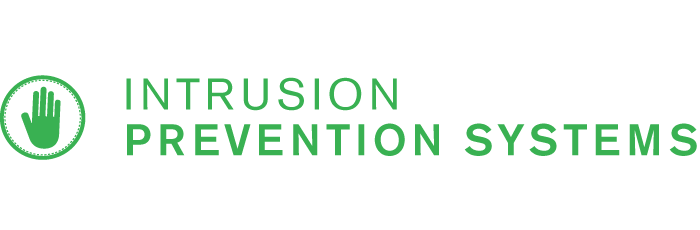


DESZCZ Sébastien

DURAK Thomas

MEURILLON Grégoire

STALTER Marianne



**Années 2013-2014**

**B3**

Projet de Veille Technologique

Sujet : IPS Appliance

Synthèse

Dans un monde de plus en plus informatisé et connecté, l’IPS devient indispensable pour tout système informatique. En effet, devant la prolifération des virus informatiques et des hackers, il convient de protéger toutes les informations sensibles d’une structure, d’autant plus lorsqu’il s’agit d’une entreprise.

L’outil présenté dans ce document s’appelle IPS (« Intrusion Prevention System »).

Il permet à un utilisateur de contrôler tous les flux réseaux d’un système informatique. En cas d’actions anormales sur le réseau, l’IPS en informe l’utilisateur. Il peut tout aussi bien nettoyer le problème, s’il s’agit de logiciels malveillants.

Mots clés : système, informatique, sécurité, prévention, alerte, quarantaine, intrusions, hackers, virus, nettoyage.

Préambule

De notre sujet, nous y en avons retiré une problématique, qui est la suivante :

**L'IPS : LA solution pour lutter contre les menaces venant d'Internet ?**

De ce fait, on évoque tous les sujets importants : les acteurs du marché, ainsi que la technologie, en abordant aussi bien les points positifs que les points négatifs. Le terme « LA » a été choisi pour couvrir l’étude des parts de marché et l’implantation du logiciel.

En effet, on suppose dans cette problématique que l’IPS serait la meilleure solution pour répondre aux besoins des entreprises, notamment à la vue des statistiques concernant l’usage de l’IPS dans le monde.

Le guide de lecture suivant aidera le lecteur à se repérer dans le document :

|  |  |
| --- | --- |
| Le pictogramme ci-après… | …fait référence à : |
| http://thumbs.dreamstime.com/m/bulb-vector-illustration-icon-36622935.jpg | Une remarque |
|  |  |
|  |  |
|  |  |
|  |  |

Sommaire

Sommaire

1. Présentation
   1. Présentation du groupe
   2. Gantt

Chaque chapitre de niveau 1 possède son résumé qui n’est ni son intro, ni sa conclu, mais permet au lecteur de comprendre en cette lecture si le chapitre l’intéresse. Pas plus d’une demi page.

Prévoir une lecture linéaire avec accès direct à certains paragraphes.

Un plan en pyramide inversée présente l’information par ordre d’intérêt décroissant : du plus simple au plus compliqué, du plus concis au plus détaillé.

Une idée par paragraphe, détacher les paragraphes en mettant en valeur des mots ou des phrases, les relier par des intertitres.

Les phrases : courtes, passer à la ligne fréquemment, supprimer les voix passives.

1. Technologie de l’IPS

Dans cette partie, nous expliquerons les différentes technologies liées à l’IPS. Comme énoncé précédemment, il existe différentes sortes d’IPS, positionnées à différents endroits d’un réseau.

Chacune de ces technologies a des propriétés bien spécifiques. De même, chacun d’entre elles possède des avantages, comme des inconvénients. De ce fait, nous parlerons d’abord de l’IPS en général. Puis, nous évoquerons les trois types d’IPS, qui sont le NIPS, l’HIPS et le KIPS.

* 1. IPS Appliance
     1. Définition

IPS signifie « Intrusion Prevention System ». Il s’agit d’un outil basé sur la sécurité des systèmes d’information. Il s’inspire en fait de la technologie IDS. Cependant il est bien plus actif que cette dernière.

Il est dédié à une tâche de sécurité spécifique qu'est le blocage des trafics malicieux. Il agit principalement dans les couches supérieures du modèle OSI (Transport, Session, Présentation, Application).

Les types de protocoles surveillés par les solutions d'IPS peuvent être de différentes natures : réseaux (IP, TCP, UDP, ICMP, MPLS...) ou encore systèmes et applicatifs (HTTP, MIME, FTP, DHCP...).



Retrouvez la signification de ces acronymes dans le glossaire.

Ils existent donc 3 types d’IPS différents :

* Les NIPS/WIPS (« Network/Wireless Intrusion Prevention System ») qui surveillent le trafic réseau. En cas de doute, ils peuvent mettre fin à une session TCP.
* Les HIPS (Host-based Intrusion Prevention System) qui permettent de surveiller le poste de travail. Ils surveillent le processus, les driver, les .dll et en cas de détection de processus suspect, ils peuvent le détruire.
* Les KIPS (Kernel Intrusion Prevention System) qui détectent les tentatives d’intrusion au niveau du noyau de l’ordinateur.

Les IPS Appliance sont des solutions de sécurité qui réunissent pare-feu, réseaux privés et toutes les fonctionnalités de prévention des intrusions et de sécurité web.

Les IPS bloquent les menaces avant qu’elles ne pénètrent sur le réseau et endommagent les activités de l’entreprise.

Ils bloquent les visiteurs indésirables et permettent aux flux de l’entreprise de circuler. Ils prennent aussi en charge une DMZ pour héberger les serveurs importants. Ils garantissent de ce fait la sécurité du réseau interne de l’entreprise.

De même, ils permettent de contrôler l’accès aux ressources du réseau (protection des données et optimisation du temps de disponibilité du réseau). Les IPS permettent aussi d’accroitre la productivité des employés tout en sécurisant et en contrôlant l’accès au web (blocage des courriers indésirables, du phishing, des intrusions, des virus, etc...).

* + 1. Fonctionnement

L’IPS analyse les trames dans leur ensemble et non pas une par une. Il possède par ailleurs une base de connaissances sur les attaques connues.

Cela permet, grâce à une base de connaissance sur les attaques connues, de voir si certaine combinaison de trames peuvent être identifié comme une tentative d’intrusion. De plus l’IPS/IDS va garder en mémoire l’évènement afin de conserver une trace du problème et de pouvoir le résoudre plus facilement par la suite.

L’analyse de la trame est complexe. En effet elle s’effectue à l’issue d’une analyse primaire des données, c’est la remonté d’informations. Ces informations sont ensuite analysées par le SIM (Security Information Management), qui les confronte à sa base de connaissances et génère une alerte ou non.

A l’inverse de l’IDS, qui fonctionne en mode promiscuité (il réceptionne une copie du trafic sans l’influencer), L’IPS fonctionne en mode coupure de port, il ne va pas juste recenser les problèmes mais il va les bloquer en empêchant le trafic de circuler. L’IPS ne va donc pas juste détecter le problème mais il va aussi le supprimer.

* + 1. Avantages
    2. Inconvénients
  1. NIPS
     1. Définition

**NIPS** « **Network Intrusion Prevention System** »

Cette forme d’IPS permet de scanner en permanence un réseau et d’en détecter tout comportement suspect. Ainsi, il est possible d’interdire, à une machine, l’accès à un service du réseau car elle a un comportement anormal.

Par ailleurs, cet outil permet aux administrateurs de vérifier l’état de leur réseau et de vérifier qu’il fonctionne normalement. C’est en général ainsi qu’est utilisé le NIPS, on appelle alors cela un NIDS qui ne permet que la supervision et l’enregistrement des actions et non l’application de règle.

* + 1. Fonctionnement

Le NIPS agit au niveau du réseau et vérifie que chaque paquet correspond bien à la politique de sécurité mise en vigueur sur réseau. Puis, si un ou plusieurs d’entre eux ne sont pas conforment, le système NIPS va alors bloquer la source et envoyer une alerte à l’administrateur.

Comment ça marche ?

1. Un appareil envois un des paquets
2. Le NIPS intercepte les paquets
3. Le NIPS Analyse les paquets
4. Le NIPS vérifie la conformité des paquets (tailles, nombres, destination, …) dans sa base de règles.

Maintenant il existe 2 possibilités :

1. A) Le paquet est validé et continue sa route.

B) Le paquet est refusé et l’appareil est bloqué en fonction des règles mise en place.

* + 1. Avantages

Nous pouvons observer un certain nombre de point fort pour ce système :

* Détectes et bloque les intrusions
* Envois des alertes
* Possibilité de configurations très nombreuses et varié
* Analyse les paquets et les enregistres
  + 1. Inconvénients

Mais cette sécurité n’offre pas que des biens faits pour le réseau :

* Possibilité de faux-positif
* Très complexe à configurer
* Possibilité de ralentir le réseau
* La fiabilité n’est pas de 100%
* Machine dédié à ce service car énormément d’information à traiter
  1. HIPS
  2. KIPs
     1. Définition

**KIPS** «**Kernel Intrusion Prevention System** »

Cet outil permet aux administrateurs réseau de configurer une ou plusieurs réactions permettant de bloquer certaine action sur la partie du système d’exploitation d’une machine.

Le KIPS agit directement sur le « Noyaux » d’un système ce qui permet de réguler les actions et de prévenir toute défaillance ou attaque. En effet, le KIPS va vérifier chaque appel vers le système et va ainsi détecter un comportement anormal et en stopper ces actions.

Le KIPS permet par exemple de protéger un serveur web en restreignant la lecture et l’écriture des fichiers juste à la partie du service web et ainsi empêcher toute possibilité d’ouverture de « shell » de commande et de lecture sur le reste du serveur.

L’outil KIPS peut aussi détecter toutes les modifications de performance de la machine telle qu’une utilisation trop importante de mémoire et stopper le logiciel ou l’outil entrainant cette utilisation.

* + 1. Fonctionnement

Le KIPS fonctionnant sur le système d’exploitation d’une machine, va analyser toutes les actions entrant et sortant de celui-ci et pourra alors vérifier qu’elles apparaissent bien dans sa base de règle de sécurité. Si elles sont autorisées, le système les laisse s’effectuer sinon elles sont bloquées et enregistré.

Comment ça marche ?

1. La machine initialise une action système
2. L’outil KIPS analyse la commande
3. KIPS vérifie dans sa base de règle si la commande est autorisé

A présent deux possibilité

1. A) L’action est autorisé et est exécutée

B) L’action est refusé et enregistre le problème

* + 1. Avantages

Comme pour tout outil développé le KIPS possède certain avantage :

* Détecte et bloque les commandes douteuses
* Envoie une alerte en cas de problème
* Possibilité de configuration nombreuse
* Ajoute des règles de sécurité supplémentaire
  + 1. Inconvénients

Et bien entendue cet outils possède des inconvénients :

* Ralenti la machine car vérifie chaque action et dépendance
* Possibilité de faux-positif
* Rarement utiliser sur des serveurs souvent sollicité
* Complexe à configurer
  1. Localisation sur un réseau

1. Acteurs du marché
   1. Identification des constructeurs
   2. Identification des Produits
   3. Identification des OS et machines physiques
2. Parts de marché
   1. Répartition sur le marché Mondial
   2. Répartition sur le marché Européen
   3. Répartition sur le marché Français
3. Implantations
   1. Mondiale
   2. Europe
   3. France
4. Références
   1. Identification des types de clients
   2. Les grands noms parmi les clients

Conclusion

Bien organisée, dénoue l’étude écrite et le retour d’expérience permet de comprendre le choix des sources, la méthodologie et l’intérêt pour l’entreprise d’accueil de chaque membre du binôme. Cette conclusion en français précède la même conclusion en anglais. Cette conclusion est le résultat de la réflexivité clairvoyante et éveillée du binôme (auteur dudit document).

ICI : Version anglaise !

Glossaire

Seuls les mots et acronymes utilisés dans le document sont cités dans le glossaire. Ce glossaire doit être rédigé dans l’ordre alpha.

Protocoles :

IP : Internet Protocol

TCP : Transmission Control Protocol

UDP : User Datagram Protocol

ICMP : Internet Control Message Protocol

MPLS : MultiProtocol Label Switching

HTTP : Hypertext Transfer Protocol

MIME : Multipurpose Internet Mail Extensions

FTP : File Transfer Protocol

DHCP : Dynamic Host Configuration Protocol

Bibliographie

(+ webographie)

Chaque ouvrage et site sont codifiés. Seuls les ouvrages cités dans le doc sont décrit dans la bibliographie. Exemple de codification : [12] ou [Gotlieb75] dont l’auteur est Gotlieb a édité son ouvrage en 1975.

Annexes

Les annexes peuvent être un autre document non relié au document lui mêmes. Ces annexes paginées doivent avoir un lien avec l’étude du sujet et doivent être organisées dans l’ordre d’utilisation dans le texte du doc. Un sommaire des annexes est nécessaire.

Annexes – Sommaire

Summary