UNIVERSITE IBN ZOHR

CENTRE DES ETUDES DOCTORALES IBN ZOHR

Formation doctorale
Sciences, Techniques et Ingénierie

Faculté des Sciences d'Agadir
Laboratoire des Systèmes informatiques et Vision
Equipe SCCAM : Sécurité, Cryptologie, Contrôle d'Accès et Modélisation

THESE

Présenté par
Yousef FARHAOUI

Pour l'obtention de grade de
DOCTEUR de l'Université Ibn Zohr

Spécialité : Informatique

Evaluation des Systèmes de Détection et de Prévention des Intrusions et la Conception d'un BiIDS

Directeur de thèse : **M. Ahmed ASIMI**
Soutenue le 27 Décembre 2012
Devant la commission d'examen composée de :

M. Karim AFDEL	Université Ibn Zohr -FS- Agadir	Président
M. Ahmed ASIMI	Université Ibn Zohr -FS- Agadir	Directeur de thèse
M. Charaf BENSOUDA	Université Ibn Tofail -FS- Kenitra	Examinateur
Mme. Fouzia OMARY	Université Mohammed V -FS- Rabat	Rapporteur
M. Zine El Abidine GUENNOUN	Université Mohammed V -FS- Rabat	Rapporteur

قَالُوا۟ سُبْحَٰنَكَ لَا عِلْمَ لَنَآ إِلَّا مَا عَلَّمْتَنَآ ۖ إِنَّكَ أَنتَ ٱلْعَلِيمُ ٱلْحَكِيمُ ﴿٣٢﴾

REMERCIEMENTS

Les travaux présentés dans ce mémoire ont été effectués au Laboratoire des Systèmes Informatiques et Vision, Equipe SCCAM : Sécurité, Cryptologie, Contrôle d'Accès et Modélisation.

Je ne sais pas si les mots seront suffisants pour remercier **M Ahmed ASIMI**, mon cher directeur de thèse. Je le remercie d'avoir accepté de m'encadrer pour cette thèse. Je suis profondément reconnaissant de son support constant. Sans son aide, ce travail n'aurait pas été possible. Je suis impressionné par ses conseils de valeur, sa patience, ses remarques profondes.

Je remercie **M. Karim AFDEL**, qui est assuré la direction du LSIV depuis mon entrée, de m'avoir accueilli dans ce laboratoire.

J'exprime ma profonde gratitude aux personnes qui m'ont fait l'honneur de participer à mon jury de thèse : M. Karim AFDEL, professeur à la Faculté des sciences d'Agadir, M. Charaf BENSOUDA, professeur à la Faculté des sciences de Kenitra, Mme. Fouzia OMARY, professeur à la Faculté des sciences de Rabat, M. Zine El Abidine GUENNOUN, professeur à la Faculté des sciences de Rabat.

Je remercie particulièrement **M Karim AFDEL, M Zine El Abidine GUENNOUN et Mme Fouzia OMARY** qui ont accepté la charge d'être rapporteurs.

Mes vifs remerciements vont également aux membres du Centre des Etudes Doctorales Ibn Zohr (CEDIBNZOHR).

Je salue tous mes amis.

Je voudrais également exprimer toute ma reconnaissance à ma famille.

Finalement, je voudrai dire que je suis arrivé là grâce à ALLAH d'abord et grâce à vous tous.

Encore merci.

TABLE DES MATIERES

TABLE DES FIGURES

LISTE DES TABLES

ABREVIATIONS ET ACRONYMES

ACL	Access Control List
AAS	Authentication, Authorization, and Accounting
BiIDS	IDS avec les deux méthodes de détection
CSMA / CA	Carrier Sense Multiple Access - Collision Avoidance
CRC	Cyclic Redundancy Check)
DARPA	Defence Advanced Research Projects Agency
DHCP	Dynamic Host Configuration Protocol
DoS	Denial Of Service
HIDS	Host Intrusion Detection System)
HIPS	Host Intrusion Prevention System
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IDMEF	Intrusion Detection Message Exchange Format
IDXP	Intrusion detection eXchange Protocol
IDWG	Intrusion Detection Working *Group*
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
IPsec	Internet Protocol Security
IP Spoofing	Usurpation d'adresse IP.
LAN	Local Area Network
MAC	Medium Access Control || Message Authentication Code
MIC	Message Integrity Code
MITM	Man-In-The-Middle
MLS	Multi Level Security
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion **Prevention** System
RAM	Mémoire vive
RC4	Rivest Cypher 4 || Ron’s Code #4

RFC	Request For Comments
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier, identificateur de jeu de service
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
XOR	eXclusive OR

1. INTRODUCTION GENERALE

Les systèmes d'information mais aussi Internet, le réseau mondial qui interconnecte nombre d'entre eux, jouent un rôle grandissant dans la vie quotidienne et dans notre société en général. En effet, des domaines relevant de la vie privée tels que l'envoi de courrier ou bien le paiement à distance, mais aussi des domaines stratégiques comme le secteur bancaire ou encore les communications militaires, reposent de nos jours massivement sur les systèmes d'information. De ce fait, des attaques réalisées par des utilisateurs malveillants et visant à exploiter les vulnérabilités de ces systèmes d'information sont de plus en plus fréquentes. De telles attaques peuvent par exemple nuire à l'image du propriétaire du système d'information ou causer d'importants dommages financiers. La problématique de la sécurité devient donc une question essentielle aussi bien pour les utilisateurs que pour les administrateurs de ces systèmes d'information.

Tout appareil destiné à traiter de manière automatique de l'information peut être qualifié de système informatique. Les systèmes d'information reposent sur un ensemble organisé de systèmes informatiques et de systèmes de télécommunications pour gérer de l'information dans un contexte précis. Cette gestion comprend par exemple les tâches d'élaboration, de modification, de stockage ou encore de transport de l'information. Ces systèmes sont par nature en proie à des menaces vis-à-vis de l'information qu'ils traitent. En effet, pour un système d'information donné, un utilisateur malveillant pourrait chercher à altérer ou à détruire des données (on parle alors de perte d'intégrité de l'information), à révéler illégitimement des données à un tiers (on parle alors de perte de confidentialité de l'information), ou encore à empêcher un accès légitime à des données (on parle alors de perte de disponibilité de l'information).

Pour répondre à la problématique de la sécurité, une politique doit être définie en fonction du système d'information que l'on souhaite sécuriser et des objectifs de sécurité que l'on souhaite atteindre. Cette politique exprime les propriétés de confidentialité, d'intégrité et de disponibilité que doit respecter le système d'information afin de garantir sa sécurité. Pour faire respecter ces propriétés, des mécanismes préventifs, notamment de contrôle d'accès, sont mis en œuvre sur les systèmes d'information. Ces mécanismes ont accès à tout ou partie de la politique de sécurité et devraient être capables d'empêcher de manière préventive toute action qui aboutirait à une violation d'une des propriétés qu'elle exprime.

Cependant, la conception des systèmes d'information et de leurs différents composants est une tâche complexe. Cela implique que le risque qu'une faute de conception ou de configuration soit présente dans le système d'information n'est pas nul. Ces fautes sont autant de vulnérabilités potentielles que pourraient chercher à exploiter un utilisateur malveillant

pour contourner les mécanismes préventifs et effectuer des opérations proscrites par la politique de sécurité. On désigne alors par le terme intrusion toute violation intentionnelle d'une des propriétés exprimées par la politique de sécurité.

Tenant compte de l'éventualité d'une intrusion malgré la présence de mécanismes préventifs, des mécanismes capables de détecter une violation de la politique de sécurité une fois que celle-ci a effectivement eu lieu ont été mis en place. On appelle ce type de mécanismes des systèmes de détection et de prévention d'intrusion. L'objectif de ces mécanismes et de lever une alerte en cas d'intrusion afin de la signaler à l'administrateur du système. Ce dernier devra alors procéder à l'analyse du rapport d'alerte pour remettre le système d'information dans un état opérationnel mais aussi pour identifier la vulnérabilité à l'origine de l'intrusion afin de pouvoir la corriger. Eventuellement, l'administrateur pourra également juger de la sévérité de la compromission. Par exemple, une compromission qui a permis à l'utilisateur malveillant d'obtenir sur le système d'information ciblé des droits administrateur est plus sévère que si des droits restreints ont seulement pu être obtenus.

Les systèmes de détection et de prévention d'intrusion peuvent être classés en deux catégories:

Ceux qui cherchent à détecter des malveillances (on parle alors d'approches par signature) et ceux qui cherchent à détecter des anomalies (on parle alors d'approches comportementale). Dans le premier cas, le modèle de détection repose sur la connaissance que l'on a des attaques tandis que dans le second cas, celui-ci repose sur la connaissance que l'on a de l'entité surveillée en situation de fonctionnement normal.

Une approche comportementale présente l'avantage de pouvoir détecter des attaques encore inconnues au moment de la modélisation. Toutefois, la construction d'un tel modèle de détection peut être une tâche difficile. En effet, il n'est pas simple de définir ce qui est caractéristique du comportement normal de l'entité surveillé et toute erreur de modélisation risque d'entraîner la levée de fausses alertes. Le modèle de détection d'intrusion que nous proposons dans cette thèse est de type d'approches par signature et aussi par comportementale.

Au niveau logiciel, on distingue parmi les vulnérabilités à l'origine des intrusions les fautes de conception préalablement présentes dans les programmes et les fautes de configuration de ces derniers. Les attaques qui exploitent les fautes de conception peuvent également être classées en deux catégories : les attaques contre les données de contrôle et les attaques contre les données de calcul. Les données de contrôle sont utilisées par le programme pour gérer son flot d'exécution tandis que les données de calcul sont utilisées pour contenir la valeur des

variables présentes dans le code source du programme. Dans le premier cas, une attaque va chercher à faire dévier illégalement le flot d'exécution du programme vers des instructions invalides (par exemple, vers du code injecté). Dans le second cas, elle va chercher à modifier le flux d'information du programme pour utiliser de manière illégale des instructions valides (Par exemple, au travers d'un chemin incorrect).

Cette thèse vise à contribuer à l'amélioration des méthodes d'évaluation des systèmes de détection et prévention d'intrusions (IDS et IPS). Ce travail est motivé par deux problèmes actuels : tout d'abord, l'augmentation du nombre et de la complexité des attaques que l'on observe aujourd'hui nécessite de faire évoluer les IDS pour leur permettre de les détecter. Deuxièmement, les IDS actuels génèrent de trop fréquentes fausses alertes, ce qui les rend inefficaces, voir inutiles. Des moyens de test et d'évaluation sont donc nécessaires pour déterminer la qualité de détection des IDS et des IPS et de leurs algorithmes de détection. Malheureusement, aucune méthode d'évaluation satisfaisante n'existe de nos jours. En effet, les méthodes employées jusqu'ici présentent trois défauts majeurs: une absence de méthodologie rigoureuse d'évaluation, l'utilisation de données de test non représentatives, et l'utilisation de métriques incorrectes. Partant de ce constat, nous proposons une démarche rigoureuse couvrant l'ensemble des étapes de l'évaluation des IDS et des IPS. Premièrement, nous proposons une méthodologie d'évaluation qui permet d'organiser l'ensemble du processus d'évaluation. Deuxièmement, afin d'obtenir des données de test représentatives, nous avons défini une classification des types d'attaques en fonction des moyens de détection utilisés par les IDS et les IPS. Cela permet non seulement de choisir les attaques à inclure dans les données de test, mais aussi d'analyser les résultats de l'évaluation selon les types d'attaques plutôt que pour chaque attaque individuellement. Troisièmement, nous avons analysé un grand nombre d'attaques réelles et de programmes malveillants connus, tels que les virus et les vers. Grâce à cette analyse, nous avons pu construire un modèle générique de processus d'attaques qui met en évidence la dynamique des activités d'attaque. Ce modèle permet de générer un nombre important de scénarios d'attaques, qui soient le plus possible représentatifs et variés. Pour montrer la faisabilité de notre approche, nous avons appliqué expérimentalement les étapes de notre démarche à deux systèmes différents de détection d'intrusions. Les résultats montrent que l'approche proposée permet de surmonter les deux défauts principaux des évaluations existantes, à savoir l'absence de méthodologie et l'utilisation de données non représentatives. En particulier, elle permet de mieux gérer le processus d'évaluation et de choisir les cas de test les plus adaptés à l'IDS et l'IPS sous test et

les plus pertinents vis-à-vis des objectifs de l'évaluation en cours, tout en couvrant une large partie de l'espace d'attaques.

Dans ces travaux de thèse, nos contributions sont les suivantes :

- évaluation de Performance des Systèmes de Détection et de Prévention d'Intrusion (Selon de la méthode utilisée, fiabilité, réactivité, performance, débit, comportement après l'intrusion, fausse alerte) ;
- évaluation de Performance des Systèmes de Détection et de Prévention d'Intrusion (Selon de l'objectif de la sécurité informatique : l'intégrité, la confidentialité, la disponibilité et authentification) ;
- évaluation des Performances et d'efficacité des Systèmes de Détection et de Prévention d'Intrusion basée sur le Réseau de Neurone artificiel ;
- attaques Wi-Fi WPA (TKIP) ;
- la conception d'un modèle du Systèmes de détection d'intrusion(BiIDS) dans le réseau local.

2. ATTAQUES ET LES OBJECTIFS DE LA SECURITE INFORMATIQUE

2.1. INTRODUCTION AUX ATTAQUES

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Une « **attaque** » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant des systèmes et généralement préjudiciables.

Sur Internet, des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement, il s'agit de l'action de pirates informatiques.

Afin de contrer ces attaques, il est indispensable de connaître les principaux types d'attaques pour mettre en œuvre des dispositions préventives.

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.

2.1.1. TYPES D'ATTAQUES

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

Les attaques peuvent intervenir à chaque maillon de cette chaîne, pour peu qu'il existe une vulnérabilité exploitable. Il est ainsi possible de catégoriser les risques de la manière suivante :

- **Accès physique** : il s'agit d'un cas où l'attaquant à accès aux locaux, éventuellement même aux machines :
    - Coupure de l'électricité.
    - Extinction manuelle de l'ordinateur.
    - Vandalisme.
    - Ouverture du boîtier de l'ordinateur et vol de disque dur.
    - Ecoute du trafic sur le réseau.
- **Interception de communications** :
    - Vol de session.
    - Usurpation d'identité.
    - Détournement ou altération de messages.
- **Dénis de service** : il s'agit d'attaques visant à perturber le bon fonctionnement d'un service. On distingue habituellement les types de déni de service suivant :
    - Exploitation de faiblesses des protocoles TCP/IP.
    - Exploitation de vulnérabilité des logiciels serveurs.

- **Intrusions** :
    - Balayage de ports/
    - Elévation de privilèges : ce type d'attaque consiste à exploiter une vulnérabilité d'une application en envoyant une requête spécifique, non prévue par son concepteur, ayant pour effet un comportement anormal conduisant parfois à un accès au système avec les droits de l'application.
    - Malicieux (virus, vers et chevaux de Troie ….).

- **Ingénierie sociale** : Dans la majeure partie des cas le maillon faible est l'utilisateur lui-même. En effet c'est souvent lui qui, par méconnaissance ou par duperie, va ouvrir une brèche dans le système, en donnant des informations (mot de passe par exemple) au pirate informatique ou en exécutant une pièce jointe. Ainsi, aucun dispositif de protection ne peut protéger l'utilisateur contre les arnaques, seuls bons sens, raison et un peu d'information sur les différentes pratiques peuvent lui éviter de tomber dans le piège.
- **Trappe** : il s'agit d'une porte dérobée dissimulée dans un logiciel, permettant un accès ultérieur à son concepteur.

Pour autant, les erreurs de programmation contenues dans les programmes sont habituellement corrigées assez rapidement par leur concepteur dès lors que la vulnérabilité a été publiée. Il appartient alors aux administrateurs (ou utilisateurs personnels avertis) de se tenir informés des mises à jour des programmes qu'ils utilisent afin de limiter les risques d'attaques.
D'autre part il existe un certain nombre de dispositifs (pare-feu, systèmes de détection d'intrusions, systèmes de prévention d'intrusions, antivirus) permettant d'ajouter un niveau de sécurisation supplémentaire.

2.1.1. EFFORT DE PROTECTION

La sécurisation d'un système informatique est généralement dite « asymétrique », dans la mesure où le pirate n'a qu'à trouver une seule vulnérabilité pour compromette le système, tandis que l'administrateur doit corriger toutes les failles.

2.1.2. ATTAQUES PAR REBOND

Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les **attaques par rebond** (par opposition aux **attaques directes**), consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond.
Cela montre l'intérêt de protéger son réseau ou son ordinateur personnel, il est possible de se retrouver « complice » d'une attaque et en cas de plainte de la victime, la première personne interrogée sera le propriétaire de la machine ayant servi de rebond.
Avec le développement des réseaux sans fils, ce type de scénario risque de devenir de plus en plus courant car lorsque le réseau sans fil est mal sécurisé, un pirate situé à proximité peut l'utiliser pour lancer des attaques !

2.2. LES RISQUES EN MATIERE DE SECURITE

Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

- L'interception de données qui consiste à écouter les transmissions des différents utilisateurs du réseau sans fil.
- Le détournement de connexion dont le but est d'obtenir l'accès à un réseau local ou à Internet.
- Le brouillage des transmissions qui consiste à émettre des signaux radio de telle manière à produire des interférences.
- Les dénis de service rendant le réseau inutilisable en envoyant des commandes factices.

2.2.1. L'INTERCEPTION DE DONNEES

Par défaut, un réseau sans fil est non sécurisé, c'est-à-dire qu'il est ouvert à tous et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement écouter toutes les communications circulant sur le réseau. Pour un particulier, la menace est faible car les données sont rarement confidentielles, si ce n'est les données à caractère personnel. Pour une entreprise en revanche l'enjeu stratégique peut être très important.

2.2.2. L'INTRUSION RESEAU

Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder au réseau filaire et éventuellement à internet si le réseau local y est relié. Un réseau sans fil non sécurisé représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou une organisation.
Outre le vol ou la destruction d'informations présentes sur le réseau et l'accès à internet gratuit pour le pirate, le réseau sans fil peut également représenter une aubaine pour ce dernier dans le but de mener des attaques sur Internet. En effet étant donné qu'il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise ayant installé le réseau sans fil risque d'être tenue responsable de l'attaque.

2.2.3. LE BROUILLAGE RADIO

Les ondes radio sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle

utilisée dans le réseau sans fil. Un simple four à micro-onde peut ainsi rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

2.2.4. LES DENIS DE SERVICE

La méthode d'accès au réseau de la norme 802.11 est basée sur le protocole CSMA/CA, consistant à attendre que le réseau soit libre avant d'émettre. Une fois la connexion établie, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets. Ainsi, les méthodes d'accès au réseau et d'association étant connues, il est simple pour un pirate d'envoyer des paquets demandant les désassociations de la station. Il s'agit d'un déni de service, c'est-à-dire d'envoyer des informations de telle manière à perturber volontairement le fonctionnement du réseau sans fil.

D'autre part, la connexion à des réseaux sans fil est consommatrice d'énergie. Même si les périphériques sans fil sont dotés de fonctionnalités leur permettant d'économiser le maximum d'énergie, un pirate peut éventuellement envoyer un grand nombre de données (chiffrées) à une machine de telle manière à la surcharger. En effet, un grand nombre de périphériques portables (assistant digital personnel, ordinateur portable, ...) possèdent une autonomie limitée, c'est pourquoi un pirate peut provoquer une surconsommation d'énergie de telle manière à rendre l'appareil temporairement inutilisable, c'est ce que l'on appelle un déni de service sur batterie.

2.3. ATTAQUES DE RESEAUX SANS FILS

Les ondes radioélectriques ont principalement une grande capacité à se propager dans toutes les directions avec une portée relativement grande. Il est ainsi très difficile d'arriver à confiner les émissions d'ondes radio dans un périmètre restreint. La propagation des ondes radio doit également être pensée en trois dimensions.

La principale conséquence de cette "propagation sauvage" des ondes radio est la facilité que peut avoir une personne non autorisée d'écouter le réseau, éventuellement en dehors de l'enceinte du bâtiment où le réseau sans fil est déployé.

2.3.1. ATTAQUE DE DENI DE SERVICE

Les attaques Déni de Service (DoS) sont conçues pour empêcher l'accès légitime au réseau. Cela comprend le blocage total du réseau, la dégradation des services offerts par le réseau, et l'augmentation du trafic réseau afin de surcharger les équipements du réseau.

2.3.2. L'ECOUTE DU RESEAU

La surveillance du réseau permet à un attaquant de saisir des données sensibles à partir d'un réseau sans fils. L'écoute d'un réseau sans fils non sécurisé rend possible l'interception des communications échangées sur le réseau. Afin de surmonter les risques de l'écoute, il est impératif d'utiliser un protocole de chiffrement – soit un chiffrement au niveau de la couche liaison tels que le WEP ou TKIP, ou la couche réseau tel que le cryptage IPSec.
Cependant, les protocoles de chiffrement ne sont pas tout à fait immunisés contre l'écoute passive et active. Le protocole WEP contient une faiblesse qui permet à un attaquant de craquer les clés WEP. En effet, en capturant suffisamment de trames 802.11 ayant des vecteurs d'initialisation faibles, une attaque [39] permet de récupérer la clé du cryptage de la session WEP.

2.3.3. FAUX POINTS D'ACCES

Fausse point d'accès est un outil créé à l'origine pour dissuader les attaquants en inondant le réseau par des centaines de trames balises contenant différentes adresses afin de dissimuler le véritable point d'accès. Bien que l'outil soit toujours en vigueur à cette fin, une nouvelle attaque consiste à inonder les réseaux sans fils avec des balises de faux points d'accès afin d'empêcher les utilisateurs légitimes de trouver un point d'accès et accroître le temps de traitement du système d'exploitation des stations clientes.

2.3.4. USURPATION D'IDENTITE

L'usurpation d'identité consiste à utiliser l'adresse d'une station légitime ou d'un point d'accès afin d'accéder aux services réservés aux clients valides. L'attaquant peut ainsi se procurer les privilèges d'une station pour menacer la sécurité du réseau. Cette attaque est

difficile à détecter vu que la connexion est à travers un media non physique qui ne permet pas d'identifier l'origine d'une trame.

2.3.5. ATTAQUE DE « DE-AUTHENTIFICATION »

L'attaque de « de-authentification » est un exemple d'une attaque qui est facile à monter sur tous les types des réseaux 802.11 (WEP et WPA). Elle permet de terminer la connexion de toutes les stations connectées au réseau sans fils. L'attaquant envoie une trame de «de-authentication » avec une adresse de destination "FF:FF:FF:FF:FF:FF". Les stations qui reçoivent cette trame vont automatiquement se déconnecter du réseau. L'opération est répétée continuellement afin d'empêcher les stations de maintenir leurs connections au point d'accès.

2.3.6. ATTAQUE DE DUREE

"Duration Attack" est un autre exemple d'une attaque simple qui exploite une vulnérabilité de la méthode d'accès CSMA / CA (Carrier Sense Multiple Access - Collision Avoidance).
CSMA/CA permet aux stations de réserver le canal de communication pour une durée limitée spécifiée dans le champ "duration" de la trame. L'attaquant injecte une trame avec une valeur élevée de la durée. Ceci empêche toutes les stations de communiquer avant l'expiration d'un compteur NAV initialisé à la valeur de la durée de la trame. L'attaquant envoie une deuxième trame avant l'expiration du délai. Cette opération est répétée indéfiniment ce qui interdit aux stations légitimes d'utiliser le canal de communication.

2.3.7. ATTAQUE DE FRAGMENTATION

L'attaquant envoie une trame sous forme d'une série de fragments. Le point d'accès assemble les fragments dans une nouvelle trame et la renvoie au réseau sans fil. Vu que l'attaquant connaît le texte clair de la trame, il peut récupérer la séquence clé « keystream » utilisée pour chiffrer la trame. Ce processus est répété jusqu'à ce qu'il elle récupère 1500 octets de séquence clé. L'attaquant peut utiliser la séquence clé pour chiffrer de nouveaux blocs ou décrypter une trame qui utilise le même vecteur d'initialisation. Le processus peut être répété jusqu'à ce que l'attaquant construise une table arc-en-ciel « rainbow table » qui contient les séquences clés de tous les vecteurs d'initialisation. Une telle table nécessite 23 Go de mémoire.

2.3.8. L’ATTAQUE CHOPCHOP

L'attaque ChopChop a été publiée en 2004 sous forme de programme de 188 lignes en langage C non commenté et non expliqué sous le nom de 'ChopChop attack'. L’attaque permet de décrypter une trame WEP sans connaître la clé. L'attaque ChopChop exploite à la fois les propriétés de l'opérateur XOR utilisé par le protocole RC4 pour le chiffrement des trames, et la vulnérabilité du protocole de contrôle d'intégrité CRC32 utilisé pour garantir l'intégrité des données.

2.4. LES SOLUTIONS ACTUELS

2.4.1. UNE INFRASTRUCTURE ADAPTEE

La première chose à faire lors de la mise en place d'un réseau sans fil consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir. Eviter les murs extérieurs mais choisir plutôt un emplacement central. En se promenant autour de l'immeuble, on peut établir le périmètre à l'intérieur duquel la borne est accessible. Il n'est toutefois pas rare que la zone effectivement couverte soit largement plus grande que souhaitée, auquel cas il est possible de réduire la puissance de la borne d'accès afin d'adapter sa portée à la zone à couvrir.

2.4.2. EVITER LES VALEURS PAR DEFAUT

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur. Un grand nombre d'administrateurs en herbe considèrent qu'à partir du moment où le réseau fonctionne il est inutile de modifier la configuration du point d'accès. Toutefois les paramètres par défaut sont tels que la sécurité est minimale. Il est donc impératif de se connecter à l'interface d'administration (généralement via une interface web sur un port spécifique de la borne d'accès) notamment pour définir un mot de passe d'administration.
D'autre part, afin de se connecter à un point d'accès, il est indispensable de connaître l'identifiant du réseau (SSID). Ainsi il est vivement conseillé de modifier le nom du réseau par

défaut et de désactiver la diffusion (SSID broadcast (diffusion du nom SSID)) de ce dernier sur le réseau. Le changement de l'identifiant réseau par défaut est d'autant plus important qu'il peut donner aux pirates des éléments d'information sur la marque ou le modèle du point d'accès utilisé. L'idéal est même de modifier régulièrement le nom SSID.

2.4.3. ACTIVER LE CRYPTAGE WEP OU WAP

C'est assez étonnant, mais de nombreuses bornes et interfaces WiFi sont installées sans mise en place du cryptage WEP qui permet de limiter les risques d'interception de données. Il est fortement recommandé de préférer une clé WEP sur 128 bits à celle utilisée souvent par défaut, de 64 bits. Certes l'activation du WEP est un plus mais il faut savoir qu'elle ralentisse le débit d'information: temps de cryptage - décryptage. Sans oublier de modifier les clés de cryptage WEP régulièrement.

2.4.4. LE FILTRAGE DES ADRESSES MAC

Chaque adaptateur réseau possède une adresse physique qui lui est propre (appelée adresse MAC). Cette adresse est représentée par 12 chiffres hexadécimaux groupés par paires et séparés par des tirets. Les points d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès (appelée ACL) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil. En activant ce MAC Address Filtering (Filtrage des adresses MAC), même si cette précaution est un peu contraignante, cela permet de limiter l'accès au réseau à un certain nombre de machines. En contrepartie cela ne résout pas le problème de la confidentialité des échanges.

2.4.5. AMELIORER L'AUTHENTIFICATION

Afin de gérer plus efficacement les authentifications, les autorisations et la gestion des comptes utilisateurs (AAS Authentication, Authorization, and Accounting) il est possible de recourir à un serveur RADIUS (Remote Authentication Dial-In User Service). Le protocole RADIUS (défini par les RFC 2865 et 2866), est un système client/serveur permettant de gérer de façon centralisée les comptes des utilisateurs et les droits d'accès associés.

2.4.6. MISE EN PLACE D'UN VPN

Pour connecter les utilisateurs nomades branchés au réseau par le biais d'une borne publique, et pour toutes les communications nécessitant un haut niveau de sécurisation, il faut mettre en place un réseau privé virtuel (VPN) qui offrira un bon niveau de sécurité et empêchera la plupart des intrusions indésirables.

2.4.7. DEFINIR DES ADRESSES IP FIXES

Les risques d'intrusion externes sont bien moindres en attribuant des adresses IP fixes aux stations de la flotte bénéficiant d'une connexion sans fil. Il est ainsi possible de gérer une table d'adresses des connexions autorisées. Dans ce cas, il faut désactiver la fonction DHCP au niveau du serveur auquel est connectée la borne WiFi.

2.4.8. INSTALLER UN PARE-FEU

On peut aussi installer un firewall comme si le point d'accès était une connexion internet. Ce firewall peut être le serveur IPsec (VPN) des clients sans fils. Un réseau WiFi "sécurisé" peut être schématisé comme cela. On considère ici que tout le réseau WiFi est étranger au réseau local, au même titre qu'Internet. L'utilisation d'un pare-feu (firewall), comme pour la connexion Internet, permet de filtrer les adresses MAC associées à des adresses IP fixes. Dans le cas du VPN, le firewall ou un serveur derrière ce dernier fait office de terminal VPN. Certains points d'accès proposent des "petits" firewall permettant de faire un filtrage de plus sur les clients de votre réseau.

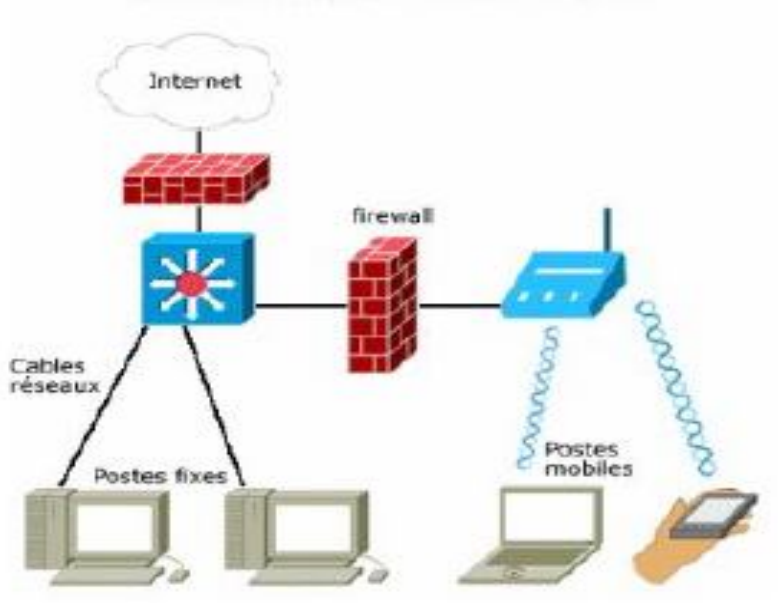

Figure 1 : Réseau filaire et Wifi sécurisé

2.5. OBJECTIFS DE LA SECURITE INFORMATIQUE

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger. La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. La sécurité informatique vise généralement six principaux objectifs : L'intégrité, c'est-à-dire garantir que les données sont bien celles que l'on croit être ; La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ; La disponibilité, permettant de maintenir le bon fonctionnement du système d'information ; La non répudiation, permettant de garantir qu'une transaction ne peut être niée ; L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources ; Le contrôle d'accès signifie que l'accès de l'utilisateur à l'information contenue dans un ordinateur est restreint et contrôlé.

2.5.1. INTEGRITE

L’intégrité signifie que les méthodes de gestion des données garantissent que ces données sont traitées sans erreurs. Les données ne doivent pas être modifiées lors de leur transfert ou de leur stockage. Personne ne peut changer le contenu de l’information ni celui des fichiers et encore moins les supprimer. Afin d’assurer l’intégrité des données, l’expéditeur doit toujours être authentifié. L’authentification, unie à l’intégrité, garantit que l’information envoyée reste identique jusqu’à ce qu’elle parvienne au destinataire [11].

L'intégrité assure que l'information ne peut être modifiée de manière inattendue. Une perte d'intégrité peut provenir d'une erreur humaine, d'une manipulation intentionnelle ou même d'une catastrophe. Les conséquences liées à l'utilisation d'informations inexactes peuvent être désastreuses. Des données, si elles ont été modifiées de façon incorrecte peuvent devenir inutiles, ou pire, dangereuses. Des efforts doivent être faits pour assurer l'exactitude et la solidité des données.

Une politique de sécurité informatique bien équilibrée aura des composants proactifs et réactifs complémentaires. La partie proactive comprend l'utilisation de contrôles de sécurité forts, alors que l'approche réactive inclut l'analyse et la surveillance de ces contrôles. Dans cette approche, le composant proactif peut être un système configuré de façon appropriée qui enregistre tous les accès système dans un log. L'administrateur réseau exécute le composant réactif en vérifiant ces logs pour chercher une activité suspecte ou tout élément anormal. Il est nécessaire de prendre ces deux approches pour avoir un contrôle de sécurité efficace. Imaginez que chaque fois qu'une porte de votre maison est ouverte, l'heure et le nom de la personne soit enregistré. Ainsi, si quelque chose manque dans une pièce, vous pouvez consulter le document d'enregistrement, voir qui était dans la pièce concernée et lui poser des questions.

2.5.2. CONFIDENTIALITE

La confidentialité signifie que l’accès à l’information disponible sur le réseau ou la circulation dans le réseau est réservé à ceux qui en ont reçu l’autorisation. Personne ne peut accéder à l’information s’il n'en a pas le droit. L’identification des utilisateurs requiert une

authentification. Maintenir l'information à l'abri des indiscrets requiert un cryptage [12], effectué par des moyens techniques.

La confidentialité est le fait selon lequel l'information n'est pas accessible à ceux qui n'en ont pas l'autorisation. Des contrôles stricts doivent être mis en place pour assurer que seules les personnes ayant besoin d'accéder à certaines informations puissent y accéder. Dans certaines situations, telles que celles concernant des informations confidentielles et secrètes, les gens ne devraient avoir accès qu'aux données nécessaires à l'exercice de leur fonction. Beaucoup de crimes informatiques concernent des fuites et des vols d'informations confidentielles [11].

2.5.3. AUTHENTIFICATION

L'authentification porte sur la capacité d'un système de démontrer à toute entité intéressée la vraie source d'un message transactionnel. Le destinataire est assuré que la transaction provient bien de l'expéditeur attendu, et ce dernier est assuré qu'il s'agit bien du destinataire présumé.

L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre l'accès à des ressources uniquement aux personnes autorisées.

Le service d'authentification permet évidemment d'assurer l'authenticité d'une communication. Dans le cas d'un message élémentaire, tel un signal d'avertissement, d'alarme, ou un ordre de tir, la fonction du service d'authentification est d'assurer le destinataire que le message a bien pour origine la source dont il prétend être issu. Dans le cas d'une interaction suivie, telle une connexion d'un terminal à un serveur, deux aspects sont concernés. En premier lieu, lors de l'initialisation de la connexion, il assure que les deux entités sont authentiques. Ensuite, le service doit s'assurer que la connexion n'est pas perturbée par une tierce partie qui pourrait se faire passer pour une des deux entités légitimes à des fins de transmissions ou de réceptions non autorisées.

2.5.4. DISPONIBILITE

La disponibilité signifie que les utilisateurs nécessitant les données et ceux à qui elles sont destinées ont toujours accès à celles-ci. Les méthodes visant à garantir la disponibilité comprennent un contrôle effectif et technique des fonctions des systèmes de données, ainsi

qu’une protection des fichiers, un entreposage correct et la réalisation de copies de sauvegarde. La disponibilité est l’aspect de la sécurité des données le plus difficile à accomplir [11].

Assurer la sécurité physique d'un réseau ou d'un système est une des manières d'assurer sa disponibilité. En limitant l'accès physique aux machines ou aux sources de données critiques, les risques d'inaccessibilité seront réduits. Si le contact avec ces ressources est restreint, les accidents ainsi que les cas de malveillances internes diminueront également. De même, protéger le réseau électroniquement est important si beaucoup de points d'entrée existent. Par exemple, un firewall est un système qui se situe entre un réseau interne, ou intranet et un réseau externe tel que l'Internet. Le firewall régule et restreint quel type de données peuvent passer entre les deux réseaux.

Un autre aspect de la disponibilité est d'assurer que les ressources nécessaires sont utilisables quand et où elles sont nécessaires. Fournir des redondances systèmes, sous la forme de données, machines et sources d'électricité de secours assurera souvent la disponibilité. Le stockage de données critiques hors-site permettra de les récupérer en cas de problèmes. En plus des serveurs de secours permettront une poursuite du travail normal si la sécurité du réseau primaire est menacée. Si ces formes de sécurité assurent la disponibilité, il est important de protéger les données des intrus et de maintenir leur confidentialité. Si nous nous référons à notre exemple, supposons que vous gardiez des copies de vos documents importants (certificats de naissance, testament, actions, etc) dans un coffre à la banque. En cas de catastrophe dans votre maison, vous aurez toujours accès à ces documents.

2.5.5. NON REPUDIATION

La non-répudiation empêche tant l’expéditeur que le receveur de nier avoir transmis ou reçu un message. Ainsi, lorsqu’un message est envoyé, le receveur peut prouver que le message a bien été envoyé par l’expéditeur prétendu. De même, lorsqu’un message est reçu, l’expéditeur peut prouver que le message a bien été reçu par le receveur prétendu.

2.5.6. CONTROLE D’ACCES

Le contrôle d’accès signifie que l’accès de l’utilisateur à l’information contenue dans un ordinateur est restreint et contrôlé. Le contrôle d’accès vérifie que l’utilisateur possède le droit d’accéder au service et à l’information. Ceci implique que seules les personnes authentifiées

peuvent y avoir accès. L’objectif du contrôle d’accès est en partie de garantir la confidentialité de l’information ainsi que son intégrité. Il garantit également la disponibilité, car il rend l’attaque du système plus difficile.

Dans le contexte de la sécurité des réseaux, le contrôle d’accès est la faculté de limiter et de contrôler l’accès à des systèmes et des applications via des maillons de communications. Pour accomplir ce contrôle, chaque entité essayant d’obtenir un accès doit d’abord être authentifiée, ou s’authentifier, de telle sorte que les droits d’accès puissent être adaptés à son cas. Le contrôle d'accès consiste à autoriser l'accès aux informations et aux ressources qu'à ceux qui en ont besoin.

La forme de contrôle d'accès la plus courante est l'utilisation de mots de passe et la forme la plus courante des infractions de sécurité concerne ces mots de passe. Exiger des mots de passe "forts", des cartes à puce ou des dispositifs de mots de passe à usage unique est le premier pas pour empêcher des personnes non autorisées d'accéder à des informations sensibles et il est la première barrière de défense du contrôle d'accès. Protéger ces mots de passe est l'un des principes fondamentaux de la sécurité informatique.

2.6. CONCLUSION

La sécurisation d'un réseau qu'il soit filaire ou sans fils est possible par de nombreux moyens matériels et/ou logiciels. Son choix dépend de l'utilisation du réseau et des moyens disponibles.

3. SYSTEMES DE DETECTION ET DE PREVENTION DES INTRUSIONS

3.1. INTRODUCTION

Aujourd'hui, les systèmes d'informations et les réseaux informatiques occupent une place centrale dans la société moderne. Plus il y a de données enregistrées et traitées, plus il est important de sécuriser les systèmes informatiques. Une intrusion se définit comme une série d'actions qui tentent de compromettre l'intégrité, la confidentialité ou la disponibilité d'une ressource [1].

La détection d'intrusions est le processus de suivi des événements survenus dans un système ou un réseau et l'analyse de ces événements pour trouver des signes d'intrusions. L'objectif est d'identifier les individus utilisant le système sans avoir l'autorisation (hackers) et les individus ayant un accès légitime au système mais qui abusent de leurs privilèges [2]. Les systèmes de détection d'intrusions (Intrusion Detection system (IDS)) peuvent être des logiciels et des matériels qui automatisent le processus d'observation et d'analyse des événements.

Pour qu'un IDS soit efficace, il doit s'exécuter continuellement, s'adapter aux changements de comportements et aux grandes quantités de données, être configurable, ne pas utiliser trop de ressources mémoires de la machine et après les pannes de système, être réutilisable sans nouvel apprentissage [3].

Actuellement, il existe deux approches principales pour la détection d'intrusions. La détection d'anomalies et la détection d'abus (Misuse Detection). Dans la première approche, les comportements normaux des utilisateurs du réseau sont connus et il est donc possible de construire des profils représentant ces comportements grâce à plusieurs caractéristiques comme les activités sur le réseau, etc. Une fois ces profils définis, les intrusions sont identifiées comme des déviations par rapport aux comportements normaux
[1][3][4].

3.2. SYSTEMES DE DETECTION D'INTRUSIONS (IDS)

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

Il existe trois grandes familles distinctes d'IDS :

- Les NIDS (Network Intrusion Detection System) qui assurent la sécurité au niveau du réseau.
- Les HIDS (Host Intrusion Detection System) qui assurent la sécurité au niveau des hôtes.
- Les IDS hybrides (NIDS+HIDS) Un "hybrid" IDS est une sorte de tout en un, c'est un HIDS avec un NIDS. Ce nom peut aussi s'appliquer à une solution mêlant plusieurs IDS, ou des IDS particuliers.

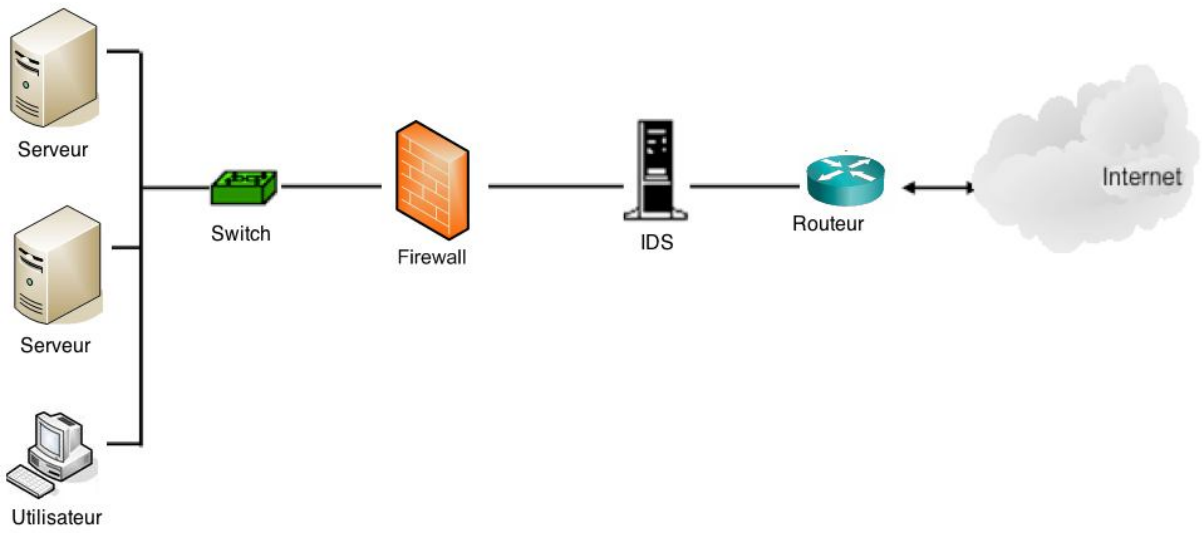

Figure 2 : Exemple d'un IDS dans un réseau

3.2.1. SYSTEMES DE DETECTION D'INTRUSION RESEAUX (NIDS)

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

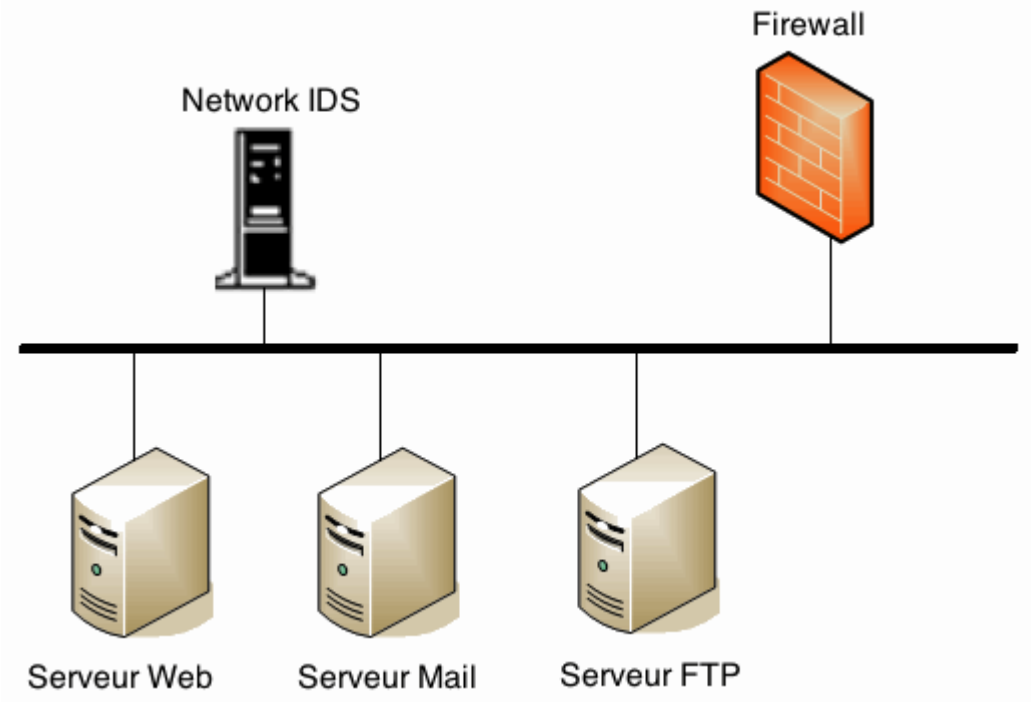

Figure 3 : Système de détection d'intrusion réseaux (NIDS)

Les avantages des NIDS sont :

- Le NIDS peut surveiller un grand réseau.
- L'déploiement de NIDS a peu d'impact sur un réseau existant. Les NIDS sont habituellement des dispositifs passifs qui écoutent sur un fil de réseau sans interférer l'opération normale d'un réseau. Ainsi, il est habituellement facile de monter en rattrapage un réseau pour inclure IDS avec l'effort minimal.
- NIDS peut être très sûr contre l'attaque et être même caché à beaucoup d'attaquants

Les inconvénients des NIDS sont :

- Il est difficile à traiter tous les paquets circulant sur un grand réseau. De plus il ne peut pas reconnaître des attaques pendant le temps de haut trafic.
- Quelques fournisseurs essayent à implémenter l'IDS dur le matériel pour qu'il marche plus rapidement.
- Plusieurs des avantages de NIDS ne peuvent pas être appliqués pour les commutateurs modernes. La plupart des commutateurs ne fournissent pas des surveillances universelles des ports et limitent la gamme de surveillance de NIDS. Même lorsque les commutateurs fournissent de tels ports de surveillance,

souvent le port simple ne peut pas refléter tout le trafic traversant le commutateur.

- NIDS ne peuventt pas analyser des informations chiffrées (cryptées). Ce problème a lieu dans les organisations utilisant le VPN.
- La plupart de NIDS ne peuvent pas indiquer si une attaque est réussie ou non. Il reconnaît seulement que une attaque est initialisée. C'est-à-dire qu'après le NIDS détecte une attaque, l'administrateur doit examiner manuellement chaque host s'il a été en effet pénétré.
- Quelques NIDS provoque des paquets en fragments. Ces paquets mal formés font devenir le IDS instable et l'accident.

3.2.2. SYSTEMES DE DETECTION D'INTRUSION SUR HOTE (HIDS)

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

- Les H-IDS Basés Application : Les IDS de ce type reçoivent les données au niveau application, par exemple, des fichiers logs générés par les logiciels de gestion de bases de données, les serveurs web ou les firewalls. Cette technique souffre du fait que les vulnérabilités de la couche application peuvent agir sur l'intégrité de l'approche de détection Basée Application.
- Les H-IDS Basés Hôte : Les IDS de ce type reçoivent les informations de l'activité du système surveillé. Ces informations sont parfois sous forme de traces d'audit du système d'exploitation, elles peuvent inclure aussi des logs système, d'autres logs générés par les processus du système d'exploitation, et les contenus des objets système non reflétés dans l'audit standard du système d'exploitation et les mécanismes de logging (comme les sockets ouvertes avec leur état et les numéros de ports associés…). Ces types d'IDS peuvent aussi utiliser les résultats retournés par un autre IDS de type Basé Application.

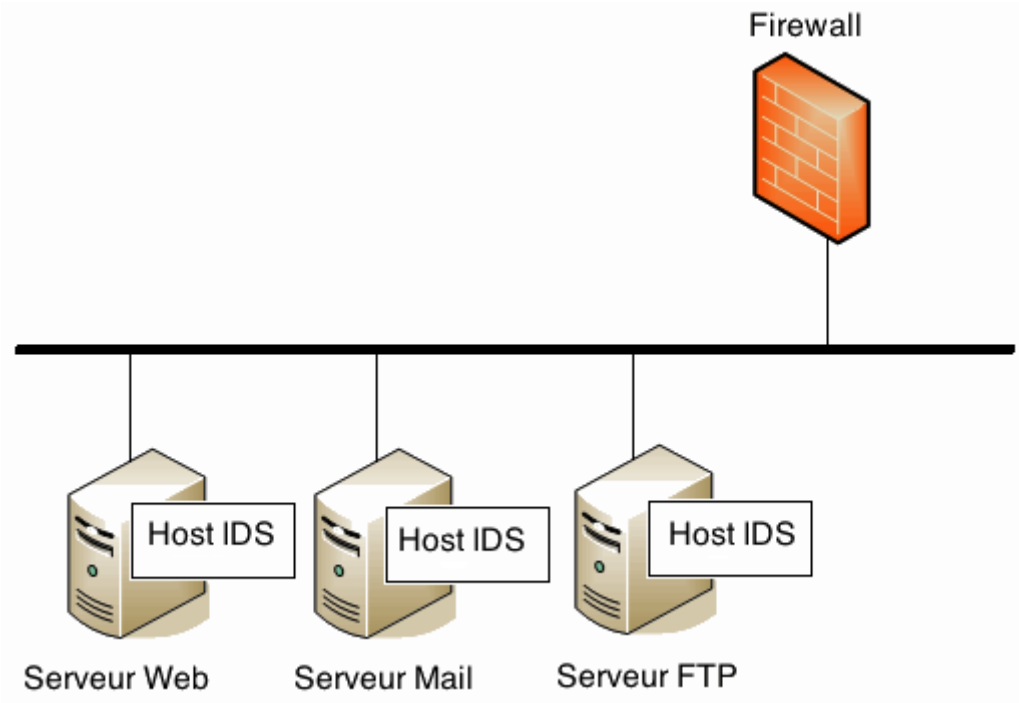

Figure 4 : Système de détection d'intrusion Hote (HIDS)

Le système de détection d'intrusions sur hôte (H-IDS) améliore la sécurité locale au niveau du système hôte dans le réseau par la surveillance automatique de chaque système hôte configuré à l'aide de signes d'intrusions inopinées et potentiellement néfastes.

Le système H-IDS surveille par exemple en permanence des signatures caractéristiques de défaillance de protection comme les intrusions de pirates informatiques ou les activités internes subversives. Il s'agit d'un fonctionnement similaire à l'analyse par « pattern matching ». Ils surveillent donc l'activité globale du système, que ce soit le lancement d'applications, de démons non autorisés ou l'accès, non autorisé, au réseau de certaines applications.

HIDS fait marcher sur les informations collectées à partir d'un système de l'ordinateur individuel. Cet avantage nous permet d'analyser des activités avec une grande fiabilité et précision, déterminant exactement quel processus et utilisateur sont concernés aux attaques particulières sur le système d'exploitation. De plus, HIDS peut surveiller les tentatives de la sortie, comme ils peuvent directement accéder et surveiller des données et des processus qui sont le but des attaques. HIDS emploie normalement des sources de l'information de deux types, la traîné de l'audit traîné du système d'exploitation et les journaux du système. La traîné de l'audit du système d'exploitation est souvent générée au niveau de noyau du SE, et elle est plus détaillée et plus protégée que les journaux du système. Pourtant les journaux sont moins obtus et plus petits que la traîné de l'audit du SE, c'est ainsi qu'il est facile à

comprendre. Quelques HIDS sont conçus pour supporter la gestion centralisée des IDS et rapportant l'infrastructure qui peut permettre une console de la gestion simple pour tracer plusieurs hosts. Les autres messages générés sous format compatible au système de la gestion de réseau.

Les avantages des HIDS sont :

- Pouvoir surveiller des événements locaux jusqu'au host, détecter des attaques qui ne sont pas vues par NIDS.
- Marcher dans un environnement dans lequel le trafic de réseau est encrypté, lorsque les sources des informations de host-based sont générées avant l'encrypte des données ou après le décrypte des données au host de la destination.
- HIDS n'est pas atteint par le réseau commuté.
- Lorsque HIDS marchent sur la traîné de l'audit de SE, ils peuvent détecter le Cheval de Troie ou les autres attaques relatives à la brèche intégrité de logiciel.

Les inconvénients des HIDS sont :

- HIDS est difficile à gérer, et des informations doivent être configurées et gérées pour chaque host surveillé [5].
- Puisque au moins des sources de l'information pour HIDS se résident sur l'host de la destination par les attaques, l'IDS peut être attaqué et neutralisé comme une partie de l'attaque.
- HIDS n'est pas bon pour le balayage de réseau de la détection ou les autres tels que la surveillance qui s'adresse au réseau entier parce que le HIDS ne voit que les paquets du réseau reçus par ses hosts [6].
- HIDS peut être neutralisé par certaine attaque de DoS.
- Lorsque HIDS emploie la traîné de l'audit du SE comme des sources des informations, la somme de l'information.

3.2.3. SYSTEMES DE DETECTION D'INTRUSION 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 les terminaux. Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces sondes remontent alors les alertes à une machine qui va centraliser le tout, et agréger/lier les informations d'origines multiples.

3.2.4. ARCHITECTURE D'UN IDS

Nous décrivons dans cette section les trois composants qui constituent classiquement un système de détection d'intrusions. La figure suivante illustre les interactions entre ces trois composants. Un **senseur** est chargé de collecter des informations sur l'évolution de l'état du système et de fournir une séquence d'événements qui renseignent de l'évolution de l'état du système. Un **analyseur** détermine si un sous-ensemble des événements produits par le senseur est caractéristique d'une activité malveillante. Un **manager** collecte les alertes produites par le senseur, les met en forme et les présente à l'opérateur. Éventuellement, le manager est chargé de la réaction à adopter. Nous détaillons ici chacun de ces trois composants.

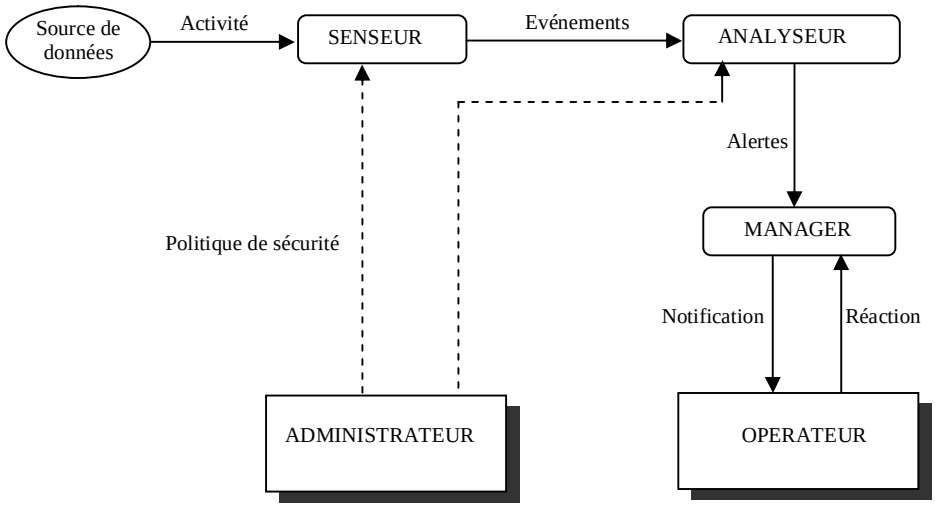

Figure 5: Architecture d'un IDS

- **Le senseur**

Le capteur observe l'activité du système par le biais d'une source de données et fournit à l'analyseur une séquence d'événements qui renseignent de l'évolution de l'état du système.
Le senseur peut se contenter de transmettre directement ces données brutes, mais en général un prétraitement est effectué. Ce traitement permet, par exemple, de filtrer un certain nombre de données considérées comme non pertinentes, afin de limiter la quantité d'information à analyser par la suite. De plus, le capteur réalise généralement une mise en forme des données brutes acquises afin de présenter à l'analyseur des données utilisant un certain format d'événements.
On distingue classiquement trois types de capteurs en fonction des sources de données utilisées pour observer l'activité du système :

- Les senseurs système collectent des données produites par les systèmes d'exploitation des machines, notamment par le biais des journaux d'audit système ou par celui des appels systèmes invoqués par les applications. On désigne les IDS utilisant des senseurs système par l'acronyme HIDS. Les capteurs réseau collectent les données en écoutant le trafic réseau entre les machines, par le biais d'une interface spécifique. On parle alors de NIDS.
- Les senseurs applicatifs collectent les données produites par une application particulière, avec laquelle des utilisateurs sont susceptibles d'interagir, comme un serveur Web ou un serveur de base de données. L'application doit bien sûr être instrumentée à cet effet.

L'avantage principal des senseurs réseau réside dans leur capacité à surveiller un grand ensemble de machines. Cette caractéristique simplifie le déploiement et la maintenance d'une solution de détection visant à garantir une couverture optimale du réseau surveillé. L'approche système est plus complexe à déployer car elle nécessite une multiplication du nombre de senseurs dans le réseau. De plus, le coût engendré par la collecte des données par ces senseurs peut dégrader sensiblement les performances des systèmes sur lesquels ils sont installés.
Cependant, on peut s'interroger sur la pérennité des capteurs réseaux pour trois raisons principales : Premièrement, la montée en débit des réseaux contraint fortement les capacités de collecte de l'intégralité du trafic. Les constructeurs de NIDS ont recours à des senseurs matériels spécifiques pour accélérer la collecte, mais la détection d'intrusions dans le cœur de

réseau peut poser problème. Deuxièmement, les senseurs réseau ne peuvent analyser le trafic chiffré. Or, la prise en compte progressive des problèmes de sécurité tend à généraliser l'utilisation du chiffrement dans les protocoles réseaux, rendant à terme les senseurs réseau inopérants. Enfin, l'analyse seule du trafic réseau s'avère souvent insuffisante pour assurer une détection fiable et pertinente des violations de politique de sécurité, l'IDS ne disposant que de trop peu d'information sur les systèmes attaqués.

- **L'analyseur**

L'objectif de l'analyseur est de déterminer si le flux d'événements fourni par le senseur contient des éléments caractéristiques d'une activité malveillante. Deux grandes approches ont été proposées : l'approche comportementale (*anomaly detection*) et l'approche par scénarios (*misuse detection*) ;

- Dans l'approche comportementale, une attaque est qualifiée par la mesure d'une déviation sensible du système surveillé par rapport à un comportement de référence, réputé sain et défini auparavant.
- Dans l'approche par scénarios, le système de détection possède une base de signatures qui modélisent les différents scénarios, c'est-à-dire les différentes attaques connues.

- **Le manager**

Le manager est responsable de la présentation des alertes à l'opérateur (fonction de console de management). Comme expliqué précédemment, il est aussi le composant qui réalisera les fonctions de corrélation d'alertes, dans la mesure de leur disponibilité. Enfin, il pourra assurer le traitement de l'incident, par exemple au travers des fonctions suivantes :

- confinement de l'attaque, qui a pour but de limiter les effets de l'attaque ;
- éradication de l'attaque, qui tente d'arrêter l'attaque ;
- recouvrement, qui est l'étape de restauration du système dans un état sain ;
- diagnostic, qui est la phase d'identification du problème et de ces causes et qui peut éventuellement être suivi d'actions contre l'attaquant (fonction de réaction).

Du fait du manque de fiabilité des systèmes de détection d'intrusions actuels, les réactions sont rarement automatisées, car elles peuvent se traduire par un déni de service en cas de faux positif.

3.3. SYSTEME DE PREVENTION DES INTRUSIONS (IPS)

La prévention d'intrusion est un ensemble de technologies de sécurité ayant pour but d'anticiper et de stopper les attaques [7]. La prévention d'intrusion est appliquée par quelques IDS récents. Au lieu d'analyser les *logs* du trafic, c'est-à-dire découvrir les attaques après qu'elles se soient déroulées, la prévention d'intrusion essaie de prévenir ces attaques. Là où les systèmes de détection d'intrusion se contentent de donner l'alerte, les systèmes de prévention d'intrusion bloquent le trafic jugé dangereux. Pendant des années, la philosophie sous-jacente dans la détection des intrusions sur le réseau s'est résumée à détecter le plus d'attaques et d'intrusions possibles et à les consigner pour que d'autres prennent les mesures nécessaires. Au contraire, les systèmes de prévention des intrusions sur le réseau ont été développés en suivant une nouvelle philosophie : « prendre les mesures nécessaires pour contrer ces attaques ou intrusions détectables avec précision ».

Tout d'abord, ils sont en ligne sur le réseau, d'où ils surveillent le trafic et interviennent activement par limitation ou suppression du trafic jugé hostile, par interruption des sessions suspectes ou par d'autres mesures en réaction à une attaque ou une intrusion. Le principe de fonctionnement d'un IPS est symétrique à celui d'un IDS (IPS hôte et IPS réseau), 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. 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 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.

La prévention d'intrusion est une technique relativement nouvelle par comparaison aux autres techniques. Cette approche fait interagir des technologies hétérogènes : pare-feu, VPN, IDS, anti-virus, anti-Spam, etc.

Les IPS sont souvent considérés comme des IDS de deuxième génération. Bien qu'il s'agisse d'un abus de langage, cette expression traduit bien le fait que les IPS remplacent petit à petit les IDS. En fait, les IPS ont avant tout été conçus pour lever les limitations des IDS en matière de réponse à des attaques. Alors qu'un IDS n'a aucun moyen efficace de bloquer une intrusion

(si ce n'est via l'utilisation de réponses actives), un IPS pourra, de part son positionnement en coupure, bloquer une intrusion en temps réel. En effet, le positionnement en coupure, tel un firewall ou un proxy, est le seul mode permettant d'analyser à la volée les données entrantes ou sortantes et de détruire dynamiquement les paquets intrusifs avant qu'ils n'atteignent leur destination. Une autre limite à laquelle devaient faire face les IDS il y a quelques années était due à leur incapacité à gérer les hauts débits du fait d'une architecture logicielle.

Les IPS fournissent les fonctionnalités suivantes [8] :

- La surveillance du comportement d'application se rapproche des IDS basés sur une application, c'est-à-dire que le comportement de l'application est analysé et noté (quelles données sont normalement demandées, avec quels programmes elle interagit, quelles ressources sont requises, etc.).
- La création de règles pour l'application : dérivé de la surveillance du comportement d'application, cet ensemble de règles donne des informations sur ce que peut faire ou non une application.
- La fonctionnalité d'alerte suite aux violations permet d'envoyer une alerte en cas de déviation (c'est-à-dire lorsqu'une attaque est détectée). L'alerte peut aller d'une simple entrée dans un journal à un blocage de ressources.
- La corrélation avec d'autres événements implique un partage d'informations entre des senseurs coopératifs, afin de garantir une meilleure protection contre les attaques.
- D'autres fonctionnalités sont possibles, comme la compréhension des réseaux IP (architecture, protocoles, etc.), la maîtrise des sondes réseau/analyse des logs, la défense des fonctions vitales du réseau, la vitesse d'analyse.

3.3.1. SYSTEMES DE PREVENTION DES INTRUSIONS RESEAUX (NIPS)

Lors de la détection d'une attaque, le système réagit et modifie l'environnement du système attaqué. Cette modification peut être le blocage de certains flux, de certains ports ou l'isolation pure et simple de certains systèmes du réseau. Le point sensible de ce genre de dispositif de prévention est qu'en cas de faux positif, c'est le trafic du système qui est directement affecté. Les erreurs doivent donc être les moins nombreuses possibles car elles ont un impact direct sur la disponibilité des systèmes. En cas de détection de trafic dangereux lié à une intrusion potentielle, l'IPS bloque ce trafic comme un firewall. Néanmoins, ce même

trafic se déroulant dans une configuration non dangereuse (pas d'enchaînement spécifique de trafic signalant une intrusion) ne sera pas bloqué. On pourrait comparer un IPS à un firewall «intelligent», qui aurait des règles dynamiques [9].

Les Avantages des systèmes NIPS sont :

- **Blocage rapide des intrusions.** Un événement d'intrusion est le début d'un processus d'atteintes aux ressources informatiques d'une organisation, sans parler des responsabilités juridiques potentielles. En intervenant dès la détection, un système IPS bloque rapidement l'intrusion et minimise la durée totale avant que le réseau ne revienne à la normale.
- **Détection précise et fiable.** A l'aide de plusieurs méthodes de détection, et tirant parti de sa position en ligne, le système IPS peut détecter les attaques et intrusions avec une précision et une fiabilité supérieures. Moins dépendant des signatures et davantage des méthodes intelligentes de détection, le système IPS génère beaucoup moins de fausses alarmes. Ainsi le temps et les efforts de l'organisation sont exclusivement concentrés sur les véritables menaces.
- **Prévention active.** Alors qu'un système NIDS prévient simplement de la présence d'un trafic suspect ou anormal, un système IPS peut lancer divers mécanismes de réaction, comme décrit précédemment. Pour les organisations, les coûts d'administration de la sécurité réseau en sont réduits d'autant, de même que le risque de dégâts ou de pertes dus aux cyberattaques.

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

Aujourd'hui, les menaces évoluent rapidement et sont de plus en plus ciblées. Aussi, il est nécessaire de disposer d'une protection capable d'arrêter les malwares avant la publication d'une mise à jour de la détection spécifique. Un système de prévention d'intrusions sur l'hôte ou HIPS (Host Intrusion Prevention System) est destiné à arrêter les malwares, avant qu'une mise à jour de la détection spécifique ne soit publiée, en surveillant le comportement du code. La majorité des solutions HIPS surveillent le code lors de son exécution et interviennent si le code est considéré suspect ou malveillant [9].

Le Système de prévention de l'intrusion de malicieux (IPS) dans un ordinateur individuel. Logiciel ou fonction d'un ensemble complexe de sécurité qui surveille en temps réel tout ou partie du comportement dynamique et de l'état du PC ...

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

3.3.3. ARCHITECTURE DES IPS

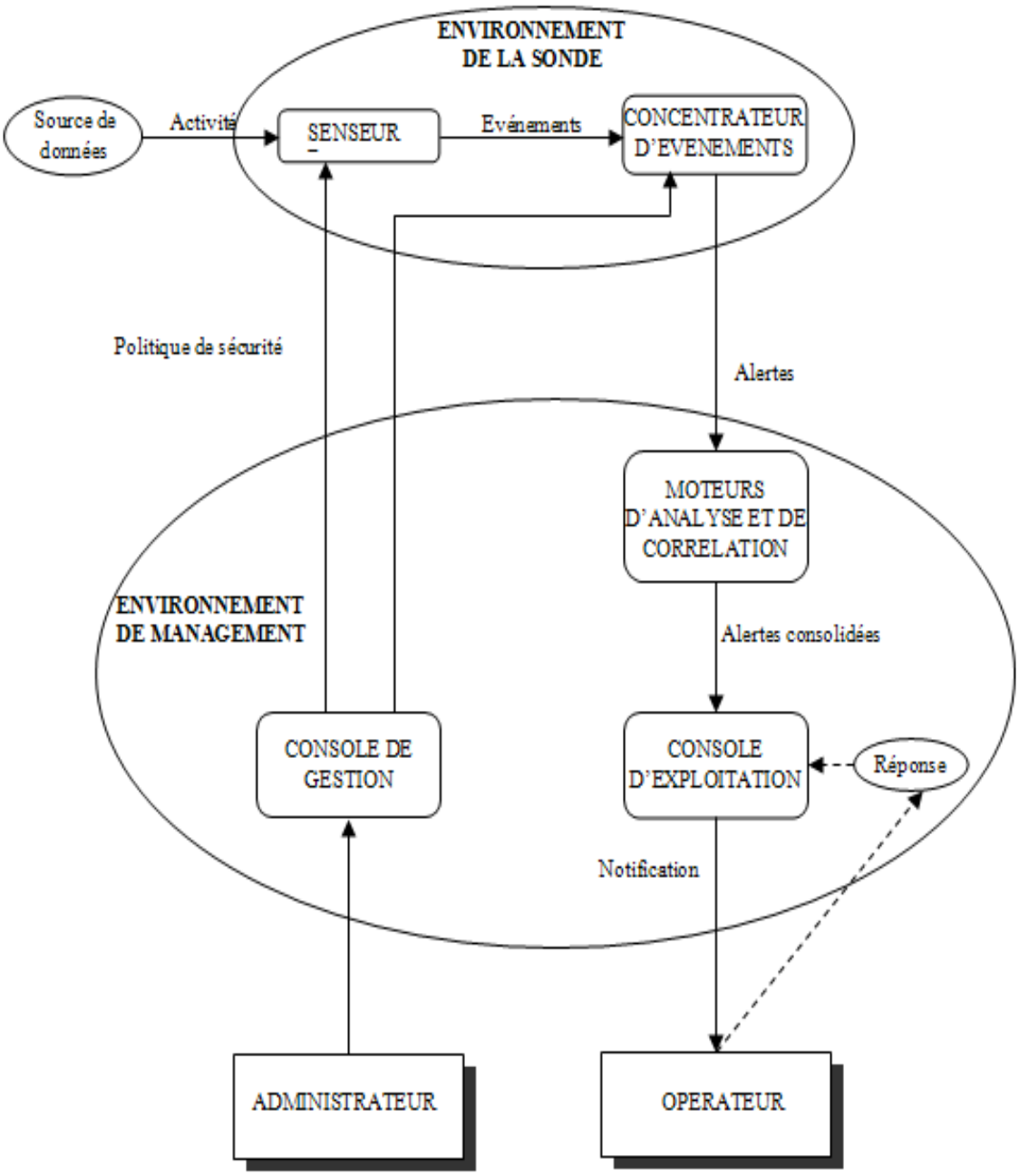

Figure 6: Architecture d'un IPS

- **Activité :** les flux d'activité émis par la source sont des éléments de données bruts qui sont identités par le senseur comme ils peuvent être intéressants pour l'opérateur.

- **Evénement :** il s'agit d'une activité détectée par le senseur et qui peut éventuellement être convertie en alerte IDMEF avent d'être transmise.
- **Alerte:** il s'agit d'un message émis d'un analyseur vers un manager et qui indique qu'un événement intéressant a été détecté. Une alerte contient généralement des informations concernant l'activité détectée ainsi que des informations complémentaire concernant les occurrences de cette activité.
- **Notification :** c'est le procédé qui permet au manager d'alerter l'opérateur d'une alerte.
- **Administrateur :** il s'agit de la composante humaine qui a la charge d'adapter les règles des IPS de manière à ce qu'elles se conforment à la politique de sécurité de l'entreprise.
- **Opérateur :** il s'agit de la personne qui est en charge de l'exploitation des IPS et notamment de la création des rapports et de l'application éventuelle des mécanismes de réponse à des alertes et des notifications.
- **Senseur :** il s'agit de l'entité qui collecte les flux de données, détecte des événements et les passe à l'analyseur.
- **Analyseur :** c'est l'entité qui analyse les événements et qui génère des alertes conformément à la politique de sécurité appliquée par l'administrateur.
- **Manager :** c'est le composant à partir duquel l'opérateur gère et interroge les différents composant du système du globale. Le manager utilise des notifications pour informer l'opérateur que des alertes ont eu lieu.

3.4. CONCLUSION

Les IDS/IPS de réseau se révèlent être les plus simples à mettre en place étant donné qu'il n'y a qu'une configuration à faire. Ces systèmes ne sont pas infaillibles, la sécurité absolue n'existe pas, mais c'est un investissement raisonnable pour protéger le système informatique.
Le principe de rendre compte après coup d'une intrusion, a vite évolué pour chercher des IDS capables de réagir en temps réel. Le constat des dégâts ne suffisait plus : il fallait réagir et pouvoir bloquer les trafics douteux détectés. Ces techniques de réponse impliquèrent les IDS actifs ou IPS.

4. CLASIFICATION ET EVALUATION DES PERFORMANCES DES IDS/IPS

4.1. EVATUATION SOLEN LA METHODE UTILISEE, FIABILITE, REACTIVITE, PERFORMANCE, DEBIT, COMPORTEMENT APRES L'INTRUSION, FAUSSE ALERTE

4.1.1. CARACTERISTIQUES A EVALUER ET A COMPARER POUR LES SYSTEMES IDS/IPS

L'expression «système de détection et de prévention des intrusions» est utilisé indifféremment pour décrire de multiples technologies et solutions de sécurité. Le présent chapitre se concentre sur les systèmes de détection et prévention des intrusions capables de prendre des mesures immédiates pour contrer les attaques et intrusions sans intervention manuelle. Les outils des systèmes de détection et de prévention des intrusions présentant les caractéristiques suivantes:

- Appareil en ligne capable de détecter de manière fiable et juste les attaques et de les bloquer avec précision : justesse et précision.
- Fonctionnement à vitesse de ligne, sans effet néfaste sur la performance ou la disponibilité du réseau : bonne citoyenneté sur le réseau.
- Intégration efficace dans un environnement de gestion de sécurité : gestion efficace centrée sur la sécurité.
- Facilité d'adaptation pour la prévention des attaques à venir : anticipation des attaques inconnues et incorporation aisée des signatures d'attaque nouvellement découvertes.
- Justesse et précision. Comme on l'a évoqué précédemment, les produits NIDS présentent un inconvénient de taille, à savoir le nombre élevé de faux résultats générés par les méthodes de détection et constitue vraiment une problématique pour un système NIDS, cette limitation devient absolument inacceptable pour un système IPS. Une détection erronée peut engendrer des mécanismes de réaction qui touchent le trafic légitime et incommodent les utilisateurs.
- Bonne citoyenneté sur le réseau. Le système IPS n'est pas un observateur : il fait partie intégrante du réseau. De ce fait, il doit supporter toutes les contraintes que l'organisation peut lui imposer. Il doit être un bon citoyen sur le réseau, en termes de performance, fiabilité et disponibilité. La performance décrit la capacité de l'IPS à laisser le trafic circulé sur le réseau. Une performance médiocre dans un environnement où le trafic est dense causera une baisse de la performance du réseau, voire des pertes de paquets. La fiabilité fait référence à la capacité du système IPS à

exécuter correctement ses fonctions, sans interférence avec les autres systèmes présents sur le réseau. La disponibilité relève de la durée d'immobilisation du produit due aux arrêts, aux blocages ou à la maintenance.

- Gestion efficace centrée sur la sécurité. Un système IPS offre à l'administrateur de sécurité réseau une grande diversité d'options : il est en effet capable de détecter les attaques et les intrusions, mais aussi d'influencer directement le trafic réseau en le limitant ou en le bloquant. Une véritable solution IPS ne doit pas être totalement indépendante, mais fonctionner dans le cadre d'une suite intégrée de gestion de la sécurité, en collaborant avec les produits et fonctions de pare-feu, de NIDS, d'antivirus et d'évaluation des vulnérabilités.
- Anticipation des attaques inconnues et incorporation aisée des signatures d'attaque nouvellement découvertes.

Un système IDS/IPS doit inclure des méthodes souples et transparentes pour mettre à jour les nouvelles signatures d'attaque, mais aussi ses fonctionnalités permettant de réagir à des classes d'attaque entièrement nouvelles à l'aide de mises à niveau du firmware ou des logiciels. En outre, les systèmes IDS/IPS doivent disposer de méthodes capables de réagir à de nouvelles attaques sans mises à jour de signature.

4.1.2. CARACTERISTIQUES DE CLASSIFICATION DES IDS ET DES IPS

Il existe aujourd'hui de nombreux produits dont la complexité de mise en œuvre et le degré d'intégration sont très divers. Les outils strictement basés sur des modèles comportementaux sont actuellement en perte de vitesse. Mais ils sont de plus en plus intégrés à des IDS /IPS initialement basés sur une bibliothèque de signatures, étant donné leur complémentarité. Les outils systèmes sont un peu en retrait face aux outils réseaux. L'arrivée des outils hybrides, qui apportent une sécurité moins parcellaire dans la protection du système d'information, pourrait remettre en question l'état du marché des outils.

Le premier critère de classification des IDS/IPS reste la méthode d'analyse.

Deux approches sont possibles :

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

système de détection dépend fortement de la précision de sa base de signature. C'est pourquoi ces systèmes sont contournés par les pirates qui utilisent des techniques dites "d'évasion" qui consistent à maquiller les attaques utilisées. Ces techniques tendent à faire varier les signatures des attaques qui ainsi ne sont plus reconnues par l'IDS/IPS.

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

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

Les systèmes de détection et prévention d'intrusion sont devenus indispensables lors de la mise en place d'une infrastructure de sécurité opérationnelle. Ils s'intègrent donc toujours dans un contexte et dans une architecture imposant des contraintes très diverses. Certains critères peuvent être dégagés:

- ***Fiabilité*** : Les alertes générées doivent être justifiées et aucune intrusion ne doit pouvoir lui échapper.
- ***Réactivité*** : Un IDS/IPS doit être capable de détecter et d'empêcher les nouveaux types d'attaques le plus rapidement possible; pour cela, il doit rester constamment à jour. Des capacités de mise à jour automatique sont pour ainsi dire indispensables.
- ***Facilité de mise en œuvre et adaptabilité***: Un IDS/IPS doit être facile à mettre en œuvre et surtout s'adapter au contexte dans lequel il doit opérer; il est inutile d'avoir un IDS/IPS émettant des alertes en moins de 10 secondes si les ressources nécessaires à une réaction ne sont pas disponibles pour agir dans les mêmes contraintes de temps.
- ***Performance*** : La mise en place d'un IDS/IPS ne doit en aucun cas affecter les performances des systèmes surveillés. De plus, il faut toujours avoir la certitude que l'IDS/IPS a la capacité de traiter toute l'information à sa disposition (par exemple un IDS réseau doit être capable de traiter l'ensemble du flux pouvant se présenter à un

instant donné sans jamais supprimer de paquets) car dans le cas contraire, il devient trivial de masquer les attaques en augmentant la quantité d'information.

Parmi les autres critères de classification existants, nous pouvons citer entre autres :

- Les sources de données à analyser (réseau/système/application).
- Le comportement du produit après intrusion (passif/actif).
- La fréquence d'utilisation (périodique/continue).
- Les systèmes d'exploitation utilisés (Linux, Windows, …).

Les outils devaient provenir du monde OpenSource pour les raisons suivantes:

- C'est gratuit. Nous ne sommes pas obligés de payer un produit pour faire une recherche qui n'est pas sûre d'aboutir.
- Les produits OpenSource sont livrés avec le code. Rien n'est caché.
- Il est possible de faire des modifications si nécessaires.
- La documentation aux grands projets OpenSource est complète.
- Nous n'avons pas de formats propriétaires avec lesquels il faut s'adapter, car il n'est pas possible, ni autorisé de modifier un programme commercial (dans la plupart des cas).
- Les mises à jour sont régulières et corrigent les bugs de manière souvent bien plus rapide que les programmes commerciaux dont le but est plus de cacher leurs faiblesses que de les corriger.
- Les mises à jour sont aussi gratuites. Il ne sera pas nécessaire de payer pour mettre à jour les règles ou les vulnérabilités détectées par ces produits.

4.1.3. CLASSIFICATION DES OUTILS IDS / IPS

Pour assurer une bonne protection des données, différents outils sont disponibles. Ils ont en général utilisés ensemble, de façon à sécuriser les différentes failles existantes dans un système. Pour éviter les inconvénients des NIDS, NIPS, HIDS ou HIPS, il est très intéressant de combiner ces différents systèmes. Chacun présente des inconvénients qui permettent leur contournement [10]. Le manque d'information au niveau hôte des NIDS et NIPS et le coût d'installation-administration des HIDS s'annulent par une bonne cohabitation de ces systèmes

sur un réseau : il n’existe pas de système complet miracle, la sécurité optimum s’obtient donc grâce à l’association de plusieurs systèmes.

Or, la plupart de ces solutions sont développées par les grandes entreprises de sécurités. Ces solutions sont complètes et peuvent être facilement mise en place dans un réseau, ce qui est vrai également pour les mises à jour. Le format modulaire utilisé par celles-ci leur permet d’avoir plusieurs agents pour une interface centralisée. Par contre, ces solutions sont particulièrement dispendieuses et leur fonctionnement obscur pour un administrateur qui souhaiterait l’optimiser pour son réseau.

La plupart des solutions existantes en matière de détection d'intrusion concernent la mise en place de NIDS complétés éventuellement par certains HIDS et du logiciel de gestion associé (manager). Dans cette section, nous étudierons certaines des solutions les plus populaires dans les domaines commerciaux et OpenSource.

Caractéristique / Produit	IPS		IDS		Méthode	plate forme	Débit (Max)	logiciel ou Appliance	libre ou comm	mise à jour	install et config	fausse alerte	Comportement après l'intrusion	fréquence d'utilisation	fiabilité	réactivité	performance
	HIPS	NIPS	HIDS	NIDS													
Cisco NetRanger		√	√	√	S	S.E plus courants	4 Gb/s	A/L	Cm	Auto	Smp	++	Actif	continu	++	Actif	++
Snort Snort		√	√	√	S	Linux Win	grand réseaux	L	Lbr	Man	Dff	++	Actif	continu	++	Actif	++
ISS RealSecure et Proventia	√	√	√	√	S/C	S.E plus courants	Jusqu'à 10 Gb/s	A/L	Cm	Auto	Smp	++	Actif	continu	++	Actif	++
Arkoon Arkoon IDS en coupure	√	√	√	√	S	Linux Win	Jusqu'à 11 Gb/s	A	Cm	Auto	Smp	++	Actif	continu	+++	Actif	+++
Enterasys Networks Dragon			√	√	S	S.E plus courants	1Gb/s	A/L	Cm	Auto	Smp	++	Passif	continu	+	Passif	+

NetScreen Intrusion Detection and Prevention (IDP)	√	√			S	S.E plus courants	1 Gb/s	A	Cm	Auto	Smp	++	Actif	continu	+	Actif	+
Symantec Host IDS et Symantec ManHunt			√	√	S	S.E plus courants	4 Gb/s	L/A	Cm	Auto	Smp	++	Passif	continu	++	Passif	++
Prelude IDS			√	√	S	S.E plus courants	1 Gb/s	L	Lbr	Man	Dff	++	Passif	continu	++	Passif	++
Network Associates Mcafee Entercept et IntruShield Network IDS Sensor	√	√	√	√	S/C	Win et Solaris	2 Gb/s	A/L	Cm	Auto	Smp	++	Actif	continu	++	Actif	++

Tripwire			√		S	linux		L	Lbr		Dff	++	Passif	continu	+	Passif	+

S: Par Signature

C: approche comportementale

L: logiciel

Lbr: Libre

Cm: Commercial

Auto: Automatique

Smp : Simple

Dff : Difficile

+ : Faible

++ : Moyenne ; +++ : Bonne

Tableau 1 : les caractéristiques des outils IDS et IPS

4.2. EVATUATION SOLEN LES OBJECTIFS DE LASECURITE INFORMATIQUE

La détection d'intrusion a pour objectif de détecter toute violation de la politique de sécurité sur un système informatique. Elle permet ainsi de signaler les attaques (en temps réel ou en différé) portant atteinte à la sécurité de ce système.

Par sécurité du système, nous considérons l'intégrité, la confidentialité, la disponibilité, l'authentification, la non répudiation et le contrôle d'accès du système et des données.

Par attaque, nous ne considérons pas seulement les intrusions ou tentatives d'intrusion mais aussi d'autres actions telles que les scans, dénis de service, utilisations non autorisées de systèmes/services, mauvaises utilisations de systèmes/services...

Pour mettre en œuvre ce concept de détection d'intrusion, des outils spécifiques sont nécessaires : les IDS ou IPS (systèmes de détection et de prévention d'intrusions). Ils vont permettre de collecter de façon automatisée les données représentant l'activité des systèmes (serveurs, applications, systèmes, réseaux), de les analyser et d'avertir les administrateurs et arrêter l'intrus en cas de détection de signes d'attaques.

4.2.1. CLASSIFICATION DES ATTAQUES

Les attaques portées à la sécurité d'un ordinateur ou d'un réseau sont mieux caractérisées en considérant le système en tant que fournisseur d'information. En général, il existe un flot d'information issu d'une source - un fichier ou une zone de la mémoire centrale- vers une destination - un autre fichier ou utilisateur-. Il existe quatre catégories d'attaques : interruption, interception, modification, fabrication.

- ***Attaques de sécurité : interruption***

Un atout du système est détruit ou devient indisponible ou inutilisable. C'est une attaque portée à la *disponibilité*. La destruction d'une pièce matérielle (tel un disque dur), la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichiers.

- ***Attaques de sécurité : interception***

Une tierce partie non autorisée obtient un accès à un atout. C'est une attaque portée à la *confidentialité*. Il peut s'agir d'une personne, d'un programme ou d'un ordinateur. Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichiers ou de programmes.

- ***Attaques de sécurité : modification***

Une tierce partie non autorisée obtient accès à un atout et le modifie de façon indétectable. Il s'agit d'une attaque portée à *l'intégrité*. Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau.

- ***Attaques de sécurité : fabrication***

Une tierce partie non autorisée insère des contrefaçons dans le système. C'est une attaque portée à *l'authenticité*. Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrements à un fichier.

4.2.2. ATTAQUES PASSIVES ET ATTAQUES ACTIVES

Il peut être utile de distinguer deux catégories d'attaques : les attaques passives et les attaques actives.

- ***Attaques passives***

Écoutes indiscrètes ou surveillance de transmissions sont des attaques de nature passive. Le but de l'adversaire est d'obtenir une information qui a été transmise. Ces attaques passives sont la capture du contenu d'un message et l'analyse de trafic. La capture du contenu de messages est facilement compréhensible. Une conversation téléphonique, un courrier électronique ou un fichier transféré peuvent contenir une information sensible ou confidentielle. La seconde attaque passive, l'analyse de trafic, est plus subtile. Supposons qu'un moyen de masquer le contenu des messages ou des informations soit à disposition (par exemple, un système de chiffrement), de sorte que les adversaires, même en cas de capture, ne pourront en extraire l'information contenue. Cependant l'adversaire pourra être en mesure d'observer le motif de ces messages, déterminer l'origine et l'identité des systèmes en cours de communication, et observer la fréquence et la longueur des messages échangés. Cette information peut être utile pour deviner la nature de la communication. Les attaques passives sont très difficiles à détecter car elles ne causent aucune altération des données.

- ***Attaques actives***

La seconde catégorie d'attaques est l'attaque active. Ces attaques impliquent certaines modifications du flot de données ou la création d'un flot frauduleux ; elles peuvent être subdivisées en quatre catégories : mascarade, rejeu, modification de messages et déni de

service. Une mascarade a lieu lorsqu'une entité prétend être une autre entité. Une attaque de ce type inclut habituellement une des autres formes d'attaque active. Par exemple, des séquences d'authentification peuvent être capturées et rejouées, permettant ainsi à une entité autorisée munie de peu de privilèges d'en obtenir d'autres en usurpant une identité possédant ces privilèges. Le rejeu implique la capture passive de données et leur retransmission ultérieure en vue de produire un effet non autorisé. La modification de messages signifie que certaines portions d'un message légitime sont altérées ou que les messages sont retardés ou réorganisés. Par exemple, le message " autoriser X à lire le fichier confidentiel comptes " est modifié en " autoriser Y à lire le fichier confidentiel comptes ". Le déni de service empêche l'utilisation normale ou la gestion de fonctionnalités de communication. Cette attaque peut avoir une cible spécifique ; par exemple, une entité peut supprimer tous les messages dirigés vers une destination particulière. Une autre forme de refus de service est la perturbation d'un réseau dans son intégralité, soit en mettant hors service le réseau, soit en le surchargeant de messages afin de dégrader ses performances.

4.2.3. ATTAQUES CONTRE LES IDS

Un IDS étant le moyen de protéger un système, les attaquants voudront souvent l'attaquer avant de s'attaquer au système qu'il protège, et puisque les IDS sont des systèmes informatiques, ils contiennent des failles. Il existe plusieurs types d'attaques telles que le déni de service, l'insertion, l'évasion et la modification des paquets transitant du senseur jusqu'à l'analyseur. Dans ce cas de déni de service, l'IDS devient non fonctionnel en le saturant d'information. Pour contrer cela, il est nécessaire de filtrer et stocker correctement les informations et avoir un IDS performant qui gère un ensemble de paquets sans perte. De plus, un système de monitoring permet de vérifier l'efficacité réelle de l'IDS.
Détection d'un IDS Tout comme pour attaquer une machine, pour attaquer un IDS, il faut pouvoir le détecter. En voici quelques exemples :

- Usurpation d'adresse MAC: les NIDS mettent l'interface de capture de paquet réseau en mode promiscuité où ils voient tout paquet qui transite. Ainsi, en envoyant un paquet ICMP de type « echo request » où la machine le recevant doit émettre un paquet ICMP de type « echo reply » , avec une adresse MAC destinataire inexistante dans le réseau, on peut vérifier si la machine répond. Ainsi, puisque le NIDS est en

mode promiscuité, il verra le paquet et renverra un echo reply sans même vérifier qu'il est bien le destinataire du paquet ICMP.

- Mesure de temps de latence : puisque les NIDS sont en mode promiscuité, ils doivent gérer l'ensemble des paquets du réseau. Ainsi, si après un envoi massif de paquets à toute les machines, une machine devient de plus en plus lente à répondre, on peut supposer qu'elle est en mode promiscuité et qu'elle est donc probablement un NIDS.

Observation des requêtes : après une attaque, les IDS envoient généralement des messages à un ordinateur central qui va gérer l'ensemble des alertes. Ainsi, en observant les paquets, on peut essayer de retrouver la centrale. Un des problèmes de ce genre d'attaques est que, dans la plupart des cas, l'IDS ne prévient pas l'ensemble du système qu'il ne fonctionne plus. Ceci est d'autant plus dangereux quand l'IDS ne sait pas s'il fonctionne correctement ou pas. Ainsi, après avoir attaqué l'IDS, le pirate peut attaquer le système en toute impunité. Par conséquent, un IDS doit pouvoir distinguer si un pirate attaque l'IDS ou le système des machines protégées par l'IDS pour éventuellement prévenir le système.

4.2.4. EVALUATION DES PERFORMANCES DES OUTILS DE DETECTION ET PREVENTION D'INTRUSION

La sécurité informatique est l'utilisation de la technologie, des politiques et de l'éducation des personnes pour assurer la confidentialité, l'intégrité, authenticité et l'accessibilité des données durant leur stockage, leur traitement et leur transmission. La sécurité des données doit dépendre du système à sécuriser. Ainsi, selon ce dernier, on insistera plus ou moins sur l'intégrité, l'authenticité, la confidentialité ou la disponibilité.

Pour assurer la confidentialité, l'intégrité, authenticité et la disponibilité, on utilise un ensemble de règles de sécurité: enlever les programmes non utilisés, utiliser des firewalls, utiliser des contrôles d'accès, configurer correctement les programmes, algorithme de chiffrement, utiliser des anti-virus, utiliser des IDS,.... Nous allons nous focaliser sur les systèmes de détection et de prévention.

Parmi les méthodes utilisées en évaluation des systèmes de détection [13][14][11][15][16][17], ce travail met l'accent sur la méthode des objectifs de la sécurité :

- Intégrité : le nombre des bits qui robuste (ou le nombre des bits erroné)
  On pose n(I) le nombre des bits erroné et D le débit;
- Confidentialité : algorithme de chiffrement ;

- Disponibilité : le temps de fonctionnement ;
- Authentification : assurer l'identité d'un utilisateur.

Afin de répondre à notre objectif susmentionné, nous utilisons les paramètres de variation de réseau axés principalement sur :

- Le débit (bits/s) ;
- Les données (les attaques) ; visant l'utilisation des quatre types les plus adéquats à savoir : déni de service, man in the middle (MITM), chopchop et usurpation d'adresse MAC.

Dans ce cas, on teste six outils de détection d'intrusion, trois pour les réseaux filaires et trois pour les réseaux ans fils.

4.2.4.1. Evaluation par le débit

Concernant le paramètre débit, les performances des outils de Detection des intrusions peuvent être testées via l'augmentation de débit des données circulées sur les réseaux testés. Le test sera opéré au niveau de deux types de réseaux (filaire et sans fil).

- **Intégrité**

Il faut pouvoir garantir que les données sécurisées par le système IDS/ IPS n'ont pas été modifiées pas une personne non autorisée. Donc au niveau de ce test, le nombre des bits erroné sera examiné en faisant augmenter le dédit des données circulées sur le réseau.(tableau2)

outil / débit	Snort	CISCO NetRanger	NetScreen (IDP)	Snort-Wireless	AirMagnet	AirDefense
5 MB/s	Normal	Normal	normal	normal	normal	normal
10 MB/s	Normal	Normal	normal	normal	anormal	anormal
1 GB/s	Normal	Normal	normal			
4 GB/s	Normal	Normal	anormal			

Tableau 2 : Niveau d'intégrité

On peut dire que chaque fois le débit augmente, le nombre de bits erronés sont élevés donc l'efficacité d'outil diminue.

- **Confidentialité**

Évidemment, si on n'utilise aucun mécanisme de chiffrement, on court le risque que nos données puissent être facilement interceptées par une personne malveillante. Les données ne doivent être visibles que pour les personnes habilitées. Mais il y a des algorithmes de chiffrement très faciles de déchiffrement par les attaques. Donc pour tester le niveau de la confidentialité d'un système on va tester la solidité d'algorithme de chiffrement utilisé.
Comparaison entre les algorithmes de chiffrement utilisés par chaque outil (tableau 3)

	Snort	CISCO NetRanger	NetScreen (IDP)	Snort-Wireless	AirMagnet	AirDefense
Algorithme de Chiffrement	TwoFish	RC4	RC4	TwoFish		

Tableau 3: Algorithme de chiffrement

Twofish emploie la méthode d'addition qui est très difficile à défendre contre les attaques par analyse de puissance et de temps. L'utilisation de technique de masquarade ne dégrade pas trop ses performances mais augmente de manière considérable la RAM employée. Il reste vulnérable aux attaques par analyse de puissance. Contre l'algorithme RC4 qui est très affaiblie [18][19][20].
Donc pour assurer la confidentialité d'un système informatique il faut choisir un système de détection qui intègre un algorithme de chiffrement plus solide.

- **Disponibilité**

Les données doivent rester accessibles aux utilisateurs, par exemple, une attaque de type Dos, vise à empêcher les utilisateurs normaux d'un service d'y accéder. Pour tester le niveau de la disponibilité d'un système. A cet effet, le temps de fonctionnement pour chaque outil sera comparé.
Le tableau ci-dessous illustre précisément les résultats de ce test. (Tableau 4)

	Snort	CISCO NetRanger	NetScreen (IDP)	Snort-Wireless	AirMagnet	AirDefense
Temps de fonctionnement (réel ou non)	oui	Oui	oui	oui	oui	oui

Tableau 4: Niveau de disponibilité

On peut conclure qu'actuellement tous les systèmes sont fonctionnels en temps réel donc en matière de disponibilité, il n'y pas de problème pour tous les systèmes testés.

- **Authentification**

L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Donc pour connaître le niveau d'authentification d'un système, pour cela, la méthode utilisée pour assurer l'identité d'un utilisateur va être comparée pour chaque outil. (tableau 5)

	Snort	CISCO NetRanger	NetScreen (IDP)	Snort-Wireless	AirMagnet	AirDefense
Assurer l'identité d'un utilisateur	haute	Haute	Moyenne	haute	moyenne	moyenne

Tableau 5 : Niveau d'authentification

4.2.4.2. Evaluation selon les attaques

- **Déni de service (DOS)**

L'attaque DOS est une attaque contre la disponibilité. Cette attaque consiste à paralyser temporairement et de rendre indisponible des serveurs afin qu'ils ne puissent servir et répondre aux requêtes de ses utilisateurs légitimes. Pour y parvenir, cette attaque peut exploiter des vulnérabilités et faiblesses dans la conception ou l'implémentation des

protocoles, des services et des applications. Les attaques DOS sont les plus simples et les plus à effectuer.

Les systèmes suivants selon l'attaque DOS seront testés, Le tableau ci-dessous illustre les résultats de ce test.(table 6)

	Snort	CISCO NetRanger	NetScreen (IDP)	Snort-Wireless	AirMagnet	AirDefense
fiabilité	haute	Haute	Moyenne	moyenne	moyenne	moyenne

Tableau 6: Niveau de fiabilité par rapport a l'attaque DOS

Au niveau des outils testés, ils peuvent conduire à des faux positifs et des faux négatifs surtout les outils sans fil.

- **Maine in the Middle (MITM)**

L'attaque MITM est une attaque contre l'intégrité. L'attaque MITM est une redirection complète d'une connexion entre deux machines. Chacun des deux interlocuteurs croit dialoguer directement avec l'autre, mais en réalité, il adresse ses données à une troisième machine qui joue le rôle d'un routeur et renvoie les trames modifiées vers le véritable destinataire (tableau 7).

Le test des systèmes suivants selon l'attaque MITM sera effectué. Le tableau ci-dessous illustre les résultats de ce test.

	Snort	CISCO NetRanger	NetScreen (IDP)	Snort-Wireless	AirMagnet	AirDefense
fiabilité	haute	Haute	Haute	moyenne	faible	faible

Tableau 7 : Niveau de fiabilité par rapport a l'attaque MITM

- **Usurpation d'adresse MAC**

Les attaques Usurpation d'adresse MAC sont des attaques contre l'authentification.

L'attaque d'usurpation d'adresse MAC *(MAC spoofing)* consiste donc à se faire passer pour quelqu'un qu'on n'est pas en réalité. Il suffit à l'intrus d'utiliser l'identité d'une autre station (son adresse MAC) soit pour monter une attaque sans se faire repérer, soit pour accéder à

des services privilégiés, soit pour détourner un système de filtrage par adresse MAC. Techniquement, il est facile de changer l'adresse MAC d'une interface sans-fil. Mais l'intrus n'a pas besoin de changer son adresse puisqu'il lui suffit de forger une trame 802.11 avec les adresses MAC de son choix.

Plusieurs travaux ont tenté de détecter l'attaque *MAC spoofing* [21][22][23] mais aucun ne réussit à le faire de façon efficace, des cas de faux positifs et de faux négatifs persistent. Les systèmes suivants selon l'attaque usurpation d'adresse MAC seront testés, Le tableau ci-dessous illustre les résultats de ce test.(table VII)

	Snort	CISCO NetRanger	NetScreen (IDP)	Snort-Wireless	AirMagnet	AirDefense
Fiabilité	moyenne	moyenne	moyenne	faible	faible	faible

Tableau 8 : Niveau de fiabilité par rapport à l'attaque usurpation MAC

- **Chopchop**

Chaque paquet est constitué de deux parties : les données et le CRC32 qui permet d'assurer l'intégrité de ces données. Le tout est ensuite envoyé à l'algorithme de chiffrement WEP c'est à dire RC4 : le paquet chiffré envoyé sur le réseau est le résultat du xor entre la concaténation du message et de son CRC32 et le keystream qui est fonction de la clef WEP et du vecteur d'initialisation courant. Si D est le message en clair, ICV l'opération de CRC32 (Integrity Check Value), C le message chiffré, K la clef WEP, IV le vecteur d'initialisation courant et || l'opérateur de concaténation alors ce que je viens d'écrire peut se résumer de cette façon :

C = RC4(IV || K) xor (D || ICV(D))

A la base, le CRC32 était écrit pour assurer l'intégrité des données et en aucun cas pour assurer leur sécurité. L'attaque ChopChop [24] va donc utiliser plusieurs faiblesses de cet algorithme pour injecter des données sur le réseau.

Si l'on souhaite injecter des données dans le réseau à partir d'un paquet chiffré capturé alors nous avons les relations suivantes :

C = RC4(IV || K) xor (D || ICV(D)) est le paquet capturé.

D' représente les données que l'on va injecter dans le réseau tel que : D' = D xor Mod

Nous avons donc :

C’ = RC4(IV || K) xor (D’ || ICV(D’))

Ici comme nous ne connaissons pas D, nous ne connaissons pas non plus D’.

D’ || ICV(D’) = (D || ICV(D)) xor (Mod || ICV’(Mod)) ou ICV’ est un CRC32 modifié

donc

C’ = RC4(IV || K) xor (D || ICV(D)) xor (Mod || ICV’(Mod))

C’ = C xor (Mod || ICV’(Mod))

Cette relation montre qu’à partir d’un paquet chiffré valide, il est possible d’injecter n’importe quelle modification de ce paquet. C’ qui était inconnu est en définitif seulement fonction d’élément connu.

L’attaque ChopChop utilise une autre vulnérabilité du CRC32. Si le message C est tronqué de son dernier octet de données, le message devient donc invalide car le CRC32 ne correspond plus. Cependant si on xor C avec une certaine valeur Mod, alors le paquet redevient valide. Une démonstration mathématique montre que Mod ne dépend que de la valeur en clair de l’octet tronqué.

On peut donc écrire que Mod = f(X) où X est la valeur en clair de l’octet tronqué. L’attaque coule maintenant de source. Étant donné qu’il y a 256 valeurs possibles pour X, il suffit de toutes les tester.

On prend donc notre paquet capturé C, on lui enlève le dernier octet de données. On prend comme hypothèse que la valeur non chiffrée X de cet octet tronqué est 0 et on génère notre modification :

C’ = C xor f(x) avec x=0

On envoie C’ et si C’ est rejoué par l’Access Point alors c’est que notre paquet C’ était valide, donc notre hypothèse sur X était bonne. On vient donc de trouver un octet en clair de C (donc un octet de D), notre hypothèse sur X était bonne. On vient donc de trouver un octet en clair de C (donc un octet de D), et donc un octet du keystream utilisé pour chiffrer cet octet. Si le paquet C’ n’est pas rejoué par l’Access Point, alors c’est que notre paquet C’ n’est pas valide, donc notre hypothèse sur X était fausse. On retente en incrémentant X, jusqu’à que le paquet C’ soit rejoué. En moyenne il faudra donc envoyer 128 paquets pour décrypter un octet. La suite est évidente, on réitère la même méthode pour trouver tous les octets de D, donc octet par octet.

ChopChop est une attaque contre la confidentialité, pour détecter cette attaque, on utilise les IDS. Pour ce faire, On testera trois outils de détection d’intrusion pour les réseaux sans fils (tableau 9).

	Snort-Wireless	AirMagnet	AirDefense
Fiabilité	Moyenne	faible	Faible

Tableau 9 : Niveau de fiabilité par rapport à l'attaque chopchop

Avec le chiffrement des donnes dans le réseau sans fil les IDS testés sont faibles.
Donc la solution est l'utilisation des IPS pour assurer le réseau sans fil.

4.3. CLASSIFICATION DES OUTILS ID/PS BASEE SUR LE RESEAU DE NEURONE ARTIFICIEL

4.3.1. NEURONE ARTIFICIEL

Les réseaux de neurones est un modèle de calcul inventé dans les années 40 et s'inspirent de la conception du système nerveux humain. Le neurone est la base d'un réseau de neurones artificiels. Il est décrit par son état, une fonction de combinaison et une fonction d'activation. L'état du neurone, qui est une valeur booléenne ou réelle, est la valeur de sortie du neurone. Chaque neurone est connecté à d'autres neurones via des connexions synaptiques. La synapse est associée d'un poids qui est utilisé par la fonction de combinaison pour effectuer un prétraitement, généralement une somme pondérée, des entrées. La fonction d'activation, appelée aussi fonction de transfert, calcule à partir du résultat de la fonction de combinaison la valeur de sortie du neurone.
Les neurones artificiels sont des petites unités de traitement composés d'une ou plusieurs entrées, d'une sortie et d'un corps de cellule qui effectue des calculs à partir des données de l'entrée pour produire la sortie (Figure 7). En pratique, un neurone est capable de discriminer deux classes, c'est à dire de produire 1 ou -1 à sa sortie.

4.3.1.1. Entrées

Soit $(x_1, \ldots, x_n)$ un vecteur des données en entrée du neurone. Celles-ci peuvent être des données d'entrée du réseau ou des valeurs intermédiaires provenant de sorties d'autres neurones. Un vecteur

$E^T_{entree} = (x_1, \ldots, x_i, \ldots, x_n)$ caractérise un élément d'entrée du neurone. Il peut s'agir par exemple de coordonnées cartésiennes $(x, y, z)^T$

Chacune de ces entrées est pondérée par un poids. Ces poids constituent un vecteur de pondération des entrées $P^T_{entree} = (w_1, \ldots, w_i, \ldots, w_n)$.

La dernière entrée est appelée entrée de biais. Sa valeur est toujours égale à 1, son poids associé b est appelé le biais du neurone.

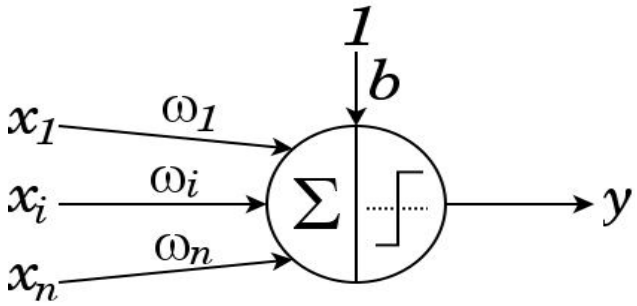

Figure 7 : Structure d'un neurone

4.3.1.2. Cellule

L'unique fonction de la cellule est de produire une sortie égale à 1 ou -1.

Pour cela, elle effectue la somme pondérée des éléments entrés :

$$f(S) = b + \sum_{i=1}^{n} x_i w_i$$

Connaissant cette somme, on utilise une fonction de seuil qui renvoie -1 si la somme est négative ou 1 si la somme est positive :

$$y = \begin{cases} 1 & \text{si } f(s) \geq 0 \\ -1 & \text{sinon} \end{cases}$$

4.3.1.3. Sortie

La sortie d'une cellule est une valeur binaire 1 ou -1 dans le cas d'un neurone à seuil. C'est la réponse du neurone à un problème de tri entre deux ensembles d'éléments de dimension n. Dans un réseau de neurones, cette sortie (pondérée ou non) peut constituer l'entrée d'un nouveau neurone (Figure 8).

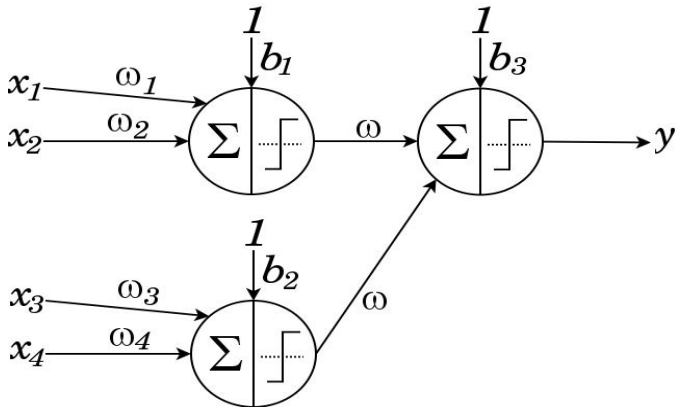

Figure 8: Réseau de deux neurones d'entrées et un neurone de sortie

4.3.2. APPRENTISSAGE ET CLASSEMENT

Nous nous intéresserons pour la suite au plus simple des réseaux de neurones : le perceptron. Il peut être vu comme un unique neurone capable de séparer linéairement un ensemble de vecteurs E_{entree} en deux groupes distincts étiquetés *A* et *B*.

4.3.2.1. Apprentissage

Dans son état initial, un perceptron ne sait pas comment séparer les deux groupes, il faut qu'il "apprenne". Nous disposons pour cela d'un échantillon d'apprentissage constitué de vecteurs d'entrée particuliers, dont on connaît le groupe g d'appartenance :

$E_{learn}^{T} = (x_1,\ldots, x_n, g)$ avec

$$y = \begin{cases} 1 & \text{si } E_{learn} \in A \\ -1 & \text{si } E_{learn} \in B \end{cases}$$

L'algorithme d'apprentissage consiste à donner les vecteurs E_{learn} en entrée du perceptron et comparer la sortie *y* à la sortie attendue *g*. Si sortie réelle et sortie attendue sont différentes, on va adapter le vecteur de pondération des entrées P_{entree} et le biais b en les incrémentant ou décrémentant d'un pas d'apprentissage α fixée arbitrairement. On répète ces étapes *t* fois. Plus *t* est grand, plus le perceptron apprend (Figure 9).

Initialiser P_{entree} et *b* à 0
Initialiser α ($0 < \alpha \leq 1$)
Initialiser *t*
Pour *j* allant de 1 à *t* faire
    Présenter un vecteur E_{learn} à l'entrée du perceptron
    Calculer la réponse *y* du perceptron
    si $y \neq g$ alors
        Pour chaque dimension *w* de P_{entree},
        i allant de 1 à dim(P_{entree}), faire
            $w_i \leftarrow w_i + x_i * \alpha * g$
        Fin pour
        $b \leftarrow b + \alpha * g$
    Fin si
Fin pour

Figure 9 : Algorithme du perceptron

4.3.2.2. Classement

Après l'apprentissage, les poids et le biais du perceptron sont fixes. On soumet alors des vecteurs E_{entree} et la sortie du perceptron doit correspondre au groupe g dans lequel ils seraient classés.

4.3.3. CLASSIFICATION DES OUTILS ID/PS

Dans ce test, on veut tester six outils de détection d'intrusion, trois pour les réseaux filaires et trois pour les réseaux sans fils (Snort, CISCO NetRanger et NetScreen (IDP) des outils pour les réseaux filaires et Snort-wireless, AirMagnet et AirDefense des outils pour les réseaux sans fils).

4.3.3.1. Les données

Les données d'apprentissage et de test ont été collectées à partir d'un réseau local filaire pour les outils filaire et un réseau local sans fils pour les trois outils sans fils. Le réseau est constitué de trois machines et un point d'accès. Une machine est utilisée pour l'émission du trafic normal, la deuxième machine envoie en alternance les données d'attaques et la dernière machine sert pour collecter le trafic. La collecte des données se fait par un logiciel que nous avons développé spécialement pour cet objectif.

Les intrusions que nous avons utilisées sont : l'attaque DOS, MITM, MAC spoofing et l'attaque chopchop pour le réseau sans fil.

Les données collectées sont séparées dans deux ensembles : ensemble d'apprentissage et de test. Le premier ensemble est utilisé pour calculer les poids optimaux des synapses. A chaque entrée est associée la valeur réelle de la sortie. En itérant sur cet ensemble de données, le classificateur est capable d'adapter dynamiquement les valeurs des poids des connexions pour minimiser le taux d'erreur entre les valeurs de sortie du réseau et les valeurs réelles. Le réseau de neurones peut produire des performances élevées sur l'ensemble d'apprentissage, mais affiche des résultats médiocres sur l'ensemble de test. Ces données ne sont pas directement utilisées par dans l'algorithme d'apprentissage. Elles sont gardées à part et le réseau peut les utiliser pour mesurer l'erreur entre les données de sortie et les données désirées. Le réseau converge lorsque cette erreur est inférieure à un seuil prédéfini. Une fois le réseau est entraîné et validé, il doit être en mesure de prédire la classe de chaque entrée de l'ensemble de test.

4.3.3.2. Résultats expérimentaux

Les résultats des tests sont obtenus à partir du logiciel NeuroSolutions. Les trois types des réseaux de neurones ont été entraînés avec l'ensemble complet des paramètres [28][29][34][36]. Nous avons évalué les performances des classificateurs en utilisant le taux de détection et le temps d'apprentissage. Les résultats démontrent que les efficacités des outils IDS/IPS.

Les diagrammes suivants détaillent le résultat pour chaque outil.

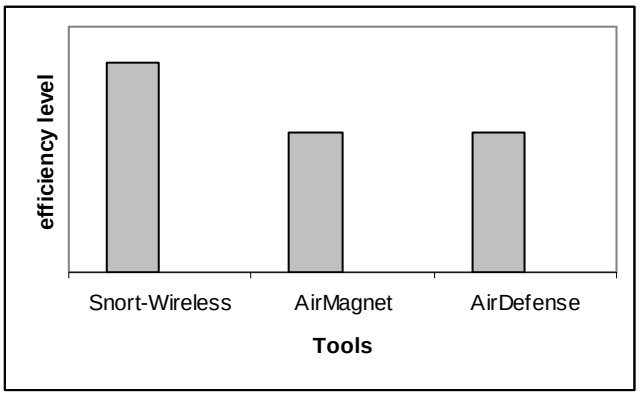

Figure 11 : L'efficacité des outils sans fil expérimentés

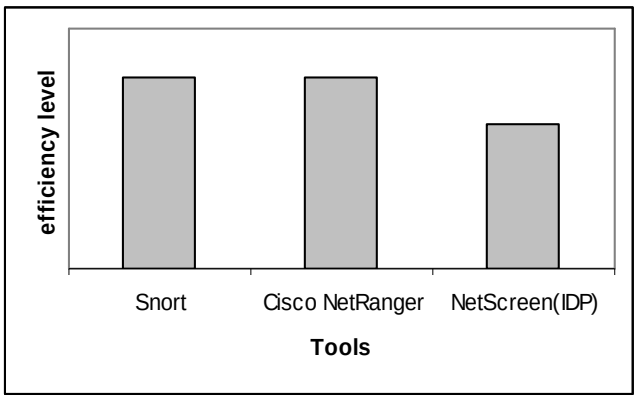

Figure 11 : L'efficacité des outils filaire expérimentés

4.4. CONCLUSION

Avec la multiplication des réseaux d'entreprise et l'importance croissant d'Internet au niveau consommateur, les entreprises cherchent à se rendre de plus en plus présentes et visibles sur Internet. Cette présence sur Internet, que ce soit à travers des sites Internet, de la vente en ligne ou même les courriels se fait souvent au détriment de la sécurité du ou des réseaux de l'entreprise et des données de l'entreprise. Comme nous l'avons vu, de nombreux systèmes permettent de renforcer la sécurité sur les réseaux d'entreprise. Que ce soit les firewalls, qui filtrent l'entrée des réseaux, les NIDS, qui contrôlent à travers leurs sondes, des points précis des réseaux, les HIDS, qui surveillent les intrusions directement au niveau des hôte, ou même les NIPS qui ont la capacité de réagir lors de la détection d'activités dangereuses, aucun système ne constitue le remède miracle au menace d'attaque informatique.

Du fait des limites inhérentes à chacun de ces systèmes ou des techniques connues de contournement de ces systèmes, nous avons vu que la meilleure protection était constituée d'une combinaison de tous ces systèmes.

De plus en plus de versions de ces systèmes de protection sont proposées commercialement par différentes sociétés ou organisations, sous forme propriétaire ou libre. Selon la taille des entreprises et les moyens de celles-ci, il existe des solutions propriétaires très faciles d'installation et de configuration mais malheureusement très coûteuses, il existe aussi des solutions libres et peu coûteuses mais malheureusement plus difficiles à installer et à

configurer. La définition des besoins est donc une étape préliminaire indispensable avant de mettre en place ces types de systèmes.

De plus, ces systèmes ne peuvent agir que dans le cadre d'un complément à une politique de sécurité globale à toute l'entreprise, et ne constitue qu'une petite partie de l'infrastructure de sécurité.

Afin d'améliorer les capacités de contrôle et de protections de ces systèmes, les recherches sont toujours en cours. Ces recherches cherchent à optimiser les systèmes actuels ou à trouver de nouvelles solutions de détection, de filtrage ou de réaction après alerte.

On voit, par exemple, de plus en plus apparaître des routeurs firewall ou des firewall intégrant des IDS ou des IPS, même au niveau du grand public. La démocratisation de ces types de systèmes permet, peu à peu, d'amener un début de sécurité, qui n'était pas souvent considéré comme important par les décideurs dans le passé. De manière générale, l'efficacité d'un système de détection d'intrusion dépend de sa "configurabilité" (possibilité de définir et d'ajouter de nouvelles spécifications d'attaque), de sa robustesse (résistance aux défaillances) et de la faible quantité de faux positifs (fausses alertes) et de faux négatifs (attaques non détectées) qu'il génère. Les paragraphes qui précèdent ont pour objectifs à la fois d'illustrer la complexité d'une détection d'intrusion et d'expliquer les limites des IDS actuels. Une lutte entre techniques d'intrusion et IDS s'est engagée, les IDS ayant pour conséquence une plus grande technicité des attaques sur IP, et les attaques actuelles imposant aux IDS d'être plus complets et plus puissants [10]. Les IDS/IPS apportent un plus indéniable aux réseaux dans lesquels ils sont placés. Cependant, leurs limites ne permettent pas de garantir une sécurité parfaite, impossible à obtenir. Il faut alors y tendre… Le futur de ces outils permettra de combler ces lacunes en évitant les "faux positifs" (pour les IDS) et en affinant les restrictions d'accès (pour les IPS) [7].

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.

Les IPS, qui tentent de pallier en partie à ces problèmes, ne sont pas encore suffisamment efficaces pour être utilisés dans un contexte de production. Ils sont actuellement surtout utilisés dans des environnements de tests afin d'évaluer leur fiabilité. Ils manquent également d'un principe de fonctionnement "normalisé", comme il en existe pour les IDS.

5. CONCEPTION D'UN BiIDS

5.1. INTRODUCTION

Les attaques informatiques ont été depuis leur apparition une vraie menace. Avec leur grande diversité et spécialité aux systèmes, ces dernières peuvent avoir des conséquences catastrophiques. Différentes contre-menaces permettant d'éviter ces attaques ou de diminuer de leur gravité existent mais aucune solution ne peut être considérée satisfaisante et complète. Les systèmes de détection d'intrusion sont l'une de ces contre-menaces les plus efficaces. Leur rôle est de reconnaitre des intrusions ou des tentatives d'intrusions par des comportements anormaux des utilisateurs ou par la reconnaissance d'attaque à partir du flux des données du réseau. Différentes méthodes et approche ont été adoptées pours la conception de systèmes de détection d'intrusions.

Un IDS est un outil qui vient s'ajouter à une panoplie d'utilisateurs utilisés pour avoir un certain niveau de sécurité. Nous présentons dans ce chapitre les différentes architectures des IDS. Nous aborderons également les mesures qui permettent de définir le degré d'efficacité d'un IDS et pour finir les travaux très récents de standardisation et d'homogénéisation des IDS. On fin notre proposition est un nouveau modèle des IDS qui s'appel BiIDS.

Un BiIDS, un IDS Basé sur les deux Principes de détection :

- ***Approche par scénario :*** Le système à base de signatures qui consiste à rechercher dans l'activité de l'élément surveillé les signatures (empreintes) d'attaques répertoriées et donc connues. Ce principe de détection d'intrusion est réactif et pose plusieurs contraintes, en effet il ne détecte que les attaques répertoriées dont il possède l'empreinte. De ce fait il nécessite des mises à jour fréquentes. Ce principe de détection implique aussi que les pirates peuvent contourner celui-ci en maquillant leurs attaques, il modifie en fait la signature connue par les IDS et de ce fait l'attaque devient invisible par l'IDS.
- ***Approche comportementale :*** Le système à approche comportementale consiste à détecter les différentes anomalies sur le réseau. C'est l'administrateur qui définira le fonctionnement "normal" des éléments surveillés, il y a donc une phase d'apprentissage pour fixer ce niveau. Par la suite l'IDS sera en mesure de signaler à l'administrateur toute situation qui divergera du niveau de fonctionnement de référence. Le fonctionnement de référence peut être élaboré par différentes analyses statistiques de l'élément à surveiller. Ce système de détection présente un avantage par

rapport au précèdent, il détecte les nouveaux types d'attaques. Cependant il faudra faire parfois des ajustements afin que le fonctionnement de référence corresponde au mieux à l'activité normale des utilisateurs et ainsi réduire les fausses alertes qui en découleraient.

5.2. ARCHITECTURE D'UN RESEAU AVEC IDS

La stratégie de contrôle permet de déterminer la manière de gérer plusieurs sondes du même IDS, ou la façon de gérer plusieurs IDS dans un réseau. Selon la disposition des différents composants de l'IDS, plusieurs architectures peuvent être adoptées :

5.2.1. ARCHITECTURE CENTRALISEE

Une certaine disposition permettra de contrôler tous les événements à partir d'une console centrale, analyser, et décider des mesures à entreprendre. Différents modèle d'IDS 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.

5.2.2. ARCHITECTURE PARTIELLEMENT DISTRIBUEE

Cette disposition permet de décharger le serveur de l'ensemble des tâches. Une hiérarchie est mise en place. Chaque sous réseau est géré par un point local. Les mesures sont prises par la console de niveau supérieur.

5.2.3. ARCHITECTURE TOTALEMENT DISTRIBUEE

Dans ce cas le réseau est décomposé en plusieurs sous réseau, chacun d'entre eux est géré par son propre IDS. Les tâches d'audits et d'analyses sont prises au niveau local.

5.3. EVALUATION D'UN IDS

Des mesures permettent de comparer et de mesurer l'efficacité des IDS. Les IDS sont des éléments très importants dans une stratégie de sécurité ; pour cela le choix de l'IDS est très décisif et doit être basé sur les caractéristiques de ce dernier.
Les mesures permettant de mieux choisir son IDS. Dons [28][29][36][37] nous pouvons évaluer les IDS selon plusieurs critères par exemple :

- Le taux de faux positif et de faux négatif ;
- Réponse de l'IDS dans un environnement surchargé ;
- La possibilité mettre à jour la base des signatures ou de modifier certaines signatures ;
- …..

5.4. STANDARDISATION ET NORMALISATION

Le groupe IDWG a participé à la standardisation des IDS en définissant la norme IDMEF (Intrusion Detection Message Exchange Format) pour le format des messages échangés entre IDS et le protocole IDXP (intrusion detection eXchange Protocol) qui définie les procédures de transport entre IDS.
Un comité du DARPA [25] a défini quatre briques pour décrire l'architecture d'un IDS, et c'est ce modèle Figure 2 qui a été adopté par la suite pour l'ensemble des IDS :

- Générateur d'événements : envoie des événements ;
- Analyseur d'événements : analyse les événements reçus et produit des alertes ;
- Base de données événementielles : pour stoker tous types d'informations relatifs aux événements, alertes ;
- Système de réponse : réponse en temps réel face aux attaques.

La sonde (analyseur) envoie une alerte vers un collecteur, ce modèle permet d'avoir une communication hétérogène hormis l'environnement sur le quel se passent les communications.
Plusieurs IDS sont composés d'un seul bloc qui se charge de toute l'analyse. Cette approche monolithique imposée a énormément de contraintes telles que [25]

- La consommation de ressources système ;
- Difficulté de mise à jour ;
- Le point central est lui-même le point faible si une attaque est lancée contre l'IDS ;

- Nécessité de plusieurs de données d'audit.

Pour palier à ces faiblesses, de nouvelles tendances pour la conception d'IDS existent. Les tendances actuelles vont vers la détection d'intrusion distribuées.
Le premier projet ayant utilisé cette approche de récolte d'informations d'audit a été le projet NADIR qui faisait l'analyse par un système expert [26].
Un modèle standard pour les IDS, qui a été mis en place par le comité DARPA. Ce modèle est adopté dans le développement de la majorité des nouveaux IDS de nos jours. Ce modèle est composé de quatre briques qui sont : la source d'information, le senseur, l'analyseur et le manager. Pour une détection d'intrusion efficace, il est important de rappeler les caractéristiques que doit satisfaire tout IDS, à savoir [28] [29] : la distributivité, l'autonomie, la communication et la coopération, la réactivité et l'adaptabilité.

5.5. MODELE D'UN BiIDS

L'étude des systèmes de détection d'intrusion nous a permis de réaliser l'importance du rôle que jouent. Ces derniers au sein d'une stratégie de sécurité. Différents types d'IDS (HIDS, NIDS), chacun caractérisé par une certaine architecture et une méthode d'analyse.
Les caractéristiques des IDS doivent répondre à certaines exigences, le choix de l'adoption d'un certain type par rapport à un autre doit être fondé essentiellement sur les besoins en matière de sécurité et les contraintes logicielles et matérielles. Nous pouvons déterminer le type d'IDS selon [36]:

- L'emplacement de l'IDS (NIDS, HIDS) ;
- La fréquence d'utilisation (continue ou périodique) ;
- La méthode de détection (comportementale ou par scénario) ;
- La réponse de l'IDS (passive ou active).

Dans ce chapitre nous nous proposons une nouvelle architecture pour la détection d'intrusion en rassemblant les deux approches: la détection d'intrusions avec approche comportementale et la détection d'intrusion avec approche par scénario.
Le choix par cette approche est essentiellement fondé sur le fait que l'IDS est composé de différents modules qui doivent être distribués sur un ensemble de station du réseau pour effectuer des tâches différentes. Les différents composants de l'IDS doivent être en permanente interaction.

Notre modèle est composé d'un IDS primaire qui a pour rôle d'organiser les différentes tâches et gérer les différents IDS seconds, qui eux auront pour tâche la capture d'événements et la transmission des conclusions.

Les HIDS doivent se baser sur des profils utilisateurs décrivant leurs comportements normaux. Cette solution est très intéressante dans la mesure où la seule source d'information nécessaire est le comportement des utilisateurs au sein d'un réseau. Cette source d'information peut être maintenue à jour seulement avec des phases d'apprentissage. Cependant, le point négatif de cette solution est le taux de faux positifs dû aux comportements anormaux ou inhabituels des utilisateurs, qui ne sont pas forcement nocifs.

Les NIDS avec approche par scénario utilisent essentiellement une base de données de signatures d'attaques connues. Cette source d'information nous permet de diminuer significativement le taux de faux positif. Cependant, le point faible de cette solution est la source d'information qui doit être régulièrement mise à jour. Une attaque non répertoriée n'a aucune chance d'être détectée par le NIDS.

A fin de tirer profit des deux approches (comportementale et par scénario) et qui nous semblent complémentaires, notre choix s'est porté sur la conception d'un IDS hybride.

5.5.1. DESCRIPTION DE LA SOLUTION

Le noyau de notre BiIDS génère des variantes des signatures d'attaques et des profils des utilisateurs de manière pseudo-aléatoire. Cette méthodologie nous permet de perfectionner l'analyseur afin de découvrir éventuellement de nouvelles attaques ou des variantes d'attaques.

5.5.2. ARCHITECTURE GLOBALE DE BiIDS

Notre IDS est composé de (figure 12):

- ***a.*** ***NIDS*** génére des détections sur la base des signatures. Ces détecteurs seront utilisés pour analyser le trafic réseau.
- ***b.*** ***HIDS*** sur la base de profils des comportements normaux des utilisateurs. Génére des détecteurs capables de reconnaitre des comportements inhabituels des utilisateurs.
- ***c.*** ***Administrateur*** peut configurer les différents paramètres de l'IDS, visualiser les différentes alertes, lancer la commande d'apprentissage….

Les composants de notre solution doivent être déployés de la sortie : le NIDS sera installé sur la machine qui est le proxy du réseau pour pouvoir analyser des paquets du réseau.
Tandis que le HIDS sera déployé sur l'ensemble des machines qui constituent le réseau local.

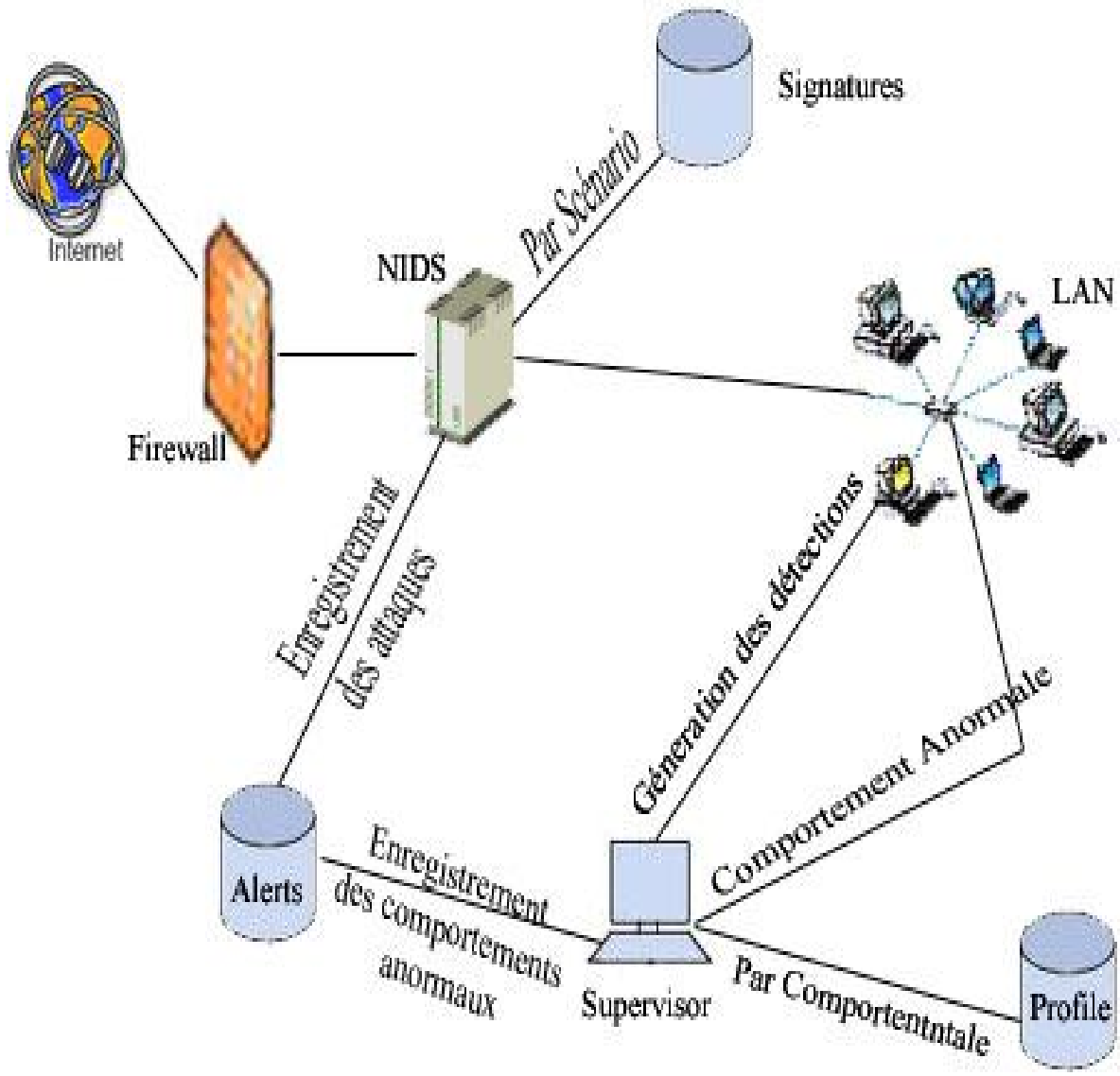

Figure 12 : Schéma globale de la solution

L'utilisation des bases de données est très importante dans notre modèle, nous avons opté pour l'utilisation de trois bases de données :

a. ***Base de données profils*** contient l'ensemble des informations relatives aux profils utilisateurs. Les données contenues dans cette base sont générées par le HIDS durant la phase d'apprentissage.

b. ***Base de données signatures*** est la base du NIDS. Elle regroupe l'ensemble des attaques connues en utilisant un certain format.

   Il n'existe aucun modèle standard pour la codification des signatures.

   Les attributs à utiliser pour représenter une attaque doivent être basés sur les informations contenues dans les paquets [27].

c. ***Base de données alertes*** permet de répertorier l'ensemble des alertes générées par les détecteurs des deux composants de l'IDS (HIDS et NIDS). Cette base de données sera consultée par l'administrateur afin de relever les traces d'attaques ou de comportements anormaux.

5.5.3. LES HIDS DE CETTE ARCHITECTURE

La première étape du déploiement du HIDS, est sans doute l'étape d'apprentissage durant laquelle on sauvegarde les traces des comportements normaux des utilisateurs en créant un profil pour chacun.

Notre HIDS sera constitué d'un HIDS superviseur et d'un ensemble de HIDS esclaves qui seront déployés sur l'ensemble des machines constituants le réseau.

a. ***HIDS superviseur*** a pour rôle de :
   - Extraire les profils des utilisateurs de base de données ;
   - Générer les détecteurs et les envoyer au HIDS esclaves ;
   - Analyser les rapports des HIDS esclaves et répertorier les alertes dans une base de données ;
   - Envoyer des commandes permettant de lancer les phases d'apprentissage, analyser, lancer et arrêter des HIDS esclaves.

b. ***HIDS esclave a*** pour rôle de :
   - Générer le profil des utilisateurs durant la phase d'apprentissage ;
   - Utiliser des capteurs d'événement pour extraire le comportement actuel de l'utilisateur.

5.5.4. NIDS DE CETTE ARCHITECTURE

En utilisant l'analyse avec approche par scénario, la fonction d'analyse de notre NIDS contient deux processus de génération de détecteurs et leur mise en place pour l'analyse du flux de paquets. Les étapes de son exécution :

- Capture des paquets ;
- Extraction et formatage des attributs ;
  - Structurer les données ;
  - Résumer les données ;
  - Fournir des attributs.
- Analyse des attributs ;
- Envoi des rapports.

5.6. CONCLUSION

Le choix de l'implémentation d'un IDS est très important, surtout si on prend en considération que l'IDS sera déployé sur un réseau contenant plusieurs machines avec différentes configurations matérielle et logicielle. Cela fait que l'IDS sont conçus de manière hiérarchique et sont distribués sur plusieurs machines nécessitant l'analyse de données en provenance de différentes sources.

6. CONCLUSION ET PERSPECTIVES

D’une manière générale, l'efficacité d'un système de détection d'intrusion dépend de sa “configurabilité” (possibilité de définir et d’ajouter de nouvelles spécifications d'attaque), de sa robustesse (résistance aux défaillances) et de la faible quantité de faux positifs (fausses alertes) et de faux négatifs (attaques non détectées) qu'il génère. Une lutte entre techniques d’intrusion et IDS s’est engagée, les IDS ayant pour conséquence une plus grande technicité des attaques sur IP, et les attaques actuelles imposant aux IDS d’être plus complets et plus puissants. Les IDS sont actuellement des produits mûrs et aboutis. Ils continuent d'évoluer pour répondre aux exigences technologiques du moment mais offrent d'ores et déjà un éventail de fonctionnalités capable de satisfaire les besoins de tous les types d'utilisateurs. Néanmoins, comme tous les outils techniques, ils ont des limites que seule une analyse humaine peut compenser. A la manière des pare-feu, les détecteurs d'intrusion s’améliorent chaque jour grâce à l'expérience acquise, mais ils deviennent aussi de plus en plus sensibles aux erreurs de configuration et de paramétrage. Par conséquent, il est plus que fondamental de former correctement les personnes chargées de la mise en œuvre et de l'exploitation des IDS. Malheureusement, il semble que subsiste là une grande partie de la difficulté. A ce jour, aucun outil ne permet de remplacer l'être humain dans un test d'intrusion.

Enfin, une attention particulière doit être accordée aux discours commerciaux. En effet, si la détection d’abus fonctionne aujourd’hui plus ou moins correctement (par exemple, Snort), la détection d’anomalie en revanche n’est pas encore fiable (autrement dit, elle ne fonctionne pas).

Si les IDS au niveau réseau ont déjà été énormément étudiés, depuis peu ils le sont aussi au niveau service ; les articles produits sur les IDS réseau sont assez directement applicables au niveau service. Un seul et unique modèle de détection d’anomalie au niveau service est fiable à ce jour.

Cette thèse a présenté trois approches pour améliorer le processus d'évaluation des IDS et des IPS.

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.

Les IPS, qui tentent de pallier en partie à ces problèmes, ne sont pas encore suffisamment efficaces pour être utilisés dans un contexte de production. Ils sont actuellement surtout utilisés dans des environnements de tests afin d’évaluer leur fiabilité. Ils manquent également d’un principe de fonctionnement "normalisé", comme il en existe pour les IDS.

Néanmoins, ces technologies sont amenées à se développer dans les prochaines années, du fait des besoins de sécurité croissants des entreprises et de l'évolution des technologies qui permet un fonctionnement plus efficace des systèmes de détection et de prévention d'intrusion.

En guise de conclusion, les IDS/IPS apportent un plus indéniable aux réseaux dans lesquels ils sont placés. Cependant, leurs limites ne permettent pas de garantir une sécurité à 100%, impossible à obtenir. Il faut alors y tendre et le futur de ces outils permettra de combler ces lacunes en évitant les "faux positifs" (pour les IDS) et en affinant les restrictions d'accès (pour les IPS).
Il serait intéressant de mener des évaluations des IDS et des IPS existants en suivant les approches que nous avons proposées et les outils développés au cours de ce travail.

REFERENCES

[1] Abhinav Srivastava, Shamik Sural, and Arun K. Majumdar. Weighted intratransactional rule mining for database intrusion detection. In PAKDD, pages 611_620, 2006.

[2] B. Mukherjee, L.T. Heberlein, and K.N. Levitt. Netword intrusion detection. IEEE Network, 8(3) :26_41, 1994.

[3] J. S. Balasubramaniyan, J. O. Garcia-Fernandez, D. Isaco_, Eugene H. Spa_ord, and Diego Zamboni. An architecture for intrusion detection using autonomous agents. In ACSAC, pages 13_24, 1998.

[4] Karen Scarfone and Peter Mell. Guide to intrusion detection and prevention systems (idps). Technical Report SP800-94, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, U.S. Department of Commerce, February 2007.

[5] Crying wolf: False alarms hide attacks Newman, Snyder & Thayer Network World, 24/06/02 http://www.nwfusion.com/techinsider/2002/0624security1.html

[6] ISS Internet Risk Impact Summary – Juin 2002.

[7] F. Cikala, R. Lataix, S. Marmeche, « Les IDS/IPS. Intrusion Detection/Prevention Systems », Présentation, 2005.

[8] K. Müller, « IDS - Systèmes de Détection d'Intrusion, Partie II », July 2003, http://www.linuxfocus.org/Francais/July2003/article294.shtml.

[9] Janne Anttila, « Intrusion Detection in Critical Ebusiness Environment », Présentation, 2004.

[10] Herve Schauer Consultants, « La détection d'intrusion… », Présentation : extrait du cours sécurité TCP/IP du Cabinet HSC, Mars 2000.

[11] Marcus A. Maloof (2005), « Machine Learning and Data Mining for Computer Security »,Springer London Ltd, ISBN-10 184628029X ; ISBN-13 978-1846280290.

[12] Herve Schauer Consultants, « La détection d'intrusion… », Présentation : extrait du cours sécurité TCP/IP du Cabinet HSC, Mars 2000.

[13] Hervé Debar and Jouni Viinikka, « Intrusion Detection: Introduction to Intrusion Detection and Security Information Management», Foundations of Security Analysis and Design III, Lecture Notes in Computer Science, Volume 3655, 2005. pp. 207-236.

[14] Hervé Debar, Marc Dacier and Andreas Wespi, «A Revised Taxonomy for Intrusion Detection Systems», Annales des Telecommunications, Vol. 55, Number: 7-8, pp. 361-378, 2000.

[15] Mohammed Gadelrab and A. Abou El Kalam, «Testing Intrusion Detection Systems: An Engineered Approach», Proceeding of IASTED International Conference on Software Engineering and Applications (SEA 2006), USA, 2006.

[16] Mohammed S. Gadelrab, Anas Abou El Kalam and Yves Deswarte, «Defining categories to select representative attack test-cases", Proceedings of the 2007 ACM workshop on Quality of protection (QoP '07), Alexandria, Virginia, USA, pp. 40-42, 2007.

[17] Mohammed Gadelrab, Anas Abou El Kalam et Yves Deswarte, «Modélisation des processus d'attaques pour l'évaluation des IDS», Act de la 3ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information, Loctudy, France, 2008.

[18] S. Fluhrer, I. Mantin,, A. Shamir. " Weaknesses in the Key Scheduling Algorithm of RC4 ". Selected Areas in Cryptography -SAC 2001, 2259 Lecture Notes in Computer Science, 1-24. Springer-Verlag, 2001.

[19] C. Gehrmann, M. Naslund. "ECRYPT Yearly Report on Algorithms and Keysizes". www.ecrypt.eu.org/documents/D.SPA.10-1.1.pdf, 2005.

[20] I. Mantin, A. Shamir. "A practical attack on broadcast RC4". Fast Software Encryption - FSE 2001, 2335 Lecture Notes in Computer Science, 152-164. Springer-Verlag, 2001.

[21] L. Butti. Détection d'Intrusion dans les Réseaux 802.11. In Symposium sur la Sécurité des Technologies de l'Information et des Communications 2006, pages 411-433. École Supérieure et d'Application des Transmissions,

[22] F. Guo and T.-C. Chiueh. Sequence number-based l'l'lAC address spoof detection. In Proceedings of the 8th International Symposium on Recent Advances in Intrusion Detection (RAID '05), pages 309-329, Seattle, WA, USA, September 2005.

[23] J.Wright. Deteeting Wireless LAN MAC Address Spoofing, January 2003. http://forskningsnett.uninett.no/wlan/download/wlan-mac-spoof.pdf.Consulté en novembre 2007.

[24] KoreK, \chopchop (Experimental WEP attacks), 2004, available at http://www. netstumbler.org/showthread.php?t=12489

[25] MIT Lincoln Laboratory, DARPA Intrusion Detection Evaluation Data Sets, www.ll.mit.edu/IST

[26] K. Boudaoud, "Un systeme multi_agents pour la détection d'intrution » Institution EURECOM Sophia-Antipolis.

[27] J. Hochberyn K. Jackson, C Stallings, J.F Mclary, D. Dubois, J. Ford, NADIR "An automated system for detection network intrusion and misuse" , Cpmputers and Security.

[28] Y. Farhaoui, A. Asimi, "Performance method of assessment of the intrusion detection and prevention systems," *IJEST , Vol. 3 No. 7 July 2011*

[29] Y. Farhaoui, A. Asimi, "Performance Assessment of tools of the intrusion Detection and Prevention Systems," IJCSIS , Vol. 10 No. 1 January 2012

[30] Y. Farhaoui, A. Asimi, "Model of an effective Intrusion Detection System on the LAN," IJCA , Vol. 41 No. 11 March 2012

[31] Conférence Méditerranéenne sur l'ingénierie sûre des systèmes complexes (MISC11), Mai 2011 Agadir, Maroc « Evaluation des Performances et d'efficacité des Systèmes de Détection et de Prévention d'Intrusion basée sur le Réseau de Neurone artificiel »

[32] Congrès International Informatique et Sciences de l'Ingénieur (ISI 2011), Juin 2011 Meknès, Maroc « Evaluation de Performance des Systèmes de Détection et de Prévention d'Intrusion (*Selon leurs caractéristiques: la méthode d'analyse, la fiabilité, la réactivité, l'installation, l'adaptabilité et la performance)* »

[33] Congrès International Informatique et Sciences de l'Ingénieur (ISI 2011), Juin 2011 Meknès, Maroc « Attaques Wi-Fi WPA (TKIP) »

[34] Congrès International Informatique et Sciences de l'Ingénieur (ISI 2011), Juin 2011 Errachidia, Maroc « Evaluation de Performance des Systèmes de Détection et de Prévention d'Intrusion (*Selon les objectifs de sécurité: l'intégrité, la confidentialité, la disponibilité et l'authentification) »*

[35] 3ème édition des Journées Doctorales en Technologies de l'Information et de la Communication (JDTIC 2011), juillet 2011 Tanger, Maroc "Performance Assessment of the intrusion Detection and Prevention Systems *(According to their features: the method of analysis, reliability, reactivity, facility, adaptability and performance)"*

[36] Y. Farhaoui, A. Asimi, «Performance Assessment of the intrusion Detection and Prevention Systems: According to their features: the method of analysis, reliability, reactivity, facility, adaptability and performance», The 6th IEEE international conference Sciences of Electronics Technologies Information and Telecommunication (SETIT 2012), Sousse, Tunisia, 2012.

[37] Y. Farhaoui, A. Asimi, « Performance Assessment of Tools of the intrusion Detection/Prevention Systems », The 3rd IEEE International Conference on Multimedia Computing and Systems (ICMCS'12), Tangier, Morocco, 2012.

[38] Y. Farhaoui, A. Asimi, « Model of an effective Intrusion Detection System on the LAN », International Symposium on Security and Safety of Complex Systems (2SCS'12), Agadir, Morocco, 2012.

[39] Scott Fluhrer, Itsik Mantin, and Adi Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4"

LISTE DES PUBLICATIONS

PUBLICATION

1. Y. Farhaoui, A. Asimi, "Performance method of assessment of the intrusion detection and prevention systems," *IJEST , Vol. 3 No. 7 July 2011*
2. Y. Farhaoui, A. Asimi, "Performance Assessment of tools of the intrusion Detection and Prevention Systems," IJCSIS , Vol. 10 No. 1 January 2012
3. Y. Farhaoui, A. Asimi, "Model of an effective Intrusion Detection System on the LAN," IJCA , Vol. 41 No. 11 March 2012

COMMUNICATION

1. Y. Farhaoui, A. Asimi, Conférence Méditerranéenne sur l'ingénierie sûre des systèmes complexes (MISC11), Mai 2011 Agadir, Maroc « Evaluation des Performances et d'efficacité des Systèmes de Détection et de Prévention d'Intrusion basée sur le Réseau de Neurone artificiel »
2. Y. Farhaoui, A. Asimi, Congrès International Informatique et Sciences de l'Ingénieur (ISI 2011), Juin 2011 Meknès, Maroc « Evaluation de Performance des Systèmes de Détection et de Prévention d'Intrusion (*Selon leurs caractéristiques: la méthode d'analyse, la fiabilité, la réactivité, l'installation, l'adaptabilité et la performance)* »
3. Y. Farhaoui, A. Asimi, Congrès International Informatique et Sciences de l'Ingénieur (ISI 2011), Juin 2011 Meknès, Maroc « Attaques Wi-Fi WPA (TKIP) »
4. Y. Farhaoui, A. Asimi, Congrès International Informatique et Sciences de l'Ingénieur (ISI 2011), Juin 2011 Errachidia, Maroc « Evaluation de Performance des Systèmes de Détection et de Prévention d'Intrusion (*Selon les objectifs de sécurité: l'intégrité, la confidentialité, la disponibilité et l'authentification) »*
5. Y. Farhaoui, A. Asimi, 3ème édition des Journées Doctorales en Technologies de l'Information et de la Communication (JDTIC 2011), juillet 2011 Tanger, Maroc "Performance Assessment of the intrusion Detection and Prevention Systems *(According to their features: the method of analysis, reliability, reactivity, facility, adaptability and performance)"*

6. Y. Farhaoui, A. Asimi, «Performance Assessment of the intrusion Detection and Prevention Systems: According to their features: the method of analysis, reliability, reactivity, facility, adaptability and performance», The 6th IEEE international conference Sciences of Electronics Technologies Information and Telecommunication (SETIT 2012), Sousse, Tunisia, 2012.
7. Y. Farhaoui, A. Asimi, « Performance Assessment of Tools of the intrusion Detection/Prevention Systems », The 3rd IEEE International Conference on Multimedia Computing and Systems (ICMCS'12), Tangier, Morocco, 2012.
8. Y. Farhaoui, A. Asimi, « Model of an effective Intrusion Detection System on the LAN », International Symposium on Security and Safety of Complex Systems (2SCS'12), Agadir, Morocco, 2012.