes composantes d'une politique de sécurité

II.2. Les politiques et modèles de sécurités

Une politique de sécurité doit prendre en considération les règlements qui doivent être appliqués ainsi que les menaces éventuelles dues à l'utilisation du système informatique. Elle peut se développer dans trois directions distinctes : les politiques de sécurité physique, administrative et logique.

II.2.1 La politique de sécurité physique

Précise un ensemble de procédures et de moyens qui protègent les locaux et les biens contre des risques majeurs (incendie, inondation, etc.) et contrôlent les accès physiques aux matériels informatiques et de communication (gardiens, codes, badges, ...).

II.2.2 La politique de sécurité administrative

Définit un ensemble de procédures et moyens qui traitent de tout ce qui ressort de la sécurité d'un point de vue organisationnel au sein de l'entreprise. La structure de l'organigramme ainsi que la répartition des tâches (séparation des environnements de développement,

d'industrialisation et de production des applicatifs) en font partie. Les propriétés de sécurité recherchées visent, par exemple, à limiter les cumuls ou les délégations abusives de pouvoir, ou à garantir une séparation des pouvoirs.

II.2.3 La politique de sécurité logique

Elle Fait référence à la gestion du contrôle d'accès logique, lequel repose sur un triple service d'identification, d'authentification et d'autorisation. Elle spécifie qui a le droit d'accéder à quoi, et dans quelles circonstances. Ainsi, tout utilisateur, avant de se servir du système, devra décliner son identité (identification) et prouver qu'il est bien la personne qu'il prétend être (authentification). Une fois la relation établie, les actions légitimes que peut faire cet utilisateur sont déterminées par la politique d'autorisation.

Cette autorisation consiste à gérer et à vérifier les droits d'accès, en fonction des règles spécifiées dans la politique de sécurité. On dit qu'un sujet (entité qui demande l'accès, dite aussi entité active) possède un droit d'accès sur un objet (entité à laquelle le sujet souhaite accéder, dite aussi entité passive) si et seulement s'il est autorisé à effectuer la fonction d'accès correspondante sur cet objet.

Les droits d'accès peuvent être symboliquement représentés dans une matrice de droits d'accès dont les lignes représentent les sujets et les colonnes représentent les objets. Une cellule de la matrice contient donc les droits d'accès d'un sujet sur un objet. La matrice est gérée conformément aux règles définies dans la politique de sécurité.

D'une manière générale, les règles de la politique de sécurité sont spécifiées en terme de permissions (par exemple tout médecin a le droit d'accéder aux dossiers médicaux de ses patients) et d'interdictions (par exemple, les médecins n'ont pas le droit d'effacer de diagnostics déjà établis), mais aussi en terme d'obligations (les médecins sont obligés de conserver les dossiers médicaux pendant la durée fixée par la loi) [7] ;

II.3 Critères d'évaluation

Les premiers critères d'évaluation de la sécurité ont été définis aux États-Unis dans ce qui est couramment appelé le Livre Orange ou TCSEC (Trusted Computer System Evaluation Criteria). Ces critères, fondés à la fois sur des listes de fonctions de sécurité à remplir et sur les techniques employées pour la vérification, conduisent à classer les systèmes en sept catégories ou niveaux (D, C1, C2, B1, B2, B3, A1).

Pour chaque niveau, quatre familles de critères sont définies, traitant de la politique d'autorisation, de l'audit, de l'assurance et de la documentation :

- ✓ La politique d'autorisation stipule une politique précise à suivre en fonction des différents niveaux de certifications visés.
- ✓ Les critères d'audit précisent les fonctions requises en matière d'identification, d'authentification et d'audit des actions.
- ✓ Les critères d'assurance fixent des recommandations concernant des méthodes de conception et de vérification utilisées afin d'augmenter la confiance de l'évaluateur. Il s'agit de garantir que le système implémente bien la fonctionnalité qu'il prétend avoir.
- ✓ Les critères de documentation spécifient les documents qui doivent être fournis avec le produit lors de l'évaluation.

Les caractéristiques principales des différents niveaux définis par le livre orange sont ainsi :

- ✓ Jusqu'aux niveaux C1 et C2, le système peut utiliser une politique discrétionnaire (voir dans la suite de ce chapitre).
- ✓ Pour les niveaux B1, B2, et B3 le système utilise une politique obligatoire (voir dans la suite de ce chapitre).
- ✓ Un système classé A1 est fonctionnellement équivalant à un système classé B3, sauf qu'il est caractérisé par l'utilisation de méthodes formelles de vérification pour prouver que les contrôles utilisés permettent bien d'assurer la protection des informations sensibles.

Les TCSEC visent d'abord à satisfaire les besoins du DoD (Department of Defense) des États-Unis, privilégiant ainsi la confidentialité des données militaires. Par ailleurs, le manque de souplesse et la difficulté de leur mise en œuvre, ont conduit au développement de nouvelles générations de critères. À titre d'exemple abordons les critères adoptés par l'ex-Communauté Européenne (ITSEC, 1991), mais d'autres pays tels que le Canada (CTCPEC, 1993) et le Japon (JCSEC, 1992) ont également élaboré leurs propres critères d'évaluation.

Les ITSEC (Information Technology Security Evaluation Criteria) sont le résultat d'harmonisation de travaux réalisés au sein de quatre pays européens : l'Allemagne, la France, les Pays-Bas et le Royaume-Uni. La différence essentielle entre les TCSEC et les ITSEC réside dans la distinction entre fonctionnalité et assurance.

Une classe de fonctionnalité décrit les fonctions que doit mettre en œuvre un système tandis qu'une classe d'assurance décrit l'ensemble des preuves qu'un système doit apporter pour montrer qu'il implémente les fonctions qu'il prétend fournir [8].

II.4 Classifications des politiques de sécurités

La plupart des politiques de sécurité reposent sur les notions de sujets, d'objets et de droits d'accès.

- **Sujet :** Un sujet est une entité active, correspondant à un processus qui s'exécute pour le compte d'un utilisateur. Dans ce contexte, un utilisateur est soit une personne physique connue du système informatique et enregistrée comme utilisateur, soit un serveur, sorte de personne morale représentant des fonctions de service automatiques, tel que le serveur d'impression, serveur de base de données, serveur de messagerie, etc.
- **Objet :** Un objet est une entité considérée comme "passive" qui contient ou reçoit des Informations.
- **Droit d'accès :** À un instant donné, un sujet a un droit d'accès sur un objet si et seulement si le processus correspondant au sujet est autorisé à exécuter l'opération correspondant à ce type d'accès sur cet objet.

Les politiques de sécurité, ou plus précisément leurs schémas d'autorisation, se classent en deux grandes catégories :

- ✓ **Les politiques discrétionnaires** (ou **DAC** pour Discretionary Access Control).
- ✓ **Les politiques obligatoires** (ou **MAC** pour Mandatory Access Control).

Il existe également des variantes de ces politiques qui peuvent mieux s'adapter à des organisations particulières, comme les politiques basées sur la notion de rôles (ou RBAC pour Role-Based Access Control) ou encore sur la notion d'équipes (ou TMAC pour TeaM-based Access Control). Idéalement, il faut construire une politique de sécurité de telle sorte qu'aucune séquence valide d'applications des règles (du schéma d'autorisation) ne puisse amener le système dans un état tel qu'un objectif de sécurité soit violé, en partant d'un état initial sûr (on parle de politique de sécurité cohérente).

II.4.1 Les politiques discrétionnaires (DAC)

Dans le cas d'une politique discrétionnaire, les droits d'accès à chaque information sont manipulés librement par le responsable de l'information (généralement le propriétaire), à sa discrétion. Les droits peuvent être accordés par ce responsable à chaque utilisateur, à des groupes d'utilisateurs, ou bien aux deux. Ceci peut parfois amener le système dans un état d'insécurité (c'est-à-dire contraire aux objectifs de sécurité qui ont été choisis).

Prenons un exemple simple, reposant sur les mécanismes de protection d'Unix. Dans un tel système, les droits d'accès à un fichier sont définis et modifiables librement par l'utilisateur propriétaire du fichier (et donc par les processus qui s'exécutent pour son compte).

Supposons que le schéma d'autorisation se définisse (informellement) de la manière suivante : un utilisateur peut créer des fichiers dont il devient alors propriétaire ; le propriétaire d'un fichier peut décider quels utilisateurs sont autorisés à lire ses fichiers. D'autre part, supposons que la politique exige de respecter l'objectif suivant : les utilisateurs qui n'ont pas le droit de lire un fichier ne doivent pas pouvoir en connaître le contenu.

-
- Si s1 est un sujet s'exécutant pour le compte de l'utilisateur u1 propriétaire du fichier f1, il peut donner au sujet s2 (s'exécutant pour le compte d'u2) le droit de lecture sur f1 : ce que l'on note par (s1; f1; propriétaire) $\longrightarrow$ (s2; f1; lire).
- s2 peut créer un fichier f2 (dans lequel il peut donc écrire) sur lequel il peut donner le droit de lecture à s3 (s'exécutant pour le compte d'u3) :
  (s2; f2; créer) $\longrightarrow$ (s2; f2; écrire) et (s3; f2; lire)
- s2 peut alors recopier f1 dans f2 pour transmettre les informations de f1 à s3 à l'insu du propriétaire s1 :
  (s2; f1; lire) et (s2; f2; écrire) et (s3; f2; lire) $\longrightarrow$ (s3; c(f1); lire) où (c(f1) désigne une copie de f1).

Une politique discrétionnaire n'est donc applicable que dans la mesure où il est possible de faire totalement confiance aux utilisateurs et aux sujets qui s'exécutent pour leur compte. Une telle politique est par là même vulnérable aux abus de pouvoir provoqués par maladresse ou par malveillance. Ainsi, s'il est possible à un utilisateur d'accéder à certains objets ou d'en modifier les droits d'accès, il est possible qu'un cheval de Troie s'exécutant pour le compte de cet utilisateur (à son insu) en fasse de même. De plus, si un utilisateur a le droit de lire une information, il a (en général) le droit de la transmettre à n'importe qui [9].

II.4.2 les politiques obligatoires(MAC)

Comme énoncé précédemment les politiques obligatoires décrètent des règles pour contrôler les flots d'informations, afin de contrer le transfert illégal et les fuites. Ces politiques sont généralement des politiques multi-niveaux basées sur une classification des sujets et des objets imposée par une autorité centrale.

Les règles qui régissent les autorisations d'accès sont basées sur une comparaison de l'habilitation de l'utilisateur et de la classification de l'objet. Ces règles incontournables assurent que le système vérifie des propriétés générales de confidentialité ou d'intégrité, par exemple, un utilisateur sera autorisé à manipuler une information dans le système si l'utilisateur en question possède le droit de lecture sur l'information (contrôle discrétionnaire) et s'il est habilité à manipuler cette information (contrôle obligatoire).

II.4.3 Les politiques et modèles basés rôles « RBAC »

Le modèle RBAC (Rôle Based Access Contrôl) est principalement issu d'Internet afin de prendre en compte des applications déployées sur de vastes organisations ou des applications inter-organisations (Extranet par exemple).

En effet, les politiques obligatoires et notamment les politiques multi-niveaux sont trop contraignantes pour les systèmes informatiques des organisations, et leur utilisation est généralement limitée au domaine militaire. Les politiques discrétionnaires, quant à elles, confient les autorisations sur les objets à la discrétion de leurs possesseurs. Cependant, dans la plupart des organisations, les utilisateurs finaux d'une information n'en sont pas généralement les propriétaires et le contrôle d'accès est plutôt relatif aux fonctions et aux responsabilités des employés (leurs rôles). D'où l'avènement de l'idée de base de RBAC :

Il s'agit d'intercaler des rôles entre les utilisateurs et les permissions. D'un côté des permissions sont accordées aux rôles, de l'autre, les utilisateurs se voient affecter un ou plusieurs rôles. Ils obtiennent ainsi les permissions accordées aux rôles qu'ils jouent.

Au fil des années, différentes variantes du modèle RBAC ont été proposées afin d'introduire de nouveaux concepts, comme les sessions, les hiérarchies de rôles et les contraintes sur les rôles. Toutefois l'idée de base est toujours la même, le rôle est le concept central de la politique de sécurité.

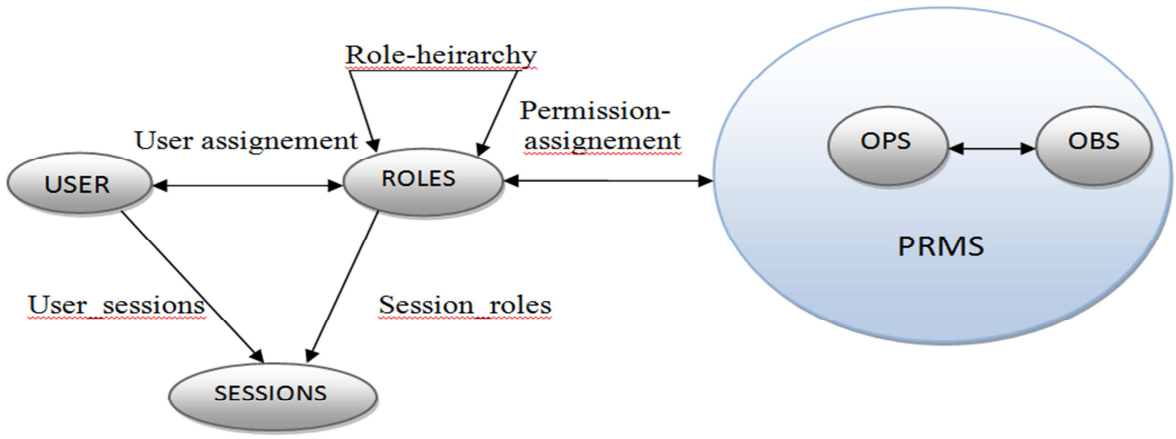

Figure II.1 : Le modèle RBAC

Par la suite, il conviendra de détailler les concepts utilisés dans le modèle RBAC : Les utilisateurs (USERS) : Ce terme fait en général référence à un être humain mais il peut aussi désigner des machines, networks ou des agents intelligents. Les rôles (ROLES) : Un rôle est une fonction d'un emploi dans une organisation faisant allusion aux autorités et aux responsabilités accordés aux utilisateurs.

Les opérations (OPS) : une opération représente l'image exécutable d'un programme. L'appel de cette dernière exécute des fonctions pour l'utilisateur. Par exemple, dans la protection d'un système de fichiers les opérations peuvent être lire, écrire, exécuter ; dans un système de gestion de bases de données, les opérations sont : insérer, supprimer, ajouter et mettre à jour. Les permissions symbolisées par PRMS sont matérialisées par des opérations effectuées sur les objets. PRMS⊆ OPS ×OBS. Comme le montre la figure, les utilisateurs sont assignés à des rôles via la relation UA / UA ⊆ USERS ×ROLES.

Par ailleurs, le côté dynamique du modèle est matérialisé par la notion de session. Une session est attribuée à un utilisateur qui, en l'activant, exerce un ou un ensemble de rôles qu'il assume. Un utilisateur peut ouvrir plusieurs sessions en même temps, cependant à un instant donné, un utilisateur exerce un seul rôle. C'est la notion de rôle actif. Le contrôle d'accès se déroule au cours d'une session. Un utilisateur a le droit d'exécuter sur les objets les seules opérations que son rôle activé lui autorise [9].

II.4.4 Le modèle OrBAC

Le contrôle d'accès basé sur l'organisation OrBAC (Organization-Based Access Control) a été présenté pour la première fois en 2003. Il reprend les principes de rôles des modèles du type RBAC, en offrant en plus la possibilité de modifier la politique de sécurité de façon dynamique en fonction du contexte.

Dans OrBAC, la possibilité d'exprimer des permissions, des obligations et des interdictions, qui dépendent de contextes est un élément qui va vers une plus grande expressivité.

L'abstraction des entités traditionnelles du contrôle d'accès (sujet, action, objet) en méta entités (rôle, activité, vue) permet d'élaborer une politique de sécurité à deux niveaux, un niveau concret et un niveau abstrait.

Le niveau abstrait sert à spécifier une politique de sécurité indépendamment de l'implantation qui en sera faite. En fin, le concept d'organisation, qui est central dans OrBAC, offre la

possibilité de définir une politique de sécurité de façon modulaire. On peut ainsi analyser l'interopérabilité d'organisations ayant chacune leur politique de sécurité en suivant une hiérarchie d'organisations.

Contrairement aux modèles DAC, les modèles MAC et RBAC tentent de structurer les sujets, soit en fonction de la confiance qu'on leur accorde (habilitation) soit en fonction de leurs rôles. En effet, la gestion et l'administration d'une politique de contrôle d'accès deviennent vite ardues si le système d'informations comporte un grand nombre de sujets, d'actions et d'objets. On voit ainsi apparaître l'idée qu'il peut exister d'un côté une forme de structuration des sujets. Et de l'autre la définition de l'ensemble des règles de contrôle d'accès. Ainsi, dans un modèle MAC, on s'attachera dans un premier temps à définir les niveaux de confiance, puis à attribuer des permissions en fonction de ces niveaux. Dans un modèle RBAC, on commencera par définir l'ensemble des rôles puis on leur accordera des privilèges.

II.4.4.1 Objectifs et avantages d'OrBAC

L'objectif d'OrBAC est de permettre la modélisation d'une variété de politiques de sécurité basées sur le concept de l'organisation. Pour arriver à ce but, et afin de réduire la complexité de gestion des droits d'accès, le modèle OrBAC repose sur quatre grands principes :

- ✓ L'organisation est l'entité centrale du modèle.
- ✓ Il y a deux niveaux d'abstraction (Les interactions d'OrBAC) :
  - **un niveau concret** : sujet, action, objet;
  - **un niveau abstrait** : rôle, activité, vue.
- ✓ La possibilité d'exprimer des permissions, des interdictions, et des obligations.
- ✓ La possibilité d'exprimer les contextes.

L'introduction d'un niveau abstrait organisationnel permet aussi la structuration d'entités comme on le voit sur la Figure 4 :
Ainsi dans OrBAC, un rôle est un ensemble de sujets sur lesquels sont appliquées les mêmes règles de sécurité. Identiquement, une activité est un ensemble d'actions sur lesquelles sont appliquées les mêmes règles de sécurité. Une vue est un ensemble d'objets sur lesquels sont appliquées les mêmes règles de sécurité.

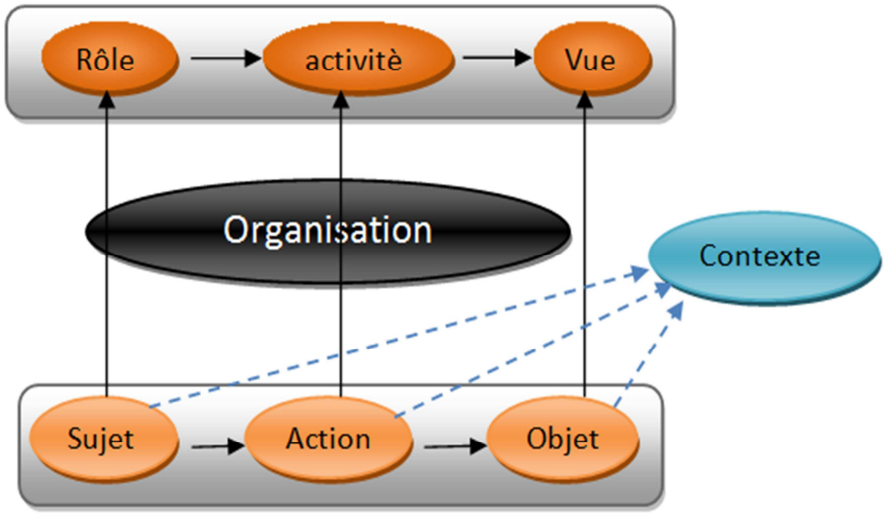

Figure II-2 Le modèle OrBAC.

Ce modèle de contrôle d'accès nous permet de structurer l'ensemble des sujets, l'ensemble des objets ainsi que l'ensemble des actions au sein d'un réseau social. La possibilité d'exprimer des permissions, des interdictions, et des obligations, peut être utile pour faire le filtrage au sein des catégories des utilisateurs définies dans un réseau social [9].

II.5 La mise en place d'une démarche sécuritaire

La mise en place d'une stratégie de sécurité repose sur des invariants qui, s'ils sont adoptés par l'ensemble de l'organisation, facilitent la mise en place et la gestion de la sécurité. Il s'agit des principes de base suivants :

- ✓ Principe de vocabulaire qui est une absolue nécessité de s'accorder, au niveau l'organisation, sur un langage commun de définition de la sécurité ;
- ✓ Principe de cohérence, car une accumulation d'outils sécuritaires n'est pas suffisante pour réaliser un niveau global et cohérent de sécurité. La sécurité d'un système d'information résulte de l'intégration harmonieuse des outils, mécanismes et procédures liés à la prévention, à la détection, à la protection et à la correction des sinistres relatifs à des fautes, à la malveillance ou à des éléments naturels ;
- ✓ Principe de volonté directoriale qui résulte directement de la considération de l'information comme ressource stratégique de l'entreprise. Il est donc de la responsabilité de ses dirigeants de libérer les moyens nécessaires à la mise en œuvre et à la gestion de la sécurité informatique ;

- ✓ Principe financier : le coût de la sécurité doit être en rapport avec les risques encourus.

Le budget consacré à la sécurité doit être cohérent vis-à-vis des objectifs de sécurité fixés :

- ✓ Principe de simplicité et d'universalité : les mesures de sécurité doivent être simples, souples, compréhensibles pour tous les utilisateurs et doivent s'appliquer à l'ensemble du personnel ;
- ✓ Principe de dynamicité : la sécurité doit être dynamique pour intégrer la dimension temporelle de la vie des systèmes et de l'évolution des besoins et des risques ;
- ✓ Principe de continuum : L'organisation doit continuer à fonctionner même après la survenue d'un sinistre.il faut disposer de procédures d'urgence et de reprise ;
- ✓ Principe d'évaluation, de contrôle et d'adaptation : il est impératif de pouvoir évaluer constamment l'adéquation des mesures de sécurité au regard des besoins effectifs de la sécurité. Cela permet de contrôler et de vérifier que les risques sont maitrisés de manière optimale dans un environnement dynamique et d'adapter si nécessaire les solutions de sécurité mis en œuvre. Des outils de type « tableau de bord » de la sécurité favorisent le suivi de la sécurité par une meilleure appréciation de la variabilité des critères de sécurité. L'adéquation du niveau de sécurité par rapport aux besoins de sécurité de l'entreprise, qui sont par nature évolutifs, est un souci constant du responsable sécurité.

Une organisation peut ainsi renoncer à mettre en œuvre un dispositif de secours (backup) de son centre informatique au regard de son coût récurent. En effet, ce coût peut s'avérer être très élevé en termes de ressources et de procédures à utiliser si l'on tient compte :

- ✓ De la probabilité du risque de destruction physique totale des infrastructures ;
- ✓ Coût des mesures :
  1. De surveillance et de détection (incendie, inondation, intrusion, etc.…..) ;
  2. De partitionnement des salles machines ignifugées à deux heures garanties, sur lesquelles sont réparties les applications critiques.

De ce fait, les risques résiduels (attentats, chutes d'avion, etc.) est le plus souvent jugé comme acceptable par les organes dirigeants des institutions [10].

II.5.1 Pourquoi les stratégies de sécurité ?

Les risques et menaces pesant constamment sur les systèmes d'information, une défaillance de la sécurité de ces dernières serait capable d'entrainer des conséquences irréversibles sur la réalisation des objectifs stratégiques de l'organisation ou vis-à-vis de ses collaborateurs ou engagements.

C'est pour cette raison que la stratégie de sécurité doit impérativement provenir des plus hautes sphères dirigeantes de l'organisme, en tant qu'instrument de gestion des risques sécurité du système d'information. La stratégie de sécurité des systèmes d'information traduit fortement la reconnaissance formelle de l'importance accordée par la direction de l'organisme à la sécurité de son ou ses systèmes d'information.

Face à ces menaces sur les systèmes d'information, les utilisateurs exigent une protection adaptée des informations et des services de traitement, d'archivage et de transport de l'information. La sécurité est immédiatement devenue l'une des dimensions essentielles de la stratégie de l'organisme et elle doit être prise en compte dès la conception d'un système d'information afin d'assurer la protection des biens, des personnes et du patrimoine de l'organisme.

Ainsi, la sécurité des systèmes d'information vise en particulier à protéger les composantes suivantes du patrimoine :

- ✓ Le patrimoine matériel, composé de biens matériels nécessaires au fonctionnement de ses activités et dont la détérioration pourrait interrompre, diminuer, ou altérer son activité ; ce patrimoine est essentiellement composé des technologies de l'information et de communication (serveurs, réseaux, postes de travail, téléphonie), mais aussi des procédures et applications logicielles traduisant les processus et les fonctions métiers de l'organisme ;
- ✓ Le patrimoine immatériel et intellectuel, composé de toutes les informations concourant au métier de l'organisme (données scientifiques, techniques, administratives) ;
- ✓ Les informations relatives aux personnes (physiques ou morales) avec qui l'organisme est en relation, dont la destruction, l'altération, l'indisponibilité ou la divulgation pourrait entrainer des pertes ou porter atteinte à son image de marque voire entrainer des poursuites judiciaires.

II.5 .2 Conditions de succès d'une démarche sécuritaire

Les conditions de succès de la réalisation d'une stratégie sécuritaire sont, entre autres :

- ✓ Une volonté directoriale, car il ne peut y avoir de succès d'une stratégie sans la volonté directoriale ;
- ✓ Une politique de sécurité simple, précise, compréhensible et applicable ;
- ✓ La publication et diffusion de la politique de sécurité ;
- ✓ Une gestion centralisée de la sécurité et une certaine automatisation des processus de sécurité ;
- ✓ Un niveau de confiance déterminé des personnes, des systèmes, des outils impliqués ;
- ✓ Du personnel sensibilisé et formé à la sécurité, possédant une haute valeur morale ;
- ✓ Des procédures d'enregistrement, de surveillance et d'audit assurant la traçabilité des événements pour servir de preuve en cas de nécessité ;
- ✓ La volonté d'éviter de mettre les systèmes et les données en situation dangereuse ;
- ✓ L'expression, le contrôle et le respect des clauses de sécurité dans les différents contrats;
- ✓ Une certaine éthique des acteurs et le respect des contraintes légales.

L'efficacité des mesures de sécurité d'un système d'information ne repose pas uniquement sur les outils de sécurité, ni sur le budget investi, mais sur la qualité de la stratégie définie, sur l'organisation mise en place pour la réaliser, l'évaluer, la faire évoluer en fonction des besoins. Cela nécessite une structure de gestion adéquate pour concevoir la stratégie, définir une politique de sécurité, gérer, spécifier des procédures et des mesures cohérentes, mettre en place, valider et contrôler.

Il est clair que la stratégie relève du domaine de la direction générale ; il faut donc comprendre que les prérogatives de la structure organisationnelle s'inscrivent dans un degré de délégation appropriée. Cette structure détermine le comportement, les privilèges et les responsabilités de chacun. Elle contribue à faire comprendre à l'ensemble des acteurs de l'organisation l'importance de la sécurité et du respect des règles de sécurité. Elle spécifie (en fonction de facteurs critiques de succès qui permettent d'atteindre les objectifs de l'entreprise) les mesures et les directives sécuritaires appropriées. Ces dernières doivent être relationnelles par rapport aux plans de l'entreprise et de l'informatique. Une vision stratégique de la sécurité globale de l'organisation est donc primordiale [10].

II.5.3 Réalisation d'une démarche sécuritaire

La stratégie de sécurité réside dans un compromis judicieux entre le coût des outils et des procédures à supporter pour pallier les risques réels qui pourraient affecter le patrimoine de l'entreprise et le coût des impacts de la réalisation des risques.

Il n'existe pas de stratégie prédéterminée ou générale, ni de recette pour définir une stratégie. Chaque contexte d'organisation, de scénario de risques ou d'environnement est particulier. On ne peut définir de règles générales qui déterminent quelles sont les stratégies ou solutions de sécurité à implanter pour maîtriser un risque donné.

La démarche sécuritaire se subdivise en trois grands axes :

- ✓ La stratégie globale d'entreprise ;
- ✓ La stratégie de sécurité ;
- ✓ La politique de sécurité.

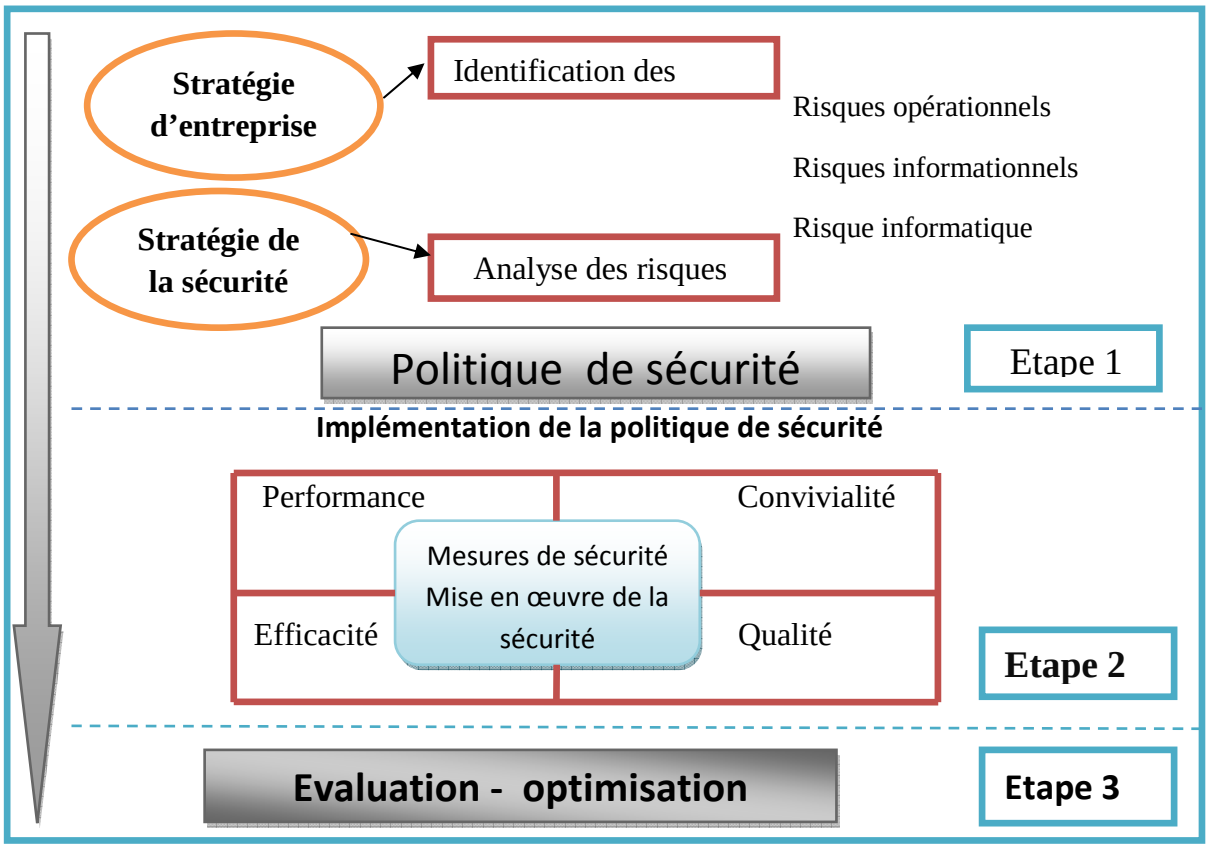

Figure II-3 : étapes de réalisation d'une démarche sécuritaire

La première étape stratégique consiste à identifier les valeurs de l'entreprise, leur niveau de vulnérabilité en fonction de menaces particulières et le risque de perte totale ou partielle de ces valeurs. À l'issue de cette analyse des risques, une vision de ce qui doit être protégé, contre qui et pourquoi est formulée sous la forme d'une politique de sécurité. Il s'agit alors de définir une véritable stratégie de protection et de gestion de la sécurité en fonction des besoins, valeurs et menaces réelles qu'encoure l'organisation. De la pertinence de l'analyse des risques dépendra l'identification correcte des moyens et des mesures de sécurité à mettre en œuvre pour protéger efficacement les ressources du système d'information.

L'étape suivante consiste à choisir puis à mettre en place les outils et les procédures nécessaires à la gestion des risques et à la sécurité des systèmes, services et données.

Enfin, il est impératif de contrôler non seulement l'adéquation des solutions de sécurité et leur cohérence les unes par rapport aux autres, mais également la pertinence de la politique de sécurité en fonction des risques et des moyens financiers et la cohérence des outils vis-à-vis de la politique. Une évaluation périodique, voire constante des mesures de sécurité en vue de leur optimisation, permet de répondre au mieux à l'évolution de l'environnement dans lequel elles s'inscrivent.

II.5.4 Méthodes et normes d'élaboration de démarches sécuritaires

La démarche sécuritaire traite de l'organisation de la sécurité, de l'inventaire des risques relatifs aux actifs informationnels, de la définition d'une architecture de sécurité, de l'établissement d'un plan de continuité.

Pour débuter une démarche sécuritaire, on s'appuie sur une méthode qui facilite l'identification des points principaux à sécuriser (notion de Check List). Dans un premier temps, il faut pouvoir identifier les risques afin d'identifier les parades à mettre en place et gérer le risque résiduel. Jusqu'à présent, la sécurité repose plus sur un ensemble reconnu de bonnes pratiques que sur une méthodologie unique.

Diverses méthodes propriétaires comme des normes internationales existent et peuvent servir de guide à l'élaboration d'une politique de sécurité. Elles sont utilisées plus ou moins complètement et le plus souvent adaptées à un contexte d'analyse.

Les méthodes préconisées par le Clusif (Club de la Sécurité de l'Information Français) sont le MARION (Méthode d'Analyse des Risques Informatiques et Optimisation par Niveau) et MEHARI (Méthode Harmonisée d'Analyse des Risques).

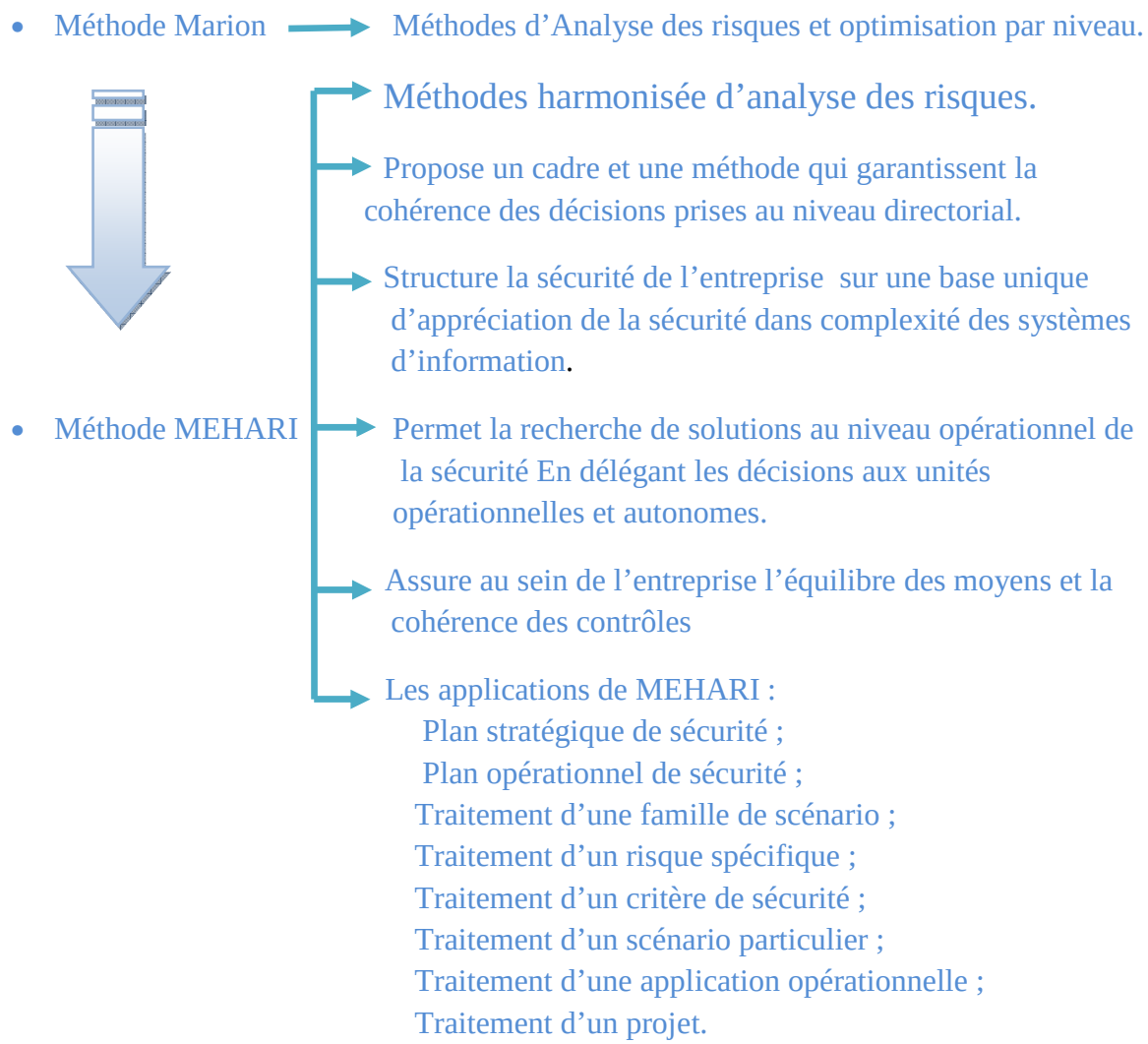

Figure II-4: les méthodes préconisées par le Clusif

Au-delà de l'aide à l'analyse des vulnérabilités et des risques, Méhari permet d'avoir une vision globale et stratégique de la problématique de la sécurité des entreprises, par la définition d'un plan stratégique de sécurité à partir duquel des plans opérationnels pourront être définis. Les différents niveaux de la sécurité sont ainsi appréhendés. Les vues stratégiques, tactiques et opérationnelles ainsi que les mesures spécifiques à leurs réalisations sont distinguées.

La méthode d'analyse des risques Méhari se veut adaptable, évolutive et compatible avec la norme ISO 17799.

Par ailleurs, la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) propose une méthode largement documentée, présentée et téléchargeable sur son site (http://www.ssi.gouv.fr). Dénommée Ebios (Expression des besoins et identification des objectifs de sécurité), cette méthode adoptée par les administrations françaises, permet de spécifier les objectifs de la sécurité des organisations, pour répondre à des besoins déterminés. Elle facilité largement l'appréhension du contexte de sécurité et constitue une véritable aide à la définition des objectifs et des politiques de sécurité. Cela peut conduire à remplir le document « Fiche d'Expression Rationnelle des Objectifs de Sécurité (Feros) » pour ce qui concerne toutes les ressources classées « défense », afin de déterminer au mieux les mesures de sécurité nécessaires à leur protection.

Il existe également diverses directives nationales : allemandes issu du Bundesamt für Sicherheit Informationstechnik, canadiennes du CST (Centre de la Sécurité des Télécommunications), américaines issues du NSI (National Standards Institue) des Etats-Unis, par exemple, qui traitent des politiques de sécurité [11].

II.5.4.1 Normes internationales ISO/IEC 17799

L'origine de la norme ISO 17799 adoptée par l'ISO à la fin de l'année 2000 est la norme BS 7799 élaborée par l'association de normalisation britannique en 1995. Avant d'être reconnue comme une méthode de référence, la norme internationale ISO 17799 a tout d'abord été contestée du fait de sa procédure accélérée de normalisation : elle n'avait pas été révisée par les états membres avant d'être publiée et n'avait donc pas tenu compte des savoir-faire et autres méthodes existants dans d'autres pays.

L'adoption par le marché de la norme ISO a été favorisée par le fait que certaines compagnies d'assurance demandent l'application de cette norme afin de couvrir les cyber-risques.

Basée sur la gestion des risques, la norme propose un code de pratique pour la gestion de la sécurité et identifie des exigences de sécurité sans toutefois spécifier la manière de les réaliser. On peut ainsi considérer cette norme tour à tour comme un référentiel contribuant à la définition d'une politique de sécurité, comme une liste de points de risques à analyser (Check List), comme une aide à l'audit de sécurité en vue ou non d'une procédure de certification ou encore, comme un point de communication sur la sécurité. Diverses interprétations et réalisations de cette norme sont possibles.

Son intérêt réside dans le fait que la norme aborde les aspects organisationnels, humains, juridiques et technologiques de la sécurité en rapport aux différentes étapes de conception, mise en œuvre et maintien de la sécurité.

Elle traite de dix domaines de sécurité, de 36 objectifs de sécurité et de 127 points de contrôle.

Une nouvelle version de cette norme (lSO/IEC 17799 : 2005) a été éditée en juillet 2005, elle adjoint aux dix domaines de sécurité préalablement identifiés de nouveaux paragraphes qui concernent l'évaluation et l'analyse des risques, la gestion des valeurs et des biens ainsi que la gestion des incidents. On remarque toute l'importance accordée à la dimension managériale de la sécurité dans la nouvelle version [11].

La norme propose plus d'une centaine de mesures possibles réparties en **10 chapitres:**

1. Politique de sécurité
2. Organisation de la sécurité
3. Classification et contrôle des actifs
4. Sécurité et gestion de ressources humaines
5. Sécurité physique et environnementale
6. Exploitation et gestion des systèmes réseaux
7. contrôle d'accès
8. développement des maintenances des systèmes
9. Continuité des services
10. Conformité

Figure II-5: Domaines de sécurité de la norme ISO 17799 2000.

1. **Politique de sécurité :** Ce chapitre mentionne notamment la nécessité pour l'entreprise de disposer d'une politique de sécurité et d'un processus de validation et de révision de cette politique.

2. **Organisation de la sécurité :** Ce chapitre comporte 3 parties. Une partie traite de la nécessite de disposer au sein de l'entreprise d'une organisation dédiée à la mise en place et au contrôle des mesures de sécurité en insistant sur :

- ✓ L'implication de la hiérarchie et sur la coopération qui devrait exister entre les différentes entités de l'entreprise ;
- ✓ La désignation de propriétaires de l'information, qui seront responsables de leur classification ;
- ✓ L'existence d'un processus pour la mise en place de tout nouveau moyen de traitement de l'information.

Une deuxième partie traite des accès aux informations de l'entreprise par une tierce partie. Ces accès doivent être encadrés par un contrat qui stipule les conditions d'accès et les recours en cas de problèmes.

Une troisième partie indique comment traiter du cas où la gestion de la sécurité est externalisée (Outsourcing).

3. **Classification et contrôle des actifs :** Ce chapitre traite de la nécessité de répertorier l'ensemble des informations (ou types d'information) de l'entreprise et de déterminer leur classification. La mise en place d'une classification de l'information doit s'accompagner de la rédaction de guides pour la définition des procédures de traitement de chaque niveau de classification.

4. **Sécurité et gestion de ressources humaines :** Ce chapitre mentionne trois types de mesures :
   - ✓ Lors du recrutement de personnel, il est tout aussi important d'enquêter sur le niveau de confiance que l'on peut accorder aux personnes qui auront accès à des informations sensibles que de mentionner dans les contrats d'embauche des clauses spécifiques à la sécurité comme une clause de confidentialité ;
   - ✓ Une sensibilisation à la sécurité doit être proposée à toute personne accédant à des informations sensibles (nouvel arrivant, tierce partie) ;
   - ✓ L'ensemble du personnel doit être informé de l'existence et du mode d'emploi d'un processus de remontée d'incidents.

5. **Sécurité physique et environnementale :** Ce chapitre traite de toutes les mesures classiques pour protéger les bâtiments et les équipements:
   - ✓ Délimitation de zone de sécurité pour l'accès aux bâtiments (attention aux accès par les livreurs) ;

- ✓ Mise en place de sécurité physique comme la lutte contre l'incendie ou le dégât des eaux ;
- ✓ Mise en place de locaux de sécurité avec contrôle d'accès et alarmes, notamment pour les salles machines ;
- ✓ Mise en place de procédures de contrôle pour limiter les vols ou les compromissions ;
- ✓ Mise en place de procédures pour la gestion des documents dans les bureaux.

6. **Exploitation et gestion des systèmes réseaux :** Ce chapitre traite des points suivants :
   - ✓ Rédiger et mettre à jour l'ensemble des procédures d'exploitation de l'entreprise (que ce soit pour de l'exploitation réseau, système ou sécurité) ;
   - ✓ Rédiger et mettre à jour les critères d'acceptation de tout nouveau système ;
   - ✓ Prévoir un planning pour l'achat de composants ou matériels pour éviter toute interruption de service ;
   - ✓ Mettre en place un certain nombre de politique organisationnelle et technique (anti-virus, messagerie, diffusion de document électronique en interne ou vers l'extérieur, sauvegarde et restauration, etc..).
7. **Contrôle d'accès :** Ce chapitre comprend beaucoup de propositions de mesures par rapport aux autres chapitres. Sans être exhaustif, on peut cependant retenir :
   - ✓ La nécessité pour l'entreprise de disposer d'une politique de contrôle d'accès (qui a droit à quoi et comment il peut y accéder) ;
   - ✓ La mise en place d'une gestion des utilisateurs et de leurs droits d'accès sans oublier la révision de ces droits (gestion de droits, gestion de mot de passe ou plus généralement d'authentifiant) ;
   - ✓ La responsabilité des utilisateurs face à l'accès aux informations (ne pas divulguer son mot de passe, verrouiller son écran quand on est absent par exemple) ;
   - ✓ Des propositions de mesures pour mettre en œuvre la politique de contrôle d'accès comme l'utilisation de la compartimentation de réseaux, de firewalls, de proxis, ..., la limitation horaire d'accès, un nombre d'accès simultanés limité, etc.… ;
   - ✓ La mise en place d'un système de contrôle de la sécurité et de tableaux de bord.
   - ✓ L'existence et la mise en place de procédures concernant le télétravail.

8. **Développement des maintenances des systèmes :** Ce chapitre, de la même manière que précédemment, propose des mesures incontournables comme des exemples de mise en œuvre. Sans être exhaustif, on peut retenir :
   - ✓ La nécessité d'intégrer les besoins de sécurité dans les spécifications fonctionnelles d'un système ;
   - ✓ Des conseils de développement comme la mise en place d'un contrôle systématique des entrées sorties au sein d'un programme ;
   - ✓ Des propositions d'intégration de services de sécurité comme le chiffrement, la signature électronique, la non-répudiation, ce qui nécessiterait pour l'entreprise la définition d'une politique d'usage et de contrôle d'outils à base de cryptographie ainsi qu'une politique de gestion des clés associées ;
   - ✓ La mise en place de procédures pour l'intégration de nouveaux logiciels dans un système déjà opérationnel ;
   - ✓ La mise en place d'une gestion de configuration.

9. **Continuité des services :** Ce chapitre traite de la nécessité pour l'entreprise de disposer de plans de continuité ainsi que de tout le processus de rédaction, de tests réguliers et de mise à jour de ces plans.

10. **Conformité :** Ce chapitre traite pour l'essentiel de deux points :
    - ✓ La nécessité pour l'entreprise de disposer de l'ensemble des lois et règlements qui s'appliquent aux informations qu'elle manipule et des procédures associées ;
    - ✓ La mise en place de procédures pour le déroulement d'audit de contrôle.

On peut donc noter que le contenu de l'ISO 17799 est à la fois un ensemble de mesures techniques et organisationnelles que l'entreprise devrait mettre en place pour gérer de manière sécurisée ses informations mais aussi un ensemble de propositions de solutions comme l'utilisation de firewall ou la composition des mots de passe (8 caractères, des caractères alphanumériques,...) [11].

Par conséquent il est très intéressant de s'inspirer de cette norme pour s'informer sur les mesures qu'une entreprise peut mettre en place pour gérer la sécurité de ses informations. Par contre comme il n'existe pas encore de référence qui permette de situer une entreprise sur une

échelle de gestion allant d'une mauvaise gestion à la gestion idéale, il est aujourd'hui très difficile d'apprécier le respect de cette norme par une entreprise.

III Les Systèmes de Protection contre les Intrusions

Introduction

L'objectif de cette partie est de présenter le concept d'IDS (Intrusion Detection System) et d'IPS (Intrusion Prevention System). Il s'agit de techniques permettant de détecter les intrusions et éventuellement de les prévenir. Ces techniques sont utilisées en association avec tous les éléments d'une politique de sécurité.

En effet de plus en plus d'entreprises subissent des attaques qui peuvent entraîner des pertes conséquentes. Le besoin des entreprises en sécurité informatique est de plus en plus important, et un élément essentiel d'une bonne politique de sécurité est l'utilisation d'un IDS.

Notons qu'un IDS ne remplace, en aucun cas, un pare-feu ou tout autre mécanisme de sécurisation des systèmes d'information. Cependant il renforce la sécurité en ajoutant une couche de sécurité et permettant ainsi la mise en place d'une défense en profondeur sur l'architecture réseau.

Nous présenterons ensuite le concept d'IDS, les différents types d'IDS, leur mode de fonctionnement…

Nous verrons alors que ces outils ont certaines limitations en présentant quelques méthodes de contournement d'un IDS.

Enfin, on parle de plus en plus d'IPS. A l'avantage des IDS, qui n'ont qu'un rôle de reconnaissance et de signalisation des intrusions, les IPS constituent un système de Prévention/Protection contre ces intrusions.

III.1 Concepts des systèmes de protection contre les intrusions

III.1.1 Définition et principes de fonctionnement

On entend par systèmes de protection contre les intrusions les logiciels ou appliance (c'est-à-dire des boîtes noires) capables de protéger les réseaux et systèmes informatiques contre les intrusions. Comme nous l'avons mentionné précédemment, ces systèmes se basent surtout sur les différentes techniques de détection d'intrusions qui existent aujourd'hui.

Ainsi, il existe des systèmes de détection d'intrusions dits « passifs » qui a été déployés de

plus en plus largement et qui sont talonnées aujourd'hui par des systèmes dits « actifs » de prévention d'intrusions. La recherche et les découvertes en détection et prévention d'intrusions sont toujours d'actualité, notamment en raison des évolutions rapides et incessantes des technologies des systèmes d'information.

La détection d'intrusions peut se définir comme l'ensemble des pratiques et des mécanismes utilisés, qui permettent de détecter les actions visant à compromettre la confidentialité, l'intégrité ou la disponibilité d'une ressource. La notion d'intrusion est à considérer au sens large et comprend les notions d'anomalies et d'usage abusif des ressources.

D'un côté, il y a les systèmes de détection d'intrusions (IDS pour Intrusion Detection System) qui sont des mécanismes destinés à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Ils permettent ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

Dans le processus de détection procède à l'examen d'intrusion manuelle, un analyste humain procède à l'examen de fichiers de logs (journaux) à la recherche de tout signe suspect pouvant indiquer une intrusion. Un système qui effectue une détection d'intrusion automatisée est appelé système de détection d'intrusion (IDS). Lorsqu'une intrusion est découverte par un IDS, les actions typiques qu'il peut entreprendre sont par exemple d'enregistrer l'information pertinente dans un fichier ou une base de données, de générer une alerte par e-mail ou un message sur un pager ou un téléphone mobile. Déterminer quelle est réellement l'intrusion détectée et entreprendre certaines actions pour y mettre fin ou l'empêcher de se reproduire, ne font généralement pas partie du domaine de la détection d'intrusion. Cependant, quelques formes de réaction automatique peuvent être implémentées par l'interaction de l'IDS et de systèmes de contrôle d'accès comme les pare-feu **[12]**.

Le diagramme suivant illustre le fonctionnement d'un IDS :

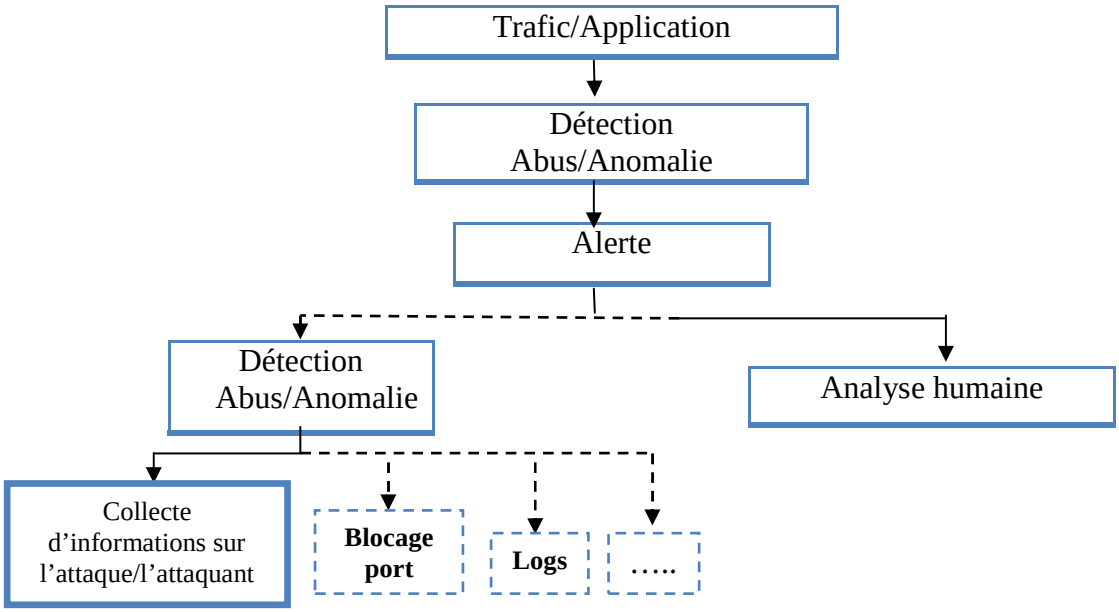

Figure III-1 : fonctionnement d'un IDS

D'un autre côté, il y a les systèmes de prévention d'intrusions (IPS pour Intrusion Prevention System) qui sont des mécanismes ayant pour but d'anticiper et de stopper les attaques. La prévention d'intrusion est appliquée par quelques IDS récents et diffère des techniques de détection d'intrusion décrites précédemment. Au lieu d'analyser les logs du trafic, c'est-à-dire découvrir les attaques après qu'elles se soient déroulées, la prévention d'intrusion essaie de prévenir ces attaques. Là où les systèmes de détection d'intrusion se contentent de donner l'alerte, les systèmes de prévention d'intrusion bloquent le trafic jugé dangereux.

Le principe de fonctionnement d'un IPS est symétrique à celui d'un IDS (IDS hôte, IDS réseau et hybrid IDS), ajoutant à cela l'analyse des contextes de connexion, l'automatisation d'analyse des logs et la coupure des connexions suspectes.

Contrairement aux IDS classiques, aucune signature n'est utilisée pour détecter les attaques. Avant toute action, une décision en temps réel est exécutée (c'est-à-dire que l'activité est comparée à un ensemble de règles). Si l'action est conforme à l'ensemble de règles, la permission de l'exécuter sera accordée et l'action sera exécutée. Si l'action est illégale (c'est-à dire que si le programme demande des données ou veut les changer alors que cette action ne lui est pas permise), une alarme est donnée. Dans la plupart des cas, les autres détecteurs du

réseau (ou une console centrale) en seront aussi informés dans le but d'empêcher les autres ordinateurs d'ouvrir ou d'exécuter des fichiers spécifiques.

Plusieurs stratégies de prévention d'intrusion existent :

- **Host-based memory and process protection** : qui surveille l'exécution des processus et les tue dès lors qu'ils ont l'air dangereux (buffer overflow). Cette technologie est utilisée dans les KIPS (Kernel Intrusion Prevention System).
- **Session interception** : (ou session sniping) qui termine une session TCP avec la commande TCP Resest (« RST »). Ceci est beaucoup utilisé dans les NIPS (Network Intrusion Pevention System).
- **Gateway intrusion detection** : si un NIPS est placé en tant que routeur, il bloque le trafic ou envoie des messages aux autres routeurs du réseau pour modifier adéquatement leurs listes d'accès pour bloquer les sources jugées agressives **[13]**.
  Le diagramme ci-après illustre le fonctionnement d'un IPS :

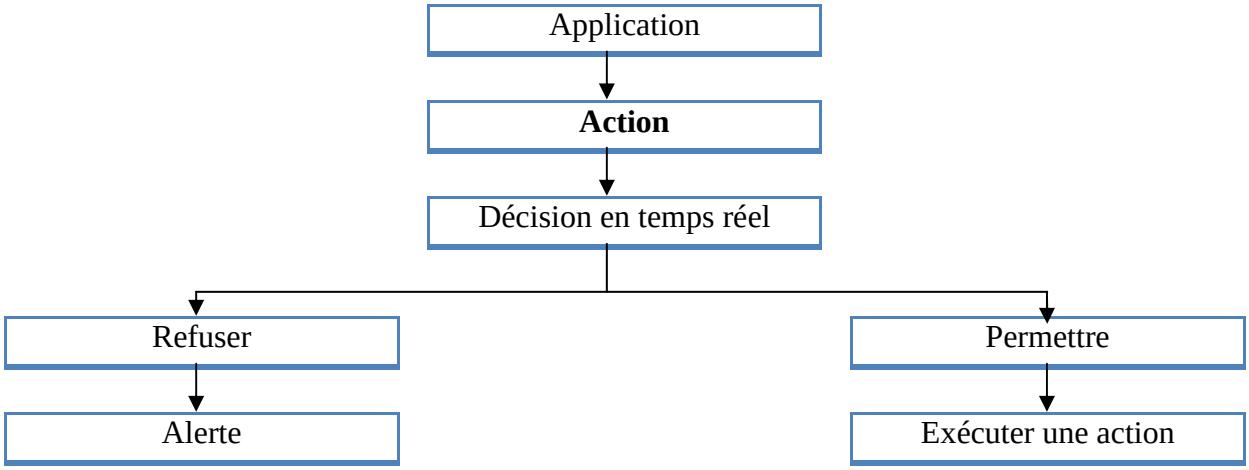

Figure III-2: Fonctionnement d'un IPS

III.1.2 Avantages des systèmes de protection contre les intrusions

En profitant des bugs logiciels, en exploitant les faiblesses des protocoles et en piratant les mots de passe, les pirates peuvent rechercher et exploiter des portes ouvertes dans les lignes de défense d'un réseau d'entreprise.

Or ces portes peuvent être fermées par un système de détection ou de prévention d'intrusions :

- ✓ Détection précise des attaques,
- ✓ Arrêt des attaques,
- ✓ Simplification de la gestion de la sécurité,

- ✓ Documentation appropriée (journaux détaillés),
- ✓ Flexibilité requise pour respecter les règles de sécurité,
- ✓ Double vérification (après celle des pare-feux mal configurés),
- ✓ Vérification de la bonne application des règles de sécurité,
- ✓ Interception des attaques que les pare-feu laissent passer de manière légitime,
- ✓ Interception des tentatives infructueuses,
- ✓ Interception des piratages venant de l'intérieur,
- ✓ Détection des attaques anormales lancées depuis un terminal inoccupé,
- ✓ Détection de failles pouvant être exploitées par des intrus,
- ✓ Documentation fournie avant, pendant et après une attaque.

Les systèmes de protection contre les intrusions peuvent être déployés au niveau des points d'accès, derrière les pare-feu, sur divers segments et serveurs ou à différents emplacements où ils feront office d'agents de sécurité du périmètre. En surveillant le trafic pour protéger les systèmes des attaques internes et externes sur le réseau, ces systèmes détectent et arrêtent les pirates qui tentent de s'introduire dans les réseaux. Les méthodes de détection incluent l'utilisation de signatures d'attaque, la vérification d'anomalies de protocoles et d'actions inhabituelles.

Les pirates exploitent constamment de nouvelles failles. En trouvant d'autres méthodes pour accéder à votre réseau interne, ils lancent de nouvelles attaques sophistiquées qui ne suivent pas un schéma défini. Tandis que la détection basée sur les signatures est un système robuste, la détection des anomalies de protocoles peut être utilisée pour identifier les diverses attaques qui n'observent pas les scénarii habituels.

Ainsi, un grand nombre d'attaques réseau peuvent être déjouées grâce aux systèmes de détection et de prévention des intrusions. Ce sont des outils qui demandent une configuration fine et une analyse régulière des fichiers journaux.

Les systèmes IDS et IPS appliquent des méthodes similaires lorsqu'ils essaient d'intercepter des intrus ou des attaques sur le réseau. Ils ont généralement une base de données de signatures, qui peut être régulièrement mise à jour à mesure que de nouvelles menaces sont identifiées.

Les administrateurs de sécurité déploient des agents ou des capteurs, logiciels ou matériels, en des points clés de leur réseau. Généralement en périphérie ou sur les passerelles vers d'autres

réseaux en des endroits où le trafic réseau converge, et qui ont été identifiés comme étant des points de détection et d'interception stratégiques. Les placer derrière les pare-feu est toujours un bon choix. Les capteurs à distance envoient alors leurs rapports à une machine centrale qui gère les règles du système. Il stocke les données dans un seul endroit afin de faciliter l'enregistrement, les alertes et l'élaboration de compte-rendu.

Les capteurs IDS/IPS déployés sur le réseau examinent les flux de données qui transitent à leur niveau, puis analysent le trafic et le comparent aux signatures contenues dans leurs bases de données. Lorsqu'une correspondance est trouvée, le système active et effectue les tâches définies par l'administrateur: interrompre la connexion TCP, alerter l'équipe de sécurité ou stocker les informations dans un journal ou log en vue d'une analyse ultérieure.

Naturellement, les performances du réseau doivent être évaluées avant de déployer un capteur.

Il est également possible de déployer différents types de systèmes pour offrir au réseau plusieurs niveaux de sécurité. Par exemple, en combinant une solution matérielle (appliance) pour contrôler les points d'entrée/sortie du réseau avec des logiciels basés sur hôte pour surveiller les machines critiques.

III.2 Typologies et familles des systèmes de protection contre les intrusions

III.2.1 Typologies des systèmes de protection contre les intrusions

La caractérisation des différents systèmes de protection contre les intrusions permet de les différencier suivant un certain nombre de caractéristiques. Cette caractérisation a conduit à la classification terminologique présentée dans la figure suivante **[14]** :

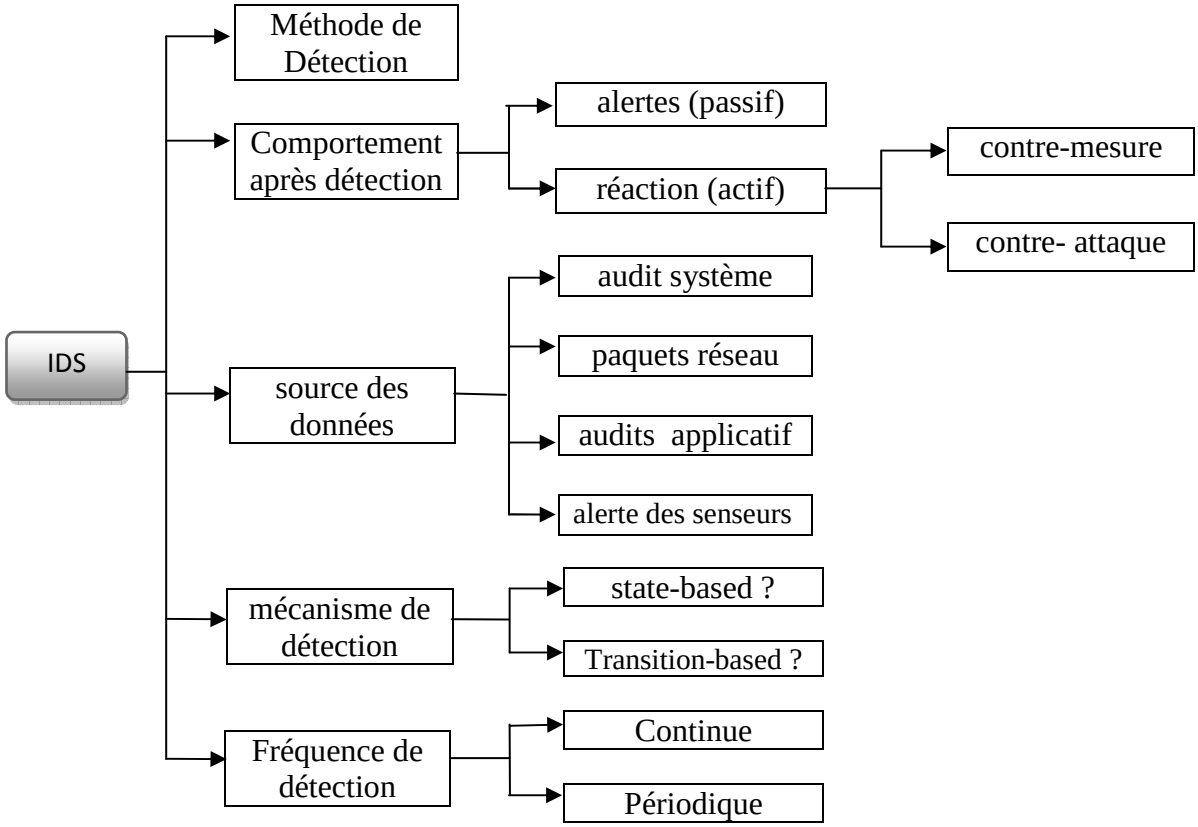

Figure III-3 : Classification terminologique des systèmes de protection contre les intrusions

Dans un premier temps, on peut faire une distinction assez fondamentale sur la méthode de détection utilisée par les systèmes de protection contre les intrusions. Il existe deux grandes catégories de méthodes de détection:

- ✓ Celles basées sur une approche comportementale (exemple l'analyse statistique, l'analyse bayésienne, les réseaux neuronaux).
- ✓ Et celles basées sur une approche par scénarii (exemple la recherche de signatures ou le pattern matching).

Globalement, les approches comportementales visent à reconnaître un comportement anormal, que ce soit par rapport à une définition du comportement normal ou anormal fournie au système de détection d'intrusion (exemple une spécification de protocole de communication) ou par rapport à une modélisation des comportements normaux ou anormaux apprise à partir d'une observation préalable du système (en salle blanche, ou tout simplement en réel). Dans le cadre d'une approche comportementale, l'apprentissage semble donc possible, tout comme la possibilité de détecter des attaques inconnues au moment de la conception de l'IDS, à condition qu'elles génèrent des anomalies perceptibles dans le fonctionnement normal.

Par contre, dans une approche par scénarii, les systèmes de protection contre les intrusions s'appuient sur une base de connaissance préexistante décrivant les comportements normaux ou anormaux et utilise cette connaissance pour la reconnaissance des évènements produits par des actions d'intrusions dans le système informatique qu'ils observent. Cette méthode implique donc la constitution et la mise à jour régulière d'une base de connaissance référençant les différentes attaques connues susceptibles d'être mises en œuvre dans un système informatique. C'est à partir de ces informations, affinées par l'administrateur en fonction du système surveillé, que les systèmes de protection contre les intrusions identifient les éventuelles attaques ayant lieu dans les systèmes informatiques.

Dans cette approche, les systèmes de protection contre les intrusions se focalisent donc sur l'identification des utilisations abusives (misuse). Une autre mise en œuvre conforme à la terminologie mais originale dans la pratique de cette approche de détection par scénarii consiste à constituer une base de connaissance des comportements permis dans le système (et non des comportements abusifs) pour configurer les actions de détection (des utilisations normales en quelque sorte).

Dans un second temps, on peut aussi comparer les systèmes de protection contre les intrusions en fonction du mode de fonctionnement des mécanismes de détection qu'ils mettent en œuvre.

De manière générale, un système de protection contre les intrusions 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, les transferts de droits, etc.).

III.2.2 Familles des systèmes de protection contre les intrusions

Selon l'endroit qu'ils surveillent et ce qu'ils contrôlent (les 'sources d'information'), plusieurs familles principales d'IDS et IPS sont usuellement distinguées.

III.2.2.1 Les IDS

Tout d'abord, IDS signifie ‘‘Intrusion Detection System’’. 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.

Pour présenter le concept d'IDS, nous allons tout d'abord présenter l'architecture des IDS, apprêt les différentes sortes d'IDS, chacun intervenant à un niveau différent.

Nous étudierons ensuite leur mode de fonctionnement, c'est à dire les modes de détection utilisés et les réponses apportées par les IDS. Enfin, nous détaillerons les points forts et les points faibles des IDS.

Il existe plusieurs endroits stratégiques où il convient de placer un IDS.

Le schéma suivant illustre un réseau ainsi que les positions que peut y prendre une IDS :

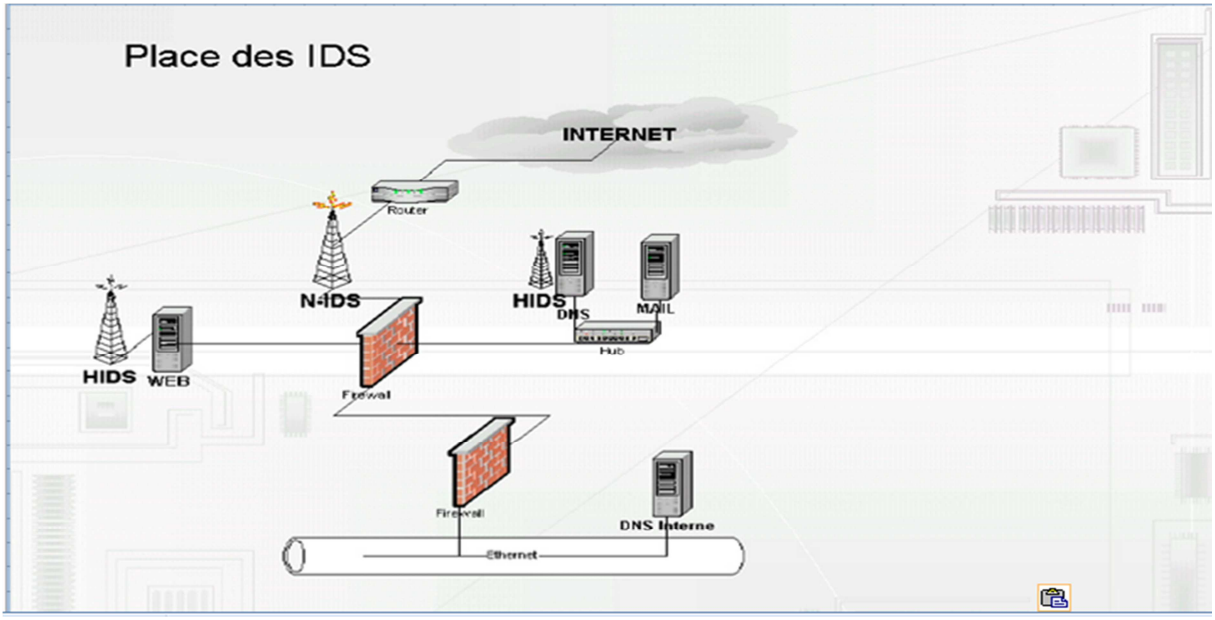

Figure III-4 : Emplacement de l'IDS au sein d'un réseau.

III.2.2.1.1 L'architecture des IDS

La majorité des systèmes de détection d'intrusion peuvent être décrits en termes de trois composants fonctionnels fondamentaux :

- **La source d'informations**: (sonde) Les différentes sources des évènements utilisées pour déterminer les intrusions qui ont eu lieu. Ces sources peuvent être fournies par les différents niveaux du système d'information : les réseaux, les hôtes, et les applications.
- **L'analyse**: La partie du système de détection d'intrusions qui réellement organise et

donne un sens aux évènements dérivés des sources d'informations, décidant quand ces évènements indiquent que des intrusions se produisent ou ont déjà eu lieu. Les principales approches communes d'analyse sont : détection d'abus (The misuse detection) ou encore dite approche par scénarios et détection d'anomalie (Anomaly detection) ou encore dite approche comportementale qui seront expliquées par la suite.

- **La réponse**: L'ensemble de contre-mesures que le système prend une fois qu'il détecte des intrusions. Celles-ci sont typiquement groupées dans des mesures actives et passives, les mesures actives comportent une certaine interposition automatisée de la part du système, alors que les mesures passives rapportent des résultats issus de l'analyse aux responsables, qui sont alors prévenus pour agir et prendre une action basée sur ces rapports.

III.2.2.1.1.1 Architecture centralisé

Une certaine disposition permettra de contrôler tous les événements à partir d'une console centrale, analyser, et décider des mesures à entreprendre. Différents modèles d'IDS (qui seront abordés plus loin) peuvent être utilisés dans un même réseau à différents points stratégiques, afin de récolter les informations en provenance des différents IDS et les traiter à un point central. En cas de doutes, des actions peuvent être entreprises à partir du même point d'analyse **[12]**.

III.2.2.1.1.2 Architecture distribuée

- **Architecture distribuée partiellement**: Cette disposition permet de décharger le serveur (le point central d'analyse et de traitement) de l'ensemble des tâches. Une hiérarchie est mise en place. Chaque 'sous partie' ou bien sous réseau est géré par un point local. Les 'conclusions' et les rapports sont communiqués à un nœud d'ordre supérieur hiérarchiquement qui transmet ses conclusions au nœud suivant et ainsi de suite. Les mesures sont prises par la console de niveau supérieur.
- **Architecture distribuée totalement**: Cette disposition est adoptée dans le cas des réseaux de grande taille. Dans ce cas le réseau est décomposé en plusieurs sous-réseaux, chacun d'entre est géré par son propre IDS. Les tâches d'audits et d'analyses sont prises au niveau local.

III.2.2.1.2 Les différentes sortes d'IDS

Les différents IDS se caractérisent par leur domaine de surveillance. Celui-ci peut se situer au niveau d'un réseau d'entreprise, d'une machine hôte, d'une application…

Nous allons tout d'abord étudier la détection d'intrusion basée sur l'hôte, puis basée sur une application, avant de nous intéresser aux IDS réseaux, NIDS et NNIDS (Network IDS et Node Network IDS) et on termine avec les IDS hybrides.

III.2.2.1.2.1 Le Host IDS

Les systèmes de détection d'intrusion basés sur l'hôte ou HIDS (Host IDS) analysent exclusivement l'information concernant cet hôte. Comme ils n'ont pas à contrôler le trafic du réseau mais "seulement" les activités d'un hôte, ils se montrent habituellement plus précis sur les types d'attaques subies.

En somme, le Network IDS est un gendarme qui compare chaque trame à une banque de portraits robots. Mais il ne garantit pas à lui seul un niveau de sécurité proche de 100 %. Pour y parvenir, il faut mettre en fonction un autre gendarme, qui observera le comportement de chaque trame et signalera tout ce qui lui paraîtra inhabituel. C'est le rôle du HIDS, une véritable sonde qui est placée individuellement sur chaque système à protéger. Un système qui corrige les faiblesses des Network IDS.

La technologie Host IDS excelle dans la détection des anomalies connues et inconnues, si une attaque parvient à se faufiler à travers les mailles du filet, la sonde va la repérer, "Le Host IDS réalise une photographie du système à un moment donné. Il définit tout ce qui est légitime. Tout ce qui sort du cadre et des habitudes du système est considéré comme une attaque. Une modification de la base de registres sera donc bloquée et fera l'objet d'une alerte", explique Pascal Delprat (Consultant en sécurité chez Cisco en France) [13]. Un travail complémentaire à celui du Network IDS.

Une sonde Host IDS est moins onéreuse qu'un Network IDS, mais on doit en placer une sur chaque machine à surveiller. On les réserve donc le plus souvent aux machines très protégées. Elles sont également beaucoup moins gourmandes en ressources systèmes qu'un Network IDS, on les trouve donc sous forme de logiciel, et non plus intégrées à un serveur ou une appliance comme les Network IDS. Placées sur une machine, elles ne consomment en effet pas plus de 5 % des ressources.

Ensemble, les deux gendarmes font accéder un réseau d'entreprise à un niveau de protection optimal. A condition d'être chapeautés par un brigadier-chef, ils ne savent pas travailler correctement sans être encadrés, le problème de l'administration des IDS au quotidien représente en effet le point le plus délicat et le plus crucial pour un système de détection d'intrusion. Si on le néglige, il est préférable de garder son budget pour l'investir ailleurs.

Les systèmes de détection d'intrusion basés sur l'hôte (poste de travail, serveur, etc.), ou HIDS (Host-based IDS), analysent exclusivement l'information concernant cet hôte. Comme ils n'ont pas à contrôler le trafic du réseau mais "seulement" les activités d'un hôte, ils se montrent habituellement plus précis sur les variétés d'attaques. Ces IDS utilisent deux types de sources pour fournir une information sur l'activité : les logs et les traces d'audit du système d'exploitation. Chacun a ses avantages : les traces d'audit sont plus précises, détaillées et fournissent une meilleure information ; les logs, qui ne fournissent que l'information essentielle, sont plus petits et peuvent être mieux analysés en raison de leur taille. Il n'existe pas de solution unique HIDS couvrant l'ensemble des besoins, mais les solutions existantes couvrent chacune un champ d'activité spécifique, comme l'analyse de logs système et applicatifs, la vérification de l'intégrité des systèmes de fichiers, l'analyse du trafic réseau en direction provenance de l'hôte, le contrôle d'accès aux appels système, l'activité sur les ports réseau, etc.… (Exemple, le démon syslog), peut être considéré partiellement comme un système HIDS, car il permet de consigner certaines activités, et à l'aide d'un analyseur comme Swatch, de détecter certaines tentatives d'intrusion (comme bad login).

Les systèmes de détection d'intrusion basés sur l'hôte ont certains avantages : l'impact d'une attaque peut être constaté et permet une meilleure réaction, des attaques dans un trafic chiffré peuvent être détectées (impossible avec un NIDS), les activités sur l'hôte peuvent être observées avec précision, etc. Ils présentent néanmoins des inconvénients, parmi lesquels : les scans sont détectés avec moins de facilité ; ils sont plus vulnérables aux attaques de type DoS, l'analyse des traces d'audit du système est très contraignante en raison de la taille de ces dernières ; ils consomment beaucoup de ressources CPU, etc.….

Et le schéma ci-dessous vous montre les positions possibles pour placer un HIDS **[13]**.

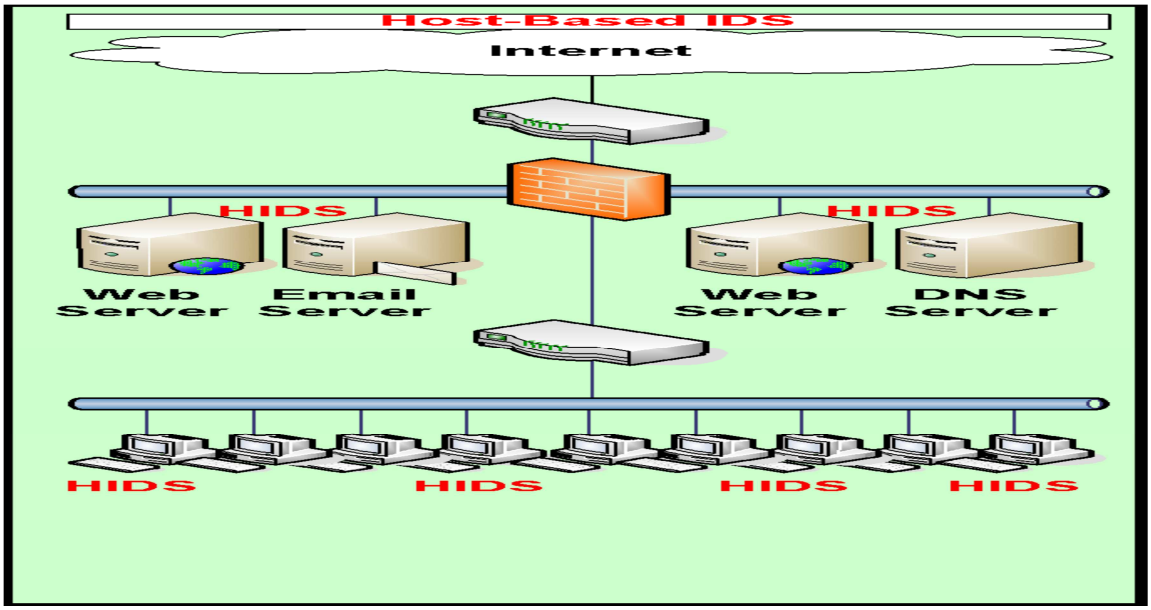

Figure III-5 : Emplacement de HIDS au sein d'un réseau

III.2.2.1.2.2 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.

III.2.2.1.2.3 Les IDS réseaux (NIDS)

Imaginons qu'une requête malintentionnée ait passé le barrage du firewall, il faut donc l'arrêter. La méthode la plus classique consiste à faire appel à un Network IDS :

- ✓ Une solution de détection d'intrusion largement éprouvée. Son rôle sera d'immobiliser chaque requête, de l'analyser et de lui laisser continuer son chemin seulement si elle ne correspond pas au portrait-robot d'une attaque référencée. Avant d'opter pour un tel système, il faut connaître les points clés de cette solution.

Le rôle essentiel d'un IDS réseau, appelé NIDS (Network-based Intrusion Detection System), est l'analyse et l'interprétation des paquets circulant sur ce réseau. Afin de repérer les paquets à contenu malicieux comme par exemple des expressions contenant « /etc/password », des signatures sont créés. Des détecteurs (souvent de simples hôtes) sont utilisés pour analyser le trafic et si nécessaire envoyer une alerte. Un IDS réseau travaille sur les trames réseau à tous les niveaux (couches réseau, transport, application). De plus en plus, en disséquant les paquets et en ‘‘comprenant’’ les protocoles, il est capable de détecter des paquets malveillants conçus pour outrepasser un pare-feu aux règles de filtrage trop laxistes, et de chercher des signes d'attaque à différents endroits sur le réseau. Quelques exemples de NIDS : NetRanger, NFR, DTK, ISS RealSecure7, Snort.

Les IDS réseau ont des atouts, par exemple, les détecteurs peuvent être bien sécurisés puisqu'ils se « contentent » d'observer le trafic, les scans sont détectés plus facilement grâce aux signatures, etc. Cependant, les problèmes majeurs liés aux NIDS sont de conserver toujours une bande passante suffisante pour l'écoute de l'ensemble des paquets, et de bien positionner l'IDS pour qu'il soit efficace.

Premier gage de qualité pour un Network IDS, l'exhaustivité du fichier contenant les signatures des attaques. Ce fichier est centralisé et mis à jour par le fabricant de solutions de Network IDS. Il faut donc penser très régulièrement à en télécharger la liste la plus récente.

Par extension, la qualité des équipes de veille du fabricant conditionne largement l'efficacité de ses produits, les plus grandes marques emploient plusieurs dizaines de personnes à la mise à jour de cette liste de signatures.

Un des points cruciaux des NIDS concerne le choix de leurs emplacements. ``Une sonde placée à un mauvais endroit peut être inefficace``, soutient Philippe Solini, Network Design Consultant chez Unisys. Il est d'ailleurs courant que l'on ne puisse pas se contenter d'un seul système de filtrage : plus un réseau est complexe, plus il présente de vulnérabilités. Il en devient logiquement plus difficile à protéger. Mais chaque network IDS rajouté coûte cher, ces machines sont particulièrement gourmandes en ressources. "Les débits analysés sont très lourds, il est donc nécessaire de dédier au Network IDS des machines très puissantes, ou des appliances (des boites noires) spécialisés pour parvenir à les soutenir", explique Philippe Solini.

Tel que Le schéma ci-dessous vous montre les positions possibles pour placer un NIDS **[13]**.

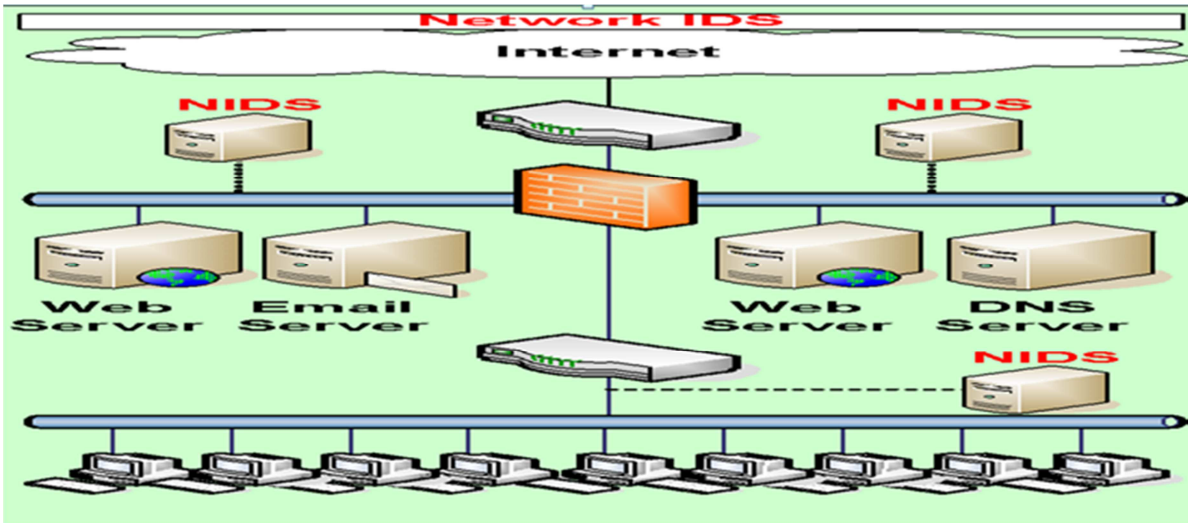

Figure III-6 : Emplacement de NIDS au sein d'un réseau

III.2.2.1.2.4 Système de Détection d'Intrusion de Nœud Réseau (NNIDS) :

Ce nouveau type d'IDS (NNIDS) fonctionne comme les NIDS classiques, c'est-à-dire vous analysez les paquets du trafic réseau. Mais ceci ne concerne que les paquets destinés à un nœud du réseau (d'où le nom).

Une autre différence entre NNIDS et NIDS vient de ce que le NIDS fonctionne en mode "promiscues", ce qui n'est pas le cas du NNIDS. Celui-ci n'étudie que les paquets à

destination d'une adresse ou d'une plage d'adresse. Puisque tous les paquets ne sont pas analysés, les performances de l'ensemble sont améliorées.

Ce type d'IDS n'est pas encore très répandu, mais il est de plus en plus utilisé pour étudier le comportement de nœuds sensibles d'un réseau.

De nouveaux types d'IDS sont conçus actuellement, comme les IDS basés sur la pile, qui étudie la pile d'un système. Le secteur des IDS est en plein développement, le besoin des entreprises en sécurité réseaux étant de plus en plus pressant, du fait de la multiplication des attaques **[17]**.
Actuellement, les IDS les plus employés sont les NIDS et HIDS, de plus en plus souvent en association. Les ABIDS restent limités à une utilisation pour des applications extrêmement sensibles.

Les recherches en cours visent également à améliorer les performances des IDS, notamment dans ce qui concerne les faux positifs et faux négatifs et la complexité d'administration (actuellement il faut souvent une personne dédiée à la gestion de l'IDS).

Nous allons à présent nous pencher sur le mode de fonctionnement d'un IDS.

III.2.2.1.2.5 IDS hybrides

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 réseau et l'hôte. Les sondes sont placées dans 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, agréger, et lier les informations d'origines multiples.

Le schéma ci-dessous vous montre les positions possibles pour placer un IDS hybrides **[16]**.

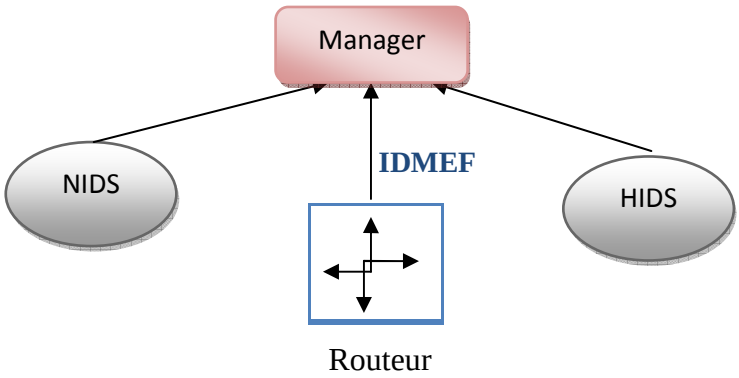

Figure III-7 : architecture distribuée d'un IDS hybride

III.2.2.2 Le Système de Prévention d'Intrusion IPS

Un système IPS est placé en ligne et examine en théorie tous les paquets entrants ou sortants. Il réalise un ensemble d'analyses de détection, non seulement sur chaque paquet individuel, mais également sur les conversations et motifs du réseau, en visualisant chaque transaction dans le contexte de celles qui précédent ou qui suivent.

Les systèmes de prévention d'intrusions sont des systèmes de détection d'intrusions particuliers qui permettent, en plus de repérer les tentatives d'intrusion à un système, d'agir pour contrer ces tentatives. En effet, les IPS constituent des IDS actifs qui tentent de bloquer les intrusions. Cependant, les IPS ne sont pas une solution parfaite comme nous pourrions le penser, ces derniers présentent certaines limitations, notamment le blocage de toute activité qui leurs semblent suspecte. Or il est impossible d'identifier de manière fiable toutes les attaques informatiques.

Si le système IPS considère le paquet inoffensif, il le transmet sous forme d'un élément traditionnel de couches 2 ou 3 du réseau. Les utilisateurs finaux ne ressentent aucun effet. Cependant, lorsque le système IPS détecte un trafic douteux, il peut lancer un de ses nombreux mécanismes de réponse. Il peut limiter le trafic, en le transférant normalement jusqu'à un certain niveau de bande passante ou de connexions TCP. Sinon, le système IPS peut supprimer complètement le paquet.

Evidemment, un système IPS doit également disposer d'un mécanisme complet de comptes-rendus, qui ne doit pas se résumer à un simple journal d'activités. Le système IPS peut créer une alarme et la transmettre aux destinations adéquates. Il peut envoyer des copies du trafic réel à travers un port d'examen pour une analyse et un diagnostic immédiats par le personnel de sécurité informatique. Il peut même créer une copie complète récurrente Flow Mirror™ du trafic de session pour l'envoyer vers un port miroir.

De l'avis des analystes, le concept d'IPS (systèmes de prévention des intrusions), vise à anticiper les attaques de pirates informatiques dès lors que leur empreinte est connue. Il ne s'agit plus seulement de réagir à une attaque en cours, mais d'empêcher que celle-ci puisse seulement débuter **[15]**.

L'IPS doit aussi, offrir un moyen de diminuer considérablement l'utilisation des ressources humaines nécessaires au bon fonctionnement des IDS. Cela doit aboutir, notamment, à une

automatisation des fonctions d'analyse des logs, même si ce point demeure encore une tâche difficile. La prise de décision doit ainsi pouvoir être automatisée non seulement grâce à la reconnaissance de signatures mais aussi, et de plus en plus, grâce à l'utilisation d'analyses heuristiques provenant du monde des anti-virus.

Deux voies principales sont actuellement explorées par les promoteurs d'IPS.

- ✓ La première est l'approche des constructeurs d'IDS dont les produits n'ont que faiblement convaincu le marché français alors qu'ils sont utilisés dans plus d'une entreprise sur deux aux Etats-Unis. Comme pour les IDS, les IPS peuvent être orientés Host(HIPS) ou Réseaux (NIPS).
- ✓ La seconde approche touche les fournisseurs de pare-feu qui commencent à intégrer des systèmes IPS au sein de leurs matériels qui savent fonctionner "en ligne". Cela passe par exemple par l'intégration de signatures et d'un contrôle des protocoles HTTP, FTP et SMTP, mais aussi pour certains constructeurs de la mise en ASIC (Application Specific Integrated Circuit) de leurs IPS afin de s'intégrer facilement à leurs matériels.

De plus les pirates peuvent utiliser cette fonctionnalité de blocage assurée par les IPS pour mettre hors service un système. Ainsi les IPS se transforment en vecteurs d'attaques qui peuvent nuire au bon fonctionnement d'un système d'information. Par ailleurs, un IPS est peu discret puisqu'il montre sa présence à chaque blocage d'attaques. Ainsi, un pirate peut détecter sa présence sur le réseau et tente de trouver une faille ou des techniques pour contourner les restrictions imposées par l'IPS en question.

III.2.2.2.1 Les systèmes de prévention d'intrusions Kernel (KIDS /KIPS)

Ce type d'IDS fait partie de la famille des HIDS. Cependant, sa fonctionnalité principale est de détecter les intrusions au niveau noyau. L'utilisation d'un KIPS s'avère parfois nécessaire selon le niveau de sécurité à apporter pour une machine et permet de reconnaître, non seulement les caractéristiques des failles présentes sur un système, mais aussi d'interdire l'OS d'exécuter des appels systèmes qui peuvent s'avérer dangereux ou qui visent la compromission du système.

Toutefois un ralentissement dans le fonctionnement peut être observé sur un système protégé par un KIPS. En effet, ce dernier analyse les appels systèmes et bloque tout accès suspect au système. Ainsi les KIPS sont des solutions rarement utilisés sur des serveurs souvent sollicités. Un exemple de KIPS est Secure IIS qui constitue une surcouche.

Nous l'évoquions précédemment dans le cadre du HIDS, l'utilisation d'un détecteur d'intrusions au niveau noyau peut s'avérer parfois nécessaire pour sécuriser une station.
Prenons l'exemple d'un serveur web, sur lequel il serait dangereux qu'un accès en lecture/écriture dans d'autres répertoires que celui consultable via http, soit autorisé. En effet, cela pourrait nuire à l'intégrité du système. Grâce à un KIPS, tout accès suspect peut être bloqué directement par le noyau, empêchant ainsi toute modification dangereuse pour le système.

Le KIPS peut reconnaître des motifs caractéristiques du débordement de mémoire, et peut ainsi interdire l'exécution du code. Le KIPS peut également interdire l'OS d'exécuter un appel système qui ouvrirait un shell de commandes. Puisqu'un KIPS analyse les appels systèmes, il ralentit l'exécution. C'est pourquoi ce sont des solutions rarement utilisées sur des serveurs souvent sollicités **[15]**.

Exemple de KIPS : SecureIIS, qui est une surcouche du serveur IIS de Microsoft.

III.2.2.2.2 Avantage des systèmes IPS

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

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

Prévention active. Alors qu'un système NIDS prévient simplement de la présence d'un trafic suspect ou anormal, un système IPS peut lancer divers mécanismes de réaction, comme décrit précédemment. Pour les organisations, les coûts d'administration de la sécurité réseau en sont réduits d'autant, de même que le risque de dégâts ou de pertes dus aux cybers attaque.

III.3 Limites des systèmes de protection contre les intrusions

La plupart des reproches faits aux systèmes de protection contre les intrusions concerne en réalité les systèmes de détection d'intrusion. C'est pourquoi les systèmes de prévention d'intrusions sont souvent considérés comme les améliorations des IDS.

Les systèmes de protection contre les intrusions doivent pouvoir supporter le trafic maximal attendu à l'endroit où ils seront placés. Si un capteur ne peut pas gérer le débit, des paquets de données seront perdus, et les données transitant par ce point ne seront pas toutes analysées.

Cette situation peut même avoir un impact sur les performances globales du réseau en créant un goulet d'étranglement. Il est donc préférable de surestimer le trafic réseau potentiel transitant par le point de déploiement du capteur que le contraire.

La plus grande menace qui pèse sur les déploiements d'IDS/IPS est que, au fil du temps, l'équipe de sécurité ne fasse plus attention aux données enregistrées. C'est un point qu'il faut prendre en compte lors du choix des règles de sécurité. Même si un grand nombre de messages sont interceptés à tort lorsqu'un système est déployé la première fois, celui-ci doit être constamment reconfiguré pour en réduire peu à peu le nombre. Le but étant de disposer d'un système robuste et pratique susceptible un jour de sauver les données de l'entreprise.

L'une des principales limites qu'on connaît aux IDS est le phénomène des faux positifs et des faux négatifs. Après le phénomène de faux positifs et des faux négatifs, il existe encore plusieurs autres imperfections et limites souvent attribuées aux IDS. Il s'agit entre autres du mode promiscuité, de la définition et maintenance des signatures, leur apprentissage et leur configuration de l'IDS et enfin les limites générales.

III.3.1 Faux positifs et faux négatifs

Parmi les comportements possibles pour un IDS, on peut envisager les quatre possibilités recensées dans le tableau suivant qu'une intrusion soit ou non en cours dans le système informatique et que le système de détection d'intrusion ait émis ou non une alerte.

	Pas d'alerte	**Alerte**
Pas d'attaque	Vrai négatif	Faux négatif
Attaque en cours	Faux négatif	Vrai négatif

Tableau III-1: Comportements envisageables pour un IDS

Parmi ces quatre comportements, les vrais négatifs et les vrais positifs correspondent aux comportements souhaités. Toutefois un IDS est généralement imparfait et conduit à l'apparition des deux autres comportements non désirés. Parmi eux, un faux négatif correspond à une attaque non détectée, et un faux positif à l'émission d'une fausse alerte. Les différents IDS souffrent généralement d'imperfections donnant lieu à l'apparition de ces comportements non désirés, mais selon des axes différents suivant les méthodes de détection qu'ils utilisent.

Un reproche fréquemment fait en direction des IDS utilisant une méthode de détection comportementale est de contenir dans leur principe même de fonctionnement la possibilité de fausses alertes (un changement de comportement légitime détecté comme anormal) ou de faux négatifs (par exemple pour une attaque très lente) ; tandis que les approches par scénarii semblent théoriquement être plus exactes. Toutefois, la base de connaissance utilisée dans les IDS par scénarii exige une maintenance constante et, dans la pratique, souffre également nécessairement d'imperfections.

Bien que les faux négatifs soient effectivement le premier des comportements indésirables pour un IDS, les faux positifs sont importants aussi : ils peuvent conduire à une réelle perte de confiance dans les capacités de détection de l'IDS de la part des administrateurs qui peut finir par remettre en cause la finalité de l'IDS. C'est même une des voies d'attaque envisageables contre un système équipé d'un IDS : générer un nombre suffisamment important de fausses alertes pour réduire l'attention des administrateurs et dissimuler une attaque réelle. De plus, dans la pratique, les faux positifs dus à l'environnement de l'IDS ou à des signatures d'attaque un peu trop affirmatives sont souvent nombreux, et ceci nécessite généralement un paramétrage de l'IDS pour faciliter son exploitation, au prix de l'introduction de possibilités de faux négatifs. La gestion des faux positifs est le premier problème auxquels sont confrontés les administrateurs d'un IDS, et il est généralement de taille.

Les IDS basés sur une approche par scénarii, c'est à dire la plupart des IDS courants, souffrent sur ce point d'un réel problème qui demanderait certainement de développer à la fois les possibilités d'adaptation de l'IDS à son environnement (peut-être par des moyens de corrélation) et une meilleure validation des signatures d'attaque disponibles.

L'utilisation de techniques de corrélation d'alertes provenant de plusieurs IDS semble être une des voies envisageables pour traiter ces problèmes d'analyse des alertes et notamment des fausses alertes. Dans ce cadre, la diversification des méthodes de détection utilisées par les différents IDS, ainsi que de leurs sources de données est aussi à nouveau envisageable. (Dans un certain sens, il s'agit d'ailleurs de réinventer la roue une fois de plus puisque le précurseur des systèmes de détection d'intrusion, nommé IDES, combinait déjà l'utilisation d'une approche comportementale -statistique- et d'une approche à base de règles -système expert-, dans les années 1980 du côté de Stanford).

III.3.2 La définition et la maintenance des signatures

Toutes les attaques ne sont pas détectées, selon les fonctionnalités du système, la définition de la signature, la mise à jour de la base, la charge du système, etc.… :

- **Limites "humaines" :** Signatures pas à jour ou mal conçues. La détection d'abus a pour impératifs une bonne conception des signatures d'attaques et une mise à jour continue de la liste des signatures ;
- **Contexte d'utilisation:** Parfois la technologie est basée sur des signatures qui ne reposent pas sur le contexte d'utilisation. La conséquence est double: de nombreux faux positifs et une dégradation importante des performances du système ;
- Même si la méthode des signatures de corps (y compris les signatures de chaîne) semble être assez sûre, il y a moyen de les contourner ;
- **Vulnérabilité aux mutations :** De par son manque de flexibilité, la détection par signatures d'attaques est très vulnérable aux mutations. D'une part, pour pouvoir définir une signature, il faut avoir déjà été confronté à l'attaque considérée.

D'autre part, certaines de ces signatures se basent sur des caractéristiques 'volatiles' d'un outil, comme par exemple le port qu'un cheval de Troie ouvre par défaut ou la valeur d'ISN (Initial Sequence Number) choisie par certains outils de piratage. Or ces logiciels sont souvent soit hautement configurables, soit open source donc librement modifiables. Les caractéristiques

retenues pour définir la signature sont donc fragiles, et les signatures extrêmement sensibles aux mutations.

- Faute de définition, les nouvelles attaques passent l'IDS sans être détectées.

III3.3 L'apprentissage et la configuration des IDS

L'apprentissage du comportement ''normal'' n'est pas aisé. Automatiser le raisonnement conduisant à penser que le comportement est "déviant" par rapport à celui connu est une tâche difficile. Par contre, cette technique est appliquée par défaut (la plupart du temps) par les administrateurs réseau ou système : lorsque quelque-chose paraît inhabituel (par exemple, des pics de bande passante, des services qui tombent, des systèmes de fichiers qui se remplissent plus vite qu'à l'accoutumée, etc.), l'usage veut que des recherches plus poussées soient entreprises.

Par ailleurs, toute anomalie ne correspond pas forcément à une attaque, cela peut être un changement de comportement de l'utilisateur ou un changement de la configuration du réseau.

En règle générale, la convergence vers un modèle comportemental "normal" est plutôt longue. Lors du paramétrage de l'IDS, toute la difficulté pour une détection efficace réside dans le choix des métriques, des modèles de comportement et dans la définition des différents profils. Pour toutes ces raisons, les IDS fonctionnant par détection d'anomalie sont reconnus comme étant très longs et fastidieux à configurer.

Même après une configuration efficace, rien n'empêche un pirate se sachant surveillé de "rééduquer" un tel système en faisant évoluer progressivement son modèle de convergence vers un comportement anormal pour l'analyste, mais tout-à-fait "normal" d'un point de vue statistique.

IV Mise en place d'un IDS

IV.1 NIDS: Snort

IV.1.1 Description

Snort est un NIDS / NIPS provenant du monde Open Source. C'est pourquoi nous le recommandons fortement aux petites entreprises et organisations en général car ces dernières n'ont pas souvent suffisamment de ressources financières à accorder à l'achat des logiciels propriétaires.

Avec plus de 2 millions de téléchargements, il s'est imposé comme le système de détection d'intrusions le plus utilisé. Sa version commerciale, plus complète en fonctions de monitoring (supervision), lui a donné bonne réputation auprès des entreprises.

Snort est capable d'effectuer une analyse du trafic réseau en temps réel et est doté de différentes technologies de détection d'intrusions telles que l'analyse protocolaire et le pattern matching (filtrage par motif). Snort peut détecter de nombreux types d'attaques : buffer overflows (dépassement de tampon), scans de ports furtifs, attaques CGI, sondes SMB, tentatives de fingerprinting (La prise d'empreinte de la pile TCP/IP) de système d'exploitation etc. [18]

Snort est doté d'un langage de règles permettant de décrire le trafic qui doit être accepté ou collecté. De plus, son moteur de détection utilise une architecture modulaire de plugins (extensions).

Notons que Snort dispose de trois modes de fonctionnement : sniffer de paquets, logger de paquets et système de détection/prévention d'intrusions :

- **Le mode sniffer :** dans ce mode, SNORT lit les paquets circulant sur le réseau et les affiche d'une façon continue sur l'écran.
- **Le mode logger de paquets « packet logger » :** dans ce mode SNORT journalise le trafic réseau dans des répertoires sur le disque.
- **Le mode détecteur d'intrusion réseau (NIDS)** : dans ce mode, SNORT analyse le trafic du réseau, compare ce trafic à des règles déjà définies par l'utilisateur et établi des actions à exécuter.

IV.1.2 Où positionner son IDS ??

L'emplacement physique de la SNORT sur le réseau a un impact considérable sur son efficacité.
Dans le cas d'une architecture classique, composée d'un Firewall et d'une DMZ, trois positions sont généralement envisageables :

Le schéma suivant illustre un réseau local ainsi que les trois positions que peut y prendre un IDS :

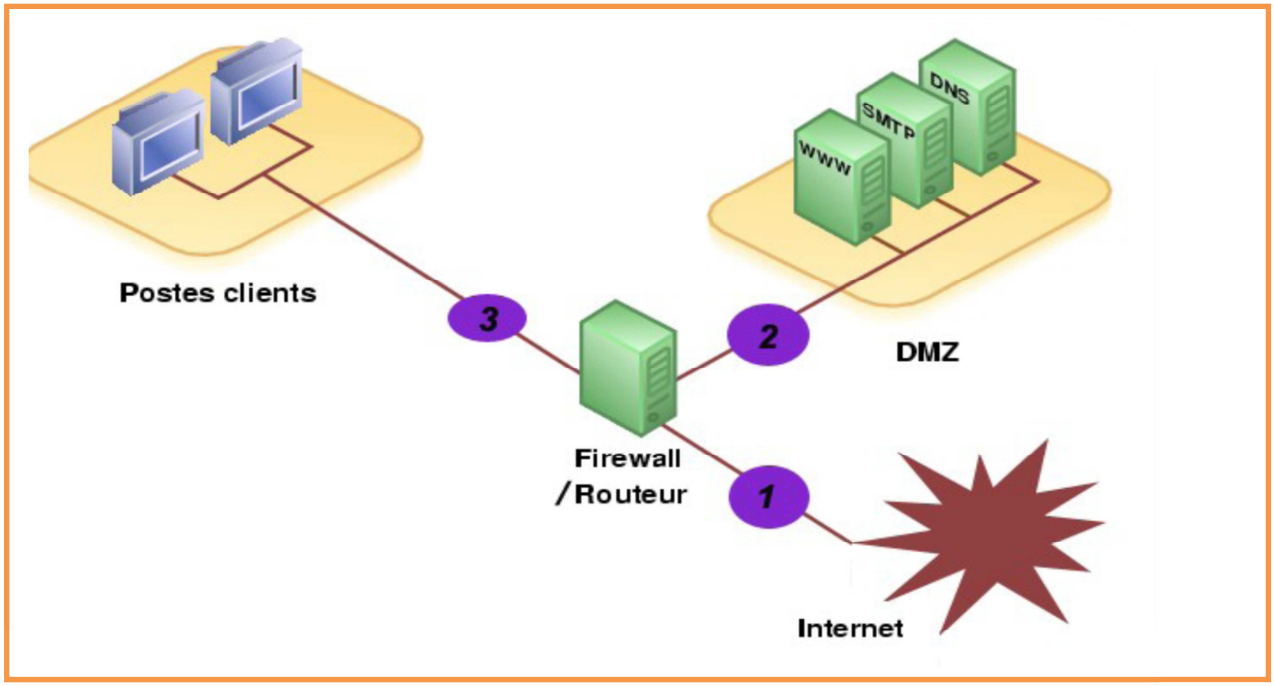

Figure IV.1 Position d'un IDS dans un réseau local

- **Position (1):** Sur cette position, l'IDS va pouvoir détecter l'ensemble des attaques frontales, provenant de l'extérieur, en amont du firewall. Ainsi, beaucoup d'alertes seront remontées ce qui rendra les logs difficilement consultables.
- **Position (2):** Si l'IDS est placé sur la DMZ, il détectera les attaques qui n'ont pas été filtrées par le firewall et qui relèvent d'un certain niveau de compétence. Les logs seront ici plus clairs à consulter puisque les attaques bénines ne seront pas recensées.
- **Position (3):** L'IDS peut ici rendre compte des attaques internes, provenant du réseau local de l'entreprise. Il peut être judicieux d'en placer un à cet endroit étant donné le fait que 80% des attaques proviennent de l'intérieur. De plus, si des trojans ont contaminé le parc informatique (navigation peu méfiante sur internet) ils pourront êtres ici facilement identifiés pour être ensuite éradiqués.

Idéalement, on placerait des IDS sur les trois positions puis on délèguerait la consultation des logs à l'application ACID "Analysis Consol for Intrusion Databases " (cf http://acidlab.sourceforge.net/) qui permet d'analyser les alertes et d'en présenter clairement les résultats via une interface web complète. Si une seule machine peut être déployée, autant la mettre sur la position 2, cruciale pour le bons fonctionnement des services [19].

IV.2 Installation

Au préalable on a installé la distribution Debian dans sa version stable dénommée *squeeze* sur notre machine virtuelle (Oracle VM virtualbox).

Pour installer *Snort*, deux méthodes sont possibles :

- ✓ La première méthode consiste à télécharger les sources et de les compiler soi-même avec les options et les bibliothèques que l'on désire,
- ✓ La deuxième méthode est celle de l'installation automatique et qui consiste sur un système d'exploitation telle que Linux Debian par exemple à exécuter tout simplement la commande suivante **:**

#apt-get install snort.

Il faut noter qu'avec une telle installation toutes les bibliothèques et autres logiciels nécessaires sont aussi automatiquement proposés et installés par le système, car Debian est la solution idéale (installation de l'outil + règles).

On a opté pour la deuxième méthode, et l'installation est faite à partir d'un miroir que la section réseaux de l'université de Bejaia a mis en place http://mirror-local.univ-bejaia.dz

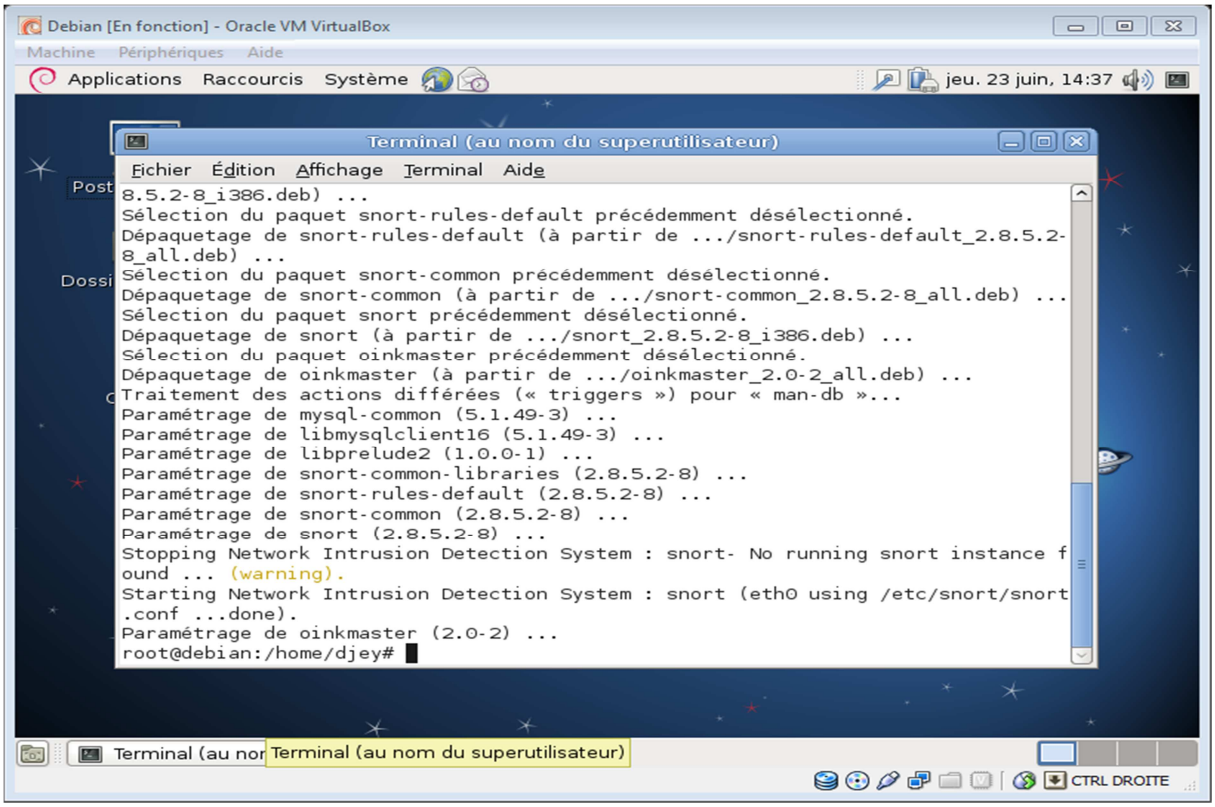

Figure IV.2 un extrait lors de l'installation de snort

IV.2.1 Installation des prérequis de snort

Les packages suivants sont requis pour le fonctionnement de snort sur linux Debian Squeez :

- ✓ mysql-server,
- ✓ mysql-client,
- ✓ php5-mysql,
- ✓ apache 2.

Sur Debian, il suffit de taper la commande **apt-get install ''nom_du_paquet''** (depuis le site miroir).

Toutes les manipulations sont faites en **root** (sup-utilisateur).[20]

IV.3 configuration

IV.3.1 Editer le fichier snort.conf

Afin de configurer correctement Snort pour qu'il puisse fonctionner en mode détection d'intrusions, il faut modifier le fichier **snort.conf**. Tous les paramètres à régler de se trouvent dans ce fichier. L'emplacement par défaut de ce fichier doit normalement être /etc/snort.conf.

Cependant, il sera possible de spécifier un autre emplacement lors de l'exécution de Snort, à l'aide de l'option -c.

Snort se base sur le fichier de configuration pour initialiser son environnement. Il est donc important de bien configurer tout ceci. Il faut tout d'abord configurer les variables réseau du fichier de configuration snort.conf :

- ✓ La variable HOME_NET permet de spécifier quels réseaux ou quelles interfaces seront surveillées par Snort. Il faut pour cela modifier les variables suivantes:

var HOME_NET [10.28.0.0/22] # SNORT travaille sur le réseau 10.28.0.0 (notre VLAN).
var HOME_NET any **#** La valeur any signale à Snort de surveiller tout le trafic.

- ✓ Dans le même fichier on recherche les lignes les lignes commençant par « **#output database »** et on les remplace par :
  - **output database: log, mysql, user=djey password=my_pass dbname=Debian host=localhost**

Pour que SNORT logs (remonter les alarmes et enregistrer les alertes) dans la base données mysql qu'on va créer dans la suite de la configuration.

- ✓ Si le réseau à surveiller possède des serveurs DNS, SMTP, FTP, etc , il est possible de spécifier les adresses IP de ces serveurs via les variables DNS_SERVERS, SMTP_SERVERS, ... Si le réseau ne possède pas un type spécifique de serveur, il est conseillé de commenter (avec le caractère #) la ligne concernée, afin d'optimiser le traitement de Snort. En effet, il est inutile d'analyser du trafic HTTP si aucun serveur Web n'est disponible. Par exemple les serveurs suivant :

var DNS_SERVERS 172.17.1.11/255.255.0.0.
var SMTP_SERVERS adresse IP/masque.
var HTTP_SERVERS adresse IP/masque.
var SQL_SERVERS adresse IP/masque.
var TELNET_SERVERS adresse IP/masque.
var SNMP_SERVERS adresse IP/masque.

- ✓ Certains ports de services peuvent être configurés via des variables telles que HTTP_PORTS ou ORACLE_PORTS.
- ✓ La variable RULE_PATH est très importante. Elle permet de spécifier le répertoire où sont stockés les fichiers de règles de Snort.

On doit modifier la ligne **var RULE_PATH** *par «***var RULE_PATH /etc/snort/rules***»*

- ✓ Les directives **include** permettent d'inclure des fichiers de règles. Ici encore, il est conseillé de n'inclure que les règles nécessaires en fonction des services disponibles sur le réseau. [20]

La figure suivante nous montre une partie de fichier configuration **snort.con**

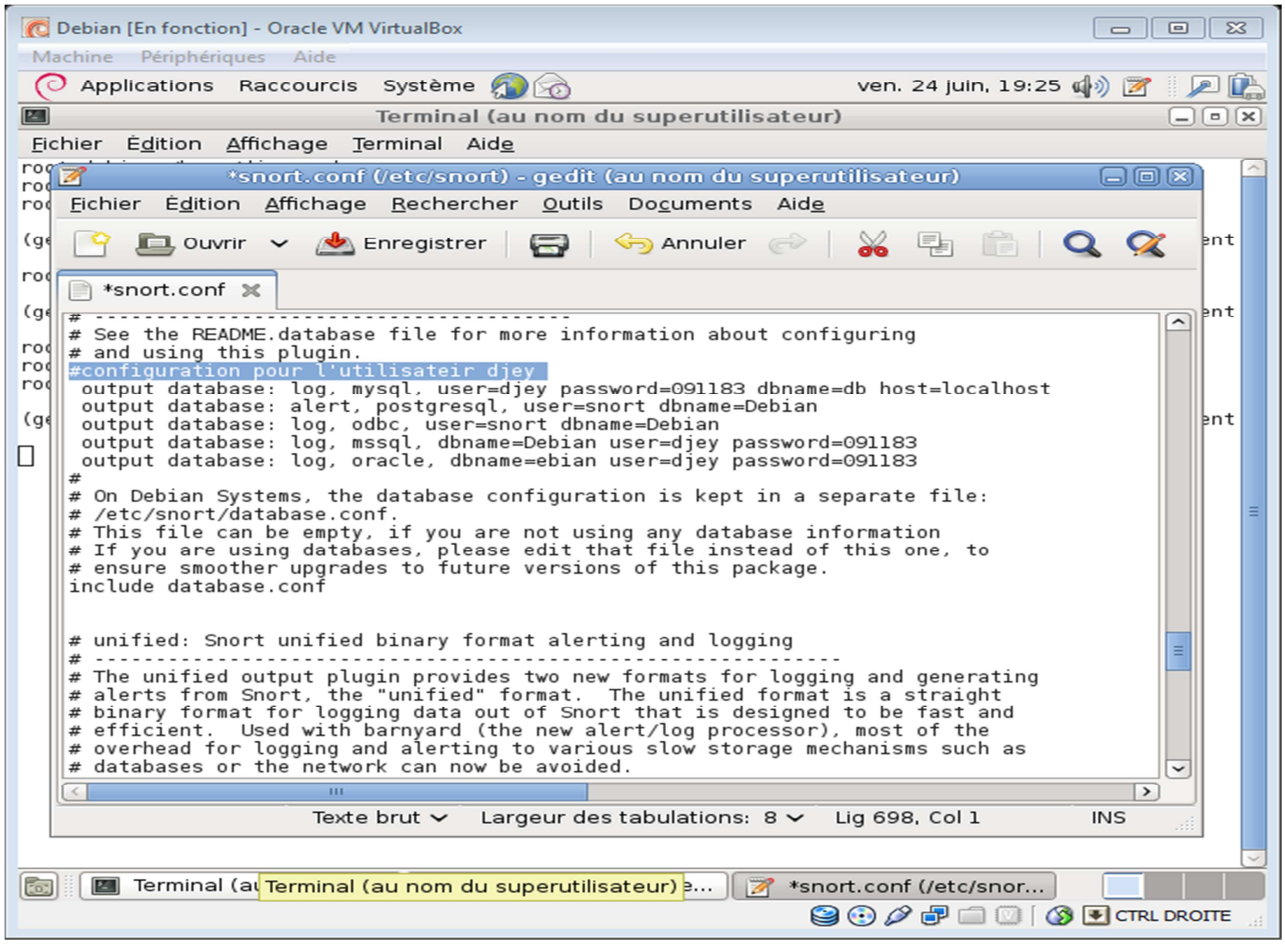

Figure IV.2 : Extrait de fichier de configuration snort.conf

IV.3.2 liaison des logs de snort avec mysql

On commence par la création de la base de données de snort :

On appelle mysql par la commande :

#mysql -u root –p

enter password **"**my_pssword**"**

Ici on constate par la commande suivante que la base de données n'est pas créée :

mysql> SHOW DATABASES; || on aura l'affichage suivant :

```
+-------------------------+
| Database                |
+-------------------------+
|information_schema       |
|mysql                    |
+-------------------------+
2 rows in set (0.00 sec)
```

On crée alors la base de données snort:

mysql> CREATE DATABASE snort;

Query OK, 1 row affected (0.00 sec) # indique que la base de données a été créée et on vérifiera avec cette commande :

mysql> SHOW DATABASES;

```
+------------------------+
|Database                |
+------------------------+
|information_schema      |
|mysql                   |
|snort                   |
+------------------------+
3 rows in set (0.00 sec)
```

On donne les droits et on attribue un mot de passe, dans notre cas :

- ✓ Utilisateur de la db (Debian): **djey ;**
- ✓ Mot de passe de la db: « **my_password** » ;
- ✓ Nom de la db: **Debian :**

mysql> grant CREATE, INSERT, SELECT, UPDATE on snort.* to djey@localhost;

mysql> grant CREATE, INSERT, SELECT, UPDATE on snort.* to djey;

mysql> SET PASSWORD FOR djey@localhost=PASSWORD('my_password');

mysql> flush privileges;

On vérifie que les changements ont bien eu lieu:

mysql> show grants for 'djey'@'localhost';

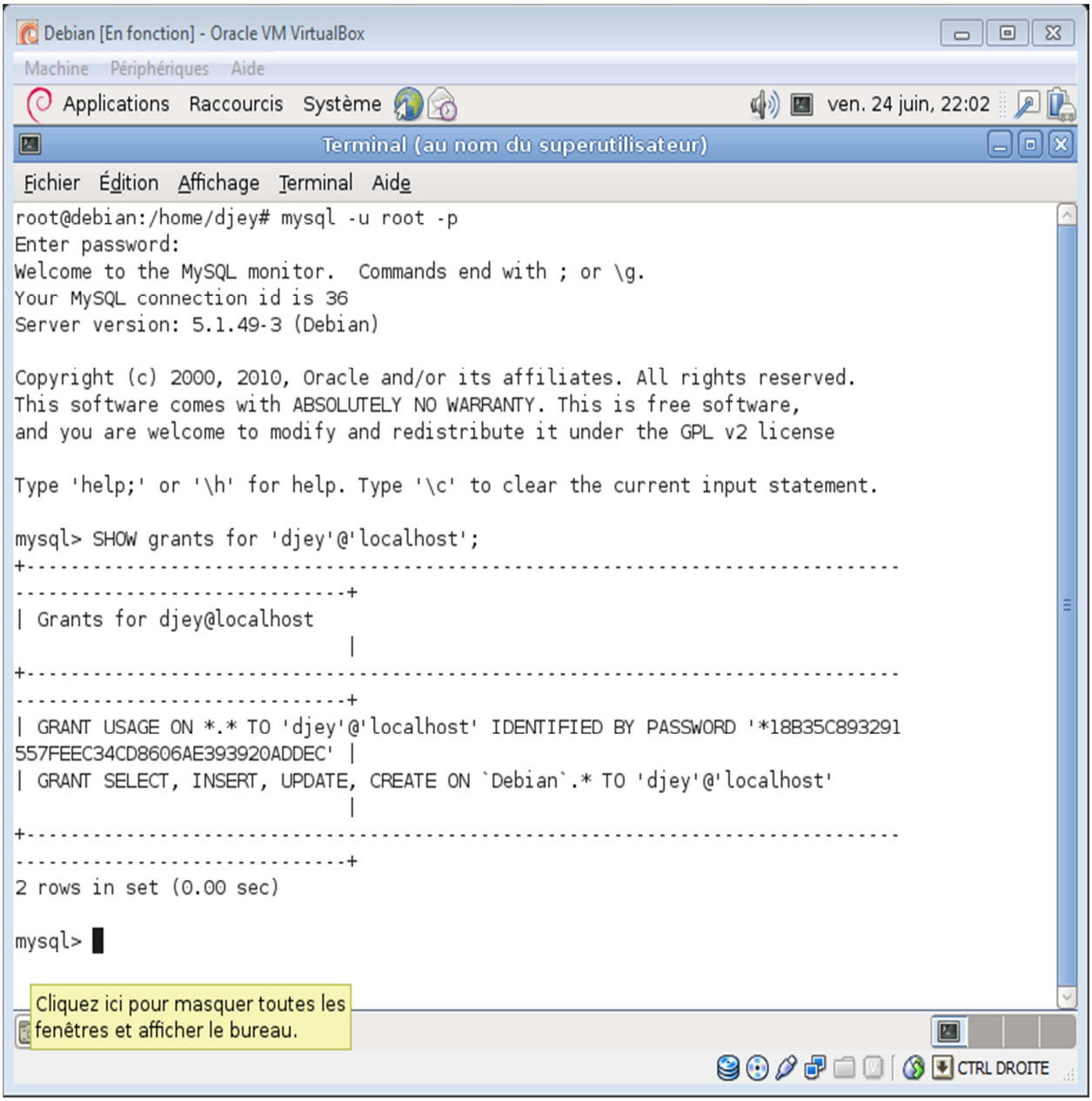

Figure IV.3 : vérification des changements sur la BDD

On quitte mysql:

mysql>quit

Bye

Importer les tables de la base de données à partir de snort, elles doivent se trouver dans le dossier /usr/share/doc/snort-mysql, on lance les commandes :

$ cd /usr/share/doc/snort-mysql

$ zcat create_mysql.gz | mysql -u djey -D snort –pmy_massword

L'importation s'est bien passée, on doit voir les tables dans la base snort et on vérifie que les tables ont été bien créées comme suit :

mysql> use snort;

mysql> SHOW TABLES;

```
+------------------+
|Tables_in_snort |
+------------------
|data           |
|detail         |
|encoding       |
|event          |
|icmphdr        |
|iphdr          |
|opt            |
|reference      |
|reference_system|
|schema         |
|sensor         |
|sig_class      |
|sig_reference  |
|signature      |
|tcphdr         |
|udphdr         |
+------------------+
16 rows in set (0.00 sec)
```

mysql> quit

Bye

Une fois l'installation terminée on aura un message comme quoi l'installation n'est pas complète, snort aura créé un fichier 'flag' empêchant la suite du paramétrage.

On supprime le 'flag' qui nous empêchait de le configurer :

 # rm /etc/snort/db-pending-config

On finit de faire le ménage à l'aide de la commande:

 # dpkg --configure -pending

Snort se lance à l'issue de la configuration, on vérifie:

 # /etc/init.d/snort status

Status of snort daemon(s): eth0 OK.

IV.3.3 Création de nouvelles règles

Bien que le site officiel de Snort propose des règles prêtes à l'emploi et régulièrement mises à jour, il peut être intéressant de créer ses propres règles afin d'adapter au mieux snort au réseau qu'il doit surveiller et protéger. Par convention, les nouvelles règles personnelles sont à placer dans le fichier local.rules.

Exemple de règle: alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-ATTACKS /bin/ls command attempt"; uricontent:"/bin/ls"; nocase; classtype:web-application-attack;

Cette règle permet de générer une alerte quand un paquet provient d'un couple (adresse/port) quelconque, est à destination des serveurs HTTP définis dans snort.conf, et contient la chaîne «/bin/ls » dans l'URI. Le message de l'alerte sera « WEB-ATTACKS /bin/ls command attempt ». Cette attaque sera classée dans la classe web-application-attack (priorité medium par défaut) [20].

Il est bien sûr impossible d'être exhaustif ici pour décrire le format des règles Snort. Le manuel utilisateur disponible sur le site officiel (http://www.snort.org/) indique comment utiliser au mieux le langage des signatures de Snort.

IV.3.4 Exécution

L'exécution de Snort se fait en lançant l'exécutable snort en mode root et avec différentes options. Voyons les principaux arguments de Snort :

- ✓ -A : générer des alertes. Activé par défaut avec l'option –c.
- ✓ -c <emplacement de snort.conf> : lancer Snort avec des fichiers de règles.
- ✓ -l <répertoire de log> : spécifier le répertoire où les logs d'alertes seront stockés (défaut/var/log/snort).
- ✓ -v : mode verbose. Permet d'afficher les paquets capturés.
- ✓ -T : mode test. Permet de tester la configuration de Snort.

Avant de lancer Snort en mode NIDS, il est préférable de tester si le programme arrive à récupérer les paquets qui circulent sur le réseau. Pour cela, nous pouvons par exemple lancer Snort en simple mode Sniffer : snort -v. Si aucun paquet n'est capturé et affiché, il est

probable que Snort n'écoute pas sur la bonne interface. L'option -i permet de spécifier une autre interface.

Lançons maintenant Snort en mode NIDS. Pour cela, nous lui précisons l'emplacement du fichier de configuration avec l'option –c :

#snort -c /opt/snort/rules/snort.conf .

Toutes les alertes détectées sont ainsi stockées dans le fichier « /var/log/snort/alert ». Pour chaque alerte, Snort donne une priorité, une description, les flags des paquets et éventuellement des adresses sur Internet où se trouvent de plus amples informations sur la tentative d'intrusion.

IV.3.5 Exploitation des alertes à l'aide de l'interface web ACID

Par défaut, les alertes de Snort sont enregistrées dans un simple fichier texte. L'analyse de ce fichier n'est pas aisée. C'est pour cette raison qu'il est vivement conseillé d'utiliser des outils de monitoring.

ACID (Analysis Consol for Intrusion Databases) est une interface PHP qui permet de visualiser les remontées d'alarmes générées par snort. ACID dépend de ces deux paquets :

Adodb : Contient des scripts PHP génériques de gestion de bases de données. Nous avons utilisé la librairie PHP libphp-adodb de Debian.

PHPlot : librairie de scripts PHP utilisée par ACID pour présenter graphiquement certaines données statistiques. [21]

Après avoir téléchargé ACID, PHPlot et ADODB,par la commande #**apt-get install acidbase** il faut installer ces derniers dans la racine d'Apache de la manière suivante :

#cd /var/www/

#tar -xvzf acid*

#tar -xvzf phplot*

#tar –xvzf adodb*

Une fois l'installation terminée, il convient de configurer ACID dans son fichier de configuration /var/www/acid/acid_conf.php. En ce qui nous concerne, certains champs ont été modifiés comme suit :

DBlib_path="/usr/share/php/adodb";

Chartlin_path="/var/www/phplot-5.0.5";

alert_dbname="Debian".

alert_host="localhost";

alert_user="djey";

alert_password="my_pass" ;

Voilà, maintenant nous pouvons vérifier qu'ACID est bien configuré en saisissant l'url http://localhost/acid dans le navigateur.Le résultat de ce test dans notre cas est le suivant **:**

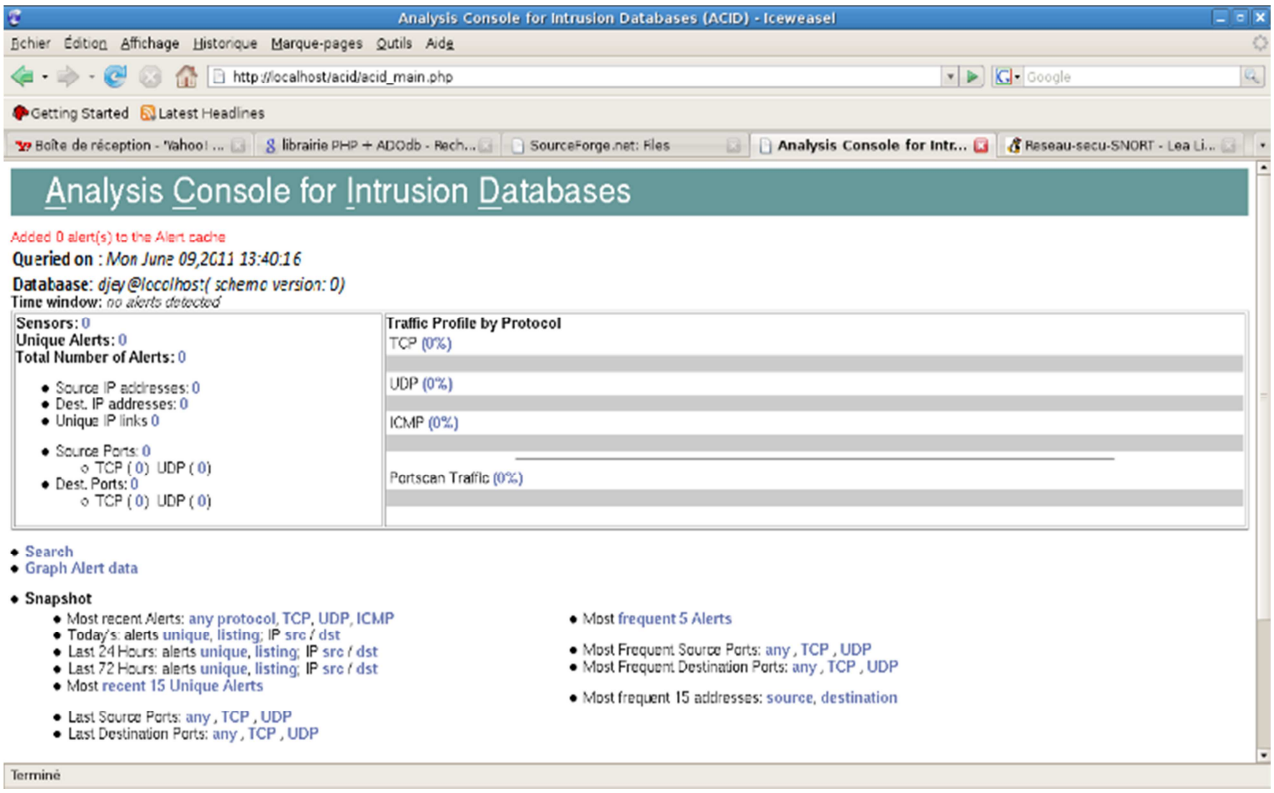

Figure IV.3 l'interface Web ACID

Pour terminer cette présentation de Snort et ces composants, nous dirons tout simplement que Snort est un très puissant outil connu comme un des meileurs sur le marché, même quand il est comparé à des IDS et IPS commerciaux. Il a une plus grande communauté d'utilisateurs et de chercheurs (de nombreux plugins, frontends, consoles de management etc.…). Sa mise en œuvre basique peut-être rapidement effectuée grâce notamment aux nombreux livres et documentations existants à son sujet.

Conclusion générale

Les attaques contre les réseaux informatiques et leurs ressources sont en augmentation constantes est devient de plus en plus sophistiquées .cette affirmation est confirmée par les rapports annuel du « Computer Emergency Response Team » (CERT), qui mentionnent aussi l'insuffisance des mesures destinées à contrer ces attaques et mettent en évidence la nécessité de toujours améliorer la protection des systèmes d'information.

Face aux attaques et menaces auxquelles les systèmes d'information sont exposés, ce travail nous a permis de savoir que l'unique porte de sortie pour les entreprises et organisations demeure la conduite d'une véritable démarche sécuritaire aboutissant à la définition d'une stratégie de sécurité claire et adaptée ; elle-même, conduisant à la mise en application d'une politique de sécurité fiable et rigoureuse.

Bien que répandus dans les organisations aujourd'hui, les systèmes de détection d'intrusions ne représentent qu'un maillon d'une politique de sécurité. C'est pourquoi, les entreprises et organisation sont recommandées à mettre en place non seulement des stratégies et politiques de sécurité, mais aussi d'adopter et d'y intégrer les nouvelles méthodes et systèmes de sécurité comme les sauvegardes hors sites, les plans de reprise d'activité et les systèmes de détection et de prévention d'intrusions.

L'étude que nous avons menée nous a permis de découvrir les systèmes de détection d'intrusion.

Il nous est paru évident que ces systèmes sont à présent indispensables aux entreprises afin d'assurer leur sécurité informatique. Cependant, nous avons pu constater également que les produits existants ne sont pas encore suffisamment fiables (notamment en ce qui concerne les faux positifs et faux négatifs) et qu'ils restent lourds à administrer.

De ce fait, pour une sécurité optimale, ces outils doivent être couplés à d'autres, comme l'indispensable pare-feu. Mais ils doivent aussi être mis à jour, aussi bien le cœur du logiciel comme la base de signatures, qui constitue la base d'une détection efficace. Il faut également coupler les systèmes de détection entre eux : c'est-à-dire ne pas hésiter à placer des NIDS, HIDS et KIDS dans le même réseau. Leurs rôles sont différents, et chacun apporte ses fonctionnalités.

Nous avons étudié le fonctionnement de ces systèmes en particulier nous avons pris comme exemple l'outil Open Source *Snort* qui est le plus réputé en terme d'efficacité et présente une souplesse en terme de personnalisation.

Toutefois, même si une certaine maturité dans le domaine de la détection d'intrusion commence à se sentir, le plus important reste de savoir de quoi il faut se protéger. Les failles les plus répandues proviennent généralement de l'intérieur de l'entreprise, et non de l'extérieur. Des mots de passe simples, des droits d'accès trop élevés, des services mal configurés, ou encore des failles dans les logiciels demeure les bêtes noires en matière de sécurité informatique.

Après tout, on est tenté de se demander « A quand la sécurité à 100% » ?

Bibliographie

[1] Sécurité informatique : principes et méthode. Bloch, Laurent. Livre 2009.

[2] Tout sur la sécurité informatique, Pillo, J-F. livre 2009.

[3] La sécurité des réseaux et des systèmes. Renaud Tabary 2009
http://www.labri.fr/perso/tabary/cours/0809/secu_lp/cours1.pdf

[4] Sécurité informatique. Sécurité des systèmes d'information. Marie Claude Quidoz 2004
http://www.dgdr.cnrs.fr/fsd/securite-systemes/revues-pdf/num51.pdf

[5] Sécurité informatique : les protocoles de sécurité, Belhadi.Hakima, Thèse de magister. Université de Bejaia 2003

[6] Portail de la sécurité informatique. Marie NAUDON et Jérôme RABENOU 2009.
http://www.securite-informatique.gouv.fr/

[7] Sécurité : la qualité, les méthodes à mètre en œuvre pour atteindre un niveau de sécurité optimale. Florence Celen 2005
http://www.ja-psi.fr/formation-securite-informatique/JA-PSI_Formation-Securite-Informatique.pdf

[8] Guide de bonne pratique organisationnelle. Jacque Lavielle 2010
http://www.dgdr.cnrs.fr/fsd/securite-systemes/revues-pdf/SI7.pdf

[9] Plan de Continuité d'Activité. Stratégie et solutions de secours du S.I. Robert Bergeron 2003.
https://www.clusif.asso.fr/fr/production/ouvrages/pdf/PlanContinuiteActivite.pdf

[10] La sécurité des réseaux informatiques. Masaudi Smail. Thèse magister. 2004

[11] Les normes de sécurité informatique. Dr AlaEddineBarouni 2007
http://xa.yimg.com/kq/groups/24705607/1476251542/name/Les+normes+Securite.pdf

[12] « IDS - Systèmes de Détection d'Intrusion, Partie I ». K. Müller. May 2003.
http://www.linuxfocus.org/Francais/May2003/article292.shtml

[13] Network Intrusion Detection Signatures. Part One. Neal Hindoucha 2003.
http://www.symantec.com/connect/articles/network-intrusion-detection-signatures-part-_one

[14] Prelude HandBook. Prelude Hybrid IDS project - Yoann Vandoorselaere 1998.
http://www.prelude-ids.org

[15] Détection et prévention d'intrusion : présentation et limites. Nathalie Dagorn 2006
http://www.netiq.com/products/sm/default.asp/hal.inria.fr/docs/00/08/42/02/PDF/RR_DetectionIntrusion.pdf

[16] Prelude HandBook . Prelude Hybrid IDS project - Yoann Vandoorselaere - 1998
http://www.prelude-ids.org

[17] L. Hamza. Génération automatique des scénarios d'attaques(IDS), Thèse de magister. Université de Bejaia 2007.

[18] N. Bouasla, H. mnie Fillali ; A.Skalli, sécurité dans les réseaux avec snort 2007.

Université d'AVIGNON. 2007

[19] K.tayeb. Détection d'intrusion coopérative basée sur la fusion de données .Thèse de Magister. Institut National de I 'informatique (INI) 2006.

[20] Snort User Manual. The Snort Project. Chris Green 2001-2003; Martin Roesch 1998-2003 http://www.snort.org

[21] Linux Server Hacks 100 Industrual-Strengh Tipsand tools; Rob Flickener;

O'Reilly and Associates . 2003.

Lists des abreviations

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

Snort: The Open Source Network Intrusion Detection System

OSI: Open Systems Inter connection

Bonux: Surnom donné à Linux par les esclaves de Microsoft.

bot nets : roBOT NETwork

Backbone: Partie central d'un réseau d'entreprise, elle permet de connecter entre eux plusieurs sous réseau et représente la zone la plus performante et la plus sure du réseau.

Backdoor: porte dérobée, une application afin de créer artificiellement une faille de sécurité.

Core-Switch: commutateur principal

Addresse IP: addresse Internet Protocol

Adresse MAC: Adresse identifiant un élément actif sur un réseau

ARP: Address Resolution Protocol

SYN: Synchronous idle. Etat de départ de l'établissement d'une connexion TCP

Nmap: Network Mapper

TCP: Transmission Control Protocol

UDP: User Datagramme Protocol

NIS: tests relatifs aux services d'informations sur le réseau

SSL: Secure Socket Layer

TLS: Transport Layer Security

IPSec: Internet Protocol sécurisé

DMZ: Demilitarized Zone

DNS: Domain Name Service

FTP: File Transfer Protocol

ICMP: Internet Control Message Protocol

ITSEC: Information Technology Security Evaluation Criteria

DoD: Department of Defense

CTCPEC: Canadian Trusted Computer Product Evaluation Criteria

JCSEC: The Japanese Computer Security Evaluation Criteria

TCSEC: Trusted Computer System Evaluation Criteria

DAC: Discretionary Access Control

MAC: Mandatory Access Control

RBAC: Role-Based Access Control

TMAC: TeaM-based Access Control

OPS: une opération représente l'image exécutable d'un programme

OBS: Osmosis Business Solutions

Clusif : Club de la Sécurité de l'Information Français

MARION : Méthode d'Analyse des Risques Informatiques et Optimisation par Niveau.

MEHARI : Méthode harmonisée d'analyse des risques, développée par le CLUSIF.

ORBAC: Organisation Based Access Control

DCSSI: Direction Centrale de la Sécurité des Systèmes d'Information

CST: Centre de la Sécurité des Télécommunications

NSI: National Standards Institue)

ISO: Organisation internationale de normalisation

KIPS: Kernel Intrusion Prevention System

KIDS: Kernel Intrusion detection System

NIPS: Network Intrusion Pevention System

HIDS: Host Intrusion-based detection System

NIDS: Network-based Intrusion detection System

bad login : mal identifient

DoS: attaques dont le but est de rendre indisponible des services

CPU: Central Processing Unit

NFR: Network Flight Recorder (system)

NNIDS: Node Network Intrusion detection System

IDS hybrids: hybrids Intrusion detection System

NIPS: Network Intrusion Pevention System

HIPS: Host Intrusion Pevention System

HTTP: HyperText Transfert Protocol

FTP: File Transfert Protocol.

SMTP: Simple Mail Transfer Protocol

Asic: Application specific integrated circuit

CGI: Common Gattaway Interface

Résumé

En se basant sur les études et enquêtes menées à travers le monde, on se rend bien compte qu'il devient de plus en plus compliqué de garantir la sécurité des systèmes d'informations.
Cette situation qui est essentiellement due à la multiplication inquiétante des menaces en matière de sécurité informatique s'explique par la multiplication des outils permettant de réaliser les attaques informatiques et par la décroissance continue du niveau de connaissance nécessaire pour l'utilisation de ces outils. Face à cette situation, de nouvelles solutions et mesures de sécurité n'ont pas aussi cessé de voir le jour et de se proliférer.
Cependant le problème qui se pose toujours c'est de savoir comment mettre en place ces mesures et solutions de sécurité efficacement afin de réellement protéger les systèmes d'information car le fait d'associer et de multiplier les solutions de sécurité sans analyser au préalable leur compatibilité et leurs objectifs respectifs n'a jamais été une solution fiable.
Dans ce contexte, les stratégies de sécurité dont l'implémentation se traduit par la définition et la mise en application d'une politique de sécurité constituent le meilleur moyen d'atteindre les objectifs de la sécurité informatique.
Malheureusement, on se rend bien compte aujourd'hui que malgré toutes les mesures et stratégies de sécurité qu'on peut mettre en place, les systèmes d'informations restent néanmoins vulnérables à certaines attaques ciblées ou à des intrusions. C'est pourquoi depuis quelques années, les experts de la sécurité parlent de plus en plus d'un nouveau concept à savoir la détection d'intrusion. L'étude de la détection d'intrusion nous permettra de mieux comprendre les systèmes de détection et de prévention d'intrusions et de voir comment ils arrivent à renforcer la sécurité en fermant les trous de sécurité laissés par les mesures classiques de sécurité.

Mots clés : politique de sécurité, détection et prévention d'intrusion, l'IDS snort

Abstract

Based on studies and surveys around the world, it realizes that it is becoming increasingly difficult to guarantee the security of information systems.
This situation which is principally owed to multiplication worrying threads in computer security explain by the multiplication of tools allowing to accomplish the computer attacks
and by the uninterrupted reduction of the level of necessary knowledge for the use of these tools. Faced with this situation, new resolutions and safety measures also did not cease coming into the world and proliferating.
However the problem which always settles it is to know how to set up these measurements and resolutions of security efficiently to really protect information systems because the fact of associating and increase security solutions without analyzing their compatibility in advance their respective goals and has never been a reliable solution.
In this context, a Security policy whose implementation results by the definition and implementation of a security policy is the best way to achieve the goals of computer security.
Unfortunately, it is very obvious now that despite all the measures and security policies that can be put in place, information systems still remain vulnerable to some targeted attacks or intrusions. That is why in recent years, the security experts talk more and more a new concept namely, the intrusion detection. The study of intrusion detection will allow us to better understand detection systems and intrusion prevention and see how they manage to strengthen security closing security holes left by traditional security measures.

Key words: Security Policy, detection and intrusion prevention, the snort IDS