MISE EN PLACE D'UN IPS PAR DETECTION D'INTRUSION A TROIS NIVEAUX ET

Mr A.RADI (Ingénieur Télécoms & Doctorant), **Mr. B. REGRAGUI** (PES), **Mr A. RAMRAMI** (consultant en SI)
a.radi@amitt.ma , regragui@ensias.ma , azzeddine.ramrami@free.fr,

Université Mohammed V-Agdal / Faculté des Sciences - Rabat Maroc,
Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes Rabat Maroc,
Université Mohammed V-Agdal / Faculté des Sciences - Rabat Maroc,

Mots Clés:
Sécurité des réseaux, attaques, systèmes de détection d'intrusions, scénario, corrélation des alertes, fusion de données, prévention d'intrusions.

Key words:
Security of the networks, attacks, Intrusions detection systems, scenario, alerts correlation, fusion of data, intrusions prevention.

Las palabras clave:
Seguridad de las redes, ataques, sistemas de descubrimiento de intrusiones, el guión, correlación de las alarmas, fusión de datos, prevención de intrusiones,

Résumé

L'omniprésence des outils informatiques s'intensifie chaque année dans les entreprises. Ils intègrent des équipements, des données et des services qui constituent des richesses à protéger. De nombreux mécanismes ont été développés pour assurer la sécurité des systèmes d'Informations « SI ».
Les systèmes de détection d'intrusions « IDS » ont montrées leurs insuffisances pour la protection du réseau de l'intérieur et à la prévention des intrusions, sachant que 70% des attaques causent des dégâts viennent de l'intérieur du SI.
L'approché proposée dans ce papier consiste en la définition d'une politique de sécurité globale à trois niveaux. C'est une nouvelle méthode intéressante qui permettra aux responsables de la sécurité des SI « RSSI » de détecter, prévenir même des intrusions et l'application des réponses proactives.

1 Introduction

La sécurité des SI vise à protéger l'accès et la manipulation de ses données et ressources par des mécanismes d'authentification, d'autorisation, de contrôle d'accès, etc. Néanmoins, avec l'ouverture et l'interconnexion des SI le contournement des mécanismes de sécurité est toujours possible. Il n'est donc pas suffisant d'agir préventivement, par la définition d'une politique de sécurité, en termes de confidentialité, d'intégrité et de disponibilité « D.I.C » des données et ressources du SI à protéger, mais il faut aussi être capable de détecter toute tentative de violation de cette politique, c'est-à-dire toute intrusion. A cette fin, on peut mettre en place un IDS, ce qui implique une surveillance permanente des actions entreprises sur le système afin de s'assurer de leur légitimité. [1]

2 Méthodes et systèmes de détection d'intrusions

2.1 Détection d'intrusions

La détection d'intrusions a été introduite en 1980 par J.P Anderson qui a été le premier à montrer l'importance de l'audit de sécurité [2] dans le but de détecter les éventuelles violations de la politique de sécurité d'un système. S'ajoutent en suite les travaux de Denning [3], qui posent les fondations de la détection d'intrusions.

2.2 Sécurité des attaques et propriétés

Partant du principe que la fonction d'un SI est de fournir de l'information et ressources aux utilisateurs. Par conséquent, il y a un flux de données échangé entre une source (ex: hôte, serveur,…) et une destination (ex: hôte, serveur,…) sur un canal de la communication (ex: fil, onde, bus du données,…). La tâche du système de la sécurité est restreindre l'accès à cette information seulement aux parties (personnes ou processus) qui sont autorisées d'avoir l'accès, selon une politique de la sécurité mise en place**.**

Le flux normal d'information est visé par plusieurs catégories d'attaques qui sont illustrées dans la figure -1 (d'après [Stalling, 2000]) [4] :

- **Interception**: tierce partie intercepte les données sans pour autant les modifier.
- **Modification : l**'information est interceptée et modifiée de manière non autorisée.
- **Interruption :** de toutes ou partie des données et ressources d'un SI afin de les rendre inutilisables ou non fiables.
- **Mascarade** : insertion des faux objets dans le SI en prétendant être la source légitime.

Ces quatre classes d'attaques violent différentes propriétés de la sécurité du SI (D.I.C.).

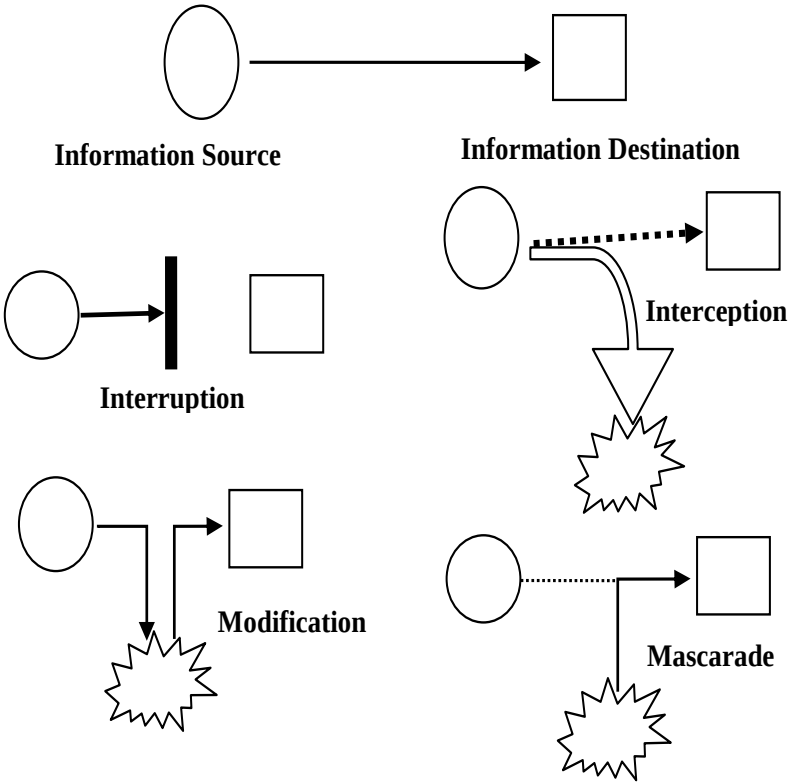

Figure 1: Catégories d'attaques.

2.3 Systèmes de détection d'intrusions

Il n'est pas envisageable de détecter les intrusions manuellement car le volume d'informations à analyser est immense. Les IDS sont des outils (logiciels et/ou matériels) charges d'analyser les flux de trafic dans le réseau pour y détecter automatiquement des actions non autorisées effectuées dans SI surveillés.[1]
D'après [Dacier et al, 1999], un IDS doit accomplir les exigences suivantes [4]:

- **L'exactitude** : ne pas détecter une action légitime comme une action malicieuse (faux positif).
- **La complétude** : ne pas manquer une vraie intrusion (fausse négative).
- **La performance** : effectuer une détection temps réel (avant que des dégâts considérables soient produits).
- **Résistance** : devrait être résistant aux attaques.
- **Remontée** : être capable de fonctionner, au cas pire, avec un nombre important d'événements sans laisser tomber d'information.

2.4 Classification des IDS

Un grand nombre d'IDS ont été développés à ce jour, dans [5,6] on comptabilise une centaine d'outils commerciaux dans le domaine public ou bien prototypes de recherche.
Les critères de classification des IDS illustrés dans la figure -2. sont [7]:

- le principe de détection utilisé,
- le comportement en cas d'attaque détectée,
- la source des données à analyser,
- La fréquence d'utilisation.

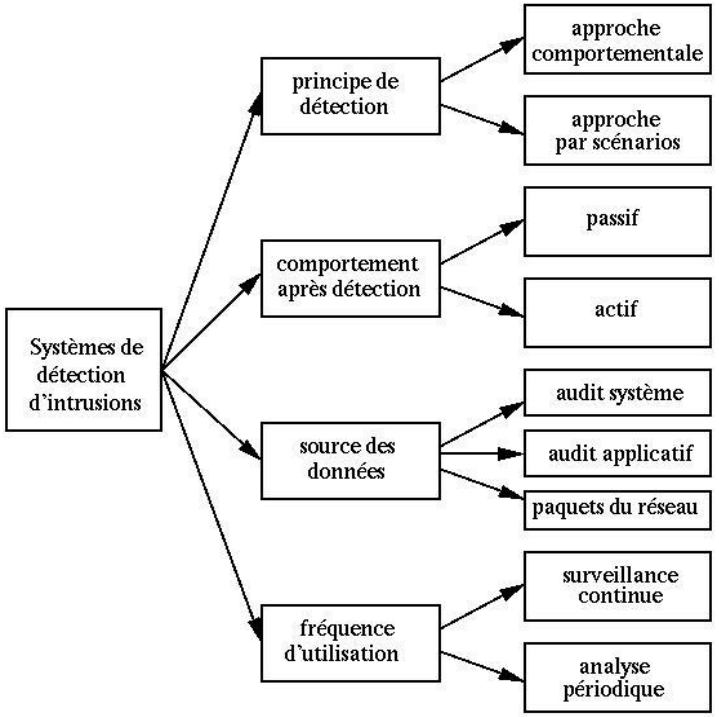

Figure 2: Classification des IDS

Les deux critères les plus importants qui sont : la nature des données analysées (trafic réseau, audits système et audits applicatifs) et la méthode d'analyse utilisée (comportementale ou par scénario) [8], que nous allons détailler par la suite.

- **Analyse par scénarios :** technique la plus utilisée, nécessite une base de connaissances des scénarios des attaques interdites au niveau de la source de données (figure-3). Ainsi, tout ce qui n'est pas explicitement interdit est autorisé. Pour gérer cette base des scénarios, plusieurs techniques sont utilisées, les plus connues : Pattern matching, Détection par inférence, Algorithmes génétiques et Systèmes experts.

```
Alert tcp $EXTERNAL_NET any -> $IXTERNAL_NET 80
(msg : « WEB-PHP edit_image.php access » ;
flow:established,to_server;
uricontent:"/edit_image.php";
reference :nessus,11104 ;
reference :cve,CVE-2001-1020 ;
classtype:web-application-activity;
sid:1999;
rev:1;)
```

Figure -4 : Exemple d'une Signature

- **Analyse comportementale:** Dans cette analyse, un modèle de comportement « normal » du système surveillé, des utilisateurs, des applications, etc. est préalablement construit. Toute déviation significative du comportement courant par rapport au comportement de référence est signalée comme étant suspect et donne lieu à une alerte (figure-5) [9, 10]. L'avantage principale de cette approche, c'est qu'elle peut détecter des attaques inconnues, ce pendant la construction du modèle de référence n'est pas facile, elle se fait le plus souvent par apprentissage.

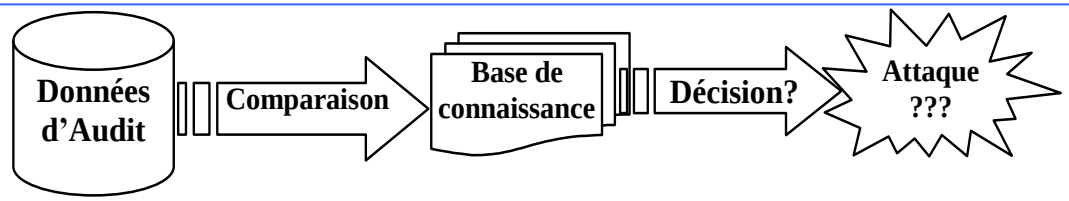

Figure -3 : schéma synoptique de l'analyse par scénarios

Figure 5 : schéma synoptique de l'analyse comportementale

La construction du modèle de référence se fait le plus souvent par apprentissage. Debar [11] propose par exemple d'utiliser des réseaux de neurones; Forrest et al [12] proposent pour leur part d'appliquer une approche immunologique. Des méthodes statistiques ont aussi été suggérées dans [13]. Le modèle peut aussi être construit par spécification de politiques de sécurité, comme dans l'approche de Zimmermann et al [14].

3 Mise en place d'un IPS par détection d'intrusion à trois niveaux

Les approches classiques présentées ci-dessus ont montrées leurs insuffisances quand à la protection du réseau, en particulier, de l'intérieur. Ils permettent uniquement la sécurisation du réseau de l'entreprise en son point d'entrée contre les attaques provenant de l'extérieur. Cependant, selon des études réalisées ont montré que 60 à 70% des attaques proviennent de l'intérieur des SI. [15]:

1.1. Garthner Inc.: 70% des attaques causent des dégâts proviennent de l'intérieur du réseau.
1.2. IDC et Pricewaterhouse Coopers : les entreprises ont enregistrés une hausse de 44% entre 2004 et 2005 pour les attaques provenant de l'intérieur.

D'autres études réalisées ont montré que via un ordinateur portable ou des logiciels, qui sont disponibles gratuitement sur le web, un pirate peut facilement avoir un accès à distance sur le réseau interne de l'entreprise, en prenant le contrôle sur une machine et peut, ainsi, naviguer sur le réseau interne de l'entreprise comme un utilisateur normal. D'où l'idée de chercher des solutions permettant la protection du réseau de l'intérieur.

La solution proposée, dans ce qui suit, venant compléter certaines lacunes relatives aux approches classiques. Elle consiste en la définition d'une politique de sécurité globale à trois niveaux, cette solution proposée sera plus adaptée aux grandes entreprises ayant un grand réseau desservant plusieurs départements.

C’est une nouvelle méthode qui parait intéressante, dans le but d'offrir aux RSSI de nouveaux techniques, adéquat quant à la résolution des problèmes relatifs à la sécurité des réseaux.

3.1 Niveau 1 : Protection externe

Le premier niveau de détection consiste on l’utilisation d’un IDS tournant avec une approche classique mono ou hybride profitant des avantages des approches précitées. Ce système sera capable de détecter des intrusions provenant de l’extérieur sur la base de scénarios d'attaques et/ou de profils empiriques, il sera donc placé à l’entrée du réseau. Ce niveau à pour objectif principale de protéger le réseau interne des attaquants externes.

3.2 Niveau 2 : Politique de sécurité fonctionnelle

Le second niveau de détection consiste on la définition d’une politique de sécurité fonctionnelle, c'est-à-dire tenant compte des tâches attribuées aux utilisateurs au sein de l’entreprise par la segmentation du réseau en réseau local virtuel « VLAN : Virtuel Local Area Network» et l’utilisation des listes de contrôle d’accès « ACL : Access Control Lists». Ainsi :

- les utilisateurs d’un même département, ou de plusieurs départements, et qui sont susceptibles de communiquer et/ou de partager des données entre eux seront configurées dans le même VLAN.
- les machines Gateway des différents VLAN seront configurées avec des ACL définissant la liste des actions autorisées pour les utilisateurs appartenant au VLAN (toutes les autres actions étant interdites) ou le contraire. Aussi, l’utilisation des VLAN, vue leur fonction de blocage des broadcastes, permettent au pire des cas, si un attaquant a réussi à prendre le contrôle d’une machine appartenant à un VLAN (tel que : lancement de virus, vert, …) l’attaque sera restreint à ce petit segment du réseau et ne va pas contaminer le réseau tout entier.

Ce niveau à pour objectif principale de protéger le réseau interne des attaquants internes qui peuvent abuser des droits qui leur sont octroyés. Comme il peut aussi protéger le réseau interne des attaquants externes qui arrivent à s’infiltrer par usurpation.
Cette configuration permet à l’administrateur d'enregistrer toutes actions effectuées sur le système par chaque utilisateur ou groupe d’utilisateur. Une analyse ultérieure des informations enregistrées permettra de prévenir et de détecter d'éventuelles intrusions ou tentatives d’intrusions.
Aussi, on peut prévoir la possibilité d’offrir à l’utilisateur, dans le cadre de la politique de sécurité interne, une marge de paramètres spécifiques de protection locale à sa demande. Cette action visera deux objectifs :

- ✓ le 1er objectif ; le renforcement de la sécurité globale du réseau de l’entreprise.

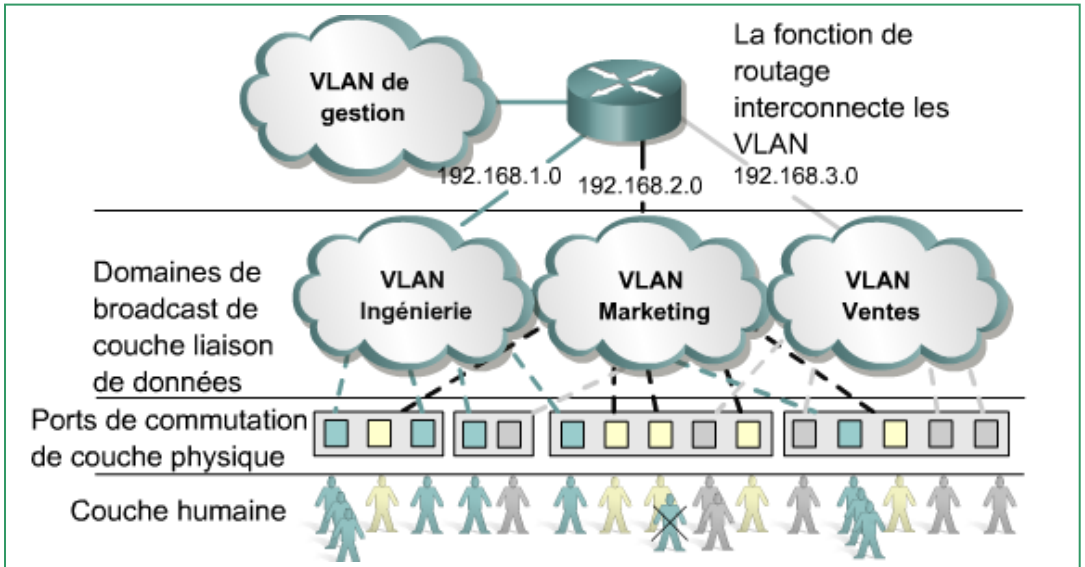

Figure 6 : Organisation de réseau en VLAN

- ✓ le 2è objectif ; l'implication de l'utilisateur dans la politique de sécurité globale du réseau de l'entreprise.

3.2.1 Sécurité par utilisation des LAN virtuels [16]

Un VLAN est un domaine de broadcast créé par un ou plusieurs commutateurs. La structure des réseaux présentés dans la figure-6 et montrent trois domaines de broadcast distincts.
Le routeur achemine le trafic entre les VLAN à l'aide du routage de couche 3 et contrôle l'accès aux VLANs.
Le Switch transmet les trames aux interfaces du routeur, s'il s'agit de trames de broadcast ou si elles sont destinées à l'une des adresses MAC du routeur.
L'en-tête d'une trame est encapsulé ou modifié pour inclure un identificateur (ID) de VLAN avant que la trame ne soit envoyée sur la liaison entre les commutateurs, et à l'arrivée le format d'origine de la trame est rétabli avant le transfert vers l'unité de destination.

Configuration des VLAN

***Creation**

```
sw1#vlan database
sw1(vlan)#vlan 500 name marketing
VLAN 500 added:
 Name: marketing
sw1(vlan)#vlan 700 name ingenierie
VLAN 700 added:
 Name: ingenierie
sw1(vlan)#exit
Exiting....
sw1#sh vlan
VLAN Name  Status Ports
---- -------------------------------- -----------
1 default   active  Fa0/3, Fa0/4, Fa0/5, Fa0/6
.....       Fa0/23
500 marketing  active Fa0/2
700 ingenierie  active
```

***Encapsulation**

```
rabat#conf t
rabat(config)#int f0/0.500
rabat(config-subif)#encapsulation dot1Q 500
rabat(config-subif)#ip address 131.107.1.1 255.255.0.0
rabat(config-subif)#exit
rabat(config)#int f0/0.700
rabat(config-subif)#encapsulation dot1Q 700
rabat(config-subif)#ip address 131.107.2.1 255.255.0.0
rabat(config-subif)#end
```

3.2.2 Sécurité par utilisation des ACL [16]

Les ACL se sont des groupes d'instructions de condition qui sont appliquées au trafic circulant via les interfaces de routeur, ces instructions indiquent au routeur les types de paquets à accepter ou à rejeter. L'acceptation et le refus peuvent être basés sur des conditions qui portent sur les @ source et destination, les protocoles et les numéros de port de couche supérieure (figure-7).
Les principales raisons pour lesquelles il est nécessaire de créer des ACL :

- ➢ Limiter le trafic réseau et accroître les performances.
- ➢ Fournir un niveau de sécurité d'accès réseau.
- ➢ Permettre le contrôle d'accès au réseau.

La configuration suivante montre la syntaxe globale pour la création d'une ACL standard nommée *Internetfilter* et d'une ACL étendue nommée *marketing_group* :

```
interface  ethernet0/5
ip  address  192.168.5.1   255.255.255.0
ip  access-group  Internetfilter  out
ip  access-group  marketing_ group  in
ip  access-list  standard  Internetfilter
permit  10.1.1.1
deny any
ip  access-list  extended  marketing_ group
permit  tcp any 172.30.0.0 0.255.255.255  eq telnet
deny  udp  any  any
deny  udp  any  171.30.0.0  0.255.255.255  lt  1024
```

deny ip any log

3.2.3 Remarque : **L'emplacement des ACL est très important. Si les ACL sont correctement placées, non seulement le trafic peut être filtré, mais tout le réseau devient plus performant. L'ACL doit être placée à l'endroit où elle aura le plus grand impact sur les performances.**

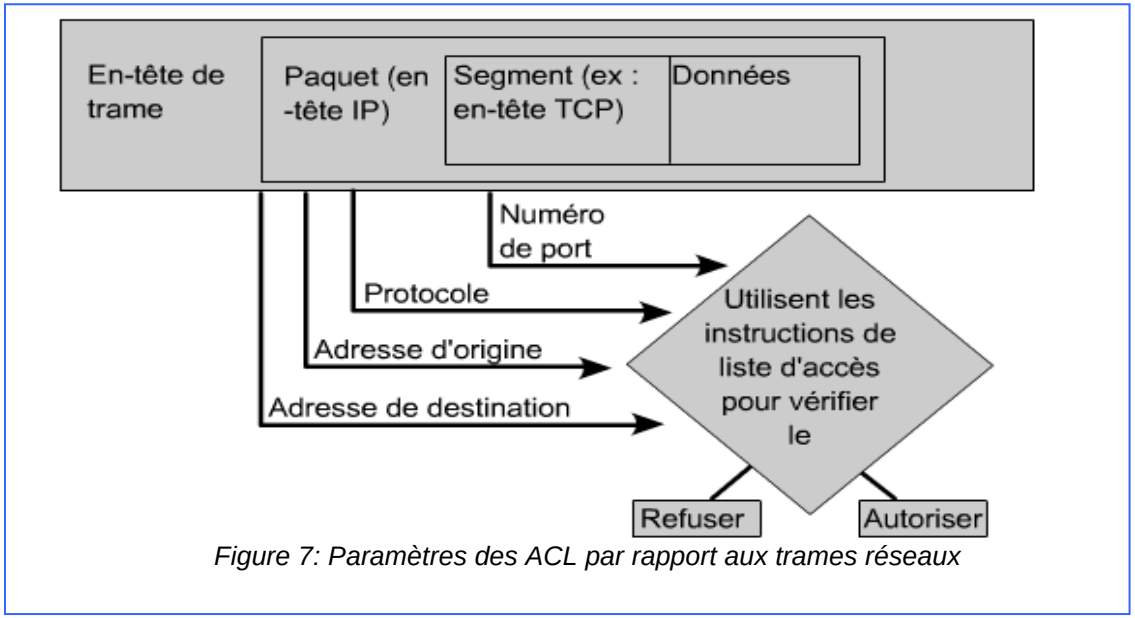

Figure 7: Paramètres des ACL par rapport aux trames réseaux

3.3 Niveau 3 : Politique de sécurité opérationnelle

Le troisième niveau de détection, qui vient renforcer le deuxième niveau, consiste on la définition d'une politique de sécurité opérationnelle via un mécanisme de corrélation de données de la liste de contrôle d'accès physique aux locaux de l'entreprise et la liste de contrôle d'accès logique aux machines des utilisateurs. C'est-à-dire ne permettre l'accès au réseau de l'entreprise qu'aux utilisateurs qui sont réellement opérationnels au sein de l'entreprise. Ce contrôle limitera l'usurpation d'identité de l'intérieur ou de l'extérieur.

Ces niveaux de détection d'intrusions permettent de détecter automatiquement les violations de la politique globale de sécurité au lieu de se contenter d'une base de scénarios d'attaques ou de profils empiriques.
L'analyse du comportement du réseau dans cette approche permettra de connaître le trafic anormal d'une machine sur le réseau tel que :

- Tentative de connexion au serveur réseau par utilisateur qui n'est pas présent dans l'entreprise (en congé, ou en mission, …).
- Tentative de connexion sur une machine ou ressource non autorisée pour cet utilisateur.
- Recherche de services spéciaux non accessibles pour un utilisateur.

La détection de ce genre d'attaques est alors automatiquement réalisée et des actions de réaction active ou des contre mesures peuvent être paramétrés (blocage du trafic en provenance ou vers la machine source ou carrément l'isolement total de cette machine), ce qui va améliorer les performances de notre IDS en se transformant en un système de prévention d'intrusion « IPS: Intrusion prevention System ». Ainsi, l'analyse du fichier log permettra de comprendre comment l'intrus a pu pénétrer dans le réseau et la modélisation de ce scénario servira pour la mise à jour de la base des scénarios utilisée au niveau 1. D'où l'amélioration des performances de notre IDS au niveau 1, et par la suite notre système devient de plus en plus sûre.
Potentiellement, cette voie présente un double avantage :

- la politique de sécurité globale est explicitement définie, ce qui n'est pas le cas avec les méthodes classiques. L'adéquation de la base de scénarii ou des profils à une politique donnée est en effet un problème délicat ;
- l'audit observé étant désormais comparé à une politique et non à une base de scénarii, un tel système peut théoriquement détecter de nouvelles attaques. De même, la comparaison de l'audit à une politique et non à un profil doit réduire considérablement le taux de faux négatifs engendrés par le système car un comportement inhabituel, mais légitime, ne doit pas être signalé.

Les approches présentées au paragraphe §2.4. sont rendues nécessaires par le fait que les mécanismes de contrôle d'accès et d'authentification, implémentés dans les systèmes informatiques utilisés, ne suffisent pas à assurer les propriétés de la disponibilité, de l'intégrité et de la confidentialité requises.
Leurs failles peuvent théoriquement être résolus en utilisant des modèles de contrôle de transfert de flux d'informations entre différentes parties du réseau et en cas de difficulté en passe au contrôler de l'accès à l'information (c'est-à-dire l'accès à un objet du système). Dans ce cas, une intrusion correspond à l'accès à un objet réalisé dans un contexte dans lequel la capacité d'effectuer cet accès ne devrait pas exister.
De façon générale, l'approche consiste à associer des droits particuliers à des scénarii d'exécution logique (c'est-à-dire à des séquences d'opérations causalement liées). Les droits détenus par un sujet particulier évoluent ainsi dynamiquement au cours de l'exécution, on considère qu'une intrusion se produit lorsqu'un ensemble de droits qui ne sont pas liés permet d'exécuter une opération interdite par la politique de sécurité globale ou locale.

4 Corrélation de données dans le domaine de la Détection d'Intrusion

Dans notre étude, précitée, nous avons proposé un système de détection à trois niveaux. Chaque niveau va nous fournir un nombre d'alertes qui va alourdir le système. Pour résoudre ce problème on propose l'utilisation de la Corrélation de données.

4.1 Définition

D'après Arian Mavriqi, de l'université de Graz: *"La Corrélation de données est l'association de plusieurs événements détectés via différentes méthodes et sur lesquels nous appliquons différentes techniques dans le but de déterminer si les évènements détecter son relier entre eux, et si oui de quelle manière. Cette méthode de corrélation nécessite la comparaison de différents paramètres tels que l'IP source/destination, les commandes entrées par le probable attaquant, le temps de la session etc... Toutes ces sources d'informations peuvent venir de détecteurs déployés sur le réseau, de fichiers log, ou des bases de données dédiées à la détection d'intrusion."*. [17]

4.2 Corrélation de données

Donc pour avoir des résultats de détection pertinents, d'après la définition ci-dessus, l'acquisition progressive de beaucoup d'informations nous pousse à faire appel à une méthode appelée « Agrégation de données ». Dans notre cas, nous avons trois types de fichiers logs possible, un par niveau.
En général, il existe 4 méthodes de Corrélation de données :

- Corrélation d'après des attaques similaires

- Corrélation basée sur des scénarios prédéfinis
- Corrélation par analyse statistique (statistical analysis).
- Corrélation d'après les informations que nous avons avant et après l'attaque.

La corrélation de données est un outil important pour améliorer la surveillance les événements en sécurité; son but principal est de réduire le volume des données à traiter afin de détecter les intrusions et les notifier à un administrateur pour qu'il puisse décider de la réponse adéquate à l'attaque subie. D'autre part, le but ultime de la corrélation de données est de réduire le temps d'exposition à une attaque, D'après Winn Scgwartau (1999) le temps d'exposition doit être égal au temps de détection plus le temps de réaction (le temps nécessaire pour résoudre le problème).
Dans notre approche, la corrélation des informations des niveaux 2 et 3 permettra non seulement de réduire le temps d'exposition mais aussi, une réaction plus pertinente voir l'implémentation de réponses actives.

Exemple : la détection d'une intrusion provenant d'un hôte dont l'utilisateur est absent de son bureau, permettra de prendre les décisions suivantes :

- ✓ blocage de l'hôte suspecté.
- ✓ blocage de l'adresse source au niveau du firewall à l'entrée du réseau.

D'autre part, l'approche aidera énormément l'administrateur dans le problème des faux positifs et négatifs, car nous pouvons désormais corréler des données tenant compte, du contexte dans elles se présentent. Exemple : si un utilisateur est entrain d'utiliser une application Peer-to-Peer et le service FTP, l'administrateur remarquera dans les fichiers log plusieurs requêtes du même hôte, il va donc considérer c'est une attaque, tandis qu'il est sûrement probable que cela soit lié à l'utilisation de l'application Peer-to-Peer. Donc avec un IDS habituel, ce type d'événements serait listé comme une intrusion, tandis que grâce à la corrélation de données dans notre approche, on déduit que cet événement était lié à l'utilisation normale d'une application.

4.3 Technique pour la corrélation.

D'après la définition de la corrélation de données précitée, et afin d'avoir des résultats plus intéressants et pertinents, il faut recourir à l'application de certaines théories à l'ensemble d'évènements afin de déduire des corrélations entre elles. Parmi ces méthodes :

- ❖ Datamining: son principe et de déterminer des relations dans un ensemble de données, pour ensuite les analyser et les classifier selon des catégories. Le Data Mining nous extrait des relations qui ne sont pas évident à déduire par une analyse humaine sur un nombre important de variables avec une base de données de grande taille. Cette méthode, nous pouvons aussi prédire des évènements, ou encore détecter des informations cachées. Il existe deux principales méthodes en Data Mining qui sont : la Classification (classer des éléments dans des classes connues, par exemple les bons et les mauvais clients, qu'on parlera aussi d'apprentissage supervisé) et le Clustering (regrouper les éléments ayants des comportements similaires dans des classes, inconnues au départ).
- ❖ Système expert: Permet d'identifier des attaques connues, peut aussi détecter des intrusions grâce à l'implémentation de scénarios d'intrusion déjà connus. Cette méthode est fiable et flexible.
- ❖ Réseaux neuronaux: Permet d'identifier les caractéristiques d'utilisateurs au sein d'un système et identifier les variations de comportement de ces derniers. Son principal avantage est qu'il est capable d'analyser les données, même si elles sont incomplètes ou biaisées.

- ❖ Réseaux sémantique: Représentation graphique d'une méthode de raisonnement. Peut être utile pour représenter des relations entre des fichiers log et leurs inheritances.
- ❖ Inférence statistique: Processus aléatoire du comportement d'une population observé pendant une période finie dans le temps.

4.4 Sélection des informations à corréler

A première vue, il semble évident que l'on peut corréler la totalité des informations que nous pouvons collecter du réseau (IDS, Firewall, système de contrôle d'accès, Honeypot, ...), cependant, certaines d'entre elles sont inutiles à la corrélation, parce qu'elles peuvent soit prendre trop de temps à être corréler, où alors leur corrélation surcharge le "processing time" de notre système. Nous allons donc les sélectionnées.
Le NCSA (**National Centre For Super-computing Application)** [17], selon une étude effectuée sur les informations collectées, a répertorié et analysé les fichiers logs des applications les plus utilisées par les administrateurs réseaux qui sont: Netflow, DNS, DHCP, http, FTP, SMTP, SSH, Telnet, IDS/IPS et la base de données d'attaques.

L'avantage de ces logs est qu'ils sont compréhensibles et offrent une analyse intéressante du trafic réseaux, à condition de les sélectionner pour ne pas surcharger le réseau et investir dans des outils tel qu'une base de données d'attaques dont le coût d'administration, peut s'avérer très élever.
En outre, d'autres sources de données peuvent être utiles pour notre système de corrélation, tel que les résultats d'audit de vulnérabilités ou de sécurité.

D'après l'étude précitée, les informations les plus importantes à corréler sont :

- **Date/heure**
- **Protocole**
- **IP source**
- **IP destination**
- **Port source**
- **Port destination**
- **Taille des paquets**

Et en complément à notre approche, on aura besoin des informations suivant :

- **Nom de l'utilisateur**
- **Identificateur de l'utilisateur**
- **Numéro de série de sa carte d'accès**
- **Code d'accès de l'utilisateur**
- **Vlan de l'utilisateur**
- **Etat : opérationnel/absent**

4.5 Fusion de données

Toutefois, dans le premier niveau on peut faire appel à un autre processus de corrélation qui est la fusion de données communes entre les trois niveaux pour avoir une seule information. C'est la capacité pour un système de mixer des séquences qui sont similaires en fonction des évènements récupérés. Exemple: Supposons, qu'un intrus arrive à pénétrer dans le réseau et tente d'accéder à une source d'information via la machine ciblé non autorisée à y accéder. Dans ce cas nos trois systèmes N1, N2 et N3 vont simultanément générer une alerte. Grâce à la Fusion de données, ont peu aidé le travail de l'analyste en mixant les alertes contenant la même @IP source/@IP destination et même port source/port destination pour n'en faire qu'une. Donc la fusion de données réduira énormément taux d'alertes qui doit être analysé. Cela est très important quand nous savons que jusqu'à plus de 35% des alertes de nos différents systèmes sont ne seront pas traitées.

En plus, si on arrive à avoir un format commun des logs des différents outils de détection d'intrusion, le taux de traitement sera réduit d'avantage. En général, le manque de format commun aux fichiers de logs des différents outils de détection d'intrusion utilisés reste l'une des barrières au déploiement de la fusion de données.

4.6 Critères pour établir un système fusion

Les principaux critères que nous devons respecter lors de la fusion des alertes ont été mis en évidence dans un article publié 1990 par Waltz et Llinas. Même si il est fortement improbable qu'un système remplisse tous ces critères, plus ces critères seront respectés et meilleur la fusion sera :

- Distinguer les paramètres avec intérêt ;
- Distinguer parmi des objets différents dans l'espace et le temps ;
- Prélever les données avec une fréquence assez courte ;
- Fournir des résultats précis ;
- Fournir un accès aux données brut et aux données corrélées ;
- Utiliser un format commun pour les alertes ;

5 Architecture générale du système IPS proposé

La figure-8 ci-contre résume les étapes importantes du processus de notre système IPS. Nous avons besoin d'amasser des données à partir des fichiers log des différents niveaux de notre système, ensuite de réaliser l'agrégation de données, fusionner les alertes et enfin corréler les informations dans le but de détecter des intrusions ou des tentatives d'intrusion.

Dans le cas de la détection d'une intrusion issue du niveau N2 ou N3, la corrélation de données permettra à l'administrateur de déterminer l'origine de l'attaque ou de la menace par reconstitution de l'information initiale dans le but de mettre en évidence qu'est ce qui c'est vraiment passé. Cette méthode est appelée **Event Reconstruction** qui sera d'une grande utilité pour l'administrateur :

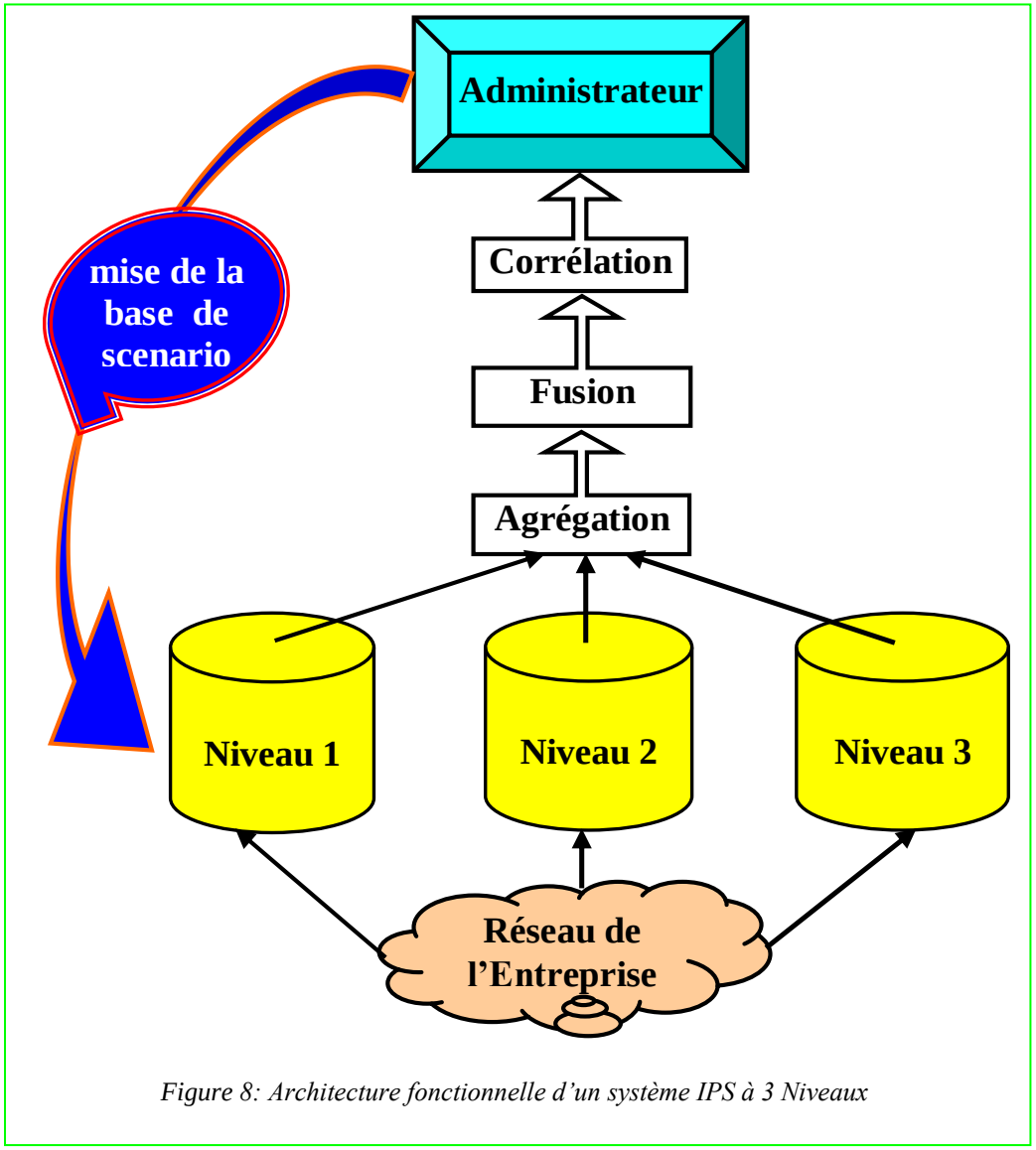

Figure 8: Architecture fonctionnelle d'un système IPS à 3 Niveaux

- ✓ parce qu'il aura accès à une meilleure compréhension des besoins du système.
- ✓ peut identifier les failles restantes sur notre système et donc y appliquer une meilleure politique de sécurité.
- ✓ mettre à jour la base des scénarios au niveau 1.
- ✓ amélioration en continu des performances de notre système. Plus qu'il y a de tentatives d'attaques plus notre IPS devient plus performant, (ceci nous rappel le proverbe : le coup qui ne casse pas le dos l'endurcit).

6 Conclusion

Nous avons montré que la détection d'intrusions dans les réseaux ne vient pas concurrencer les mécanismes de sécurité traditionnels mais, au contraire, les compléter. Même si on ne peut pas atteindre une sécurité absolue, la détection des intrusions permettra au moins d'y remédier et d'améliorer les performances du système. Nous avons également présenté les principes mis en œuvre par les IDS pour atteindre leur but. Finalement, nous avons vu que de nombreux problèmes restent à résoudre avant que la détection d'intrusions soit fiable.

Nous avons présenté dans ce papier les principales méthodes qui résident au cœur des IDS et qui utilise l'une ou l'autre des deux approches : l'approche comportementale et l'approche par scénario. Nous avons vu que chaque approche présente ses avantages et ses inconvénients. Pour contourner ces inconvénients, diverses voies de recherche sont aujourd'hui explorées. Parmi celles-ci, celle qui vise à proposer des systèmes capables de détecter automatiquement les violations de la politique de sécurité que l'on souhaite mettre en place sur le SI. Nous avons présenté, en bref, une telle approche se basant sur un système de détection à trois niveaux qui permettra de prévoir des intrusions :

- ➢ niveau 1 : « protection externe »; consiste en l'utilisation IDS mono ou hybride profitant des avantages des deux approches classiques précitées.
- ➢ niveau 2 : « politique de sécurité fonctionnelle »; consiste en la définition d'une politique de sécurité fonctionnelle, c'est-à-dire tenant compte des tâches attribuées aux utilisateurs au sein de l'entreprise.
- ➢ niveau 3 : «politique de sécurité opérationnelle »; consiste en la définition d'une politique de sécurité opérationnelle via un mécanisme de corrélation de données entre la liste de contrôle d'accès physique au locaux de l'entreprise avec la liste de contrôle d'accès logique sur machine de l'utilisateur.

D'autres voies de recherche nous paraissent également intéressantes comme la coopération inter-IDS et l'utilisation d'agent intelligent,
Sur le dernier chapitre, nous avons mis en évidence le processus et le fonctionnement la corrélation de données. Nous avons listé les différentes formes de données à corréler et les différentes techniques de corrélation. Cependant, malgré ces techniques nous avons besoin d'alerter l'administrateur lors d'une attaque afin de pouvoir y répondre le plus tôt possible. Le but principal de la corrélation est de réduire au maximum le temps d'exposition d'une attaque et de pouvoir répondre à cette attaque en temps, presque, réel.
En fin, dans le but de bénéficier au maximum de l'utilisation de la méthode de corrélation et de fusion de données, nous avons besoin d'automatiser certaines de nos taches journalières grâce à l'utilisation d'agents intelligents qui seront déployés sur le réseau afin de réduire le temps de travail de l'administrateur et le conseiller sur une réponse à une attaque probable. Ces propositions feront l'objet de travaux futures avec une implémentation de notre IPS proposé.

La technologie des IDS et IPS n'est pas encore arrivée à maturité et les outils existants ne sont pas encore à la hauteur des besoins. Cette nouvelle approche, visant la protection du réseau de l'intérieur et de l'extérieur apportera une amélioration très importante dans ce domaine.

Bibliographie et Références

[1] Mémoire de thèse de Doctorat « Corrélation d'alertes issues d'outils de détection d'intrusions avec prise en compte 'informations sur le système surveillé » par Benjamin Morin l'INSA de Rennes.

[2] J.P. Anderson. Computer Security Threat Monitoring and Surveillance. Technical report, Fort Washington - Pennsylvania - Technical Report Contract 79F26400, 1980.

[3] D. Denning. An Intrusion-Detection Model. IEEE Transactions on Software Engineering, 13(2): 222–232, 1987.

[4] [4]INTRUSION DETECTION and Correlation Challenges and Solutions - par Christophe Kruegel, Fredrik Valeur, Giovanni Vigna - Université de Californie, Père Noël Barbara, USA, édition La ©2005 Science Springer

[5] Michael Sobirey. Intrusion detection systems page. http://www-rnks.informatik.tu-cottbus.de/sobirey/ids.html. Page web en évolution constante. 1999.

[6] A. Cuff. Intrusion Detection Systems list. http://www.networkintrusion.co.uk/.

[7] H. Debar, M. Dacier, and A. Wespi. Towards a taxonomy of intrusion-detection systems. internal RZ 3030, IBM Zurich Research Laboratory, Saumerstrasse 4, CH-8803 Ruschlikon, Switzerland, June 1998.

[8] H. Debar, M. Dacier, and A. Wespi. A Revised Taxonomy for Intrusion-Detection Systems. Annales des Télécommunications, 55(7-8), 2000.

[9] Dorothy E. Denning. An intrusion-detection model. IEEE Transactions on Software Engineering 13(2):222-232, Février 1987.

[10] G. E. Liepins and H. S. Vaccaro. Anomaly detection: Purpose and framework. Proceedings of the 12th National Computer Security Conference, pages 495-504, Octobre 1989.

[11] H. Debar. Application des réseaux de neurones à la détection d'intrusions sur les systèmes informatiques. PhD thèses, Université de Paris 6, 1993.

[12] S. Hofmeyr, S. Forrest, and A. Somayaji. Intrusion Detection Using Sequences of System Calls. In Journal of Computer Security, volume 6, pages 151–180, 1998.

[13] Harold S. Javitz, Alfonso Valdez, Teresa F. Lunt, Ann Tamaru, Mabry Tyson, and John Lowrance. Next generation intrusion detection expert system (NIDES) - 1. Statistical algorithms rationale - 2. Rationale for proposed resolver. Technical Report A016–Rationales, SRI International, 333 Ravenswood Avenue, Menlo Park, CA, March 1993.

[14] J. Zimmermann, L. Mé, and C. Bidan. An Improved Reference Flow Control Model for Policy-Based Intrusion Detection. In Proceedings of the 8th European Symposium on Research in Computer Security (ESORICS), 2003.

[15] Revue Mag Securs Novembre 2005.

[16] Cours certificat CCNA de Cisco version 3.1 accès 2006 : http://cisco.netacad.net/cnams/course/.

[17] « Data Correlation dans l'Intrusion de Détection » paru le 15/08/2005 au http://www.supinfo-projects.com/fr/2005/datacor%5Ffr/introduction/ (20/09/06)