Nicolas Baudoin
Marion Karle

Ingénieurs2000
2003-2004

NT Réseaux

IDS et IPS

Enseignant : Etienne Duris 2003/2004 IR3

Table des matières

Introduction

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

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

C'est pourquoi, avant de présenter les concepts d'IDS et d'IPS, nous allons tout d'abord rappeler quelques notions de sécurité concernant la mise en place d'une politique de sécurité et les attaques qu'un réseau d'entreprise peut subir.

Nous présenterons ensuite le concept d'IDS, les différents types d'IDS, leur mode de fonctionnement…
Nous verrons alors que ces outils ont certaines limitations en présentant quelques méthodes de contournement d'un IDS.

Ceci nous mène aux IPS, censés pallier à ces faiblesses, qui seront présentés dans une dernière partie.

1. Notions de sécurité

Avant de présenter le concept d'IDS, nous allons tout d'abord rappeler quelques notions sur la mise en œuvre d'une politique de sécurité et sur les attaques existantes.

1.1 Mise en place d'une politique de sécurité

La mise en œuvre d'une politique de sécurité globale est assez difficile, essentiellement par la diversité des aspects à considérer. Une politique de sécurité peut se définir par un certain nombre de caractéristiques : les niveaux où elle intervient, les objectifs de cette politique et enfin les outils utilisés pour assurer cette sécurité.
Chaque aspect différent doit être pris en compte, de façon à atteindre les objectifs de sécurité désirés, en utilisant de façon coordonnée les différents outils à disposition.

Nous allons tout d'abord parler des différents aspects d'une politique de sécurité, avant de définir les objectifs visés, puis de voir les outils disponibles pour appliquer cette politique.

1.1.1 Différents aspects de la sécurité

Une politique de sécurité s'élabore à plusieurs niveaux.

On va tout d'abord sécuriser l'accès aux données de façon logicielle (authentification, contrôle d'intégrité).

On va également sécuriser l'accès physique aux données : serveurs placés dans des salles blindées (qui empêchent les ondes électro-magnétiques d'être captées) avec badge d'accès…

Un aspect très important pour assurer la sécurité des données d'une entreprise est de sensibiliser les utilisateurs aux notions de sécurité, de façon à limiter les comportements à risque : si tout le monde peut accéder aux salles de serveurs, peut imposte qu'elles soient sécurisées !
De même, si les utilisateurs laissent leur mot de passe écrit à côté de leur PC, son utilité est limitée…

Enfin, il est essentiel pour un responsable de sécurité de s'informer continuellement, des nouvelles attaques existantes, des outils disponibles…de façon à pouvoir maintenir à jour son système de sécurité et à combler les brèches de sécurité qui pourraient exister.

1.1.2 Objectifs

Les objectifs d'une politique de sécurité sont de garantir la sécurité des informations et du réseau de l'entreprise.

Ces impératifs peuvent être définis à plusieurs niveaux :
-Disponibilité : les données doivent rester accessibles aux utilisateurs (une attaque de type DoS, par exemple, vise à empêcher les utilisateurs normaux d'un service d'y accéder)
-Confidentialité : les données ne doivent être visibles que des personnes habilitées pour.
-Intégrité : il faut pouvoir garantir que les données protégées n'ont pas été modifiées par une personne non autorisée.
-Non répudiation : on doit pouvoir certifier, quand un fichier a subi des modifications, la personne qui l'a modifié.

1.1.3 Outils

Pour assurer une bonne protection des données d'une entreprise, différents outils sont disponibles. Ils ont en général utilisés ensemble, de façon à sécuriser les différentes failles existantes dns un système.

On va tout d'abord utiliser un firewall, qui permet de filtrer le trafic réseau entrant sur le réseau de l'entreprise.
Les antivirus seront plutôt utilisé sur les différentes machines branchées sur le réseau afin de vérifier si des virus ont pu se propager.
On dispose également d'agents d'authentification afin de contrôler l'accès aux données et aux ressources.
Enfin , ces dernières années, de plus en plus d'entreprises ont mis en place des systèmes de détection d'intrusion afin de limiter les attaques sur leurs réseaux.
De plus pour transporter les données entre différentes agences d'une même entreprise, les VPN (Virtual Private Network) sont de plus en plus utilisés, car ils permettent un cryptage des données qui transitent sur un réseau public.

Tous ces outils sont complémentaires et surveillent un aspect précis du réseau qui peut être sensible aux attaques. Nous allons maintenant présenter rapidement les types d'attaques existants.

1.2 Les attaques

1.2.1 Les différentes étapes d'une attaque

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma :

Identification de la cible : cette étape est indispensable à toute attaques organisée, elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'utilisation des bases Whois, l'interrogation des serveurs DNS,….

Le scanning : l'objectif est de compléter les informations réunies sur une cible visées. Il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée (OS, versions des services, subnet, règles de firewall….). Il faut noter que certaines techniques de scans particulièrement agressives sont susceptibles de mettre à mal un réseau et entraîner la défaillance de certains systèmes.

L'exploitation : Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau.

La progression : Il est temps pour l'attaquant de réaliser ce pourquoi il a franchit les précédentes étapes. Le but ultime étant d'élever ses droits vers root (ou system) sur un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations, installation de backdoors, nettoyage des traces ,…).

1.2.2 Les différents types d'attaques

Il existe un grand nombre d'attaques permettant à une personne mal intentionnée de s'approprier des ressources, de les bloquer ou de les modifier. Certaines requièrent plus de compétences que d'autres, en voici quelques unes :

Le sniffing
Grâce à un logiciel appelé "sniffer", il est possible d'intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées. Si quelqu'un se connecte par telnet par exemple à ce moment-là, son mot de passe transitant en clair sur le net, il sera aisé de le lire. De même, il est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception. Une restriction de cette technique est de se situer sur le même réseau que la machine ciblée.

L'IP spoofing
Cette attaque est difficile à mettre en œuvre et nécessite une bonne connaissance du protocole TCP. Elle consiste, le plus souvent, à se faire passer pour une autre machine en falsifiant son adresse IP de manière à accéder à un serveur ayant une "relation de confiance" avec la machine "spoofée". Cette attaque n'est intéressante que dans la mesure où la machine de confiance dont l'attaquant à pris l'identité peut accéder au serveur cible en tant que root.

Le DoS (Denial of Service)

Le DoS est une attaque visant à générer des arrêts de service et donc à empêcher le bon fonctionnement d'un système. Cette attaque ne permet pas en elle-même d'avoir accès à des données. En général, le déni de service va exploiter les faiblesses de l'architecture d'un réseau ou d'un protocole. Il en existe de plusieurs types comme le flooding, le TCP-SYN flooding, le smurf ou le débordement de tampon (buffer-overflow).

Les programmes cachés ou virus

Il existe une grande variété de virus. On ne classe cependant pas les virus d'après leurs dégâts mais selon leur mode de propagation et de multiplication. On recense donc les vers (capables de se propager dans le réseau), les troyens (créant des failles dans un système), Les bombes logiques (se lançant suite à un événement du système (appel d'une primitive, date spéciale)).

L'ingénierie sociale (social engineering)

Ce n'est pas vraiment une attaque informatique en soit, mais plutôt une méthode consistant à se faire passer pour quelqu'un que l'on n'est pas afin de recueillir des informations confidentielles.

Le craquage de mots de passe

Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne). Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machines.

2. Les IDS

Tout d'abord, IDS signifie Intrusion Detection System. Il s'agit d'un équipement permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion et éventuellement de réagir à cette tentative.

Pour présenter le concept d'IDS, nous allons tout d'abord présenter les différentes sortes d'IDS, chacun intervenant à un niveau différent.
Nous étudierons ensuite leur mode de fonctionnement, c'est à dire les modes de détection utilisés et les réponses apportées par les IDS. Enfin, nous détaillerons les points forts et les points faibles des IDS.

2.1 Les différentes sortes d'IDS

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

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

2.1.1 La détection d'intrusion basée sur l'hôte

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

De plus, l'impact sur la machine concernée est sensible immédiatement, par exemple dans le cas d'une attaque réussie par un utilisateur. Ces IDS utilisent deux types de sources pour fournir une information sur l'activité de la machine : les logs et les traces d'audit du système d'exploitation.
Chacun a ses avantages : les traces d'audit sont plus précises et détaillées et fournissent une meilleure information alors que les logs qui ne fournissent que l'information essentielle sont plus petits.
Ces derniers peuvent être mieux contrôlés et analysés en raison de leur taille, mais certaines attaques peuvent passer inaperçues, alors qu'elles sont détectables par une analyse des traces d'audit.

Ce type d'IDS possèdent un certain nombre d'avantages : il est possible de constater immédiatement l'impact d'une attaque et donc de mieux réagir. Grâce à la quantité des informations étudiées, il est possible d'observer les activités se déroulant sur l'hôte avec précision et d'optimiser le système en fonction des activités observées.

De plus, les HIDS sont extrêmement complémentaires des NIDS. En effet, ils permettent de détecter plus facilement les attaques de type "Cheval de Troie", alors que ce type d'attaque est difficilement détectable par un NIDS. Les HIDS permettent également de détecter des attaques impossibles à détecter avec un NIDS, car elles font partie de trafic crypté.

Néanmoins, ce type d'IDS possède également ses faiblesses, qui proviennent de ses qualités : du fait de la grande quantité de données générées, ce type d'IDS est très sensible aux attaques de type DoS, qui peuvent faire exploser la taille des fichiers de logs.
Un autre inconvénient tient justement à la taille des fichiers de rapport d'alertes à examiner, qui est très contraignante pour le responsable sécurité. La taille des fichiers peut en effet atteindre plusieurs Mégaoctets.
Du fait de cette quantité de données à traiter, ils sont assez gourmand en CPU et peuvent parfois altérer les performances de la machine hôte.
Enfin, ils ont moins de facilité à détecter les attaques de type hôte que les IDS réseaux.

Les HIDS sont en général placés sur des machines sensibles, susceptibles de subir des attaques et possédant des données sensibles pour l'entreprise. Les serveurs, web et applicatifs, peuvent notamment être protégés par un HIDS.

Pour finir, voici quelques HIDS connus: Tripwire, WATCH, DragonSquire, Tiger, Security Manager…

2.1.2 Détection d'Intrusion basée sur une application

Les IDS basés sur les applications sont un sous-groupe des IDS hôtes.
Ils contrôlent l'interaction entre un utilisateur et un programme en ajoutant des fichiers de log afin de fournir de plus amples informations sur les activités d'une application particulière. Puisque vous opérez entre un utilisateur et un programme, il est facile de filtrer tout comportement notable. Un ABIDS se situe au niveau de la communication entre un utilisateur et l'application surveillée.

L'avantage de cet IDS est qu'il lui est possible de détecter et d'empêcher des commandes particulières dont l'utilisateur pourrait se servir avec le programme et de surveiller chaque transaction entre l'utilisateur et l'application. De plus, les données sont décodées dans un contexte connu, leur analyse est donc plus fine et précise.

Par contre, du fait que cet IDS n'agit pas au niveau du noyau, la sécurité assurée est plus faible, notamment en ce qui concerne les attaques de type "Cheval de Troie".

De plus, les fichiers de log générés par ce type d'IDS sont des cibles faciles pour les attaquants et ne sont pas aussi sûrs, par exemple, que les traces d'audit du système.

Ce type d'IDS est utile pour surveiller l'activité d'une application très sensible, mais son utilisation s'effectue en général en association avec un HIDS. Il faudra dans ce cas contrôler le taux d'utilisation CPU des IDS afin de ne pas compromettre les performances de la machine.

2.1.3 La Détection d'Intrusion Réseau (NIDS)

Le rôle essentiel d'un IDS réseau est l'analyse et l'interprétation des paquets circulant sur ce réseau.
L'implantation d'un NIDS sur un réseau se fait de la façon suivante : des capteurs sont placés aux endroits stratégiques du réseau et génèrent des alertes s'ils détectent une attaque. Ces alertes sont envoyées à une console sécurisée, qui les analyse et les traite éventuellement. Cette console est généralement située sur un réseau isolé, qui relie uniquement les capteurs et la console.

Les capteurs

Les capteurs placés sur le réseau sont placés en mode furtif (ou stealth mode), de façon à être invisibles aux autres machines. Pour cela, leur carte réseau est configurée en mode "promiscuous", c'est à dire le mode dans lequel la carte réseau lit l'ensemble du trafic, de plus aucune adresse IP n'est configurée.

Un capteur possède en général deux cartes réseaux, une placée en mode furtif sur le réseau, l'autre permettant de le connecter à la console de sécurité.
Du fait de leur invisibilité sur le réseau, il est beaucoup plus difficile de les attaquer et de savoir qu'un IDS est utilisé sur ce réseau.

Placer les capteurs

Il est possible de placer les capteurs à différents endroits, en fonction de ce que l'on souhaite observer. Les capteurs peuvent être placés avant ou après le pare-feu, ou encore dans une zone sensible que l'on veut protéger spécialement.

Si les capteurs se trouvent après un pare-feu, il leur est plus facile de dire si le pare-feu a été mal configuré ou de savoir si une attaque est venue par ce pare-feu.
Les capteurs placés derrière un pare-feu ont pour mission de détecter les intrusions qui n'ont pas été arrêtées par ce dernier. Il s'agit d'une utilisation courante d'un NIDS.

Il est également possible de placer un capteur à l'extérieur du pare-feu (avant le firewall). L'intérêt de cette position est que le capteur peut ainsi recevoir et analyser l'ensemble du trafic d'Internet. Si vous placez le capteur ici, il n'est pas certain que toutes les attaques soient filtrées et détectées. Pourtant, cet emplacement est le préféré de nombreux experts parce qu'il offre l'avantage d'écrire dans les logs et d'analyser les attaques (vers le pare-feu...), ainsi l'administrateur voit ce qu'il doit modifier dans la configuration du pare-feu.

Les capteurs placés à l'extérieur du pare-feu servent à détecter toutes les attaques en direction du réseau, leur tâche ici est donc plus de contrôler le fonctionnement et

la configuration du firewall que d'assurer une protection contre toutes les intrusions détectées (certaines étant traitées par le firewall).

Il est également possible de placer un capteur et un autre après le firewall. En fait, cette variante réunit les deux cas mentionnés ci-dessus. Mais elle est très dangereuse si on configure mal les capteurs et/ou le pare-feu, en effet on ne peut simplement ajouter les avantages des deux cas précédents à cette variante.

Les capteurs IDS sont parfois situés à l'entrée de zones du réseau particulièrement sensibles (parcs de serveurs, données confidentielles…), de façon à surveiller tout trafic en direction de cette zone.

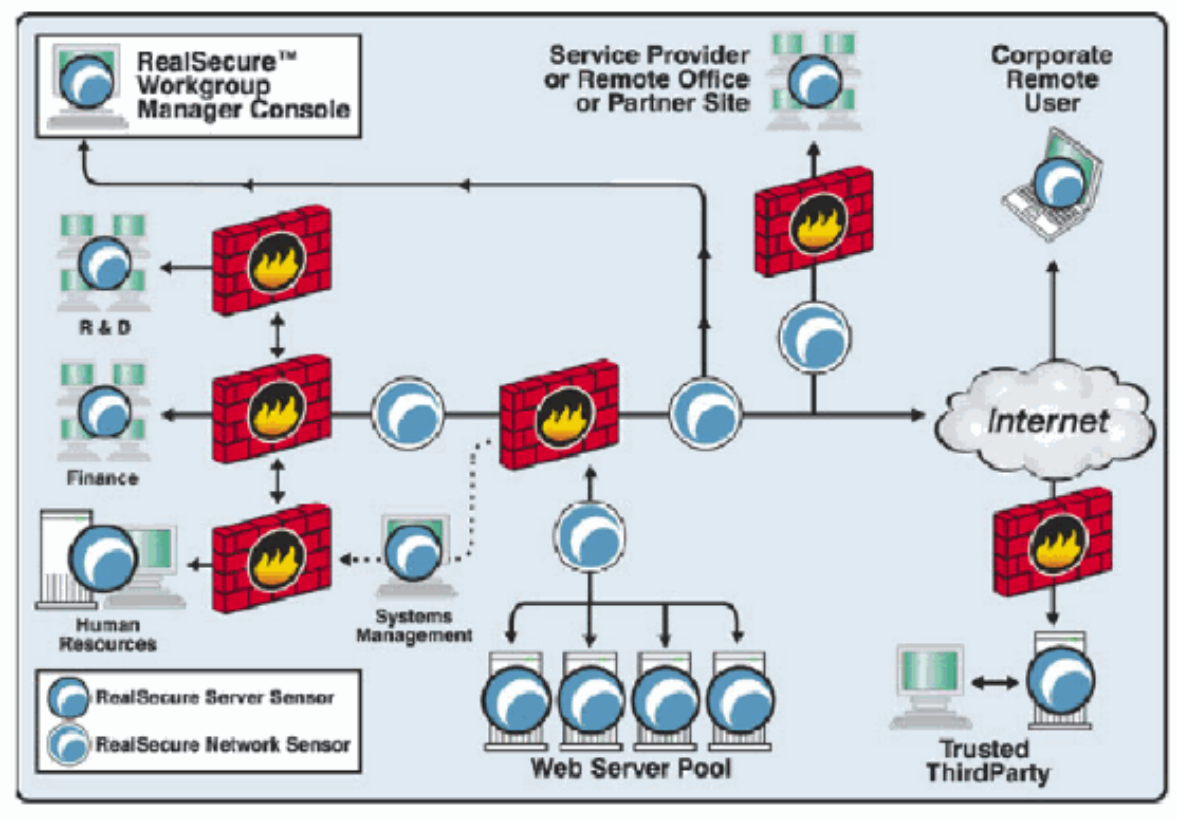
Les avantages des NIDS sont les suivants : les capteurs peuvent être bien sécurisés puisqu'ils se contentent d'observer le trafic et permettent donc une surveillance discrète du réseau, les attaques de type scans sont facilement détectées, et il est possible de filtrer le trafic.

Les NIDS sont très utilisés et remplissent un rôle indispensable, mais ils présentent néanmoins de nombreuses faiblesses. En effet, la probabilité de faux négatifs (attaques non détectées comme telles) est élevée et il est difficile de contrôler le réseau entier. De plus, ils doivent principalement fonctionner de manière cryptée d'où une complication de l'analyse des paquets. Pour finir, à l'opposé des IDS basés sur l'hôte, ils ne voient pas les impacts d'une attaque

Voici quelques exemples de NIDS : NetRanger, Dragon, NFR, Snort, ISSRealSecure.

Même si nous distinguons HIDS et NIDS, la différence devient de plus en plus réduite puisque les HIDS possèdent maintenant les fonctionnalités de base des NIDS. Des IDS bien connus comme ISS RealSecure se nomment aujourd'hui "IDS hôte et réseau". Dans un futur proche la différence entre les deux systèmes deviendra de plus en plus faible (ces sytèmes vont évoluer ensemble).

Voici un exemple de mise en place d'un IDS RealSecure avec des IDS hôtes et réseaux connectés à une console de management centrale (sur le schéma, les HIDS sont appelés RealSecure Server Sensor et les NIDS RealSecure Network Sensor).



Exemple d'architecture HIDS/NIDS

2.1.4 Système de Détection d'Intrusion de Nœud Réseau (NNIDS)

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

Une autre différence entre NNIDS et NIDS vient de ce que le NIDS fonctionne en mode "promiscuous", ce qui n'est pas le cas du NNIDS. Celui-ci n'étudie que les paquets à destination d'une adresse ou d'une plage d'adresse. Puisque tous les paquets ne sont pas analysés, les performances de l'ensemble sont améliorées.

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

De nouveaux types d'IDS sont conçus actuellement, comme les IDS basés sur la pile, qui étudie la pile d'un système. Le secteur des IDS est en plein développement, le besoin des entreprises en sécurité réseaux étant de plus en plus pressant, du fait de la multiplication des attaques.

Actuellement, les IDS les plus employés sont les NIDS et HIDS, de plus en plus souvent en association. Les ABIDS restent limités à une utilisation pour des applications extrêmement sensibles.

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

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

2.2 Mode de fonctionnement d'un IDS

Il faut distinguer deux aspects dans le fonctionnement d'un IDS : le mode de détection utilisé et la réponse apportée par l'IDS lors de la détection d'une intrusion.

Il existe deux modes de détection, la détection d'anomalies et la reconnaissance de signatures. Deux mêmes, deux types de réponses existent, la réponse passive et la réponse active. Il faut noter que les différents IDS présents sur le marché ne disposent pas toujours de l'ensemble des fonctionnalités présentées ici.

Nous allons tout d'abord étudier les modes de détection d'un IDS, avant de présenter les réponses possibles à une attaque.

2.2.1 Modes de détection

Il faut noter que la reconnaissance de signature est le mode de fonctionnement le plus implémenté par les IDS du marché. Cependant, les nouveaux produits tendent à combiner les deux méthodes pour affiner la détection d'intrusion.

La détection d'anomalies

Elle consiste à détecter des anomalies par rapport à un profil "de trafic habituel". La mise en oeuvre comprend toujours une phase d'apprentissage au cours de laquelle les IDS 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.

Dans le cas d'HIDS, ce type de détection peut être basé sur des information telles que le taux d'utilisation CPU, l'activité sur le disque, les horaires de connexion ou d'utilisation de certains fichiers (horaires de bureau…)

La reconnaissance de signature

Cette approche consiste à rechercher dans l'activité de l'élément surveillé les empreintes (ou signatures) d'attaques connues. Ce type d'IDS 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.

Il est possible d'élaborer des signatures plus génériques, qui permettent de détecter les variantes d'une même attaque, mais cela demande une bonne connaissance des attaques et du réseau, de façon à stopper les variantes d'une attaque et à ne pas gêner le trafic normal du réseau

Une signature permet de définir les caractéristiques d'une attaque, au niveau des paquet (jusqu'à TCP ou UDP) ou au niveau protocole (HTTP, FTP…).

Au niveau paquet, l'IDS va analyser les différents paramètres de tous les paquets transitant et les comparer avec les signatures d'attaques connues.

Au niveau protocole, l'IDS va vérifier au niveau du protocole si les commandes envoyées sont correctes ou ne contiennent pas d'attaque. Cette fonctionnalité a surtout été développée pour HTTP actuellement.

Nous allons maintenant étudier un exemple d'élaboration de signature trouvé sur Internet.

Exemple d'analyse d'une intrusion

Il s'agit d'un cas réel, présenté par Karen Kent Frederick dans ses articles situés sur securityfocus.com.

Il s'agit de l'attaque d'un réseau par un réseau de type ver, qui utilisait une attaque de type syn-scan. Les paquets contenant cette attaque avaient les caractéristiques suivantes :

-Diverses adresses IP sources
-TCP port source 21, port destination 21
-Type of service 0
-Numéro d'identification IP 39426

-Flags SYN et FIN positionnés
-Numéros de séquence divers
-Numéros d'acquittement divers
-Taille de la fenêtre TCP 1028
On remarque que ce paquet comporte plusieurs caractéristiques bizarres : les flags SYN et FIN sont positionnés (SYN indique une demande de connexion et FIN une demande de déconnexion), la taille de la fenêtre est fixe, alors qu'elle est normalement négociée en fonction de la quantité de données à envoyer et de l'espace de réception disponible.
De plus, les ports source et destination sont les mêmes (on dit qu'ils sont réflexifs), ce qui ne se produit pas normalement lors d'une connexion ftp. Le flag d'acquittement n'est pas positionné, pourtant un numéro d'acquittement est défini, le numéro d'identification du paquet est toujours le même…

Ce paquet comporte donc de nombreuses caractéristiques qui peuvent être exploitées pour former une signature de détection de cette attaque.

On va donc conserver ses caractéristiques les plus saillantes afin de limiter le temps d'analyse des paquets (en effet, plus il y a de paramètres à analyser, plus cette analyse va durer).
On va prendre les trois paramètres les plus adaptés pour détecter cette attaque : on va prendre tout d'abord les flags SYN et FIN positionnés ensemble, car aucun paquet normal de devrait avoir ce type de signalisation. On va également choisir comme caractéristiques le numéro d'identification IP fixe (39426) et la taille de fenêtre fixe, également très suspects.

Voici les caractéristiques de la signature :
-Uniquement les flags SYN and FIN positionnés
-Numéro d'identification IP 39426
-Taille de la fenêtre TCP 1028

Nous avons donc élaboré une signature, qui va permettre d'identifier toute tentative d'attaque de ce type. Dans le cas étudié, cette signature a fonctionné pendant quelques semaines, jusqu'au jour où une variante de cette attaque est survenue.

Ses caractéristiques étaient très semblables à la première attaque, mais suffisamment différente pour ne pas être détectée par la signature. Il était donc nécessaire d'élaborer une nouvelle signature qui permettrait de détecter les deux attaques ainsi que les variantes qui pourraient survenir.

Les différences entre le première et la deuxième attaque étaient les suivantes :

-Seulement le flag SYN positionné
-La taille de la fenêtre TCP fixée à 40
-Port réflexif 53

On élabore alors une signature qui reprend à la fois les caractéristiques de la première attaque et de la deuxième.

Pour cette nouvelle signature, on va prendre une caractéristique commune (flag ACK non positionné et valeur d'acquittement non nulle) ainsi qu'une caractéristique de chacune des attaques : flags SYN et FIN positionnés pour la première attaque, taille de fenêtre inférieure à un seuil (incluant 40 octets) pour la deuxième.
La nouvelle signature présente les caractéristiques suivantes :
-Valeur d'acquittement non nulle et flag ACK non positionné
-Uniquement les flags SYN and FIN positionnés
-Taille de la fenêtre TCP en dessous d'une certaine valeur
Cette signature s'est avérée performante pour arrêter les deux attaques connues et également arrêter une troisième variante sans avoir besoin de modifier la signature précédemment établie.

Cet exemple nous a semblé très formateur sur le rôle des signatures et leur élaboration. Il faut savoir que les sites des vendeurs d'IDS proposent des mises à jour des signatures en fonction des nouvelles attaques identifiées.
Néanmoins, plus il y a de signatures différentes à tester, plus le temps de traitement sera long, l'utilisation de signatures plus élaborées peut donc procurer un gain de temps appréciable.
Cependant, une signature mal élaborée peut ignorer des attaques réelles ou identifier du trafic normal comme étant une attaque. Il convient donc de manier l'élaboration de signatures avec précaution, et en ayant de bonnes connaissances sur le réseau surveillé et les attaques existantes.

Une fois une attaque détectée, un IDS a le choix entre plusieurs types de réponses, que nous allons maintenant détailler.

2.2.2 Réponse active et passive

Il existe deux types de réponses, suivant les IDS utilisés. La réponse passive est disponible pour tous les IDS, la réponse active est plus ou moins implémentée.

Réponse passive

La réponse passive d'un IDS consiste à enregistrer les intrusions détectées dans un fichier de log qui sera analysé par le responsable sécurité.
Certains IDS permettent de logger l'ensemble d'une connexion identifiée comme malveillante.
Ceci permet de remédier aux failles de sécurité pour empêcher les attaques enregistrées de se reproduire, mais elle n'empêche pas directement une attaque de se produire.

Réponse active

La réponse active au contraire a pour but de stopper une attaque au moment de sa détection. Pour cela on dispose de deux techniques : la reconfiguration du firewall et l'interruption d'une connexion TCP.

La reconfiguration du firewall permet de bloquer le trafic malveillant au niveau du firewall, en fermant le port utilisé ou en interdisant l'adresse de l'attaquant. Cette fonctionnalité dépend du modèle de firewall utilisé, tous les modèles ne permettant pas la reconfiguration par un IDS. De plus ,cette reconfiguration ne peut se faire qu'en fonction des capacités du firewall.

L'IDS peut également interrompre une session établie entre un attaquant et sa machine cible, de façon à empêcher le transfert de données ou la modification du système attaqué.
Pour cela l'IDS envoie un paquet TCP reset aux deux extrémités de la connexion (cible et attaquant). Un paquet TCP reset a le flag RST de positionné, ce qui indique une déconnexion de la part de l'autre extrémité de la connexion. Chaque extrémité en étant destinataire, la cible et l'attaquant pensent que l'autre extrémité s'est déconnectée et l'attaque est interrompue.

Dans le cas d'une réponse active, il faut être sûr que le trafic détecté comme malveillant l'est réellement, sous peine de déconnecter des utilisateurs normaux. En général, les IDS ne réagissent pas activement à toutes les alertes. Ils ne répondent à des alertes que quand celles-ci sont positivement certifiées comme étant des attaques. L'analyse des fichiers d'alertes générés est donc une obligation pour analyser l'ensemble des attaques détectées.

2.3 Points forts/Points faibles

Nous allons pour finir cette présentation des IDS résumer les points forts et les points faibles de ces équipements.

2.3.1 Points forts

Une surveillance continue et détaillée

Dans cette optique, nous nous intéressons aux flux valides, mais aussi au flux non-valides qui transitent sur le réseau dont nous avons la responsabilité. Comment savoir si les règles d'un firewall sont valides ? Comment savoir le nombre d'attaques subies au cours de la dernière semaine ? Comment différencier une surcharge normale du réseau d'une attaque par DoS ?

Les IDS vont permettre de répondre à ces questions. Ce sont des sondes en mode promiscuité. Ils peuvent donc analyser tout le trafic (dans le même domaine de collision), et relever des attaques, alors même qu'ils n'en sont pas la cible directe.

Bien sûr, nous évoquons ici le fonctionnement des NIDS. Les HIDS vont au contraire établir une surveillance unique du système sur lequel ils sont installés. De plus, toutes les alertes sont stockées soit dans un fichier, soit dans une base de données, ce qui permet de concevoir un historique, et d'établir des liens entre différentes attaques.

Ainsi, le responsable sécurité n'a pas besoin de surveiller le réseau en permanence pour être au courant de ce qui se passe. Une attaque de nuit ne passera plus inaperçue. Tous les IDS renvoient de nombreuses informations avec une alerte. Le type supposé d'attaque, la source, la destination, ... Tout cela permet un bonne compréhension d'un incident sécurité, et en cas de faux-positif, de le détecter rapidement

Un autre point important dans la sécurité : nous avons maintenant des outils de filtrage très intéressants qui nous permettent de faire du contrôle par protocole (icmp, tcp, udp), par adresse IP, jusqu'à du suivi de connexion (couches 3 et 4). Même si cela écarte la plupart des attaques, cela est insuffisant pour se protéger des attaques passant par des flux autorisés. Si cela est assez marginal, car difficile à mettre en place, l'ouverture de l'informatique au grand public et l'augmentation de ce type de connaissances font qu'il faudra un jour savoir s'en protéger efficacement.

Modularité de l'architecture

Il y a plusieurs solutions pour le positionnement de sondes réseaux. Il peut être intéressant de positionner les sondes pour étudier l'efficacité des protections mises en place.

Par exemple dans un réseau se cachant derrière un firewall, nous mettrons une sonde côté extérieur du firewall, et une autre côté intérieur du firewall. La première sonde permet de détecter les tentatives d'attaques dirigées contre le réseau surveillé. La seconde sonde va remonter les attaques (préalablement détectées par la première sonde) qui ont réussi à passer le firewall. On peut ainsi suivre une attaque sur un réseau, voir si elle arrive jusqu'à sa victime, en suivant quel parcours, ...

Il est aussi intéressant de définir des périmètres de surveillance d'une sonde. Ce sera en général suivant un domaine de collision, ou sur des entrées uniques vers plusieurs domaines de collision (par exemple à l'entrée d'un commutateur).
Par cette méthode, nous réduisons le nombre de sondes, car il n'y a pas de doublons dans la surveillance d'une partie du réseau. Une alerte n'est remontée qu'une seule fois ce qui allège d'autant l'administration des IDS. Et pour finir, le fait de placer les sondes après les protections est plus logique, car le but premier des IDS est d'étudier les intrusions malgré les protections.

Les HIDS et les NIDS se complètent

Nous avons évoqué jusqu'ici principalement le cas des NIDS. Les IDS se cantonnent à la surveillance des systèmes sur lesquels ils sont hébergés. Mais ils sont extrêmement utiles. Par exemple dans le suivi d'une attaque évoqué précédemment, grâce aux sondes NIDS, nous pouvons suivre son parcours. Mais quel est l'impact final sur la machine ? Un NIDS ne peut pas répondre à cela, car il ne gère pas les équipements terminaux. C'est ici que le HIDS se révèle utile. De plus, la remontée d'alerte est locale et vers un manager. Ainsi, la surveillance réseau et des équipements terminaux est centralisée.

2.3.2 Points faibles

Besoin de connaissances en sécurité

La mise en place de sonde sécurité fait appel à de bonnes connaissances en sécurité. L'installation en elle-même des logiciels est à la portée de n'importe quel informaticien. En revanche l'exploitation des remontées d'alertes nécessite des connaissances plus pointues.

Les interfaces fournissent beaucoup d'informations, et permettent des tris facilitant beaucoup le travail, mais l'intervention humaine est toujours indispensable.
A partir des remontées d'alertes, quelle mesure prendre ?
Est-il utile de relever des alertes dont toutes les machines sont protégées?
Comment distinguer un faux-positif d'un véritable incident de sécurité ?
Toutes ces questions et bien d'autres doivent se poser au responsable de sécurité en charge d'un IDS.

La configuration, et l'administration des IDS nécessitent beaucoup de temps, et de connaissances. C'est un outil d'aide, qui n'est en aucun cas complètement automatisé.

Problème de positionnement des sondes

La mise en place est importante. Il faut bien définir là où placer les sondes. Il ne s'agit pas de mettre une sonde partout où l'on veut surveiller. Il faut étudier les champs de vision des sondes suivant leur placement, si on veut recouper ces champs de vision (pour par exemple faire des doublons de surveillance ou faire un suivi d'attaque), quel détail d'analyse (à l'entrée d'un réseau, ou dans chaque domaine de collision). On découpe souvent le réseau global en un LAN, une DMZ, puis Internet. Mais il faut aussi envisager les domaines de collisions, les sous-réseaux, ...

Les connaissances réseaux sont importantes. Il faut aussi faire attention à comment sont remontées les alertes (passage par un réseau sécurisé et isolé du réseau surveillé).

Vulnérabilités des sondes NIDS

De part leur fonctionnement en mode promiscuité, les sondes sont vulnérables. Elles captent tout le trafic, et même si un ping flood est réalisé sur une autre machine, les sondes NIDS le captureront aussi et donc en subiront les conséquences, comme si l'attaque leur était directement envoyée. Les DoS classiques seront donc très nocifs pour les sondes NIDS.

Le point fort de certains IDS qui est d'archiver aussi le contenu des trames ayant levées une alerte, peut aussi s'avérer un point faible. Un hôte flood avec un paquet chargé de 64000 octets, ou encore des trames de 1500 octets pour les SYN flood vont faire exploser la taille des fichiers de logs des sondes en quelques minutes.
C'est une attaque qui porte le nom *coke* qui consiste à saturer le disque dur (http://www.securiteinfo.com/attaques/hacking/coke.shtml). La seule façon de parer cette attaque est de prévoir d'importants espaces de stockages, et gérer le stockage des fichiers de logs.

Problèmes intrinsèques à la plateforme

Beaucoup d'IDS (et plus particulièrement les IDS libres) sont des logiciels reposant sur une système d'exploitation non dédié aux IDS. Ainsi, la faiblesse d'un IDS est liée à la faiblesse de la plate-forme.
Un même logiciel sera par exemple plus vulnérable sur un PC Win98 que sur un PC OpenBSD, de part la solidité de la pile IP face aux attaques, ou tout simplement de part la stabilité du système. La mise en place d'un IDS requiert donc des compétences dans la sécurisation de la plate-forme.

Une saturation de la mémoire, de la carte réseau, ou du processeur porte atteinte directement au bon fonctionnement de tout le système et donc du logiciel IDS de la machine.
Le problème de ces dysfonctionnements est que si la sonde ne peut plus remplir son rôle, le réseau n'en est pas coupé pour autant. Le responsable sécurité ne peut donc pas voir que, la sonde étant tombée, une partie du réseau n'est plus surveillée. Une redondance des surveillances sur certaines zones devrait momentanément résoudre le problème.

Comme nous venons de le voir, les IDS sont des outils indispensables à la bonne sécurité d'un réseau, néanmoins leur utilisation reste complexe et contraignante. Ces outils sont malgré tout fiables et plutôt sûrs, mais il est possible de passer outre aux réponses d'un IDS. C'est ce que nous allons voir à présent.

3. Contourner la réponse active d'un IDS

L'interruption de session provoquée par un IDS peut être contournée de plusieurs manières. La plupart d'entre elles se basent sur le laps de temps qui existe entre la détection d'une attaque et la prise en compte du TCP Reset par la machine cible.

Dans le cas où l'exploit à réaliser par un attaquant ne nécessite pas de session interactive, celui-ci pourra simplement positionner le flag PUSH au sein de ses paquets TCP.
En général, les piles TCP/IP ne délivrent pas chaque portion de données à l'application dès que celles-ci arrivent, cela revient trop cher en terme d'interruption logicielles. La pile accumule les données dans un buffer et dès que celui-ci est plein,

elle réalise un PUSH du buffer tout entier pour envoyer les données en une seule fois.

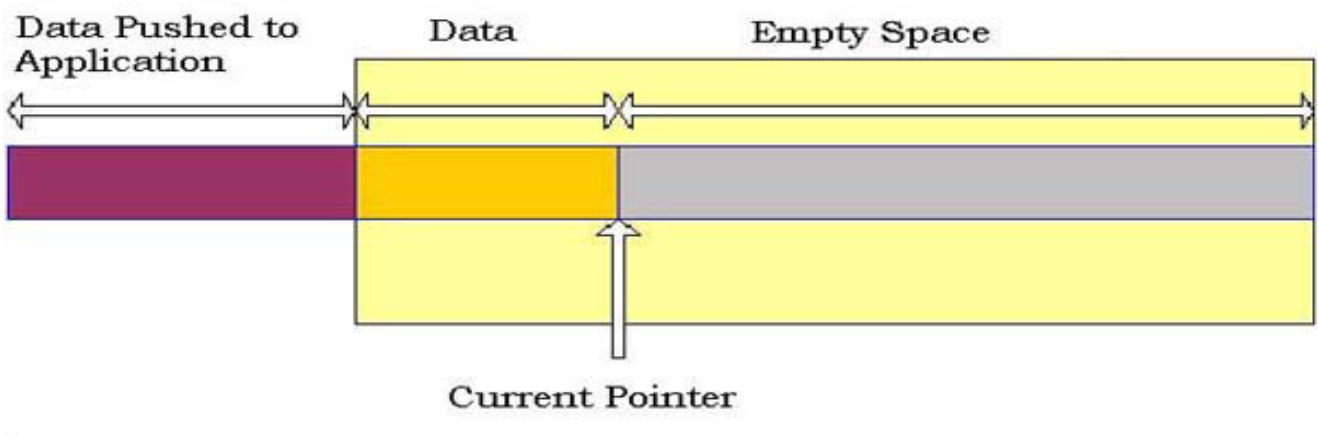
Certaines applications ont besoin de récupérer les données aussi vite qu'elles arrivent et sont prêtes à en payer le coût. Dans cette optique, le flag PUSH indique à la pile de délivrer les données à l'application aussi vite que possible.
Si un attaquant potentiel désire récupérer le contenu d'un répertoire, cela ne lui sera pas très utile car la session aura été interrompue avant que la réponse à sa requête ne soit effectuée. Par contre, si celui-ci trouve le moyen de copier le fichier hôte (par exemple) vers un répertoire accessible depuis le serveur Web du réseau, il ne s'occupera pas de savoir si la session a été interrompue ou non puisque son exploit aura réussi, simplement en positionnant le flag PUSH au sein du paquet contenant sa requête.

Si l'attaquant à besoin de conserver la session ouverte, une autre technique reste à sa disposition. L'astuce consiste à faire en sorte que la machine cible ignore le TCP Reset envoyé par l'IDS. Ce dernier croira avoir interrompu la session et l'attaquant pourra continuer son travail tranquillement.
Cette technique utilise le temps nécessaire pour un IDS de capturer le paquet, de détecter l'exploit en cours, de générer le TCP Reset et d'envoyer celui-ci sur le réseau. Une course contre la montre s'engage alors entre l'IDS et l'attaquant.

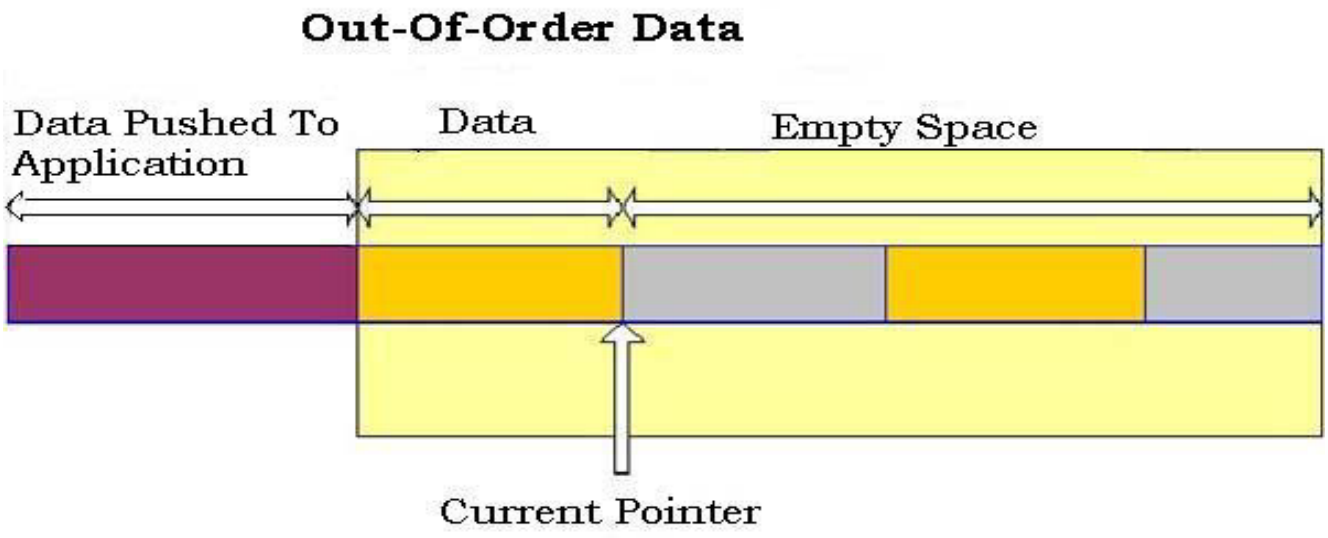
Pour que la machine cible de l'attaquant ignore le TCP Reset de l'IDS, il faut que le prochain paquet de la session engagée entre l'attaquant et la machine cible parvienne sur la machine cible avant le paquet Reset de l'IDS.

Rappel :

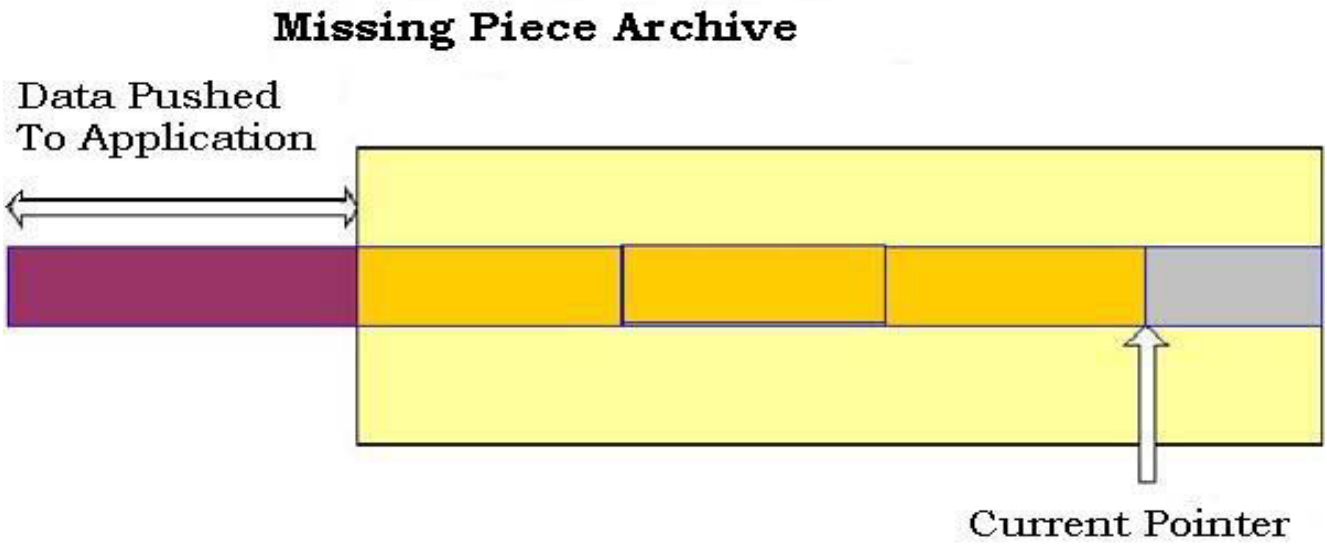
La pile TCP travaille sur une fenêtre. Certaines données reçues ont déjà été envoyées (PUSH) vers l'application et certaines attendent dans le buffer qui doit être vidé vers l'application. De plus il existe un espace vide en attente de réception de nouvelles données. Ce que l'on nomme la fenêtre n'est autre que la réunion du buffer et de l'espace vide. Seules les données présentes au sein de la fenêtre peuvent être traitées.



La pile TCP maintient également un pointeur courant (CP) qui pointe sur le prochain fragment de données que la pile s'attend à recevoir. Celui-ci correspond, de plus, au numéro d'acquittement. Par exemple, si la pile à reçu 76 octets, le numéro d'acquittement sera 77. Quand le prochain fragment de données arrivera, le pointeur courant sera immédiatement positionné à la fin de ce fragment.



Les fragments ne sont pas obligés d'arriver dans l'ordre. Un fragment commençant à l'octet 90 peut arriver avant le fragment commençant à l'octet 77, il sera copié dans le buffer mais le pointeur courant restera positionné à 77 jusqu'à ce que le fragment débutant par 77 arrive. A cet instant, le pointeur courant sera déplacé vers la fin de tous les fragments reçus, et ce en une seule fois



Sur la plupart des piles, le RESET doit coïncider avec le pointeur courant sans quoi le paquet est ignoré. En sachant cela, un attaquant peut construire un "paquet suivant" qui mettra en échec le RESET de l'IDS.
Admettons que l'attaque nécessite trois paquets. L'attaquant envoit tout d'abord les deux premiers paquets (rappelons que l'IDS à besoin des trois premiers paquets pour détecter l'attaque…).
L'attaquant va ensuite construire un quatrième paquet ne contenant aucune données menaçante au yeux de l'IDS et l'envoyer avant le troisième. A ce stade le paquet quatre sera copié dans le buffer dés son arrivée mais le pointeur courant restera positionné sur la fin du second paquet. Dès que le troisième paquet arrivera, le pointeur courant sera déplacé en une fois vers la fin du quatrième paquet.
A l'arrivée du paquet trois, l'IDS va générer et envoyer un TCP RESET basé sur le paquet trois. Celui-ci sera de toutes façons ignoré lors de sa réception par la machine cible puisqu'il ne coïncidera pas avec le pointeur courant de celle-ci (positionné sur la fin du paquet quatre).

Pour la même raison (le délai induit par la réponse active de l'IDS), il est possible de contourner la mise à jour du firewall par l'IDS. La mise à jour des règles d'un firewall prend habituellement une à deux seconde en moyenne, ce qui suffit amplement à une personne habile pour s'introduire sur une machine et y installer une "backdoor". Il ne lui reste, alors, plus qu'à changer d'adresse IP pour pouvoir administrer la machine à distance.

Les fonctions de réponses actives, peuvent s'avérer efficaces mais ne constituent en aucun cas un moyen sûr de sécuriser un réseau. N'importe qui avec un minimum de connaissances sur TCP/IP est capable de contourner les mécanismes mis en jeu.

4. Les IPS

Faute de mouvoir maîtriser correctement les fausses alertes, la plupart des systèmes actuels d'IDS sont voués à disparaître ou à évoluer grandement.
L'apparition sur le marché de la sécurité informatique des systèmes IPS est très récent et résulte de la nécessité d'améliorer, encore et toujours, les solutions existantes ayant prouvées leurs limites. Les IPS n'existent pas vraiment en tant que technologies bien définies mais plutôt en tant que concepts que tentent de mettre en œuvre les différents acteurs du marché à travers de multiples technologies et solutions de sécurité.

4.1 Principes de fonctionnement

De l'avis des analystes, le concept d'IPS (systèmes de prévention des intrusions) vise à anticiper les attaques de pirates informatiques dès lors que leur empreinte est connu. Il ne s'agit plus seulement de réagir à une attaque en cours, mais d'empêcher que celle-ci puisse seulement débuter.
Un système IPS est placé en ligne et examine en théorie tous les paquets entrants ou sortants. Il réalise un ensemble d'analyses de détection, non seulement sur chaque paquet individuel, mais également sur les conversations et motifs du réseau, en visualisant chaque transaction dans le contexte de celles qui précèdent ou qui suivent.
Si le système IPS considère le paquet inoffensif, il le transmet sous forme d'un élément traditionnel de couche 2 ou 3 du réseau. Les utilisateurs finaux ne doivent en ressentir aucun effet. Cependant, lorsque le système IPS détecte un trafic douteux il doit pouvoir activer un mécanisme de réponse adéquat en un temps record.
L'IPS doit aussi, offrir un moyen de diminuer considérablement l'utilisation des ressources humaines nécessaires au bon fonctionnement des IDS. Cela doit aboutir, notamment, à une automatisation des fonctions d'analyse des logs, même si ce point demeure encore une tâche difficile. La prise de décision doit ainsi pouvoir être automatisée non seulement grâce à la reconnaissance de signatures mais aussi, et de plus en plus, grâce à l'utilisation d'analyses heuristiques provenant du monde des anti-virus.

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

4.2 Compétences requises

Afin de pouvoir prétendre à l'appellation IPS, il faut que le produit mis en œuvre s'articule autour de fonctionnalités essentielles :

- La compréhension des réseaux IP (les architectures existantes, les protocoles utilisés…) et des couches applicatives de niveau 7 doit permettre de détecter les anomalies protocolaires qui sont synonymes d'attaques.

- La connaissance des serveurs dédiés et de leur architecture logicielle afin de les enrichir de nouvelles fonctions et de les sécuriser encore plus.

- La maîtrise des sondes réseau et l'analyse des logs dans le but de déceler les attaques et d'écrire les scripts de commande qui piloteront les firewall.

- Comprendre les besoins du client afin de consacrer en priorité la politique de défense aux fonctions vitales du réseaux de l'entreprise.

- Fonctionner à vitesse de ligne afin d'éviter tout effet néfaste sur la performance ou la disponibilité du réseau.

- Fonctionner en mode "statefull Inspection" dans le but de connaître à chaque instant le contexte de l'analyse en cours.

4.3 Exemple d'IPS : le moteur ASQ de Netasq

L'ASQ, moteur de détection et de prévention d'intrusion, est intégré dans toute la gamme des boîtiers firewalls NetASQ. Anticipant dès sa création l'évolution des technologies de sécurité Internet, les laboratoires de Recherche et Développement de NetASQ ont mis au point l'ASQ dès 1998. Ce moteur intelligent intègre un système de prévention d'intrusion (IPS : Intrusion Prevention System) qui détecte et élimine tout comportement malicieux en temps réel.

Ceci fait de chaque firewall NetASQ un outil puissant du réseau capable de protéger contre les intrusions sans avoir à rajouter d'autres éléments. L'administration de la politique de sécurité s'en trouve grandement simplifiée et donc plus performante.

Une prévention en temps Réel
L'intérêt d'avoir intégré cette technologie directement dans le firewall, est que celui ci se place en coupure sur le trajet des paquets. Contrairement à un IDS, qui se contente d'émettre des alarmes et d'envoyer des commandes RESET toujours trop tard (l'attaque est déjà passée). Le Firewall NetASQ coupe la connexion avant la transmission des derniers paquets. De ce fait l'attaque ne peut s'exécuter.

Virtualisation des couches OSI

L'ASQ n'effectue aucune désencapsulation à proprement parlé. En effet la pile IP n'est pas remontée. Donc l'ASQ réalise ses analyses sur un paquet mis en tampon. Ceci signifie que toutes les fonctions de sécurité sont réalisées au niveau du noyau sans ajout de couche supplémentaire améliorant ainsi les performances.
Une fois que toutes les analyses sont réalisées, le paquet est transmis à l'interface sortante. Le contexte de ce paquet est gardé en mémoire pour le paquet suivant. Lors du traitement du prochain paquet, l'ASQ réalisera une analyse du contexte, en

plus de l'analyse du format du paquet en lui-même. Tout paquet mal formé est détruit, tout comme les paquets participant à un contexte malicieux.

Une analyse à plusieurs niveaux

Analyse IP

Le principe de cette analyse consiste à vérifier la conformité du format des paquets et datagrammes en fonction des RFC. Cette analyse permet de vérifier l'utilisation correcte et non frauduleuse des protocoles des couches 3 et 4 du modèle OSI (réseau et transport).
Les failles de sécurité de ces protocoles proviennent pour la plupart de l'implémentation de la pile TCP/IP. Les comportements analysés à ce niveau (analyse IP) sont souvent liés à l'utilisation d'options peu ou rarement utilisées dans les communications Internet. Ces paquets « mal formés » provoquent des bugs et parfois le crash du système (Deny of Service).

Analyse des fragments

Le deuxième type de failles qui peut être exploité est le séquencement des fragments. L'analyse n'est plus effectuée au niveau du paquet en lui-même mais à un niveau d'abstraction supérieur, le datagramme. C'est désormais le fragment qui est analysé dans son environnement. C'est-à-dire la cohérence qu'il y a entre celui-ci et ceux qui suivent, ou qui précèdent.
Cette analyse cherche à vérifier qu'en assemblant les fragments le paquet obtenu reste valide. C'est à dire qu'aucun fragment ne se chevauche (recouvrement de fragment), que le paquet soit entier et ne comporte pas d'ajout effectué frauduleusement (débordement sur un fragment, trou entre fragments).

Analyse globale

Cette analyse se place à un degré d'abstraction supérieur à l'analyse des fragments mais cette fois-ci c'est le contexte des connexions qui est visé. La technologie "Statefull Inspection" basée sur la mémorisation du contexte utilisateur permet une vérification du contenu des paquets transitant par le firewall.

Filtrage (ASQ Dynamic Filtering)

Le firewall NetASQ est de type "Statefull Inspection". Cette technologie permet la conservation des contextes de connexions. L'intérêt est de pouvoir vérifier le trafic non plus au niveau paquet mais au niveau connexion. Ainsi une attaque se basant sur des paquets sains mais qui, réunis, se révèlent dangereux, sera détectée par un tel firewall. De plus cette technologie analyse le contenu des paquets à la volée et sans interruption de liaison ce qui lui assure de meilleures performances.
Pour optimiser le filtrage mis en place dans le cadre d'une politique de sécurité, NetASQ a développé un algorithme nommé SKIP. Lors de l'analyse des règles, celui-ci regroupe celles qui se suivent et qui ont un critère commun (à partir de trois règles). Le but est de sauter l'évaluation de plusieurs règles qui contiennent un critère éliminatoire. Etant donné le critère éliminatoire, l'évaluation de ces règles serait inutile (elle remontera forcément une réponse négative).

Analyse des protocoles applicatifs
L'analyse est basée sur une vérification de la conformité entre l'utilisation du protocole et sa norme. Cette norme est définie par des standards tels que les RFC's. En identifiant un tel trafic, il est possible alors d'affiner les décisions prises lors de la mise en place d'une politique de sécurité. Cette méthode est très puissante car elle permet de se prévenir d'attaques connues mais aussi inconnues. En effet tout trafic ne répondant pas aux spécifications des normes sera bloqué par cette analyse. De plus, il est intéressant de remarquer que cette analyse pourra bloquer des attaques basées sur des schémas dont la signature est connue mais qui ont été légèrement modifiés pour tromper justement les systèmes de détection uniquement basés sur la signature.
NetASQ associe à cette analyse du protocole, une analyse applicative. Cette analyse vise à établir une cohérence entre l'en-tête du paquet et la section de données de celui-ci.

La conjugaison de l'ensemble de ces analyses fait de l'ASQ un puissant analyseur temps réel de trafic sans pour autant affecter les performances globales d'un firewall NetASQ.

4.4 Bilan

Il serait illusoire de penser que les IPS constituent la parade ultime aux intrusions. D'une part, parce que le problème de la sécurité informatique existera toujours, une personne mal intentionnée , persévérante et compétente trouvera toujours un moyen de contourner, tôt ou tard les protections mises en place.
D'autre part, car les IPS mettent en œuvre des technologies immatures et qui n'ont pas encore faites leurs preuves. Beaucoup d'administrateurs hésitent encore à les intégrer dans leur réseaux fautes d'informations et de connaissance de leur fonctionnement.
De plus la diversité des technologies et des stratégies pouvant être utilisées au sein des IPS rend impossible la définition d'un standard de fait. Il est, dès lors, nécessaire de les appréhender à travers un dialogue approfondi avec leurs concepteurs (et souvent intégrateurs…) afin d'évaluer la solution la plus appropriée aux cas d'utilisations.

Même si de plus en plus de constructeurs commencent à s'intéresser à la protection de protocoles variées, la plupart des IPS du marché sont encore largement orientées autour du port 80 et souvent inefficaces contre des attaques portés sur d'autres protocoles que le http.

A la mode, les IPS sont présents sous de nombreuses formes, on retrouve ainsi énormément de solutions "tout en un" pouvant mêler pare-feu, VPN, IDS et anti-virus. Certains pouvant même y intégrer des fonctions anti-spams. Il faut alors faire

attention à la mise en œuvre car l'utilisation de certains anti-virus heuristiques, par exemple, peut faire chuter dramatiquement les performances.
L'effet marketing est très important, il est à l'origine des IPS, on prendra donc garde de bien étudier un produit et les personnes qui l'ont conçues avant de l'intégrer dans sa politique de sécurité.

Conclusion

Cette étude nous a permis de découvrir les systèmes de détection d'intrusion.
Il nous est paru évident que ces systèmes sont à présent indispensables aux entreprises afin d'assurer leur sécurité informatique.
Cependant, nous avons pu constater également que les produits existants ne sont pas encore suffisamment fiables (notamment en ce qui concerne les faux positifs et faux négatifs) et q'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.

De plus, les constructeurs de systèmes de sécurité ont tendance à intégrer les IDS et IPS directement dans les firewalls, de façon à renforcer la coopération entre ces équipements de sécurité complémentaires.

L'avenir des technologies de sécurité réseau est peut-être dans une intégration plus poussée des différents outils disponibles pour assurer la sécurité d'un réseau, car l'administration de la sécurité d'une entreprise est une tâche de plus en plus complexe et étendue, alors que les besoins en sécurité ne font que croître.

Sources :

-www.securityfocus.com
-www.01net.com
-www.linuxsecurity.com
-www.linuxfocus.org
-www.z0rglub.com/piratage/
-www.secway.fr
-les pages de man
Karen Kent Frederick (élaboration d'une signature) :
http://www.securityfocus.com/infocus/1524
http://www.securityfocus.com/infocus/1534
http://www.securityfocus.com/infocus/1544

Jason Larsen and Jed Haile (contournement de l'interruption de session) :
http://www.securityfocus.com/infocus/1540