**Institut de la Francophonie pour l'Informatique**




**Rapport de stage de fin d'études**

Sujet :

# LE SYSTÈME DE DÉTECTION DES INTRUSIONS

# ET LE SYSTÈME D'EMPÊCHEMENT DES INTRUSIONS (ZERO DAY)

**Rapporteur** : M. Tran Van Tay

**Responsable** : M. DOMINGUEZ Hugo

Montréal, Février 2005

**TABLE DES MANTIÈRES**

Remerciements....4
Résumé....5
Abstract....6
Chapitre 1: Introduction....7
I. Contexte du travail....7
II. Abréviation....8
III. Problématique....9
Chapitre 2: Résultats antérieurs....10
Chapitre 3: Système de détection des intrusions....11
I. Définition....11
II. Pourquoi a-t-on besoin de l'IDS?....11
III. Types majeurs de l'IDS....12
IV. Source des informations....13
1. Network-Based IDSs (NIDS)....13
2. Host Based IDS....14
V. SNORT....16
1. Qu'est ce que SNORT?....16
2. Installation....18
3. Les outils du SNORT rapportant....20
4. Évaluations....25

Chapitre 4: Système d'empêchement des intrusions ..... 27
I. Définition ..... 27
1. Qu'est ce que le IPS ? ..... 27
2. Qu'est ce que le Zero day exploits ..... 27
3. Qu'est ce que Zero-day Protection? ..... 28
II. Outils d'empêchement de zero day ..... 32
1. Zone Labs Integrity ..... 32
2. Symantec – Symantec Client Security ..... 34
3. McAfee System Protection – McAfee Entercept ..... 36
4. CISCO – CISCO Security Agent (CSA) ..... 41
5. ISS – Real Secure Desktop ..... 43
III. Évaluations ..... 47
Chapitre 5: Conclusions ..... 48
Chapitre 6: Références ..... 49

# Remerciements

Je tiens à remercier d'abord Monsieur Dominguez Hugo, le directeur de la sécurité informatique pour SITel (Service de l'Informatique et des Télécommunications de l'Université du Québec à Montréal), qui m'a aidé et m'a donné des conseils et des conditions favorisées  pour finir mon sujet de stage au Canada.

Ensuite, Je tiens à remercier Monsieur Lord Bouchard, ex-directeur de l'IFI, qui m'a trouvé ce sujet de stage.

Je voudrais remercier aussi à tous les professeurs de l'IFI qui m'ont donné une bonne préparation pour finir mes études à l'IFI.

Je remercie également Tuyet et Binh, stagiaires de la promotion 8 à Montréal, qui m'ont donné la motivation pour que je puisse passer six mois au Canada.

Enfin, Je remercie sincèrement tous mes amis qui m'ont donné le temps parfait et les voyages inoubliables au Canada.

# Résumé

Le problème de sécurité est le plus important dans tous les domaines en généraux et dans l'informatique en particulier. C'est la condition indispensable pour l'existe des organisations ou des sociétés, notamment des banques parce que les pirates cherchent toujours des vulnérabilités dans leurs systèmes pour attaquer et voler des informations ou faire des catastrophes aux données. Donc nous devons avoir des bons politiques pour protéger contre des attaques.

Ce sujet est relevé dans le cadre de service de l'Informatique et des télécommunications de l'UQAM. Mon travail a pour but d'obtenir des connaissances concernant au système de détection des intrusions et au système d'empêchement des intrusions. Je dois également chercher  des outils efficaces pour ces deux problèmes.

Ce rapport se divise en deux parties principales :

- Le système de détection des intrusions (IDS) : Il vous réponds les questions suivantes :
    - Pourquoi avez-vous besoin l'IDS ?
    - Comment peut on installer un système de détection des intrusions ?
    - Étude de cas avec le logiciel libre « SNORT » ?
- Le 0-jour et le système d'empêchement des intrusions (IPS) : Il vous montre la réponse des questions ci-dessous :
    - Qu'est ce que le système d'empêchement des intrusions et le 0-jour ?
    - Quel logiciel existé en réel peut empêcher des intrusions et la comparaison entre eux ?

## Abstract

The problem of security is the most important thing in all fields, especially in Information Technology. It is the vital condition for existence of organizations and companies, chiefly bank, because the hackers always seek vulnerabilities in their systems to attack and steal the important information, for example theft of the passwords. Thus, we must have good policies to protect our systems from intrusion.

This subject must have been happened in the framework of the SITel. The purpose of my work is to gain knowledge concerning with the intrusion detection systems and the intrusion prevention systems. I must also seek effective tools for these two problems.

This report/ratio is divided into two principal parts:

- The intrusion detection systems (IDS): It answers you the following questions:
  - Why do you need IDS?
  - How can one install an intrusion detection system?
  - Apply the free software "SNORT" for experiment?
- The Zero-day and the intrusion prevention systems (IPS): It shows you the key answers of the questions below:
  - What are the intrusion prevention systems and the zero-day?
  - Which software existing in reality can prevent intrusions and the comparison among them?

# Chapitre 1: Introduction

## I. Contexte du travail

Le SITel est le nom raccourci des services de l'informatique et des télécommunications de l'UQAM. Il est sert à fournir :

- Des matériels téléphoniques et des services de messagerie pour l'UQAM
- Des matériels informatiques et
- La boite aux lettres des étudiant dans le campus de l'UQAM.
- L'intranet à l'UQAM
- L'Internet à domicile.
- Des informations de la sécurité informatique dans le monde

En fait, le SITel domine une grande équipe des employeurs et l'infrastructure informatique très stable. Cet équipe se réparti en plusieurs domaine comme la base des donnés, le système d'exploitation, le système de la sécurité, les boites aux lettres, le service de matériel informatique…

Dans le cadre de mon stage, le sujet de la sécurité informatique est réalisé sous la direction de M. Dominguez Hugo- Le directeur de la sécurité informatique du SITel (Service des Informatiques et des Télécommunications de l'UQAM). Le but de mon sujet est la recherche des nouvelles techniques et des logiciels concernant aux intrusions sur le réseau Internet.

## II. Abréviation

SNORT: The Open Source Network Intrusion Detection System.

NAT: Network Address Translation

DMZ: Demilitarized Zone

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

IRC: Internet Relay Chat

NSA: National Security Agency

SANS: Computer & Information Security Training (http://www.sans.org/ )

ISS: Internet Security System

RSDP: Real Secure Desktop Protector

NAC: Network Admission Control

EAP: Extensible Authentication Protocol

VPN: Virtual Private Network

SIM: Security Information Management

CSA: CISCO Security Agent

Dos: Denial of Service

## III. Problématique

La détection des intrusions permet des organisations de protéger leur système contre des menaces qui viennent par le croisant du réseau connectivité et la confiance sur le système informatique. En donnant le niveau et la nature de réseau moderne de sécurité des menaces, la question de sécurité professionnelle s'ils ont besoin d'utiliser la détection des intrusions ? Mais quelle caractéristiques et capacités de détection des intrusions doivent être utilisés?

L'IDS sont gagnés l'acceptation comme un nécessité supplémentaire pour l'infrastructure de la sécurité de chaque organisation. En dépit des contributions documentées des technologies de détection des intrusions effectue au système de la sécurité, beaucoup d'organisations doivent justifier l'acquisition de IDS.

Il y a toujours des risques lorsque votre ordinateur connecte au réseau internet. Ces risques peuvent causer des dommages dans votre système, Par exemple vos donnés sont perdus ou volées… Les hackers malicieuses abusent toujours des vulnérabilités des services, des applications ou de réseau pour attaquer à votre ordinateur. C'est pour quoi que nous avons besoin des bons stratégie de contrôle des packages circulés sur le réseau.

Pour réaliser cette idée, il est obligatoire de comprendre quelle est l'intrusion? Comment fonctionne il sur le réseau? À partir de cela, vous pouvez choisir telle solution pour votre système.

Dans le cadre de mon stage à l'UQAM au sujet de la sécurité informatique,  le problème posé ici est autour de système des de la sécurité informatique. Ce problème est assez vaste. Donc Il n'est pas difficile à définir et comprendre les concepts autour de lui mais pour le mettre en pratique La question posée ici est autour du sujet de sécurité informatique.

# Chapitre 2: Résultats antérieurs

À cause des faits malveillant, le réseau informatique ne peut pas être existé et se développer jusqu'à aujourd'hui s'il n'y a pas des organisations de sécurité informatique comme NAS, ISS, SAN… Grâce aux experts de la sécurité informatique, notre ordinateur ou notre système a moins de risque lorsqu'il se circule sur le réseau Internet et est diminué des menaces. Ils ont trouvé beaucoup de méthodes et d'outils très efficaces  pour détecter  contre des hackers, des faits malveillants.

De nos jours, les informaticiens sont hérités des bonnes connaissances antérieures dans ce domaine. De plus, Les informations de la sécurité informatique sont partout sur l'Internet. Donc, L'apprentissage des techniques d'analyse des intrusions et la mise en pratique de ces techniques dans le  notre vive sont des missions que je dois suivre. Mon travail est l'approche aux concepts et des logiciels implémenté sur le host ou sur un poste de travail pour détecter et empêcher des intrusions qui a tentative d'attaque à un système d'ordinateur ou de réseau.

# Chapitre 3: Système de détection des intrusions

## I. Définition

Détection des intrusions est le processus de surveillance des événements se trouvant dans un système des ordinateurs ou du réseau et les analysant pour détecter les signes des intrusions, défini comme des tentatives pour compromettre la confidentialité, intégrité, disponibilité ou éviter des mécanismes de sécurité de l'ordinateur ou du réseau. L'intrusion est causée par les attaques accédant au système via l'Internet, autorisée l'utilisateur du système qui essayer à gagner les privilèges supplémentaires pour lesquels ils n'ont pas autorisés, et autorisé les utilisateurs qui abusent les privilèges donnés. Le système de détection des intrusions est un logiciel ou un matériel qui automatise des surveillances et les processus analysés.

## II. Pourquoi a-t-on besoin de l'IDS?

Pourquoi vous avez besoin d'installer un système IDS dans votre système de réseau? Pour surveiller la circulation des paquets sur le réseau. Vous pouvez considérez le IDS comme un caméra installé devant votre port. Ça pour savoir qui essaye à attaquer à votre réseau.

Quand une tentative est réussie en passant votre par feu, il va peut être provoquer des menaces. Alors, vous pouvez diminuer des fautes positives en connaissant ces tentatives. Dans l'environnement de NAT est aussi un profit parce qu'il nous permet de tenir l'adresse réelle du source par mettre en corrélation avec des événements entre le système IDS qui situe avant de après le par feu.

Cette topologie vous permettra de vérifier que votre ligne de base du par feu est suivi, ou que quelqu'un a fait une erreur en changeant une règle de par feu. Si vous savez que votre ligne de base du par feu proscrivent l'utilisation de ftp et votre système IDS montre des alertes de ftp, alors vous savez que le par feu ne bloque

pas de trafic de ftp.  C'est juste un effet secondaire et ne devrait pas être la seule manière que vous vérifiez la conformité à votre ligne de base.

## III. Types majeurs de l'IDS

Nous avons plusieurs types de l'IDS disponibles de nos jours qui sont caractérisés par des surveillances différentes et des approches d'analyse. Chaque approche a toujours des avantages et des inconvénients. De plus, tous approches peuvent être décrits dans un terme du model de processus généraux pour IDS.

Plusieurs IDS peuvent être décrits dans un terme de trois composants des fonctions fondamental :

Sources des informations : des sources différentes des informations d'événements sont habitués à déterminer si une intrusion est occupée ou non ? Ces sources peuvent être retiré à partir des niveaux différents du système, avec le réseau,  centre du serveur, et les applications surveillant la plus commune.

Analyse : la partie du système de détection des intrusions qui organise réellement  et faire des événements sensibles  dérivés des sources des informations, décidant lors que ces événements indique que l'intrusion se produit  ou a déjà eu occupé.  Des approches d'analyse, les plus communes sont mauvaise et anormale détection.

Réponse : L'ensemble des actions que le système prend détecte des intrusions.  Celles sont typiquement groupées en des mesures actives et passives, avec des mesures actives entraînant quelques interventions automatisées sur une partie du système, et des mesures passives entraînant des rapports l'IDS trouvant de humain, qui est puis attendu pour prendre des actions basées sur ces rapports.

# IV. Source des informations

## 1. Network-Based IDSs (NIDS)

**Advantages**

- Le NIDS peut surveiller un grand réseau.
- L'déploiement de NIDS a peu d'impact sur un réseau existant. L'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 se cache à beaucoup d'attaquants

**Inconvénients**

- 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 le IDS dur le matériel pour qu'il marche plus rapidement.
- Plusieurs des avantages de NIDS ne peut pas être appliqué 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 peut pas analyse des informations chiffrées (cryptées). Ce problème a lieu dans les organisations utilisant le VPN.
- La plupart de NIDS ne peuvent pas indiquer si un attaque réussi ou non. Il reconnaît seulement que un attaque est initialisé. 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.

## 2. Host Based IDS

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 détaillé et plus protégé que les journaux du système. Pourtant les journaux est moins obtus et plus petit que la traîné de l'audit du SE, c'est ainsi qu'il est facile à comprendre.

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

**Advantages**

- Pouvoir surveiller des événements local 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.
- Lors que HIDS marche sur la traîné de l'audit de SE, ils peuvent détecter le Cheval de Troie ou les autres attaques concernant à la brèche intégrité de logiciel.

**Inconvénients**

- HIDS est difficile à gérer, et des informations doivent configurées et gérées pour chaque host surveillé.
- Puisque au moins des sources de l'information pour HIDS se réside sur l'host de la destination par les attaques, le 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 autre tel que la surveillance qui s'adresse au réseau entier parce que le HIDS ne voit que les paquets du réseau reçus par ses hosts.
- 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 est immense, alors il demande le stockage supplémentaire local dans le système.

# V. SNORT

## 1. Qu’est ce que SNORT?

SNORT est un open source du système de détection des intrusions de réseau. Il a capable d’analyser le trafic sur le réseau en temps réel et des paquets circulant sur le réseau IP. Il peut exécuter l'analyse de protocole, en cherchant et s’assortant le content et peut être employé pour détecter une variété d'attaques, des tentatives comme des débordements d'amortisseur, des balayages de port de dérobée, des attaques de CGI, des sondes de SMB, des tentative d’empreinte de OS, et beaucoup plus.

SNORT emploie une langue flexible de règles pour décrire le trafic qu'elle devrait se rassembler ou passer, aussi bien qu'un moteur de détection qui utilise une architecture plug-in modulaire. SNORT a des possibilités en temps réel d'alerter aussi bien, incorporant alertant des mécanismes pour le système d’événement, un dossier indiqué par utilisateur, un socket de Unix, ou des messages de WinPopup aux clients de Windows en utilisant la smbclient.

SNORT a trois utilisations primaires.  Il peut être employé en tant qu'un renifleur de paquet comme tcpdump(1), un enregistreur de paquet (utile pour le trafic de réseau corrigeant, etc…), ou comme plein système soufflé de détection d'intrusion de réseau.

**Les plates formes pour installer SNORT**

| i386 | Sparc | M68k/PPC | Alpha | Other | |
|---|---|---|---|---|---|
| X | X | X | X | X | Linux |
| X | X | X | | | OpenBSD |
| X | | | X | | FreeBSD |
| X | | X | | | NetBSD |
| X | X | | | | Solaris |
| | X | | | | SunOS 4.1.X |
| | | | | X | HP-UX |
| | | | | X | AIX |
| | | | | X | IRIX |
| | | | X | | Tru64 |
| | | X | | | MacOS X Server |
| X | | | | | Win32 - (Win9x/NT/2000) |

*Source : [http://snort.org](http://snort.org)*

La figure illustre un réseau avec SNORT :

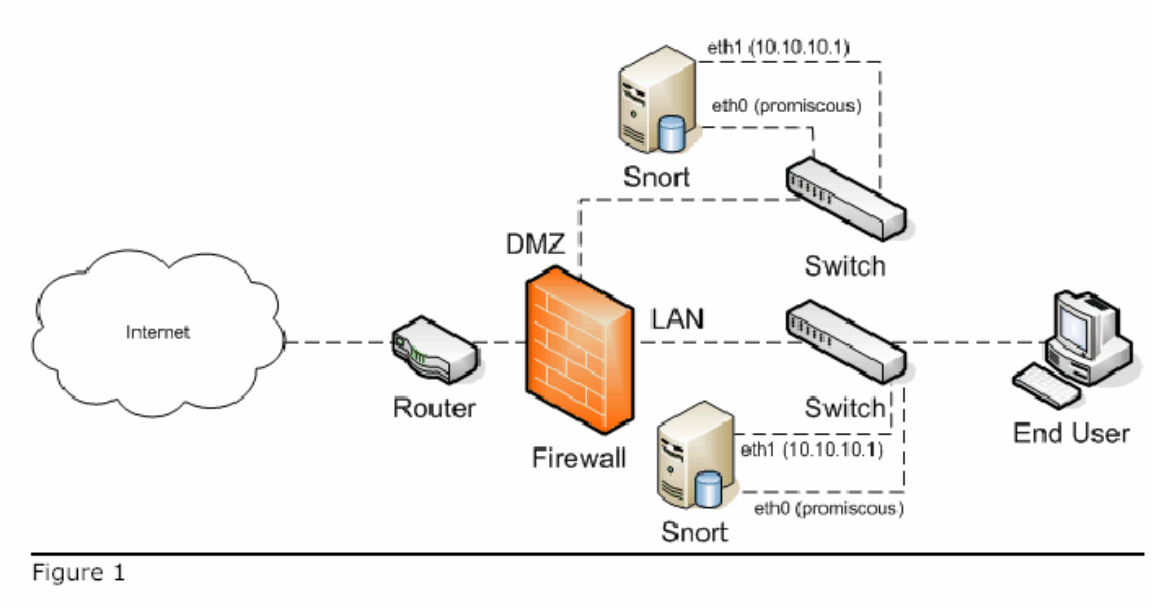



**Figure 1 : un réseau avec le SNORT**

Il y a deux postes pour mettre le SNORT : avant le par feu (externe) ou après le par feu (interne).

+ Système externe a pour but de détecter qui a tentative d'attaquer à notre système.
+ Système interne est le plus meilleur choix pour le système qui utilise « DMZ »

## 2. Installation

Il convient que vous devions installer plusieurs parties dont nous divisons en deux groupes : le serveur de l'interface et le serveur de la base de données. Alors, nous pouvons mettre chaque serveur dans un ordinateur séparé.

Nous avons trois choix pour installer le serveur de la base de données avec MYSQL ou ORACLE ou POSTGRESQLS.

Les documents de l'installation du SNORT sont partout sur le réseau, Mais j'essaie à implémenter seulement sur le Linux Mandrake 9.2 et ça fonctionne très bien.

Vous pouvez également utiliser ce site http://snort.org pour savoir plus des informations

### a) Linux (RedHat et Mandrake)

La base des données que j'ai choisit pour examiner est de MySQL sur linux (Mandrake). Pour être facile à gérer le SNORT, nous avons besoin des paquets correspondants suivants :

- Snort 2.2.0
- MySQL 4.0.15
- Apache 2.0.47
- PHP 4.3.4
- ADODB 3.90
- ACID 0.9.6b23

- ZLIB 1.2.1
- JPGraph 1.14
- LibPcap 0.8.1
- Swatch 3.0.8
- Webmin 1.160

**Références**

http://www.snort.org/docs/snort_acid_rh9.pdf

http://www.ntsug.org/docs/snort_acid_mandrake.pdf

**Remarques**

Vous pouvez télécharger la dernière version de SNORT sur le site web http://snort.org (La dernière version est de : 2.2.0)

Soyez attention avec le bibliothèque lipcap.x.x, Il a lieu peut être une erreur quand on compile le code source.

Les versions précédentes du ACID qui sont moins de 0.9.6b23 ne nous permettent que choisir le temps de janvier 2000 jusqu'à décembre 2003.

## b) Configuration

**Base de données**

La structure de la base de données contient plusieurs tables, voyez le fichier « create_mssql » ou « create_oracle.sql » ou « create_postgresql » dans le répertoire de l'installation .../snortxx/contrib/

**Ensembles des règles**

Il y a plus de 2550 règles définies par plusieurs d'organisations et plusieurs personnes travaillant dans le domaine de l'informatique.

Les utilisateurs peuvent également créer des ensembles de règle par eux même. Ces ensembles des règles sont mis à jour régulièrement.

## 3. Les outils du SNORT rapportant

Serait-il possible de voir les rapports …??

Heureusement, il y a des outils qui ont capable d'exporter des alertes vers des rapports en format de HTML ou en format de texte

### a) Snort report

**Source** : http://www.snort.org/dl/contrib/front_ends/snortreport/

**Snort report**: paquet snortreport

- Fonctionne avec MYSQL et POSTGRESQL.
- Utiliser la bibliothèque Jpgraph pour dessiner la charte
- Visualiser une charte ronde (TCP, UDP, ICMP, Portscan) dans le snort.
- Afficher les dernières alertes (timeframe) Ou des alertes hebdomadaires (daily)
- Le rapport indique les liens des sites webs pour exprimer des alertes.

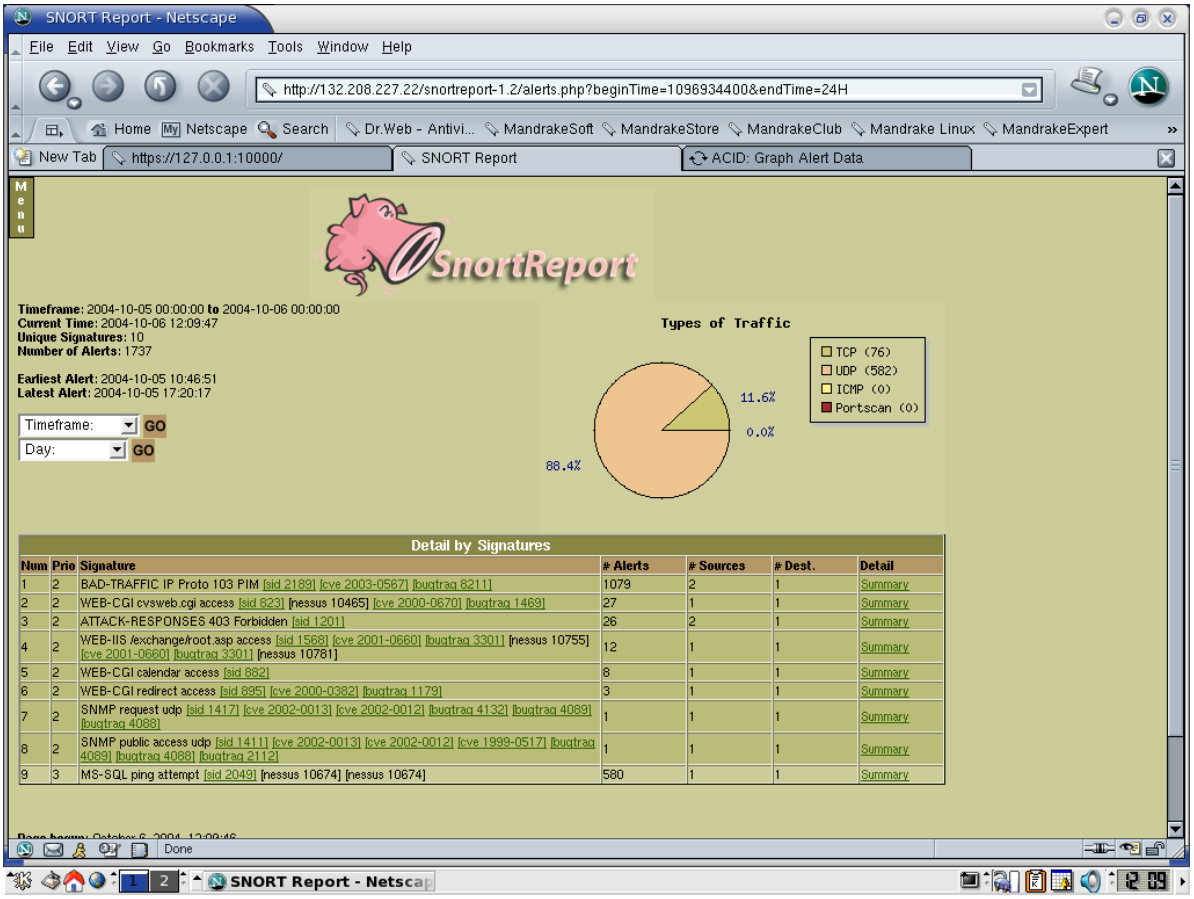



**Figure 2 : Les alertes le 05 octobre 2004**

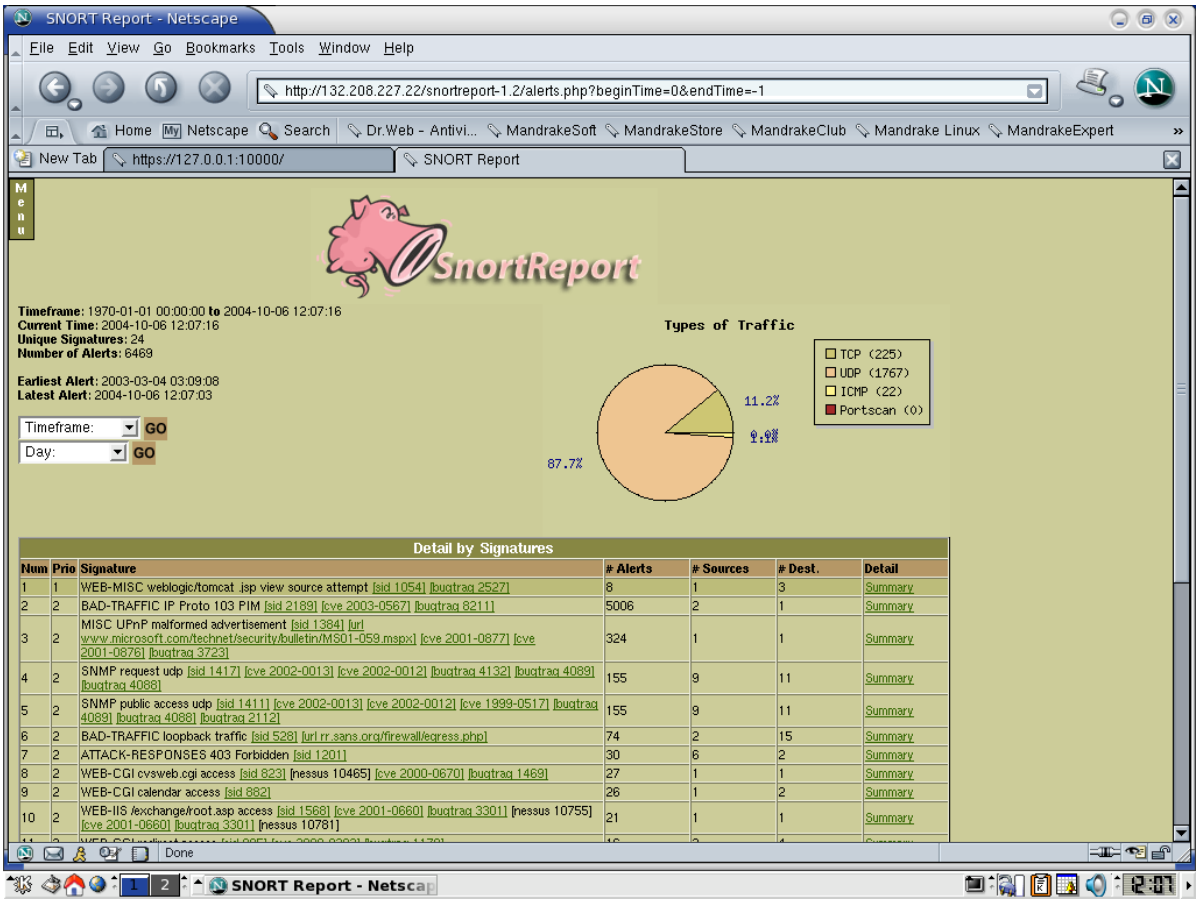



**Figure 3 : Tous les alertes**

## b) Snort-Rep

http://people.ee.ethz.ch/~dws/software/snort-rep

**Snort-rep** est un outil à rapporter le snort par deux formats (texte et HTML).

Chaque rapport contient :

- Résumé le balayage de port (port-scan)
- Résumé les alertes par ID
- Résumé les alertes par host éloigné et ID
- Résumé les alertes par host local et ID
- Résumé les alertes par port local et ID

Il est crée à utiliser pour les rapports par email hebdomadaire à les administrateurs du système. Tous les rapports en format HTML contiennent des liens aux descriptions d'IDS de whitehats.com

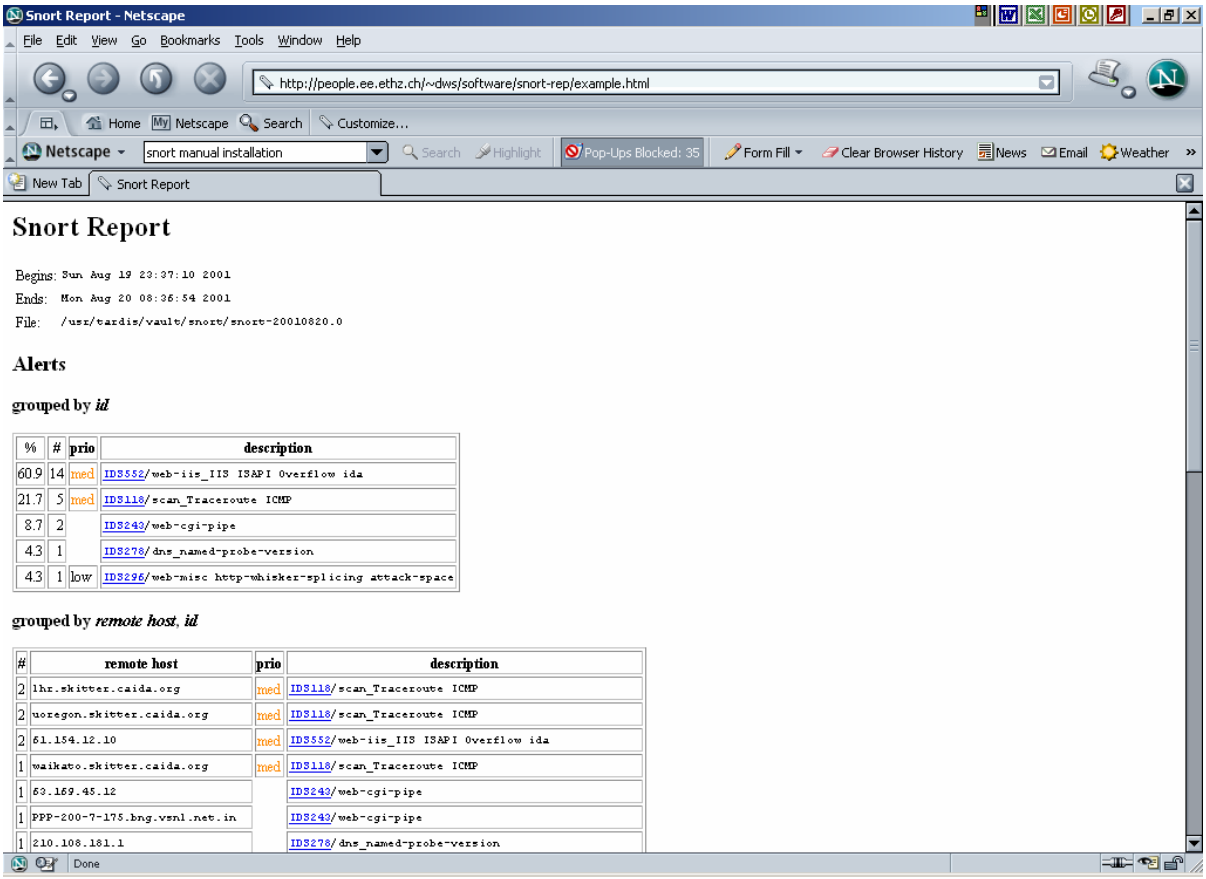



**Figure 4 : Le rapport en format HTML**

*Source : [http://people.ee.ethz.ch/~dws/software/snort-rep/example.html](http://people.ee.ethz.ch/~dws/software/snort-rep/example.html)*

## c) Acid

ACID est un moteur d'analyse de base de PHP pour chercher et traiter une base de données des incidents de sécurité qui sont générés par le logiciel de la sécurité comme IDS.

Pourtant, nous pouvons considérer ACID comme un outil exportant les rapports parce qu'il affiche les statiques des alertes comme les graphes et les chartes.

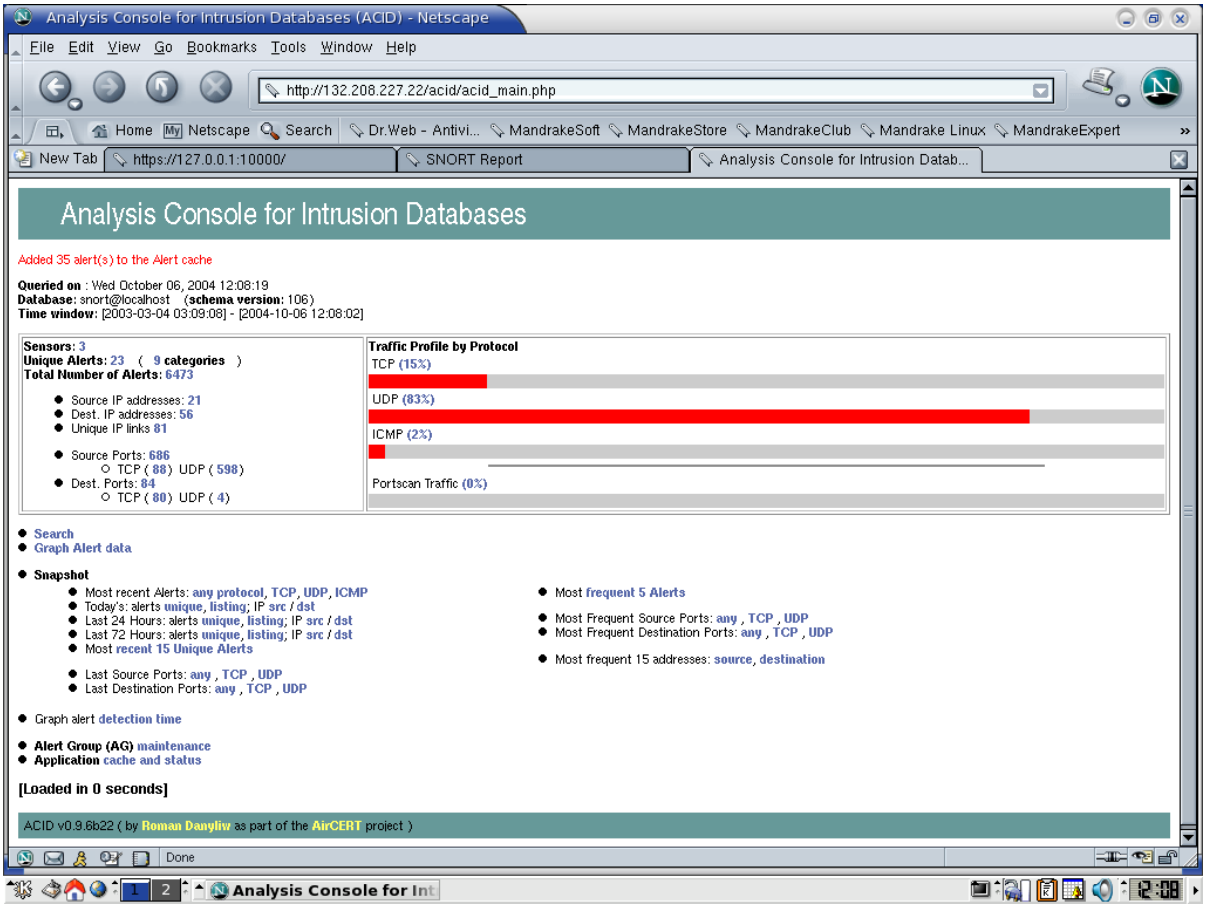



**Figure 5 : l'interface de ACID**

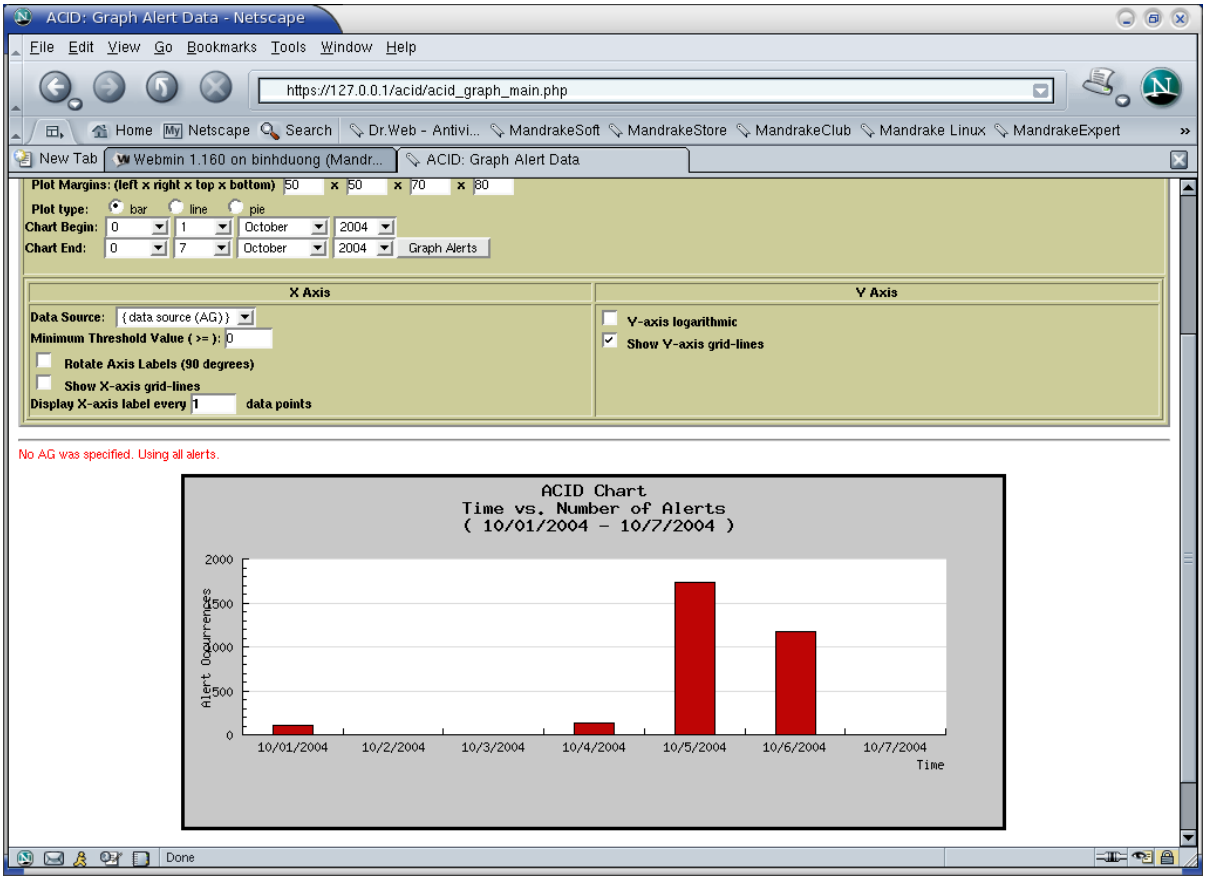



**Figure 6 : la charte de 01-10 à 07-10 par ACID**

## 4. Évaluations

### Avantages

- SNORT est un logiciel libre (Open Source) et il est mis à jour régulièrement sous la limite de GNU.
- SNORT adapte bien à plusieurs exploitations du système (Windows, Linux, FreeBSD, Solaris…).
- Un outil pour analyser les attaques, le trafic sur le réseau.
- On peut définir des signatures pour détecter des tentatives, le trafic du réseau.

- Il est disponible une ensemble des règles définies par plusieurs organisations et par plusieurs personnes.
- Toutes données sont sauvegardées dans la base de données (MYSQL, ORACLE, POSTGRESQL)

**Inconvénients**

En fait, C'est pas facile pour manipuler SNORT par ce qu'il y a beaucoup de commandes pour exécuter. C'est ainsi qu'on a ajouté les autres outils pour faciliter à gérer. Alors  les étapes d'installation sont compliquées.

# Chapitre 4: Système d'empêchement des intrusions

## I. Définition

### 1. Qu'est ce que le IPS ?

Le système d'empêchement d'intrusion a pour but d'empêcher des intrusions attaquant au moment qu'il arrive. Tandis que le système de détection a le rôle d'identifier des intrusions et vous annoncer. Tous sont basés sur l'analyse le système pour détecter et empêcher des activités malveillantes.

Le système d'empêchement d'intrusion construit sa part à résoudre le problème Zero-Day. Le moment le plus important a lieu quand les attaques reconnaissent la vulnérabilité de votre système et vous devez trouver rapidement une solution. À ce moment là, les produits d'IPS deviennent très utiles.

L'IPS est une réponse industrielle aux clients qui demandent la question « Pourquoi nous n'empêchons pas des attaques quand nous les détectons? »

Source : http://wp.bitpipe.com/resource/org_1046366622_812/IPS_Whitepaper.pdf

### 2. Qu'est ce que le Zero day exploits

Définir par : Brent Huston

Le « Zero-day exploit » est la grande énigme de la sécurité de l'information. C'est une nouvelle, inconnue vulnérabilité qu'il est difficile à prendre garde. Les attaquants passent beaucoup de temps travaillant à ces explorations, découvrant l'information priée pour tirer profit d'elles. Heureusement, les professionnels de sécurité de l'information ont une lance d'or aussi bien - la "meilleure pratique". Dans le monde de sécurité, les meilleures pratiques sont des mélanges entre des outils et des méthodologies de la sécurité utilisées pour défendre contre l'impact quotidien des

balayages, les vers et les tentatives de compromis. Mais comment vont-ils l'effet caché de ces deux armes?

Le “Zero-day exploits” sont souvent découvertes par les agresseurs qui trouvent une vulnérabilité de logiciel, une exécution ou un protocole spécifique. Elles établissent le code pour tirer profit de leur et pour compromettre un système. En fait, le “Zero-day exploits” sont l'arme la plus désirée des attaquants, et sont commercées comme les ressources naturelles valables pour d'autres exploits courantes privées, habituellement sur un canal (tunnel )de Internet Relay Chat ou un site Web souterrain privé.

**Source:** http://www.itworld.com/nl/security_strat/10302002/pf_index.html

## 3. Qu’est ce que Zero-day Protection?

### a) Définition

Jusqu’au présent, je n’ai pas encore trouvé une définition complète de Zero-day Protection. Cependant, suite à des informations dans les parties ci-dessus, nous pouvons tenir les conceptions du “Zero-day exploits”. Ce sont des tâches pour garder contre des attaquants qui tirent profit les vulnérabilités et détecter les vulnérabilités et les fixer à temps.

En fait, il y a des différences entre le “Zero-day exploits” et le Zero-day vulnérabilité. Le “Zero-day exploits” exploite une vulnérabilité inconnue, tandis que le Zero-day vulnérabilité est les trous dans un logiciel que personne ne connaît.

### b) Spécification

Le Zero-day protection fonctionne avec 2 systèmes IDS et IPS qui surveillent et analysent le trafic sur le réseau pour détecter et bloquer des attaques.

**Remarque** : Le plus grand problème du Zero-day Protection est des données chiffrées (data encryptions) parce qu’il y a quelques système de détection des intrusions ne peuvent pas analyser des données chiffrées.

Quand un attaquant exploite une vulnérabilité dans un logiciel ou dans un système, il va annoncer cette information en public. Puis il est possible que les autres vont attaquer à ce système si le fournisseur ne peut pas empêcher cette exploitation et ne pas fixer cette vulnérabilité. Nous appelons alors le « Zero-day » à ce moment. Par exemple, un des types de MyDoom a apparaît après 2 jours quand il y avait une vulnérabilité dans l'application Internet Explorer, ce n'est pas longtemps.

### c) Fonctionnements

La vulnérabilité peut devenir notoire dans diverses manières. Par exemple, une victime analyse l'exploit employé pour compromettre leur système et annonce la faiblesse précédemment inconnue au monde. Ou il peut rester dans les professionnels souterrains et éludant de sécurité pendant un certain temps. Une fois que la vulnérabilité est connue, elle peut immobile évoluer, devient un outil automatisé de malware ou aboutit à de autres trouvailles. En plus, le fournisseur peut ne pas répondre immédiatement avec une pièce rapportée ou fixer pour le problème, laissant un espace entre la connaissance de la vulnérabilité et de sa réparation. En conséquence, le travail du personnel de sécurité doit rendre l'espace le plus petit si possible.

Les meilleures pratiques sont utilisées comme la ligne de base d'effectuer l'espace de vulnérabilité et doivent être appliquées à tous les systèmes et capitaux de réseau. Même si un attaquant emploie leur Zero-day exploit pour compromettre un système, le personnel de sécurité est si tout va bien alerté par un système de détection d'intrusion (ce qui est une partie de la plupart de réseau les "meilleures pratiques") et l'accès est réduit au minimum par le reste des mécanismes de sécurité sur place qui n'ont pas été évités par l'exploit.

Tandis que beaucoup d'outils de la "meilleure pratique" existent, ils prêchent souvent des méthodologies et des mécanismes complètement différents pour réaliser l'équilibre entre la sûreté et la rentabilité. Ceci le rend difficile à mesurer qui tient les plus grands défis et qui tient les plus grandes récompenses. Par exemple, les idées de l'institut de SANS sont-elles meilleures que le centre pour les idées de la sécurité d'Internet, ou ceux mises en avant par l'agence de sécurité nationale? (NSA)

Indépendamment de votre choix des outils, les meilleures pratiques en matière de sécurité doivent être appliquées dans toute l'organisation, autrement, un attaquant peut trouver ou trébucher sur un système affaibli qui pourrait mener aux dommages significatifs aux capitaux. D'ailleurs, l'exploit d'un attaquant pourrait être contre un système qui est si critique au maintien de sécurité d'une entreprise que l'immense compromis est le résultat.

Cela a indiqué, nous sont partis avec la connaissance que le "Zero-day exploits" sera toujours abordée. Un certain attaquant saura toujours quelque chose que nous ne faisons pas et il y a peu que nous pouvons faire pour nous protéger contre l'inconnu. Les meilleures pratiques sont un bon outil pour s'assurer cela si l'inconnu nous mord, nous prennent en tant que peu de dommages comme possibles de l'assaut. Cependant, la clef à utiliser l'épée de "le meilleure pratique" est dans le choix et l'accomplissement de l'application et de la gestion. Choisissez soigneusement vos meilleures pratiques, et choisissez un qui est le meilleur des ajustements le risque tolérance de votre organisation, les politiques de sécurité et les attitudes.

### d) Caractéristiques

Le "Zero-day exploits" a lieu quand une attaquant tire profit les vulnérabilités de sécurité en même jour que ces vulnérabilités deviennent connues. Normalement, après quelqu'un a détecté une exposition potentielle dans un application ou un logiciel qu'un intrus exploite, cette personne ou la compagnie peut informer la compagnie de logiciel et parfois tout le monde dans son ensemble de sorte qu'une mesure puisse être prise à la réparation l'exposition ou défendre contre son exploitation. Temps donné, la compagnie de logiciel peut réparer et distribuer une difficulté aux utilisateurs. Même si les intrus potentiels apprennent également de la vulnérabilité, elle peut leur prendre un certain temps de l'exploiter; en attendant, la difficulté peut si tout va bien devenir première disponible.

Avec l'expérience, cependant, les intrus deviennent plus rapidement à exploiter une vulnérabilité et parfois un intrus peut être la première personne qui découvre la vulnérabilité. Dans ces situations, la vulnérabilité et l'exploit peuvent devenir apparent en même jour. Puisque la vulnérabilité n'est pas connue à l'avance, il n'y a aucune manière de garder contre l'exploit avant qu'elle se produise. Cependant, les compagnies exposées là de tels exploits peuvent instituer des procédures pour la détection tôt d'un exploit.


# II. Outils d'empêchement de zero day

## 1. Zone Labs Integrity

### a) Introductions

Le Zone Labs Integrity est une solution client/serveur distribuée qui protège tous les réseaux d'ordinateur personnel (PC). La protection des points finals de multicouche de l'intégrité sauvegarde chaque PC contre des menaces connues et inconnues, bloquant les entrés et les sortie non autorisées de réseau et les connexions d'application. Le serveur central d'intégrité offre un système flexible et facilement administré pour d'établissement des règles de sécurité de réseau; Le serveur donne également à des administrateurs un outil puissant avec lequel pour équilibrer pour la protection de réseau et la productivité des employés pour la sécurité dans le monde réel.

Le Zone Labs Integrity est un principal créateur des solutions de sécurité de point final et d'un des marques de confiance dans la sécurité d'Internet, protégeant les 20 millions PCs finis dans le monde entier.

Tandis que la prédominance connue pour son produit de ZoneAlarm®, l'entreprise de gain de récompense de Zone Labs Integrity™ est une plateforme de gestion de sécurité de point final qui protège des données et la productivité de corporation.

La protection multicouche de l'intégrité bloque efficacement les chevaux de Trojan, le spyware, les vers malveillants, et d'autres dangers inconnus au PC de point final avant qu'ils puissent pénétrer le réseau.

**Source : +** http://www.clearview.co.uk/integrity.htm
+ http://www.cisilion.com/security/integrity.htm

### b) Caractéristiques

- Blocage de l'attaque d'intrus, worms, spyware, viruses, and data theft

**Tableau 1 :** La comparaison de la Zone Labs Integrity avec des autres outils traditionnels

| | Méthodes Traditionnelles | | | Zone Labs Integrity |
|---|---|---|---|---|
| | Par feu | Anti-virus | Intrusion Détection | |
| Empêcher l'intrusion d'arrivée | Oui | Non | Non | Oui |
| Bloquer le Trojan horse | Non | Non | Non | Oui |
| Détecter les menaces connues | Oui | Oui | Oui | Oui |
| Arrêter les menaces connues et inconnues | Non | Non | Non | Oui |

**Gestion les politiques de sécurité**

- Créer centralement, mettre à jour et assigner les politiques.
- Déployer la protection immédiate.
- Personnaliser, raffiner et renforcer les politiques aux besoins du client avec le temps.
- Outils de gestion simplifiés

**Coopérativement exécution de la sécurité d'accès à distance**

- Sécurité complète de point final pour les PCs à distance.
- Sécurité inégalée d'accès à distance.
- Aucune perturbation des employés.
- Facile pour des utilisateurs de VPN de rester dans la conformité.

Vous pouvez trouver des informations plus détaillées introduisant les caractéristiques de la Zone Labs Integrity sur l'adresse *http://download.zonelabs.com/bin/media/flash/integrity/main.swf*

## c) Exigence du système

La Zone Labs Integrity ne supporte que le système d'exploitation Windows pour toutes les versions.

## 2. Symantec – Symantec Client Security

### a) Description

**Fournisseur :** Symantec Corp., www.symantec.com

Symantec Client Security fournit la protection des clients contre des menaces complexes sur l'Internet en intégrant l'antivirus, le par feu et la détection des intrusions, travers la gestion et la réponse centralisées. Il vous aide à protéger votre entreprise contre les virus, les pirates et les menaces combinées.

Cette nouvelle solution fournit un déploiement commun et fonction de mise à jour pour des technologies de sécurité multiples, permettant une sécurité plus complète de client.

**Symantec™ Client Security** est une solution facile à administrer qui garantit une sécurité multi couches performante. En protégeant votre entreprise avec Symantec, vous bénéficiez d'une protection constamment à jour contre les virus, les pirates et les menaces combinées, ainsi que d'un support de renommée mondiale. Les technologies de pointe de détection d'intrusion et de protection de pare-feu masquent automatiquement vos postes de travail et bloquent les connexions suspectes. Elles interagissent également en toute transparence avec Symantec AntiVirus pour protéger vos postes de travail, serveurs de fichiers et ordinateurs distants contre les virus, les vers, les chevaux de Troie et les menaces combinées. Les outils d'administration centralisée offrent une protection automatique en temps réel et facilitent la mise à jour de la sécurité de votre réseau à partir d'un seul emplacement. Les experts de Symantec Security Response veillent afin de fournir les mises à jour et un support professionnel en cas de nouvelles menaces.

## b) Caractéristiques

- Protège les ordinateurs personnels sur le réseau, les systèmes critiques, et les utilisateurs à distance et mobiles contre des intrusions non désiré de réseau, aussi bien que des virus, de cheval de Troy (Trojans), et des vers.
- La sentinelle de Symantec VPN donne à des administrateurs de réseau l'assurance que les utilisateurs à distance et mobiles sont dans la totale conformité aux politiques de corporation antérieurement à accéder à des ressources de réseau de corporation.
- La conscience d'endroit assure la politique de corporation de sécurité est respectée, indépendamment de l'endroit.
- Le client que le profilage réduit au minimum le nombre de popups que l'utilisateur terminal voit pendant que l'application de par feu découvre quelles applications accèdent à l'Internet ou au réseau.
- Le traceur de menace identifie la source des attaques mélangées de menace qui répandent les fichiers partagés ouverts telles que Nimda.
- L'heuristique de ver d'email de sortie empêche des systèmes de client des vers de propagation par l'intermédiaire de l'email.
- La détection augmentée de menace identifie des applications non désiré telles que le spyware et l'adware.
- Balayage d'attachement d'email d'Internet des emails entrants livrés par des clients du courrier POP3 tels que Microsoft Outlook, Eudora, et courrier de Netscape.
- Le balayage de mémoire détecte des menaces et termine les processus suspects dans la mémoire avant qu'ils puissent endommager.
- Inclure la configuration, le déploiement, l'installation, le reportage, alerter, noter, et la gestion centralisée de politique

## c) Exigence du système

Windows 9x, Windows Me, Windows 2000 Professional, Windows XP Professional/ Home Edition

## 3. McAfee System Protection – McAfee Entercept

### a) Introduction

Le McAfee System Protection est une solution qui protège le système d'une poste de travail et de serveur et des applications. Il comprend  du logiciel McAfee VirusScan,  du logiciel de McAfee ThreatScan pour évaluer des vulnérabilités de virus, McAfee Desktop Firewall, la solution d'empêchement des intrusions de hôte McAfee Entercept, et McAfee SpamKiller pour bloquer de spam.

Plusieurs de ces produits sont centralement contrôlés par la solution industrie principale McAfee ePolicy Orchestrator (ePO) qui permet la gestion de politique et le reportage de McAfee et de tiers produits de la sécurité.  En outre, dans les solutions de protection de système de McAfee, la brochure est la famille magique de bureau de service des produits, fournissant la gestion et la visibilité totales des systèmes de dessus de bureau et de serveur.

La solution d'empêchement d'intrusion de centre serveur de McAfee Entercept fournit la sécurité maniable de classe d'entreprise qui est plus rentable que juste la détection et la surveillance. La technologie de protection de serveur d'entreprise brevetée combine la signature avec les règles de comportement à empêcher toutes les attaques connues et inconnues avant qu'elles se produisent. Comme solution de logiciel seulement, McAfee Entercept peut être déployé sur une rangée des plateformes de matériel utilisant les systèmes d'exploitation principaux de l'industrie.

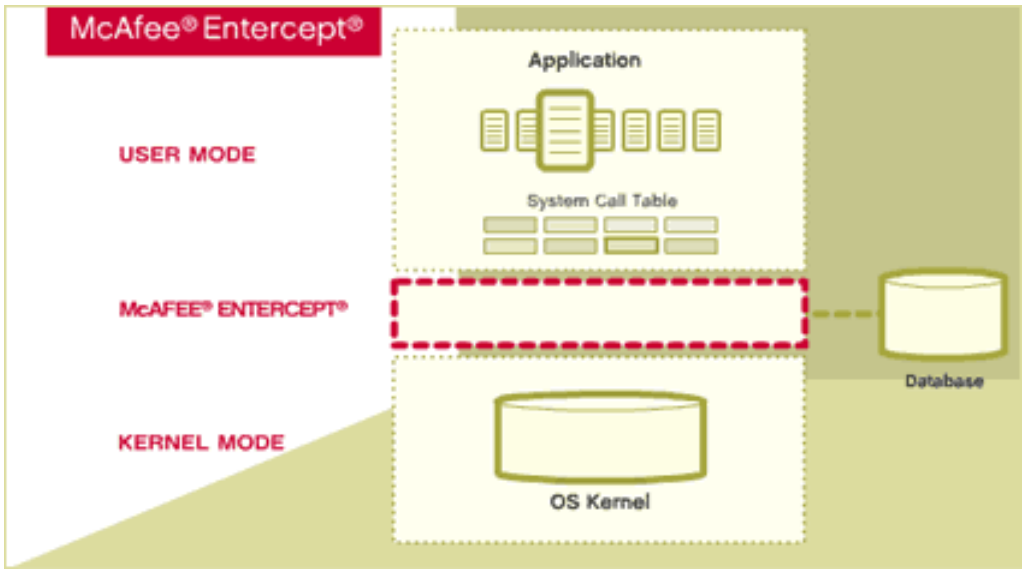



**Figure 7: McAfee Entercept System**

Le McAfee System Protection fonctionne sur tous les deux côté, le serveur et le client (post de travail).

**Source :** https://start.mcafeesecurity.com

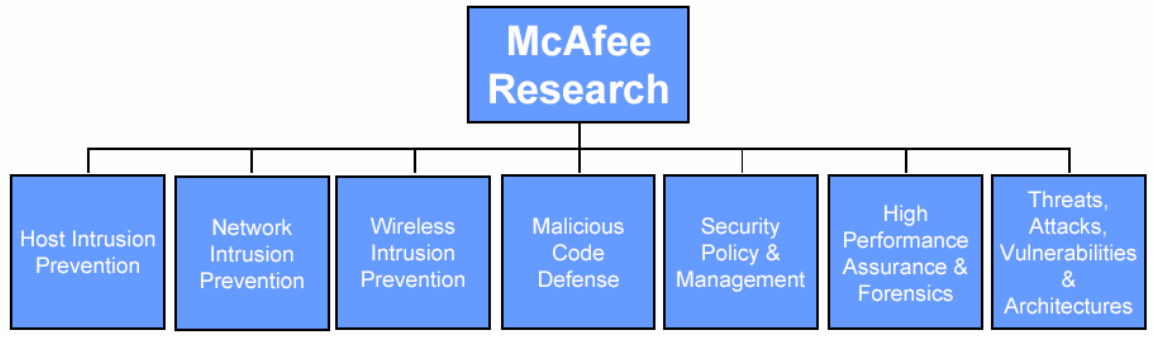



**Figure 8: Les seteurs de McAfee**

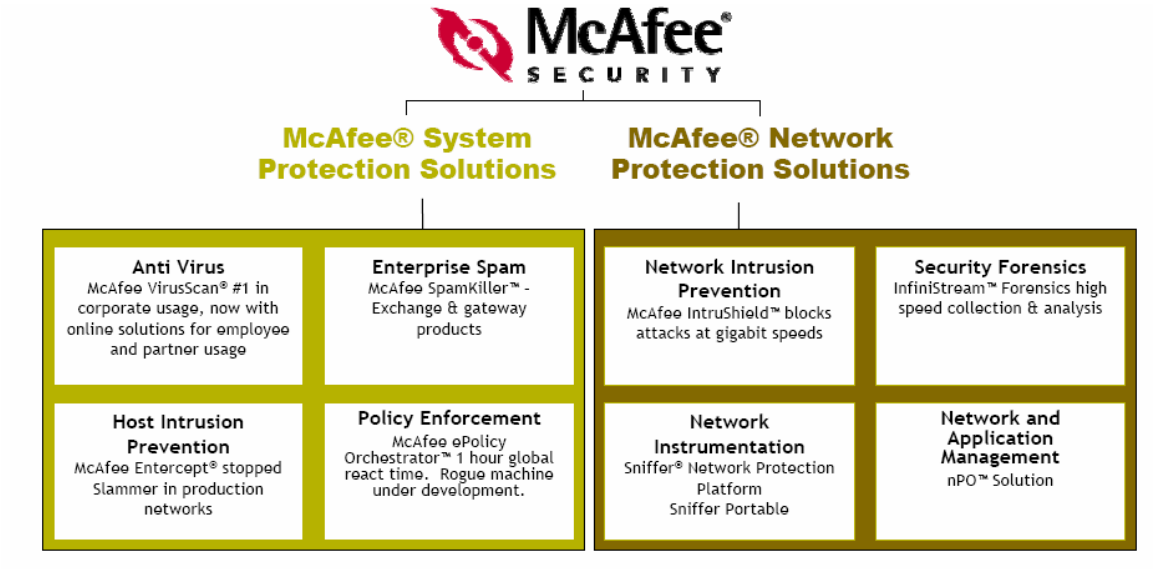



**Figure 9 : Les produits de McAfee**

Dans ce cas, je vais vous expose les caractéristiques de Host Instrusion Prevention ou le McAfee Entercept Standard Edition.

### b) McAfee Entercept Standard Edition

McAfee Entercept Standard Edition protège des serveurs et des desktops contre une chaîne plein des attaques connues et inconnues. Pendant que la seule solution d'empêchement d'intrusion de centre serveur (IPS) combinant des signatures avec des règles comportementales, McAfee Entercept assurent la protection proactive supérieure de menace (arrêt des menaces avant qu'elles puissent endommager des systèmes et des applications). McAfee Entercept diminue significativement la critique de déploiement de pièce rapportée, réduit des coûts de sécurité connexes, et protège les critiques actives.

### c) Avantages de produit

- Réduction de risque proactive : McAfee Entercept empêche des menaces avant qu'elles puissent compromettre les critiques actives, plutôt que détectant simplement des attaques après le fait.

- Protection complète (intelligent) : une combinaison puissante des règles comportementales et des blocs de signatures d'attaque connus, de zéro-day, et des exploits de débordement de tampon; un par feu de processus intégré sert comme une couche additionnelle de protection au control de trafic dans et hors d'un système.
- Exactitude supérieure : pré-configuré, les politiques personnalisables permettent l'exactitude maximum de la détection pour n'importe quel environnement.
- Manualité - écailler : déployer et contrôler les milliers d'agents avec un serveur simple de gestion de McAfee Entercept; déploiement facultatif et surveillance avec McAfee ePolicy Orchestrator® 3,5 (disponible en 2004).
- Abaissez le coût total de la propriété : Entercept abaisse des coûts en atténuant la critique de pièce rapportée, en réduisant au minimum des ressources requises pour déployer et maintenir la protection, et en maximisant la disponibilité de système et d'application

## d) Caractéristiques

- Agents assurés et indépendant : Les agents de McAfee Entercept, installés sur des serveurs de hôte, système d'interception appelle au système d’exploitation, assortissant les appels contre des règles comportementales et des signatures d'attaque, et bloquant ceux qui causeraient le comportement malveillant. Les agents reçoivent automatiquement des mises à jour de code et de nouvelles signatures d'attaque du système de gestion d'Entercept.
- Règles comportementales et signatures d'attaque : Les règles comportementales bloquent de nouvelles menaces en imposant le système d'exploitation et le comportement appropriés d'application. Le bloc de signatures attaquent et fournissent des descriptions exactes des événements, donnant des administrateurs accomplissent la compréhension des menaces qu'elles font face. Les organisations ont besoin de tous les deux technologies pour bloquer des attaques connues et de Zero day.
- Empêchement d'exploit de débordement de tampon : La technologie brevetée de McAfee Entercept exclut l'exécution de code résultant des

attaques de débordement de tampon, d'un des méthodes les plus communes d'attaque des serveurs et des desktops.

- Déploiement et surveillance de McAfee ePolicy Orchestrator 3.5 :
  Déploiement facultatif et surveillance avec le Mcafee ePolicy Orchestrator 3.5 (Q3 disponible 2004).
- Surveillance d'événement d'intégrée de centre serveur et de réseau basée IPS (Intégrée HIDS et NIDS): IntruShield 2.1 Manager importe et corresponds aux alertes d'Entercept Agents avec des alertes d'IntruShield Sensor pour consolidé, au niveau système vu d'état de sécurité.
- Modèle de politique par défaut
  La base de données de politique de McAfee Entercept embarque avec un ensemble de modèles entièrement configurés par défaut pour le déploiement rapide de produit. Il inclut les dispositifs puissants de personnalisation pour modifier des politiques quand on a besoin, presque entièrement éliminant les faux positifs.
- Dissuasion d'escalade de privilège
  Les attaquants accèdent fréquemment à un réseau par un compte non privilégié et obtiennent alors des privilèges de niveau de racine. McAfee Entercept bloque ces exploits, s'assurant que les attaquants ne peuvent pas augmenter leur niveau de privilège.
- Infrastructure de sécurité existante de compléments
  McAfee Entercept n'interférera pas les outils existants de sécurité, et n'exige pas l'intégration spéciale. Il n'exige aucun changement au système d'exploitation ou aux applications marchant dans un système.

### e) Exigence du système

Les conditions minimums que le système a besoin.

- Windows: Windows 2000 server, NT 4, Windows server 2003, Windows XP
- Solaris: Solaris 7, Solaris 8, Solaris 9 ( 32 bits et 64 bits )
- HP: HP-ux 11i (PA-RISC 64-bit), HP-ux 11,0 (PA-RISC 64-bit)

## 4. CISCO – CISCO Security Agent (CSA)

### a) Introduction

Cisco Security Agent fournit la protection contre les menaces pour un ordinateur de serveur ou de post de travail ou des points finaux. Il nous aide à réduire le prix opérationnel en identifiant, empêchant et éliminant des menaces connues et inconnues. Le CSA consolide des fonctions sécurité des points finaux dans un agent simple en fournissant des dispositifs suivants :

- Empêchement des Intrusions du Host
- Empêchement le Spyware ou le adware
- Empêchement contre des attaques de débordement de tampon
- Capacité de par feu distribué
- Protection de code mobile malveillant
- Assurance d'intégrité du système d'exploitation
- Inventaire d'application
- Consolidation des journaux de l'audit

Puisque le CSA analyse les comportements plutôt que comptant sur l'assorti de signature, alors il n'a jamais besoin de la mis à jour pour arrêter les nouvelles attaques. Cet architecture de mis à jour de zero fournit la protection avec le prix opérationnel réduit et peut identifie le menace de Zero day.

Le CSA est inclut dans le Cisco Works Management Center pour le Cisco Security Agent, une partie de CiscoWorks VPN/Security Management Solution (VMS)

### b) Avantages

- Agrège et s'étends des fonctions multiples de sécurité de point final en fournissant l'empêchement d'intrusion de host, le par feu distribué, la protection mobile malveillante de code, l'assurance d'intégrité de système d'exploitation, et la consolidation tous des journaux d'audit dans un paquet simple d'agent.

- Offre la protection contre les classes entières des attaques, y compris les balayages de porte, les débordements de tampon, les chevaux de Trojan, les paquets mal formés, les demandes malveillantes de HTML et les vers de E-mail.
- Fournit l'empêchement "Zero Update" des attaques connu et inconnu.
- Assure la protection d'industrie principale pour des serveurs et des desktops, et pour des plateformes d'Unix et de Windows.
- Assure la protection spécifique d'application pour des serveurs de webs et de base de données.
- L'architecture ouverte et extensible offre la capacité de définir et imposer la sécurité selon la politique de corporation.
- Offre une architecture d'entreprise-scalable ; le CSA est scalable aux milliers d'agents par directeur.
- Fournit à la gestion intégrée avec les dispositifs de sécurité de Cisco PIX, de Cisco Secure IDS, et Cisco VPN.

### c) Exigence du système

Le Cisco Security Agents supporte tous les deux plateforme de Windows.

## 5. ISS – Real Secure Desktop


### a) Introduction

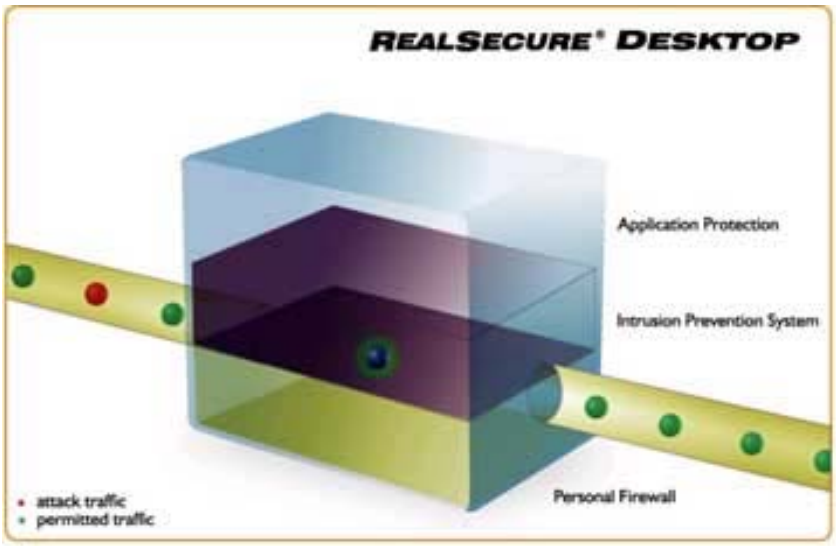
La protection de bureau de *RealSecure* de ISS est un système de protection de bureau avancé conçu pour protéger les utilisateurs à distance contre un spectre divers et croissant de menace sans affecter des opérations normales d'utilisateur ou de réseau.

La protection de bureau de *RealSecure* empêche les attaques au niveau de bureau et est entièrement intégrée avec la contrôlé centrale, le système de protection de la mesure d'entreprise pour fournir une approche holistique à la sécurité qui adressent à tous les aspects de sécurité de réseau, de serveur et de dessus de bureau pour la défense au profondeur.

L'assure de la protection en temps réel contre l'activité malveillante en analysant l'application, le réseau et le comportement du réseau privé virtuel (VPN) sur un poste de travail. *Real Secure Desktop* combine un par feu de force commercial avec un système d'empêchement d'intrusion en tête du marché et des applications de la protection pour empêcher intelligemment et discrètement des activités incorrectes. Centralement contrôlé par le système de gestion de *Site Protector* pour le reportage et l'analyse entièrement intégrés de la solution de sécurité de réseau munissent la protection de blocage active contre des attaques, ayant pour résultat une gestion plus facile et la coordination de réponse, abaissent des coûts de soutien, et un coût réduit de propriété.

### b) Fonctionnements

- Protéger contre des menaces de l'Internet complexe tel que le Nimda et Code Red.
- Sauvegarder des données confidentielles à partir de la perte et du vol.
- Réduire le temps d'arrêt de système et aider à maintenir la productivité.
- Éliminer des fardeaux administratifs de mis à jour la solution de multi fournisseur.




## c) Dispositifs et avantages

- Protection d'application : Empêcher des applications de Trojan de marcher en permettant seulement à des programmes autorisés de marcher. Les possibilités avancées de protection de l'application du RealSecure Desktop empêchent des applications restreintes en permettant à des administrateurs d'établir les listes adaptées aux besoins du client d'applications non autorisées, s'assurant contre que votre environnement de desktop reste à être protégé à partir de  l'utilisation et l'accès non autorisée.
- L'arrivée et la sortie d'IDS/Blocking : Surveiller tout le trafic d'arrivée et de sortie à partir d'attaques nouvelles et inconnu comme le bloque dynamiquement des attaques arrivées/sorties par l'analyse intelligente des applications confiées. Le bon trafic est permis tandis que le trafic malveillant ou soupçonneux n'est pas, indépendamment de si l'application "est fié", depuis beaucoup de virus, Trojans, des vers et les back doors peuvent employer à des applications confiées pour lancer des attaques.
- L'intégration de VPN : S'assurer que les clients sont conformément à la politique de corporation avant de permettre l'accès au réseau de corporation par le VPN (IIS).

- La conscience d’antivirus : S'assurer que le client a mis à jour le logiciel d'anti-virus pour contrecarrer outre de l'attaque.
- De Gestion Centralisé SiteProtector : Les clients peuvent commander, surveiller et analyser des systèmes de protection de sécurité de réseau d'un lieu d'exploitation principal avec un minimum de personnel et de coûts opérationnels. Cet environnement intégré permet surveiller l'activité d'intrusion, de l'évaluation de vulnérabilité, de la priorité d'événement et de la corrélation de l'activité continue de sécurité, aussi bien que des possibilités de gestion de multi site. Aucune autre solution ne fournit la visibilité bout à bout en temps réel dans et à travers le programme de sécurité de entreprise large tout en profitant des investissements de ressource.
- Corrélation et analyse avancées d'événement : Fournir les connaissances de sécurité de la X-Force intégrée pour escalader dynamiquement des incidents menaçants de sécurité et pour réduire les alarmes fausses. Le module corrèle immédiatement des données de sécurité des sources multiples sur pour escalader des menaces sérieuses, telles qu'une attaque sur un capitaux vulnérables ou une attaque secrète et multi pas.
- Renforcé par le X-Force : le X-Force est le groupe de recherche le plus respecté de sécurité dans l'industrie, après avoir recherché et identifié les titres de sécurité dans les produits du Cisco, du Microsoft, de IBM, de Sun, de la Hewlett-Packard, d’Oracle, du Peoplesoft, du BMC, du Polycom, de l'Apache et de beaucoup plus. Cette équipe de recherche du bord de découpage transforme activement la recherche de sécurité en améliorations de produit, permettant aux clients des systèmes de sécurité d'Internet de répondre bien plus rapidement aux menaces d'évolution.
- Soutien de Technique Global : Fournir à des clients une grande sélection d'offres de soutien, spécifiquement conçue pour satisfaire les demandes de coût et de service des environnements divers de gestion de réseau.

## d) Exigence du système

**Processus**: Pentium Class CPU ou plus

**Mémoire**: 64 Mo de RAM ou plus

**Espace de disque dur** : 20 Mo

**Connexion de réseau:**

- 10/100 mbps ou GB NIC
- TCP/IP network connection over 10/100 Ethernet LAN/WAN, cable modem, DSL router, ISDN router ou dial-up modem
- System doit employer COMCTL32.DLL version 4.72 ou plus; COMCTL32.DLL est disponible sur le site de Microsoft

**Système d'exploitation:**

- Windows NT 4.0 Workstation (SP 6a)
- Windows 2000 Professional (SP 1-4)
- Windows XP Professional (SP 1-2)
- Windows XP Home (SP 1-2)
- Windows ME
- Windows 98/98 SE

Logiciel supplémentaire : Internet Explorer 5.0 ou plus.

## III. Évaluations

Tableau de la comparaison des outils concernant au empêchement du 0-jours

| | Zone Labs Integrity | Symantec Client Security | CSA CISCO | McAfee - Entercept | ISS |
|---|---|---|---|---|---|
| Empêcher l'intrusion d'arrivée | Oui | Oui | Oui | Oui | Oui |
| Bloquer le Trojan horse | Oui | Oui | Oui | Oui | Oui |
| Détecter les menaces connues | Oui | Oui | Oui | Oui | Oui |
| Arrêter les menaces connues et inconnues | Oui | Oui | Oui | | Oui |
| Centraliser le control | Oui | Oui | Oui | Oui | Oui |
| Empêcher des applications | | | | | Oui |
| Plateformes | Windows | Windows | Windows | Windows<br>Solaris<br>HP | Windows |
| Spécialités | - Sécuriser pour tous les points finaux | - Balayer les virus par email<br>- Contre le pop-up, spyware, adware… | - Une collection des multi fournisseurs<br>- Supporter la sécurité du réseau sans fil | | -Mise à jour par multi fournisseurs |

# Chapitre 5: Conclusions

Ce rapport a disposé le problème essentiel concernant aux intrusions qui peuvent effectuer à votre système informatique. Je vous ai montré quel est un système de la détection des intrusions et un système d'empêchement des intrusions? Ce résultat est la collection des connaissances à partir de Internet.

Comme des outils d'empêchement des intrusions, j'ai réussit à implémenter un système de détection des intrusions qui s'appelle SNORT marchant sur le système d'exploitation Unix. Ce logiciel est un Open Source avec une ensembles des règles de plus 2000 règles qui sont mise à jour par plusieurs organisations de sécurité dans le monde entier.  Pourtant, nous pouvons également installer ce système sur le système d'exploitation Windows.

Lors qu'on dit le problème de sécurité informatique, on n'oublie jamais de système d'exploitation Windows parce qu'il a beaucoup de vulnérabilités. C'est pourquoi que je vous propose quelques outils très efficaces pour protéger votre ordinateur :

- Zone Labs Integrity
- Symantec Client Security
- CISCO Security Agent
- McAfee Entercept
- Internet Security System – Real Secure Desktops

En fait, je n'ai pas beaucoup d'expérience dans ce domaine, alors je ne peux pas vous dire quel est le meilleur logiciel à choisir. Donc je vous montre seulement leurs caractéristiques, leurs fonctionnements…

Enfin, pour que votre ordinateur soit sécurisé, vous devez utiliser un logiciel qui peut détecter et empêcher des intrusions comme Symantec ou McAfee… Note bien que la plupart des logiciels de la sécurité marchant sur Windows sont commercial.

# Chapitre 6: Références


[1]. http://snort.org

[2]. http://www.ntsug.org/docs/snort_acid_mandrake.pdf

[3]. http://www.tripwire.com

[4]. http://sourceforge.net

[5]. http://people.ee.ethz.ch/~dws/software/snort-rep

[6]. http://www.itworld.com/nl/security_strat/10302002/pf_index.html

[7]. http://wp.bitpipe.com/resource/org_1046366622_812/IPS_Whitepaper.pdf

[8]. http://www.zonelabs.com

[9]. http://www.cisco.com/en/US/netsol/ns466/netqa0900aecd800fdd6f.html

[10]. http://www.clearview.co.uk/integrity.htm

[11]. http://www.cisilion.com/security/integrity.htm

[12]. http://techupdate.zdnet.com/techupdate/stories/main/Cisco_Security_Agent.html

[13]. http://www.cisco.com/en/US/netsol/ns466/networking_solutions_sub_solution_home.html

[14]. http://www.iss.net

[15]. http://www.symantec.com

[16]. http://www.mcafee.com