CHAPITRE 2: LA SECURITE DES RESEAUX

Les entreprises connectés au réseau Internet haut débit bénéficient généralement de certains services tels que la téléphonie sur IP, la visioconférence, des mises à jour de sécurité gratuites... Certains pirates exploitent généralement les failles de sécurité de ces services pour attaquer ces entreprises. Ces pirates sont parfois motivés par l'argent (en attaquant des banques); ou bien par le désir d'être populaire (pour impressionner des amis); et l'envie de causer du tort à l'entreprise. Ils sont parfois attirés par tout ce est interdit.

Il faudra donc définir une **politique de sécurité informatique** en faisant des mises à jour; en sécurisant les serveurs de l'entreprise; en sécurisant le réseau sans fil (s'il existe dans l'entreprise); en sécurisant la voix sur IP. La liste est longue.

1. LES PARE-FEUX

La principale méthode pour se défendre des assaillants venus d'Internet est de mettre en place un pare-feu. Un pare-feu est un composant matériel, logiciel ou les deux. Le pare-feu Internet a pour but d'empêcher les paquets IP malveillants ou non souhaités d'accéder à un réseau sécurisé. Chaque ordinateur connecté à internet (et d'une manière plus générale à n'importe quel réseau informatique) est susceptible d'être victime d'une attaque d'un pirate informatique. La méthodologie généralement employée par le pirate informatique consiste à scruter le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant. Cette menace est d'autant plus grande que la machine est connectée en permanence à internet pour plusieurs raisons:
– La machine cible est susceptible d'être connectée sans pour autant être surveillée ;
– La machine cible est généralement connectée avec une plus large bande passante ;
– La machine cible ne change pas (ou peu) d'adresse IP.

Qu'est-ce qu'un pare-feu?

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante:
– une interface pour le réseau à protéger (réseau interne) ;
– une interface pour le réseau externe.

Fonctionnement d'un système pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies permettant :
– D'autoriser la connexion (allow) ;
– De bloquer la connexion (deny) ;
– De rejeter la demande de connexion sans avertir l'émetteur (drop).
L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :
– soit d'autoriser uniquement les communications ayant été explicitement autorisées :
– soit d'empêcher les échanges qui ont été explicitement interdits.

Catégories de pare-feu

- **Pare-feu sans état (*stateless firewall*)**

Principe

C'est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur :

- L'adresse IP Source/Destination.
- Le numéro de port Source/Destination.
- Et bien sûr le protocole de niveaux 3 ou 4.

Cela nécessite de configurer le Firewall ou le routeur par des règles de filtrages, généralement appelées des ACL (Access Control Lists).

Limites

Le premier problème vient du fait que l'administrateur réseau est rapidement contraint à autoriser un trop grand nombre d'accès, pour que le Firewall offre une réelle protection. Par exemple, pour autoriser les connexions à Internet à partir du réseau privé, l'administrateur devra accepter toutes les connexions TCP provenant de l'Internet avec un port supérieur à 1024. Ce qui laisse beaucoup de choix à un éventuel pirate.

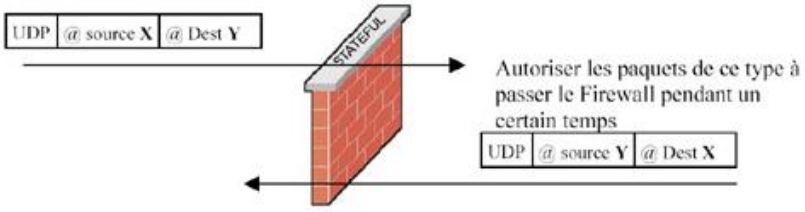
Il est à noter que de définir des ACL sur des routeurs haut de gamme – c'est à dire, supportant un débit important – n'est pas sans répercussion sur le débit lui-même. Enfin, ce type de filtrage ne résiste pas à certaines attaques de type IP Spoofing / IP Flooding, la mutilation de paquet, ou encore certaines **attaques de type DoS**. Ceci est vrai sauf dans le cadre des routeurs fonctionnant en mode distribué. Ceci permettant de gérer les ACL directement sur les interfaces sans remonter à la carte de traitement central. Les performances impactées par les Acl sont alors quasi nulles.

- **Pare-feu à états (*statefull firewall*)**

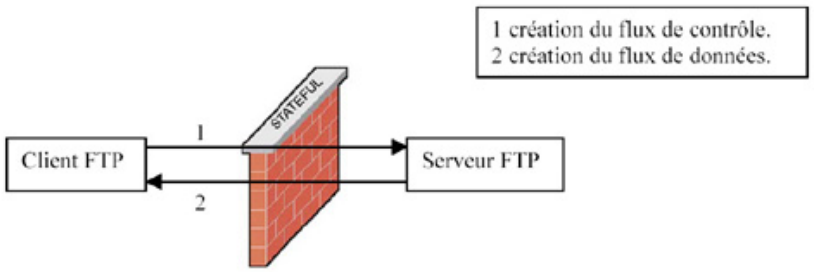
Principe

L'amélioration par rapport au filtrage simple, est la conservation de la trace des sessions et des connexions dans des tables d'états internes au Firewall. Le Firewall prend alors ses décisions en fonction des états de connexions, et peut réagir dans le cas de situations protocolaires anormales. Ce filtrage permet aussi de se protéger face à certains types d'attaques DOS.

Dans l'exemple précédent sur les connexions Internet, on va autoriser l'établissement des connexions à la demande, ce qui signifie que l'on aura plus besoin de garder tous les ports supérieurs à 1024 ouverts. Pour les protocoles UDP et ICMP, il n'y a pas de mode connecté. La solution consiste à autoriser pendant un certain délai les réponses légitimes aux paquets envoyés. Les paquets Icmp sont normalement bloqués par le Firewall, qui doit en garder les traces. Cependant, il n'est pas nécessaire de bloquer les paquets Icmp de type 3 (destination inaccessible) et 4 (ralentissement de la source) qui ne sont pas utilisables par un attaquant. On peut donc choisir de les laisser passer, suite à l'échec d'une connexion Tcp ou après l'envoi d'un paquet Udp.



Pour le protocole Ftp (et les protocoles fonctionnant de la même façon), c'est plus délicat puisqu'il va falloir gérer l'état de deux connexions. En effet, le protocole Ftp, gère un canal de contrôle établi par le client, et un canal de données établi par le serveur. Le Firewall devra donc laisser passer le flux de données établi par le serveur. Ce qui implique que le Firewall connaisse le protocole Ftp, et tous les protocoles fonctionnant sur le même principe. Cette technique est connue sous le nom de filtrage dynamique (Stateful Inspection) et a été inventée par Checkpoint. Mais cette technique est maintenant gérée par d'autres fabricants.



Limites

Tout d'abord, il convient de s'assurer que les deux techniques sont bien implémentées par les Firewalls, car certains constructeurs ne l'implémentent pas toujours correctement. Ensuite une fois que l'accès à un service a été autorisé, il n'y a aucun contrôle effectué sur les requêtes et

réponses des clients et serveurs. Un serveur Http pourra donc être attaqué impunément (Comme quoi il leur en arrive des choses aux serveurs WEB !). Enfin les protocoles maisons utilisant plusieurs flux de données ne passeront pas, puisque le système de filtrage dynamique n'aura pas connaissance du protocole.

- **Pare-feu applicatif**

Principe

Le filtrage applicatif est comme son nom l'indique réalisé au niveau de la couche Application. Pour cela, il faut bien sûr pouvoir extraire les données du protocole de niveau 7 pour les étudier. Les requêtes sont traitées par des processus dédiés, par exemple une requête de type Http sera filtrée par un processus proxy Http. Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse toutes les règles protocolaires des protocoles qu'il doit filtrer.

Limites

Le premier problème qui se pose est la finesse du filtrage réalisé par le proxy. Il est extrêmement difficile de pouvoir réaliser un filtrage qui ne laisse rien passer, vu le nombre de protocoles de niveau 7. En outre le fait de devoir connaître les règles protocolaires de chaque protocole filtré pose des problèmes d'adaptabilité à de nouveaux protocoles ou des protocoles maisons.

Mais il est indéniable que le filtrage applicatif apporte plus de sécurité que le filtrage de paquet avec état, mais cela se paie en performance. Ce qui exclut l'utilisation d'une technologie 100 % proxy pour les réseaux à gros trafic au jour d'aujourd'hui. Néanmoins d'ici quelques années, le problème technologique sera sans doute résolu.

- **Pare-feu personnel**

Les pare-feu personnels, généralement installés sur une machine de travail, agissent comme un pare-feu à états. Bien souvent, ils vérifient aussi quel programme est à l'origine des données. Le but est de lutter contre les virus informatiques et les logiciels espions.

- **Portails captifs**

Les portails captifs sont des pare-feu dont le but est d'effectuer une vérification de l'identité de l'utilisateur avant de le laisser accéder à internet. Cette vérification est sommaire et les méthodes de contournement sont nombreuses. Cependant, ces solutions sont utiles puisqu'elles permettent de limiter les utilisations abusives des moyens d'accès.

C'est par exemple le cas des points d'accès Wi-Fi qui sont souvent protégés par ce genre de solution.

2. LES IDS/IPS

Les systèmes de détection des intrusions (IDS) analysent le trafic réseau pour détecter des signatures correspondant à des cyberattaques connues. Les systèmes de prévention des intrusions (IPS) analysent également les paquets, mais ils peuvent aussi les bloquer en fonction du type d'attaques qu'ils détectent, ce qui contribue à stopper ces attaques.

Fonctionnement

Les IDS et les IPS font tous deux partie de l'infrastructure réseau. Les IDS/IPS comparent les paquets de réseau à une base de données de cyber menaces contenant des signatures connues de cyberattaques et repèrent tous les paquets qui concordent avec ces signatures.

La principale différence entre les deux tient au fait que l'IDS est un système de surveillance, alors que l'IPS est un système de contrôle.

L'IDS ne modifie en aucune façon les paquets réseau, alors que l'IPS empêche la transmission du paquet en fonction de son contenu, tout comme un pare-feu bloque le trafic en se basant sur l'adresse IP.

- **Les IDS (Intrusion Detection Systems) :** analysent et surveillent le trafic réseau pour détecter des signes indiquant que des hackers utilisent une cyber menace connue afin de s'infiltrer dans votre réseau ou y voler des données. Les systèmes d'IDS comparent l'activité réseau en cours avec une base de données d'attaques connues afin de détecter divers types de comportements tels que les violations de la politique de sécurité, les malwares et les scanners de port.
- **Les IPS (Intrusion Prevention Systems) :** agissent dans la même zone du réseau qu'un pare-feu, entre le monde extérieur et le réseau interne. Les IPS rejettent de façon proactive les paquets réseau en fonction d'un profil de sécurité si ces paquets représentent une menace connue.

De nombreux fournisseurs d'IDS/IPS ont intégré de nouveaux systèmes IPS à des pare-feu, afin de créer une technologie appelée UTM (Unified Threat Management). Cette technologie combine en une seule entité les fonctionnalités de ces deux systèmes similaires. Certains systèmes intègrent dans une même entité les fonctionnalités d'un IDS et d'un IPS.

Différences entre IDS et IPS

Les IDS et les IPS lisent tous deux les paquets réseau et en comparent le contenu à une base de menaces connues. La principale différence entre les deux tient à ce qui se passe ensuite. Les IDS sont des outils de détection et de surveillance qui n'engagent pas d'action de leur propre fait. Les IPS constituent un système de contrôle qui accepte ou rejette un paquet en fonction d'un ensemble de règles.

Avec l'IDS, il est nécessaire qu'un humain ou un autre système prenne ensuite le relais pour examiner les résultats et déterminer les actions à mettre en œuvre, ce qui peut représenter un travail à temps complet selon la quantité quotidienne de trafic généré. L'IDS constitue un très bon outil d'analyse « post-mortem » pour l'équipe CSIRT (Computer Security Incident Response Team), qui pourra l'utiliser dans le cadre de ses enquêtes sur les incidents de sécurité.

Pour sa part, l'objectif de l'IPS est de capturer les paquets dangereux et de les retirer avant qu'ils n'atteignent leur cible. Il est plus passif qu'un IDS et exige simplement de mettre régulièrement à jour la base de données pour y intégrer les informations relatives aux nouvelles menaces.

J'insiste sur le fait que l'efficacité des IDS/IPS ne vaut que par celle de leurs bases de données de cyberattaques. Vous devez les tenir à jour et être prêt à opérer des réglages manuels lorsqu'une nouvelle attaque apparaît et/ou que la signature de l'attaque ne figure pas dans la base de données.

3. SSH et Telnet

SSH et Telnet sont deux protocoles réseau, utilisés pour se connecter à un ordinateur distant en se connectant à ce système au sein d'un réseau ou via Internet, et pour contrôler ce système à l'aide de commandes à distance. Ainsi, les deux sont considérés comme des émulateurs terminaux. SSH signifie Secure Shell, et SSH permet à l'utilisateur d'échanger des données entre deux ordinateurs d'un réseau à l'aide d'une connexion cryptée sécurisée. Telnet est un protocole réseau de base utilisé pour communiquer virtuellement avec un système distant.

Qu'est-ce que SSH??

SSH, Secure Shell est un protocole de réseau utilisé pour établir une connexion sécurisée entre deux hôtes distants via Internet ou au sein d'un réseau. SSH utilise un format crypté pour transférer des données entre ordinateurs. Ce mécanisme crypté assure la confidentialité et l'intégrité des données échangées. SSH est largement utilisé pour les systèmes de connexion à distance et pour l'exécution de commandes à distance en raison de la haute sécurité disponible. Avec SSH, les utilisateurs peuvent envoyer des données confidentielles telles que le nom d'utilisateur, le mot de passe et d'autres commandes de manière sécurisée, car toutes ces données sont au format crypté et ne peuvent pas être déchiffrées et lues facilement par des pirates. SSH utilise la cryptographie à clé publique pour l'authentification du système distant. Les serveurs SSH écoutent par défaut le port 22 over TCP (Protocole de contrôle de transmission) standard et peuvent être utilisés sur des réseaux publics. Il fournit une authentification forte et un mécanisme de communication sécurisé sur les canaux non sécurisés.

Qu'est-ce que Telnet??

Telnet est également un protocole réseau utilisé pour échanger des données de manière bidirectionnelle entre deux hôtes distants d'un réseau ou via Internet. À l'aide de ce protocole, les utilisateurs peuvent se connecter à un système distant et communiquer à l'aide d'un terminal virtuel, mais l'utilisation de réseaux non fiables, tels qu'Internet, n'est pas sûre. Telnet échange des données en texte brut. Il ne convient donc pas pour l'envoi de données confidentielles contenant des noms d'utilisateur et des mots de passe à l'aide de ce protocole, car toute autre personne peut lire ce texte en cours d'échange et intercepter facilement les messages. Telnet communique généralement via le port 23 via TCP et peut également accéder à d'autres ports et services. Il peut être utilisé dans les réseaux privés en raison de la sécurité moindre.

Quelle est la différence entre SSH et Telnet?

Base de comparaison	Telnet	SSH
Sécurité	Moins sécurisé	Hautement sécurisé
Utilise le numéro de port	23	22
Format de données	Telnet transfère les données en texte brut.	Le format crypté est utilisé pour envoyer des données et utilise également un canal sécurisé.
Authentification	Aucun privilège n'est fourni pour l'authentification des utilisateurs.	Utilise le cryptage à clé publique pour l'authentification.
Adéquation du réseau	Les réseaux privés sont recommandés.	Convient aux réseaux publics.
Vulnérabilités	Vulnérable aux attaques de sécurité.	SSH a surmonté de nombreux problèmes de sécurité de telnet.
Utilisation de la bande passante	Faible	Haute

4. LES ANTI-VIRUS

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (*dont les virus informatique ne sont qu'une catégorie).* Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (*le plus souvent ceux du système d'exploitation).*

Il est intéressant de noter qu'une fois un fichier infecté, il ne l'est jamais deux fois. En effet, un virus est programmé de telle sorte qu'il signe le fichier dès qu'il est contaminé. On parle ainsi de signature de virus. Cette signature consiste en une suite de bits apposée au fichier. Cette suite, une fois décelée, permettra de reconnaitre le virus. Lorsque le virus est détecté par l'antivirus, plusieurs possibilités sont offertes pour l'éradiquer :

- Supprimer le fichier infecté ;
- Supprimer le code malicieux du fichier infecté ;
- Placer le ou les fichiers infectés en "quarantaine" pour un traitement futur.

Voici les anti-virus les plus populaires selon leurs finalités :

Les principaux anti-virus des PC and Serveurs : AhnLab V3 Internet Security - Avast Antivirus - AVG - Avira AntiVirus - Bitdefender - ClamWin - ClamAV - Comodo Antivirus - Comodo Internet Security - Dr. Web - NOD32 - F-Secure - F-PROT - Fortinet - G Data Software - Advanced SystemCare – iolo System Shield - Kaspersky AntiVirus - Kaspersky Internet Security - KingSoft - Mac Internet Security - McAfee VirusScan - Microsoft Security Essentials - Windows Defender - Panda - 360 Safeguard - Outpost Security Suite - Sophos - Symantec Endpoint Protection - Immunet - Element AntiVirus – Norton AntiVirus - Norton Internet Security - Spyware Doctor - VirusBarrier - Trend Micro Internet Security - TrustPort - Vba32 AntiVirus -Zone Alarm.

Les principaux anti-virus des mobiles et tablettes : AhnLab Mobile Security (en) - Avast Antivirus - AVG - Avira Free Android Security - Bitdefender Mobile Security - CM Security - Comodo Mobile Security - Dr. Web Mobile Security Suite - ESET Mobile Security - F-Secure Mobile Security - G Data MobileSecurity - Lookout Mobile Security - McAfee Mobile Security - FireAMP Mobile - Trend Micro Mobile Security - TrustPort Mobile Security - VirusBarrier.

FONCTIONNEMENT DE L'ANTI-VIRUS

Un logiciel antivirus vérifie les fichiers et courriers électroniques, les secteurs de démarrage (*afin de détecter les virus de boot*), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (*clefs USB, CD, DVD, etc.*), les données qui transitent sur les éventuels réseaux (*dont internet*) …. Différentes méthodes sont possibles :

- Les principaux antivirus du marché se concentrent sur des fichiers et comparent alors *la signature virale* du virus aux codes à vérifier ;
- La *méthode heuristique* est la méthode la plus puissante, tendant à découvrir un code malveillant par son comportement. Elle essaie de le détecter en analysant le code d'un programme inconnu. Parfois de fausses alertes peuvent être provoquées ;
- L'*analyse de forme* repose sur du filtrage basé entre des règles *rege-xp* ou autres, mises dans un fichier *junk*. Cette dernière méthode peut être très efficace pour les serveurs de messagerie électronique supportant les rege-xp type postfix puisqu'elle ne repose pas sur un fichier de signatures.

Les antivirus peuvent balayer le contenu d'un disque dur, mais également la mémoire vive de l'ordinateur. Pour les anti-virus les plus modernes, ils agissent en amont de la machine en scrutant les échanges de fichiers avec l'extérieur, aussi bien en flux descendant (téléchargement) que montant (*téléchargement ou upload*). Ainsi, les courriels sont examinés, mais aussi les fichiers copiés sur ou à partir de supports amovibles tels que cédéroms, disquettes, connexions réseau, clefs USB…

TECHNIQUES DE DETECTION DES ANTI-VIRUS

En général, la guerre entre virus et antivirus est bien réelle. Dès qu'un groupe agit, le camp opposé tente de trouver la parade. Pour détecter les virus, les antivirus doivent user de plusieurs techniques spécialement :

- **Le scanning des signatures (Dictionnaire)** - La détection des virus consiste à la recherche de ces signatures à partir d'une base de données de signatures (*on parle également de définitions de virus*). Le principal avantage de cette technique est qu'il est possible de détecter le virus avant qu'il ne soit en action. Cependant, il est nécessaire que sa signature soit présente dans la base de données afin qu'il soit détecté. De plus, il est nécessaire de tenir la base régulièrement à jour afin de pouvoir détecter les nouveaux virus.
- **Le moniteur de comportement** : Il s'agit ici de contrôler en continu toute activité suspecte telles que les lectures et écritures dans des fichiers exécutables, les tentatives d'écriture dans les secteurs de partitions et de boot du disque.

- **Liste blanche** - est une technique de plus en plus utilisée pour lutter contre les logiciels malveillants. Au lieu de rechercher les logiciels connus comme malveillants, on empêche l'exécution de tout logiciel à l'exception de ceux qui sont considérés comme fiables par l'administrateur système. En adoptant cette méthode de blocage par défaut, on évite les problèmes inhérents à la mise à jour du fichier de signatures virales. De plus, elle permet d'empêcher l'exécution de logiciels indésirables. Étant donné que les entreprises modernes possèdent de nombreuses applications considérées comme fiables, l'efficacité de cette technique dépend de la capacité de l'administrateur à établir et mettre à jour la liste blanche. Cette tâche peut être facilitée par l'utilisation d'outils d'automatisation des processus d'inventaire et de maintenance.

- **Le contrôleur d'intégrité** : Le principe est que l'antivirus maintienne une liste des fichiers exécutables associés à leur taille, leur date de création, de modification, voire un **CRC** (*Contrôleur Redondance Cyclique*). L'utilisation du CRC permet de vérifier qu'un exécutable n'a pas été modifié en comparant sa somme de contrôle avant et après son exécution. En effet, en dehors d'une mise à jour explicite du fichier, un fichier exécutable n'est pas censé être modifié. Le même type de vérifications peut être instauré avec la date et heure de modification. Cependant, il suffira aux virus de mémoriser ces valeurs afin de pouvoir les restaurer par la suite.

- **L'analyse heuristique** : A la différence du moniteur de comportement qui détecte les modifications causées par les virus, l'analyse heuristique tente de détecter les virus avant leur exécution, en cherchant des portions de code suspectes. Il pourrait par exemple chercher des séquences de lecture suivies de séquences d'écriture sur un même fichier exécutable. Cette technique permet donc de détecter des virus même sils ne sont pas présents dans la base de données, puisque l'analyseur teste des séquences d'instructions communes à de nombreux virus.

5. TP SUR ENSP HUAWEI