LA SÉCURITÉ DES SERVEURS

INTRODUCTION

**POURQUOI SÉCURISER SES SERVEURS ?**

La sécurité des serveurs est d’une importance capitale pour le bon fonctionnement d’une entreprise. Qu’il s’agisse de sécuriser des données ou de garantir la continuité d'un service tels que serveur web, http ou serveur de messagerie, l’administrateur réseau se doit de protéger son système contre des intrus malveillants et d'empêcher les utilisateurs d'effectuer des opérations involontaires capables de nuire au bon fonctionnement du réseau.

**DANS QUELS BUTS LES AGRESSEURS AGISSENT-ILS ?**

Les motivations des agresseurs, que l'on appelle communément pirates, peuvent être multiples:

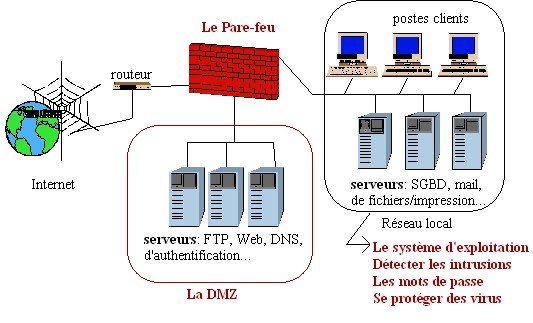
l'attirance de l'interdit, le désir d'argent, le besoin de renommée, l'envie de nuire, la vengeance ou simplement la curiosité…

Le but des agresseurs est souvent de prendre le contrôle d'une machine afin de pouvoir réaliser les actions qu'ils désirent. Pour cela ils ont recourt à différents types d’attaques qui seront étudiées dans le chapitre suivant.

A savoir, que, selon certaines études, 80% des actes de piratage se font via des collaborations internes à l'entreprise…

**COMMENT SE DEFENDRE ?**

Aucun système n’est infaillible. Néanmoins il est possible de réduire ces risques au minimum, en employant divers moyens: l’installation d’un pare-feu, d’une zone démilitarisée, la détection des intrusions, une protection antivirus et en intervenant sur différents critères tels que le choix du système d’exploitation approprié, des mots de passe…



|  |
| --- |
| LES ATTAQUES |

swordleftswordright

Pour sécuriser au mieux son système, il faut tout d’abord prendre connaissance des divers types d’attaques dont on est susceptible d’être la victime.

Voici une liste des attaques les plus courantes :

## LES ATTAQUES LOCALES

## LE DIFFING

Le diffing consiste à comparer 2 éléments en vue d’identifier leurs différences, en particulier après une modification. Il peut être pratiqué sur presque tous les types de données. Cette technique sert à localiser l’information qui intéresse l’attaquant (par exemple, un mot de passe) en provoquant des actions et en surveillant les modifications occasionnées.

**LES ENTREES IMPREVUES**

Pour dialoguer avec un utilisateur, une application doit accepter les informations qu’il lui fournit. Celui-ci peut entrer des données que l’application n’a pas prévues. Selon les cas, cette opération n’aura aucune importance ou entraînera des modifications de l’application ou du système.

Il existe 3 types d’attaques fondées sur les entrées imprévues :

* ***le dépassement du tampon***: Un attaquant envoie plus de données que ne le prévoit l’application.
* ***les fonctions système***: Les données servent à dialoguer avec une ressource extérieure à l’application, qui peut constituer une fonction système.
* ***L’altération de la logique***: Les données sont conçues pour modifier la logique de l’application

##### LES ATTAQUES A DISTANCE

Une attaque à distance est une agression contre une machine que l'on peut joindre grâce à un protocole, à travers un réseau, par une personne n'ayant pas les droits sur elle.

### LE SNIFFING

Le sniffing permet à un attaquant de compromettre le réseau de manière passive, en recueillant des informations importantes grâce à un sniffer.

Le sniffer est un petit dispositif, logiciel ou matériel, qui surveille, sans se faire repérer, un ordinateur du réseau en vue d’y trouver des informations susceptibles d’intéresser un attaquant. Souvent, ces informations sont relatives à l’authentification : il s’agit de noms d’utilisateur et de mots de passe qui permettront d’accéder à un système ou à une ressource.

### LE SPOOFING

Le spoofing consiste à usurper l’identité d’un client, afin d’accéder à des systèmes et à leurs services. Il existe 2 types de spoofing :

* ***le spoofing* *aveugle***qui consiste à soumettre des informations d’identité sans savoir si l’utilisateur légitime y a accès.
* ***Le spoofing conscient****,* contourne la protection qui contrôle la communication entre le client et le serveur.

Quant au ***spoofing IP***, c’est une méthode très astucieuse puisqu'elle consiste à se faire passer pour quelqu'un du réseau privé interne alors que l'on vient de l'extérieur.

### LE FLOOD

Le flood consiste à envoyer très rapidement de gros paquets d'information à une personne (à condition d'avoir un PING, c'est-à-dire le temps que met l'information pour faire un aller retour entre 2 machines, très court). La personne visée ne pourra plus répondre aux requêtes et le modem va donc déconnecter.

* ***le TCP/SYN flooding***:Lors d'une connexion TCP, le client et le serveur échangent des données et des accusés de réception pour établir la connexion.

Toutefois ce mécanisme possède une faiblesse: lorsque le serveur renvoie un accusé de réception mais n’en reçoit aucun en provenance du client, il crée une structure de données contenant toutes les connexions ouvertes. S'il est vrai qu'il existe un mécanisme d'expiration permettant de fermer des connexions ouvertes pendant un temps trop long, et ainsi libérer de la mémoire, il est possible pour un agresseur de vite la saturer en envoyant suffisamment rapidement des paquets SYN.

**LE MAIL BOMBING**

Le mail bombing consiste à envoyer plusieurs milliers de messages identiques à une boîte aux lettres pour la faire saturer.

**LE DENI DE SERVICE (DoS)**

Les attaques par Denial Of service consistent à paralyser temporairement des serveurs afin qu'ils ne puissent être utilisés et consultés. Tous les serveurs (Lan, Wan...) peuvent être touchés. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à des sociétés dont l'activité repose sur un système d'information en l'empêchant de fonctionner.

D’un point de vue technique, les attaques par déni de service n'exploitent non pas les failles d'un système d'exploitation particulier, mais celle du protocole TCP/IP. Elles consistent en un envoi de paquets IP de taille excessivement importante, ce qui a pour cause la saturation de la machine victime, qui ne peut plus assurer les services réseaux qu'elle propose.

### LES EXPLOITS

Un exploit est un programme qui exploite un bug dans un software spécifique.

Chaque exploit est différent et exploite des bugs précis se trouvant dans un programme utilisé par le "root".

#### LES VIRUS

Un virus est un petit programme situé dans le corps d'un autre, qui, lorsqu'on le lance, se charge en mémoire et exécute les instructions que son auteur a programmé.

On en distingue différents types :

* ***les vers*** sont des virus capables de se propager à travers un réseau.
* ***les troyens*** (chevaux de Troie) sont des virus permettant de créer une faille dans un système en se faisant passer pour un programme (un utilitaire banal du système si possible).
* ***les bombes logiques*** sont des virus capables de se déclencher suite à un événement particulier.

|  |
| --- |
| LE SYSTÈME D’EXPLOITATION |

**QUEL SYSTÈME CHOISIR ?**

Chaque système a ses points forts, mais aussi ses faiblesses. On est en droit de se demander quel est le meilleur système d’exploitation en critère de sécurité, pour son serveur.

Un système Microsoft (Windows NT, Windows 2000…) est-il comparable à un système de la famille UNIX  (AIX, BSDI, Digital Unix, FreeBSD, HP-UX, IRIX, Linux, NetBSD, OpenBSD, Solaris, SunOS…)?

A cette question chacun avance ses propres arguments, bien qu’Unix, avec ses 20 ans d'expérience dans les réseaux, les systèmes Multi-Utilisateurs et la sécurité, ait depuis longtemps fait ses preuves…

On prendra donc soin de choisir un système d’exploitation adéquat pour son serveur, selon sa fonction et le degré de sécurité imposé qui en découle.

Un serveur qui a pour fonction de partager une imprimante, ne réclame pas la même attention qu’un serveur web, et le système d’exploitation sera donc choisi en conséquence.

## LES PATCHS ET CORRECTIFS

S’il est impossible d’assurer la fiabilité d’un système à 100%, il est cependant conseillé de le mettre à jour pour y porter les améliorations.

En effet, des bugs et des failles de sécurité sont régulièrement découvertes, et le fabriquant met à disposition des correctifs qu’il est, en général, possible de télécharger par le biais d’internet.

**FAUT-IL SE PRÉCIPITER SUR LA NOUVEAUTÉ ?**

Entendons par nouveauté, nouveaux systèmes d’exploitation ou nouvelles versions.

Les gens croient souvent, à tort, que les nouveautés sont plus fiables que l’existant. L’exemple le plus flagrant est probablement celui de Windows NT:

Pendant les premières années d’existence de ce système, de nombreux défenseurs de Windows énuméraient les problèmes de sécurité recensés sur les autres systèmes d ‘exploitation et ventaient le modèle NT. Même Microsoft utilisait cet argument dans ses campagnes de publicité. Mais lorsque NT devint populaire, les hackers commencèrent à s’y intéresser et aujourd’hui, la découverte de failles dans Windows NT n’est –comme dans tout autre système d’exploitation– plus exceptionnelle.

Ceci pour expliquer qu’il est prudent d’attendre que le système ait été testé et qu’il ait fait ses preuves, avant de prendre la décision de l’acquérir.

**CONCLUSION**

Si le choix du système d’exploitation est important, savoir l’administrer l’est encore plus. Un bon système d’exploitation mal configuré est bien pire qu’un système moins puissant mais bien paramétré. Pour exploiter au mieux les moyens de sécurité offerts par son système, il faut obligatoirement en avoir une connaissance approfondie.

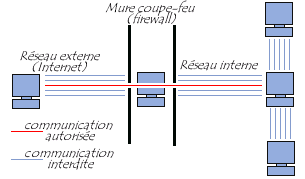
On retiendra aussi qu’avant de remplacer son système d’exploitation par un modèle plus récent, il faudra attendre que le nouveau système d’exploitation, ou sa nouvelle version, aient déjà été testés par d’autres personnes/sociétés, afin de pouvoir juger de ses performances et de sa sécurité.

|  |
| --- |
| LE PARE-FEU |

## DÉFINITION

Le pare-feu (ou Firewall ou coupe-feu) est un dispositif (logiciel ou matériel) constituant un sas de protection entre un LAN et un autre réseau et ayant pour fonction de filtrer le trafic qui passe à travers les routeurs. Il permet à l'administrateur de limiter les tentatives d'intrusion. La solution la plus adaptée consiste à filtrer les données entrantes et sortantes.

On peut, de cette façon, proposer une vision restreinte du réseau interne vu de l'extérieur et filtrer les paquets en fonction de certaines caractéristiques telles qu'une adresse ou un port de communication.



## FONCTIONNEMENT

**FILTRAGE DES PAQUETS**

Un système pare-feu fonctionnant sur le principe du filtrage de paquets analyse les en-têtes des paquets échangés entre deux machines, qui sont les suivantes:

* L'adresse IP de la machine émettrice
* L'adresse IP de la machine réceptrice
* Le type de paquet (TCP, UDP, ...)
* Le numéro de port

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

Le filtrage IP est destiné à interdire l'accès non autorisé au réseau et à tester le comportement du système de sécurité. Cependant, plusieurs facteurs compliquent le système de filtrage des paquets. C'est le cas de l'accès asymétrique (connexions de sortie plus étendues que connexions d'entrée), mais également des « privilèges » accordés à certains groupes d'utilisateurs du réseau intérieur ou extérieur et des caractéristiques des différents protocoles et services (pour lesquels le filtrage est mis en place).

Le pare-feu peut bloquer des ports TCP (rappel: un port est un numéro associé à un service ou une application réseau), c'est-à-dire en interdire l'accès aux personnes provenant de l'extérieur. Toutefois certains ports étant nécessaires et non dangereux, comme par exemple le port associé au courrier électronique, les administrateurs réseau bloquent la plupart des ports qui ne sont pas indispensables. Mais ce dispositif n'empêche pas les utilisateurs interne d'utiliser ces ports, seule la traversée du système pare-feu est impossible.

Certains techniciens préconisent de sécuriser le système en utilisant des ports non-standards. Ainsi, si les données HTTP passent généralement par le port 80, on pourra changer pour le port 81, mais cela se révèle peu efficace.

De plus un firewall permet de contrôler l'accès au réseau des applications installées sur la machine. Il permet de repérer les connexions suspectes de la machine et de les empêcher.

#### LE PROXY

Le firewall est un terme assez généraliste qui intègre parfois la fonction de proxy, passerelle intermédiaire entre sa machine et le réseau Internet. Il peut aussi servir de cache, c'est-à-dire qu'il garde en mémoire les pages les plus souvent visitées pour pouvoir les fournir plus rapidement. Il permet donc de libérer la bande passante du réseau et de limiter les accès au net.

Sur le plan de la sécurité, son rôle est important. Un serveur Proxy exécuté sur un hôte bastion (un Proxy HTTP, par exemple) masque à l'Internet toutes les adresses IP du réseau interne. Concrètement, lorsqu'un employé se procure des informations Internet à partir d'un ordinateur de l’Intranet d'entreprise, le site Internet contacté ne détient jamais que l'adresse IP du serveur Proxy, et en aucun cas l'adresse IP de l'ordinateur du réseau interne. Un pirate mal intentionné, à l'affût des échanges de données, ne lit par conséquent que l'adresse du Proxy.

Le Proxy a donc pour rôle, de masquer l'adresse de l'expéditeur des paquets de données circulant via Internet, pour empêcher tout intrus de déchiffrer les structures internes de votre réseau.

**INTÉRÊTS ET LIMITES DU PARE-FEU**

L’utilisation d’un firewall s’avère indispensable si son réseau local est connecté à Internet, tant pour limiter les accès des utilisateurs, que pour protéger son réseau interne.

Le Firewall peut vous permettre de vous protéger des chevaux de Troie et d’empêcher certaines des attaques DoS (Deny of service), comme les SYN Flood, le Ping of death et l'IP Spoofing.

A savoir qu’il existe différentes façons de paramétrer le pare-feu:

* Soit « Tout ce qui n’est pas expressément interdit est autorisé »
* Soit « Tout ce qui n’est pas expressément autorisé est interdit »

Dans le premier cas, le coupe-feu est conçu pour bloquer le trafic et tout est étudié au cas par cas après une analyse fine de tous les risques. Dans cette configuration, la protection peut-être ressentie comme une gêne par l’utilisateur.

Dans le deuxième cas, c’est l’administrateur du réseau qui doit réagir en temps réel. Il doit prévoir les attaques afin de les contrer. Cette méthode implique une "course à l’armement " entre les pirates et les responsables de la sécurité du réseau local.

Pour ouvrir le réseau tout en conservant sa sécurité : il est aussi conseillé d’instaurer une zone démilitarisée (voir chapitre suivant).

Le fait d'installer un firewall n'est bien évidemment pas signe de sécurité absolue. Il ne protège, en effet, que des communications passant à travers lui. Ainsi, les accès au réseau extérieur non réalisés au travers du pare-feu sont autant de failles de sécurité. C'est par exemple le cas des connexions effectuées à l'aide d'un modem. D'autre part, le fait d'introduire des supports de stockage provenant de l'extérieur sur des machines internes au réseau peut aussi être fort préjudiciable pour la sécurité de ce dernier.

|  |
| --- |
| **LES ZONES DÉMILITARISÉES** |

**QU’EST CE QU’UNE ZONE DÉMILITARISÉE (DMZ) ?**

Une DMZ est une zone tampon entre un réseau privé et Internet (voir le schéma page 1).

C'est le brin de réseau physique compris entre le point d'entrée et le pare-feu.

**QUE METTRE EN DMZ ?**

Cette zone est donc l’endroit où l’on sait que les éléments que l’on va y placer ne sont pas des objets à fonctionnalités et à contenus critiques. Les serveurs que l'on y met s'appellent des *Bastions*.

Un bastion est une machine proposant des services informatiques publics ou contrôlés. L'offre faite par ces ordinateurs n'est pas considérée comme sensible. Ils sont néanmoins installés de façon très sécurisée afin d'éviter des restaurations de système trop souvent.

Par exemple, on peut y mettre un serveur Web de l’entreprise si les données sont publiques: en cas de piratage, il sera très simple de restaurer une sauvegarde en local sur la machine. Bien sur, il n’est pas question de faire transiter ni de stocker des informations essentielles dessus, par exemple une base de données de commandes clients / fournisseurs ou bien une messagerie. On n’y mettra pas non plus des services tels que le proxy, la comptabilité, la paye…

Les Bastions peuvent recevoir un service de DNS externe, être des relais Mail, des serveurs publiques FTP…

**SÉCURISER LA DMZ**

Si l’on souhaite sécuriser un service Web dans cette zone, on fait en sorte que le routeur soit épaulé par un vrai pare-feu et, en plus, on ajoute un serveur d’authentification dans la DMZ. Ce serveur d’authentification est l’élément qui délivre les accès aux différents services présents dans la DMZ. Lorsqu’on souhaite se loguer sur le routeur, le routeur ne va autoriser le prompt qu’après avoir vérifié et échangé avec le serveur d’authentification les informations concernant celui qui souhaite se loguer. Ils procèdent à un échange d’informations sécurisées puisque ils ont une clé privée qui leur est commune et non transmissible en clair lors des échanges.

De plus, la station d’accueil doit exécuter une version "blindée" de son OS. Elle doit être surveillée et optimisée contre ses propres faiblesses face aux intrusions possibles. L'administrateur ne laissera que les services strictement nécessaires fonctionner car tout service non lancé ne peut pas être attaqué.

Un syslog doit être posté sur chaque machine afin d'analyser précisément les durées de connexion, le trafic, les données et le type de connexion. Si l'information ainsi générée est bien triée ( automatiquement bien entendu ) on arrive facilement à déterminer les mouvements inhabituels ou étranges.

Un autre point tout aussi important consiste à séparer au maximum les programmes qui offrent des services différents. L'avantage c'est que si un service "tombe", il est plus simple de le remettre en place après vérification et surtout on conserve une continuité sur les autres services. Sans compter qu'un programme de petite taille est plus simple à modifier, sécuriser ou mettre à jour qu'un programme trop complet... En plus, il vaut mieux que les programmes n'accèdent pas trop au disque dur (ou du moins dans des répertoires très sécurisés et isolés) car en cas de processus "en attente de propagation" qui aurait pu être introduit, il est simple de l'effacer définitivement : on reboot !

|  |
| --- |
| DÉTECTER LES INTRUSIONS : LES IDS |

On parle souvent d'IDS (Intrusion Détection System) pour désigner l'ensemble des outils de détection d 'intrusion.

## DÉFINITION

Le système de détection d'intrusion ou IDS est un système ou un ensemble de systèmes ayant pour rôle de repérer, soit une tentative d'intrusion, soit un comportement intrusif.

Les IDS s’apparentent aux pare-feu, mais leurs fonctions sont légèrement différentes. Les pare-feu sont conçus pour identifier tout trafic indésirable ; les IDS jouent également ce rôle, mais n’arrêteront pas forcément le trafic douteux.

Un IDS peut vous permettre d'envoyer une alerte à l'entité de votre choix, de clôturer la connexion suspecte, etc.

**FONCTIONNEMENT**

Les IDS se distinguent selon deux modes de fonctionnement:

* ***IDS à Bibliothèques de signatures***: Cette approche consiste à rechercher dans l'activité de l'élément surveillé, les empreintes 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 quotidiennes. Ces systèmes sont souvent contournés par les pirates qui utilisent des techniques dites " d'évasion " qui consistent à maquiller les attaques utilisées
* ***IDS à Modèles comportementaux***: Ils ont pour principe la détection d'anomalies. Ces IDS signaleront les divergences par rapport au fonctionnement de référence. Ces IDS signalent toute activité " anormale ". 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.

Les IDS diffèrent aussi selon le système à surveiller :

* ***IDS Réseau***: Ces outils analysent le trafic réseau. Les IDS Réseau à base de signatures sont confrontés actuellement à deux problèmes majeurs: le développement de l'utilisation du cryptage et le développement des réseaux commutés.
* ***IDS Système***: Les IDS Systèmes analysent quant à eux le fonctionnement ou l'état des machines sur lesquelles ils sont installés afin de détecter les attaques. Il faut cependant noter qu'ils sont incapables de détecter les attaques affectant les couches réseaux de la machine ; typiquement les Dénis de service.

**INTÉRÊTS ET LIMITES DES IDS**

Aujourd'hui les systèmes de détection d'intrusion sont réellement devenus indispensables lors de la mise en place d'une infrastructure de sécurité opérationnelle, surtout pour les entreprises connectées à Internet. Les IDS ont pour avantage d’être « invisible ». En effet, un intrus ne peut pas savoir si le système cible en est équipé ou non, contrairement au pare-feu. Ainsi l’administrateur pourra être prévenu d’une attaque sans que le pirate soit au courant.

Néanmoins, comme tous les outils techniques, ils ont des limites que seule une analyse humaine peut compenser. Un peu comme les Firewalls, les détecteurs d'intrusion deviennent chaque jour meilleurs grâce à l'expérience acquise avec le temps mais ils deviennent aussi de plus en plus sensibles aux erreurs de configuration et de paramétrage. Par conséquent, il est plus que fondamental de former correctement les personnes chargées de la mises en œuvre et de l'exploitation des IDS.

|  |
| --- |
| **LES MOTS DE PASSE** |

**POURQUOI SONT-ILS SI IMPORTANTS ?**

Les mots de passe sont la première défense contre les attaques sur un système. En effet, un intrus qui ne peut pas agir sur un système distant ne peut pas faire grand chose contre lui. Cependant, s'il a accès au fichier des mots de passe, il pourra s'introduire dans le système avec les permissions relatives au mot de passe qu'il a cracké. Si c’est celui de l'administrateur il a alors toutes les permissions...

La stratégie la plus fréquente des malveillants, consiste d’abord à usurper l’identité d’un utilisateur; puis, dans un deuxième temps, à utiliser les failles connues du système pour devenir administrateur sur une machine.

On comprendra donc que pour protéger ses serveurs, il est capital que, non seulement l’administrateur, mais aussi tous les utilisateurs du réseau, aient des mots de passe efficaces.

**TECHINIQUES DE DÉCRYPTAGE**

Les algorithmes de cryptage des mots de passe aujourd'hui sont tels, que le fait de les décrypter est très long, la clé de cryptage est par contre connue.

Les perceurs de mots de passe utilisent donc des dictionnaires dont ils cryptent les mots et les comparent au votre. Plus ce dictionnaire contient de mots, plus les recherches seront fructueuses. Il existe sur l'Internet des listes de mots dans toutes les langues, typiquement du monde d'Unix, etc. Ce qui permet de trouver des mots, qui, à priori, ne sont pas facilement décryptables. Par cette technique, on arrive à casser en moyenne plus de 20% des mots de passe d’un fichier en moins d’une heure.

Une autre technique consiste à essayer toutes les combinaisons possibles, soit sur un jeu réduit de caractères, soit en cherchant une chaîne de caractères de petite longueur.

**DES MOTS DE PASSE EFFICACES**

Il est donc très facile de découvrir un mot de passe qui est trouvable dans un dictionnaire. A éviter, aussi, les mots de passe trop évidents, tels que son login, nom/prénom, les mots à l’envers, de langues étrangères ou comportant uniquement des chiffres…

On préfèrera un mot de passe mêlant des chiffres, des lettres, des majuscules et des caractères spéciaux.

Ajoutons qu’ils devront faire au moins 7-8 caractères, car il est actuellement impossible de trouver un mot de passe « illogique » en essayant toutes les combinaisons pour un tel nombre de caractères à moins d’y passer plusieurs années de temps CPU.

A savoir que sur certains réseaux, les mots de passe circulent en clair. Des techniques simples (sniffers, espions, chevaux de Troie...), peuvent être mises en oeuvre pour capter l’identifiant et le mot de passe.

C’est pourquoi, même robuste, un mot de passe doit être modifié régulièrement (au moins tous les trois mois). Mais cette exigence pose un problème de mémorisation. Un mot de passe ne peut donc être qu’un pur aléa et il faut avoir une règle de constitution mnémotechnique.

Mais tous ces conseils ne seront d’aucune efficacité si les utilisateurs ne sont pas sensibilisés à l’importance de leur mot de passe, qui constitue un secret précieux, qui ne doit ni être prêté, ni écrit sur un support à proximité de sa machine ou de manière qu’un rapprochement puisse être fait avec le système qu’il est censé protéger.

Afin de lui permettre de vérifier la solidité des mots de passe de son système, l’administrateur devra régulièrement utiliser un logiciel tel que Crack. Ce programme, aussi convoité par les pirates, essaye de rechercher les mots de passe des utilisateurs en utilisant des combinaisons, interpolations de mots, générées à partir d'un dictionnaire.

|  |
| --- |
| **SE PROTÉGER DES VIRUS** |

Pour commencer, il faut savoir qu’une protection sans faille n’existe pas.

La règle de protection de base est de ne pas "exécuter" de programme venant de source incertaine, voire inconnue. Mais avec la diversification des applications, de nouveaux "exécutables" sont apparus, comme les macros, qui permettent de réaliser un ensemble de commande de manière automatisée.

Le point important sur lequel il faut donc être vigilant, est la provenance des fichiers Avec l'avènement de l'Internet grand public, les risques se multiplient, notamment avec le téléchargement de fichiers d'origine inconnue et de source incertaine.

Il faudrait refuser tout programme ne venant pas d'une disquette d'origine ou d’une société considérée comme sûre, dans le cas d’Internet. Pour ne pas arriver à de tel extrême, il existe des logiciels qui permettent de se prémunir et de lutter contre les virus: les antivirus.

**LES ANTIVIRUS**

Il existe différents types d’antivirus :

* ***Les scanners***: Son principe est de rechercher sur le disque dur toute chaine de caractères identifiée comme appartenant à un virus. Cette méthode présente l'avantage de détecter un virus avant qu'il ne s'exécute sur une machine. Cependant comme chaque virus a sa propre signature, il faut, pour le détecter, que la signature soit intégrée à la base de données de l’antivirus.

# *Les moniteurs de comportement*: Ils observent l'ordinateur à la recherche de toute activité de type virale. En général, un moniteur de comportement est un programme résidant en mémoire, que l'utilisateur charge au démarrage du système et qui reste actif à l’arrière plan en surveillant tout comportement inhabituel. L'antivirus peut alors éliminer le virus de la mémoire, enregistrer une partie de son code dans la base de donnée et lancer un scanning pour repérer la/les souche(s) sur le disque dur et les détruire.

* ***Les contrôleurs d'intégrité***: Un contrôleur d'intégrité va construire un fichier contenant les noms de tous les fichiers présents sur le disque auxquels sont associées quelques caractéristiques. Ceci peut simplement être la taille, la date et l'heure de dernière modification ou encore un checksum (somme de contrôle). Le contrôleur pourra détecter si une altération s'est produite et alertera l'utilisateur. Le problème de cette méthode et qu'il peut y avoir des milliers de virus sur une machine, l'utilisateur n'en sera informé que lorsque le virus s'exécutera ou modifiera un fichier.

**CONCLUSION**

Comme nous l’avons vu au chapitre traitant des attaques, les vers sont des virus capables de se propager à travers un réseau. On en déduit, que, même si votre serveur n’est en contact direct, ni avec Internet, ni avec une messagerie ou avec tout élément provenant de l’extérieur (disquettes…) il est néanmoins susceptible d’être contaminé, à cause des postes clients. Il est donc indispensable d’installer un antivirus sur chaque machine, y compris les serveurs.

Il faut savoir qu'aucun logiciel antivirus n’est efficace à 100 %. Les scanners restent actuellement la méthode la plus populaire. Pourtant, un scanner manque de détecter certains virus ou bien de signaler des programmes comme dangereux, même si ce n'est pas le cas.

Quel que soit l’antivirus que vous choisirez, il faudra, pour conserver son efficacité, effectuer des mises à jour régulières (environ tous les 15 jours), et veiller à ce qu’il surveille les messageries.

Ajoutons qu’il faudra, là encore, informer et former les utilisateurs de quelques règles à respecter, telles que se méfier des pièces jointes dans le logiciel de messagerie, de ne pas télécharger de fichiers ou de logiciels d’Internet.

|  |
| --- |
| **TESTER SON SYSTÈME** |

Afin de déterminer le degré de sécurité de votre réseau, et ainsi savoir si oui ou non, votre politique de sécurité est efficace ou s’il faut la modifier, vous devez tester votre système.

Il existe diverses moyens de le faire, comme utiliser un scanner de ports, tenter de pirater soi-même son système…

Dans tous les cas, l'idée est d’utiliser les outils des pirates pour vérifier les vulnérabilités de votre réseau.

**LES SCANNERS DE PORTS**

Un scanner est un programme qui permet de savoir quels [ports](http://www.commentcamarche.com/internet/port.php3) sont ouverts sur une machine donnée. Ces ports ouverts représentent autant de failles dans la sécurité de votre système.

Les scanners servent tant aux crackers, pour savoir comment ils vont procéder pour attaquer une machine, qu’à l’administrateur pour lui permettre de déterminer quels ports sont ouverts sur son réseau et ainsi prévenir une attaque.

On peut citer, parmi les scanners les plus connus: Nessus security, ISS Internet scanner ou encore NV e-secure.

**PAR INTERNET**

Il est aussi possible d’utiliser Internet pour testez sa configuration.

Voici un site qui remplit très biens ce rôle, mais il permet uniquement de tester la machine sur laquelle il est exécuté :

<https://grc.com/x/ne.dll?bh0bkyd2>

Ce site, de Steve Gibson, propose un diagnostic en ligne de vos ports.

Il existe d’autres sites qui ont plus ou moins la même fonction. Il suffit, pour les trouver, de faire une recherche sur internet.

**CONCLUSION**

Bien entendu, Les systèmes de détection de vulnérabilités vous aideront à sécuriser vos installations informatiques en éliminant les trous de sécurité les plus communs avant qu'un intrus malveillant n'ait l'opportunité de les découvrir avant vous et de chercher à les exploiter.

Cependant, ce type de test ne peut donner qu'une idée à un instant précis du degré de sécurisation d'un système.

Or, il est certain que dans un laps de temps relativement court suivant l'audit, il y aura :

* Soit une modification majeure dans les services offerts sur le réseau (ajout d'un service quelconque, changement logiciel, ...).
* Soit l'apparition d'une nouvelle faille dans un service existant. (ce qui est assez commun).

On arrive alors très vite à la conclusion que l'intérêt des outils de détection de vulnérabilités ne se retrouve absolument pas dans un usage ponctuel, mais plutôt dans une utilisation à intervalles réguliers, où l'apparition d'une faille générerait automatiquement une alerte.

De plus, les technologies de détection de vulnérabilités ne sont pas encore vraiment au point. On trouve en effet régulièrement des failles imaginaires et on passe de même à coté de trous de sécurité béants. Au final, ces outils peuvent juste aider à la sécurisation des systèmes (pour une utilisation ponctuelle), ou surveiller, dans la durée un ensemble donné de machines (Utilisation continue).

|  |
| --- |
| CONCLUSION |

La sécurité est un vaste domaine complexe où l’on ne peut établir un modèle unique de règles, car les moyens mis en œuvre varient selon le type de réseau et les données à protéger. Néanmoins, certaines règles basiques sont valables pour tous les cas de figure :

**FORMER LES UTILISATEURS**

La sécurité est l'affaire de tous !L'expérience démontre qu’un nombre important des incidents de sécurité trouve sa source dans le comportement indélicat et non responsable des utilisateurs de base. Il faut donc instaurer un programme de sensibilisation qui apprend à chacun quelle est sa responsabilité en matière de sécurité. Voici quelques domaines à aborder:

* *La sécurité dans la vie de tous les jours* : utiliser et gérer ses mots de passe, sauvegarder ses fichiers, détruire les documents imprimés confidentiels…
* *Comment réagir* : aux incidents (virus, intrusions…), aux pannes,
* *Ce qui est permis et interdit* : installation de logiciels, politique d'usage d'Internet et du courriel.

On peut aussi faire signer une charte de la sécurité, afin de responsabiliser les utilisateurs.

**GESTION DES DROITS**

Au sein d'un établissement, tous les utilisateurs n'ont pas à avoir les mêmes droits ! Et la sécurité débute par une bonne administration du système : chaque utilisateur ne doit avoir accès qu’à ce qui lui est utile, et seulement à cela. Il ne doit pas pouvoir supprimer tel ou tel fichier, installer un logiciel, etc. Seul l’administrateur aura tous les droits, plus éventuellement 1 ou 2 collaborateurs de confiance pour les grosses sociétés.

Pensez aussi à supprimer les comptes des personnes (employé, stagiaire, étudiant…) qui quittent l'entreprise.

**DES MISES À JOUR REGULIÈRES**

Afin de corriger les failles ou bugs de vos systèmes d’exploitation, logiciels et autres, il est important de planifier des mises à jour régulières, et appliquer dès que possible les recommandations et les patchs constructeurs.

**LES SAUVEGARDES**

Il est indispensable d’avoir une politique de sauvegarde et la respecter scrupuleusement. Comme aucun système n’est infaillible, il est prudent de prévoir le risque de perdre des données importantes, voire capitales. De plus, il faudra vérifier de temps en temps les sauvegardes en restore pour éviter des surprises, lorsque l'on en a réellement besoin.

**S’INFORMER**

L’administrateur doit sans cesse se tenir au courant, tant à propos de découvertes de bugs, que de nouveaux virus ou nouveaux software/hardware, qui peuvent remettre en cause la sécurité de son système. Il peut, pour répondre à ce besoin, soit s’abonner à une liste de diffusion, soit suivre l’actualité sur des sites Internet, ou encore lire régulièrement un magazine spécialisé, selon ses préférences.

|  |
| --- |
| **Qu'est-ce que la sécurité informatique ?** |

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre où il est prévu qu'elles le soient.

La sécurité informatique couvre généralement trois principaux objectifs :

* L'intégrité, c'est-à-dire garantir que les données sont bien celles qu'on croit être
* La confidentialité, consistant à assurer que seules les personnes autorisées ont accès aux ressources
* La disponibilité, permettant de maintenir le bon fonctionnement du système informatique

|  |
| --- |
| **Des nécessaires besoins de sécurité** |

Avec le développement des usages liés à l'utilisation d'Internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs

|  |
| --- |
| **Mise en place d'une politique de sécurité** |

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyé.

La sécurité informatique doit toutefois être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance. C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, c'est-à-dire :

* Elaborer des règles et des procédures à mettre en oeuvre dans les différents services de l'organisation
* Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une intrusion
* Sensibiliser les utilisateurs aux problèmes liées à la sécurité des systèmes d'informations

La politique de sécurité est donc l'ensemble des orientations suivies par une organisation (à prendre au sens large) en terme de sécurité. A ce titre elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

Ainsi, il ne revient pas aux administrateurs informatiques de définir les droits d'accès des utilisateurs mais aux responsables hiérarchiques de ces derniers. Le rôle de l'administrateur informatique est donc de faire en sorte que les ressources informatiques et les droits d'accès à celles-ci soient en cohérence avec la politique de sécurité retenue. De plus, étant donné qu'il est le seul à connaître parfaitement le système, il lui revient de faire remonter les informations concernant la sécurité à sa direction, éventuellement de la conseiller sur les stratégies à mettre en oeuvre, ainsi que d'être le point d'entrée concernant la communication aux utilisateurs des problèmes et recommandations en terme de sécurité.

|  |
| --- |
| **La nécessité d'une approche globale** |

La sécurité d'un système informatique fait souvent l'objet de métaphores. Ainsi on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.

Cela signifie que la sécurité doit être abordée dans un contexte global :

* **La sensibilisation des utilisateurs aux problèmes de sécurité**
* **La sécurité logique**, c'est-à-dire la sécurité au niveau des données
* **La sécurité des télécommunications**
* **La sécurité des applications**
* **La sécurité physique**, soit *la sécurité au niveau des infrastructures matérielles* \*

|  |
| --- |
| **Typologie de Pirates** |

Le risque en terme de sécurité est généralement caractérisé par l'équation suivante :

risque=(menace * vulnerabilite)/ contre_mesure

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi. Le but de ce dossier est ainsi de donner un aperçu des motivations éventuelles des pirates, de catégoriser ces derniers, et enfin de donner une idée de leur façon de procéder afin de mieux comprendre comment il est possible de limiter les risques d'intrusions.

|  |
| --- |
| **Qu'est-ce qu'un hacker ?** |

Le terme de *hacker* est souvent utilisé pour désigner un pirate informatique. Les victimes de piratage sur des réseaux informatiques aiment à penser qu'ils ont été attaqués par des pirates chevronnées ayant soigneusement étudié leur système et ayant développé des outils spécifiquement pour créer une faille dans leur système.

Le terme *hacker* a eu plus d'une signification depuis son apparition à la fin des années 50. A l'origine ce nom désignait d'une façon méliorative les programmeurs émérites, puis il servit au cours des années 70 à décrire les révolutionnaires de l'informatique, qui pour la plupart sont devenus les fondateurs des plus grandes entreprises informatiques.

C'est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.

Aujourd'hui ce mot est souvent utilisé à tort pour désigner les personnes s'introduisant dans les systèmes informatiques

|  |
| --- |
| **Les différents types de pirates** |

En réalité il existe de nombreux types d'"*attaquants*" catégorisés selon leur expérience et selon leurs motivations :

* **Les white hat hackers**, hacker au sens noble du terme, dont le but est d'aider à l'amélioration des systèmes et technologies informatiques, sont généralement à l'origine des principaux protocoles et outils informatiques que nous utilisons aujourd'hui. Le courrier électronique en est un exemple
* **Les black hat hackers**, plus couramment appelés *pirates* (ou appelés également *crackers* par extension du terme), c'est-à-dire des personnes s'introduisant dans les systèmes informatiques dans un but nuisible
  + **Les Script Kiddies** (traduisez *gamins du script*, parfois également surnommés *crashers*, *lamers* ou encore *packet monkeys*, soit *les singes des paquets réseau*) sont de jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet, généralement de façon maladroite, pour vandaliser des systèmes informatiques afin de s'amuser.
  + **Les phreakers** sont des pirates s'intéressant au réseau téléphonique commuté (RTC) afin de les utiliser gratuitement grâce à des circuits éléctroniques (qualifiées de *box*, comme la *blue box*, la *violet box*, ...) connectés à la ligne téléphonique dans le but d'en falsifier le fonctionnement.
  + **Les carders** s'attaquent principalement aux systèmes de cartes bancaires pour en comprendre le fonctionnement et en exploiter les failles
  + **Les crackers** ne sont pas des biscuits apéritifs au fromage mais des personnes dont le but est de créer des outils logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants.
* **Les hacktivistes** (contraction de *hackers* et *activistes* que l'on peut traduire en *cybermilitant* ou *cyberrésistant*), sont des hackers dont la motivation est principalement idéologique. Ce terme a été largement porté par la presse, aimant à véhiculer l'idée d'une communauté parallèle (qualifiée généralement de *underground*, par analogie aux populations souterraines des films de science-fiction.

Dans la réalité ce type de distinction n'est bien évidemment pas aussi nette, dans la mesure où certains (white hat) hackers ont parfois été crackers (black hat hackers) auparavant et parfois inversement. Les habitués des listes de diffusion et des forums voient souvent des sujets à propos de la différence qu'il convient de faire entre *pirate* et *hacker*. Le terme de *troll* est généralement utilisé pour désigner les sujets délicats déclenchant un engouement dans les réponses.

Quelques exemples de trolls :

* je me suis fait pirater par un hacker
* Windows est-il plus robuste que Mac ?
* Mieux vaut-il utiliser PHP ou ASP ?
* ...

|  |
| --- |
| **La culture du "Z"** |

Voici un certain nombre de définitions propres au milieu "underground" :

* Warez : piratage de logiciels
  + Appz (applications + warez) : piratage d'applications
  + Gamez (games + warez) : piratage de jeux vidéos
* Serialz (serials + warez): il s'agit de numéros de série permettant d'enregistrer illégalement des copies de logiciels commerciaux
* Crackz (cracks + warez): ce sont des programmes écrits par des *crackers*, destinés à supprimer de manière automatique les système de protection contre la copie des applications commerciales

|  |
| --- |
| **Le langage "C0wb0y"** |

Les adeptes de la communication en temps réél (IRC, chat) se sont sûrement déjà retrouvés engagés dans une discussion avec un utilisateur s'exprimant dans une langue peu commune, dans laquelle les voyelles sont remplacées par des chiffres. Ce langage, particulièrement utilisé dans le milieu underground, se nomme le langage "c0wb0y". Il consiste à remplacer certaines lettres (la plupart du temps des voyelles) par des chiffres. Voici quelques substitutions possibles :

* E=3
* A=4
* B=8
* O=O
* I=|

Voici ce que celà donne sur des mots courants :

* Abeille = 4B3|ll3
* Tomate = T0m4t3

Cet article a pour but d'expliquer la méthodologie généralement retenue par les pirates pour s'introduire dans un système informatique. Il ne vise pas à expliquer comment compromettre un système mais à comprendre la façon dont il peut l'être afin de mieux pouvoir s'en prémunir. En effet, la meilleure façon de protéger son système est de procéder de la même manière que les pirates afin de cartographier les vulnérabilités du système.

Ainsi cet article ne donne aucune précision sur la manière dont les failles sont exploitées, mais explique comment faire en sorte de les déceler et de les corriger.

|  |
| --- |
| **Le but de l'agresseur** |

Les hackers ayant l'intention de s'introduire dans les systèmes informatiques recherchent dans un premier temps des failles, c'est-à-dire une vulnérabilité nuisible à la sécurité du système, dans les protocoles, les systèmes d'exploitations, les applications ou même le personnel d'une organisation ! Les termes de *vulnérabilité*, de *brêche* ou en langage plus familier de *trou de sécurité* (en anglais *security hole*) sont également utilisés pour désigner les failles de sécurité.

Pour pouvoir mettre en oeuvre un *exploit* (il s'agit du terme technique signifiant *exploiter une vulnérabilité*), la première étape du hacker consiste à récupérer le maximum d'informations sur l'architecture du réseau et sur les systèmes d'exploitations et applications fonctionnant sur celui-ci. La plupart des attaques sont l'oeuvre de *script kiddies* essayant bêtement des exploits trouvés sur Internet, sans aucune connaissance du système, ni des risques liés à leur acte.

Une fois que le hacker a établi une cartographie du système, il est en mesure de mettre en application des exploits relatifs aux versions des applications qu'il a recensées. Un premier accès à une machine lui permettra d'étendre son action afin de récupérer d'autres informations, et éventuellement d'étendre ses privilèges sur la machine.

Lorsqu'un accès administrateur (le terme anglais *root* est généralement utilisé) est obtenu, on parle alors de compromission de la machine (ou plus exactement en anglais *root compromise*), car les fichiers systèmes sont susceptibles d'avoir été modifiés. Le hacker possède alors le plus haut niveau de droit sur la machine.

La dernière étape du hacker consiste à effacer ses traces, afin d'éviter tout soupçon de la part de l'administrateur du réseau compromis et de telle manière à pouvoir garder le plus longtemps possible le contrôle des machines compromises.

|  |
| --- |
| **La récupération d'informations sur le système** |

L'obtention d'informations sur l'adressage du réseau visé, généralement qualifiée de **prise d'empreinte**, est un préalable à toute attaque. Elle consiste à rassembler le maximum d'informations concernant les infrastructures de communication du réseau cible :

* Adressage IP
* Noms de domaine
* Protocoles de réseau
* Services activés
* Architecture des serveurs
* ...

En connaissant l'adresse IP publique d'une des machines de votre réseau ou bien tout simplement le nom de domaine de votre organisation, un hacker est potentiellement capable de connaître l'adressage du réseau tout entier, c'est-à-dire la plage d'adresses IP appartenant à l'organisation visée et son découpage en sous-réseaux. Pour cela il suffit de consulter les bases publiques d'attribution des adresses IP et des noms de domaine :

* http://www.iana.net
* http://www.ripe.net pour l'Europe
* http://www.arin.net pour les Etats-Unis

Lorsque la topologie du réseau est connue par le hacker, il peut le scanner (le terme *balayer* est également utilisé), c'est-à-dire déterminer à l'aide d'un outil logiciel (appelé *scanner* ou *scanneur* en français) quelles sont les adresses IP actives sur le réseau, les ports ouverts correspondant à des services accessibles, et le système d'exploitation utilisé par ces serveurs. L'outil le plus connu pour scanner un réseau est [Nmap](http://www.insecure.org/nmap/), reconnu par de nombreux administrateurs réseaux comme un outil indispensable à la sécurisation d'un réseau. Cet outil agit en envoyant des paquets TCP à un ensemble de machines sur un réseau (déterminé par une adresse réseau et un masque), puis il analyse les réponses. Selon l'allure des paquets TCP reçus, il lui est possible de déterminer le système d'exploitation distant pour chaque machine scannée.

Il existe un autre type de scanneur, appelé *mappeur passif* (le plus connu étant Siphon), permettant de connaître la topologie réseau du brin physique sur lequel le mappeur analyse les paquets. Contrairement aux scanners précédents, cet outil n'envoie pas de paquets sur le réseau et est donc totalement indétectable des systèmes de détection d'intrusion.

Enfin certains outils permettent de capturer les connexions X (un serveur X est un serveur gérant l'affichage des machines de type UNIX. Ce système a pour caractéristique de pouvoir utiliser l'affichage d'une machine à travers le réseau) des stations présentes sur le réseau, afin d'étudier ce qui est affiché sur les écrans et éventuellement d'intercepter les saisies sur le claviers des machines vulnérables.

Lorsque le "scan" du réseau est terminé, il suffit au hacker d'examiner le fichier journal (*log*) des outils utilisés pour connaître les adresses IP des machines connectées au réseau et les ports ouverts sur celles-ci. Les numéros de port ouverts sur les machines peuvent lui donner des informations sur le type de service ouvert et donc l'inviter à interroger le service afin d'obtenir des informations supplémentaires sur la version du serveur.

Ainsi pour connaître la version d'un serveur HTTP, il suffit de se connecter au serveur Web en Telnet sur le port 80 :

*telnet www.commentcamarche.net 80*

puis de demander la page d'accueil :

*GET / HTTP/1.0*

Le serveur répond alors les premières lignes suivantes :

*HTTP/1.1 200 OK*

*Date: Thu, 21 Mar 2002 18:22:57 GMT*

*Server: Apache/1.3.20 (Unix) Debian/GNU*

Le système d'exploitation, le serveur et sa version sont alors connus.

Le *Social Engineering* (que l'on pourrait traduire par *ingénierie sociale*) consiste à exploiter l'erreur humaine, c'est-à-dire d'utiliser la naïveté et la gentillesse exagérée des utilisateurs du réseau, pour obtenir des informations sur ce dernier. Ce procédé consiste à entrer en contact avec un utilisateur du réseau, en se faisant passer en général pour quelqu'un d'autre, afin d'obtenir des renseignements sur le système d'information ou éventuellement pour obtenir directement un mot de passe. De la même façon une faille de sécurité peut être créée dans le système distant en envoyant un cheval de Troie à certains utilisateurs du réseau. Il suffit qu'un des utilisateurs exécute la pièce jointe pour qu'un accès au réseau interne soit donné à l'agresseur extérieur.

C'est la raison pour laquelle la politique de sécurité doit être globale et intégrer les facteurs humains (par exemple la sensibilisation des utilisateurs aux problèmes de sécurité) car le niveau de sécurité d'un système est caractérisé par le niveau de son maillon le plus faible.

|  |
| --- |
| **Le repérage des failles** |

Après avoir établi l'inventaire du parc logiciel et éventuellement matériel, il reste au hacker à déterminer si des failles existent.

Il existe ainsi des scanneurs de vulnérabilité permettant aux administrateurs de soumettre leur réseau à des tests d'intrusion afin de constater si certaines applications possèdent des failles de sécurité. Les deux principaux scanneurs de failles sont :

* Nessus
* SAINT

Il est également conseillé aux administrateurs de réseaux de consulter régulièrement les sites tenant à jour une base de données des vulnérabilités :

* SecurityFocus / Vulnerabilities

Ainsi, certains organismes (notamment les CERT) sont chargés de capitaliser les vulnérabilités et de fédérer les informations concernant les problèmes de sécurité.

|  |
| --- |
| **L'intrusion** |

Lorsque le pirate a dressé une cartographie des ressources et des machines présentes sur le réseau, il est en mesure de préparer son intrusion.

Pour pouvoir s'introduire dans le réseau, le pirate a besoin d'accéder à des comptes valides sur les machines qu'il a recensé. Pour ce faire, plusieurs méthodes sont utilisées par les pirates :

* Le **social engineering**, c'est-à-dire en contactant directement certains utilisateurs du réseau (par mail ou par téléphone) afin de leur soutirer des informations concernant leur identifiant de connexion et leur mot de passe. Ceci est généralement fait en se faisant passer pour l'administrateur réseau.
* La consultation de l'annuaire ou bien des services de messagerie ou de partage de fichiers, permettant de trouver des noms d'utilisateurs valides
* L'exploitation des vulnérabilités des commandes R\* de Berkeley.
* le **brute force cracking**, consistant à essayer de façon automatique différents mots de passe sur une liste de compte (par exemple l'identifiant, éventuellement suivi d'un chiffre, ou bien le mot de passe *password*, ou *passwd*, ...

|  |
| --- |
| **Extension de privilèges** |

Lorsque le pirate a obtenu un ou plusieurs accès sur le réseau en se logeant sur un ou plusieurs comptes peu protégés, celui-ci va chercher a augmenter ses privilèges en obtenant l'accès *root* (en français *superutilisateur* ou superadministrateur).

Dès qu'un accès *root* a été obtenu sur une machine, l'attaquant a la possibilité d'investiguer le réseau à la recherche d'informations supplémentaires.

Il lui est ainsi possible d'installer un *sniffeur* (en anglais *sniffer*), c'est-à-dire un logiciel capable d'écouter (le terme *reniffler*, ou en anglais *sniffing*, est également employé) le traffic réseau en provenance ou à destination des machines situées sur le même brin. Grâce à cette technique, le pirate peut espérer récupérer les couples *identifiants/mots de passe* lui permettant d'accéder à des comptes possédant des privilèges étendus sur d'autres machines du réseau (par exemple l'accès au compte d'un administrateur) afin d'être à même de contrôler une plus grande partie du réseau.

Les serveurs NIS présents sur un réseau sont également des cibles de choix pour les pirates car ils regorgent d'informations sur le réseau et ses utilisateurs.

|  |
| --- |
| **Compromission** |

Grâce aux étapes précédentes, le pirate a pû dresser une cartographie complète du réseau, des machines s'y trouvant, de leurs failles et possède un accès *root* sur au moins l'une d'entre-elles. Il lui est alors possible d'étendre encore son action en exploitant les relations d'approbation existant entre les différentes machines.

Cette technique d'usurpation d'identité, appelée *spoofing*, permet au hacker (dans le sens *pirate* du terme) de pénétrer des réseaux privilégiés auxquels la machine compromise a accès.

|  |
| --- |
| **Nettoyage des traces** |

Lorsque l'intrus a obtenu un niveau de maîtrise suffisant sur le réseau, il lui reste à effacer les traces de son passage en supprimant les fichiers qu'il a créé et en nettoyant les fichiers de logs des machines dans lesquelles il s'est introduit, c'est-à-dire en supprimant les lignes d'activité concernant ses actions.

|  |
| --- |
| **Conclusion** |

Si vous êtes responsable d'un réseau connecté à internet, il vous revient d'en assurer sa sécurité, et par conséquent de tester les failles de celui-ci. C'est la raison pour laquelle, un administrateur réseau se doit d'être au courant des vulnérabilités des logiciels qu'il utilise et de se "mettre dans la peau d'un pirate" afin d'essayer de s'introduire dans son propre système. Lorsque les compétences au sein de l'entreprise ne sont pas suffisantes pour mener à bien cette opération, il convient de faire réaliser un audit par une société spécialisé dans la sécurité informatique.

**LA SÉCURITÉ**

**DES SYSTÈMES D ’INFORMATION**

**SÉCURITÉ DES SYSTÈMES D’INFORMATION**

DE NOUVEAUX ENJEUX POUR LA SÉCURITÉ

⚫ LA GÉNÉRALISATION DES SYSTÈMES DISTRIBUÉS : DE NOUVEAUX RISQUES

⇨ MULTIPLICATION DES POINTS D’ACCÈS

⇨ HÉTÉROGÉNÉITÉ DES MATÉRIELS, DÉVELOPPEMENT DE LA MICRO-INFORMATIQUE COMMUNICANTE NOTAMMENT

⇨ EXTENSION DES SYSTÈMES

🡺 vers les partenaires

🡺 internationalement

⚫ DES FREINS À LA MISE EN PLACE D’UNE POLITIQUE SÉCURITAIRE

⇨ COÛT

⇨ PARFOIS INCOMPATIBLE AVEC LES PERFORMANCES

QUI NÉCESSITENT UNE DÉMARCHE SÉCURITÉ GLOBALE

LES OBJECTIFS

⚫ DISPONIBILITÉ

Garantir la continuité de fonctionnement de l’ensemble des ressources

⚫ INTÉGRITÉ

Maintenir l’intégrité des données du point de vue physique (sauvegarde) et logique (droits d’accès)

⚫ CONFIDENTIALITÉ

Assurer l’accès aux ressources aux seules personnes autorisées

LA DÉMARCHE

⚫ PARTIR D’UNE ÉVALUATION DES RISQUES

⚫ PRIVILÉGIER UNE APPROCHE GLOBALE SELON UNE DÉMARCHE SYSTÉMIQUE

⇨ intégration au niveau du schéma directeur

⇨ définition d’un plan sécurité

⚫ METTRE EN PLACE UNE ORGANISATION

⚫ METTRE EN PLACE UNE ORGANISATION

⇨ définir un poste de ***responsable sécurité du service informatique*** (RSSI) disposant de moyens financiers à la hauteur des objectifs définis.

⇨ ***définir le responsable*** pour chaque élément du système d'information. C'est celui qui devra décider des contraintes de sécurité et des droits d'accès correspondants.

⇨ établir des règles et procédures d'***évaluation du niveau de sécurité*** pour chaque donnée ou traitement ainsi que les droits associés à chaque fonction ou type d'utilisateur ;

⇨ définir les ***procédures à adopter pour tout mouvement dans les locaux*** : arrivée ou départ d'un employé, du personnel intérimaire (pour la gestion des badges par exemple), déplacement de matériels...

⇨ prévoir un ***aménagement des locaux*** permettant d'intégrer les protections nécessaires à son bon fonctionnement ;

⇨ ***sensibiliser le personnel à l'enjeu de la sécurité*** par des programmes d'explication et de formation afin d'obtenir leur adhésion et leur respect des contraintes sécuritaires ;

⇨ ***tester régulièrement le plan de secours*** : incendie, sauvegarde, maintenance...

LES SOLUTIONS TECHNIQUES

⚫ CONTRATS D’ASSURANCE

⚫ PROTECTION DES LOCAUX

⇨ Construction des locaux

⇨ Contrôle d’accès

⇨ Protection contre l’incendie

⇨ Protection contre l’inondation

⚫ PROTECTION DES MATÉRIELS

⇨ Continuité de l’alimentation électrique : onduleurs

⇨ Dispositifs à tolérance de pannes au niveau des architectures matérielles et de communication

⇨ Sites de secours

⇨ Contrôle du routage au niveau des réseaux

⇨ Télésurveillance

⚫ PROTECTION DES ACCÈS

⇨ Authentification

⚫ PROTECTION DES DONNÉES

⇨ Contrôle d’accès, compartimentation

⇨ Sauvegarde et journalisation

⇨ Antivirus

⚫ PROTECTION DES ÉCHANGES

⇨ Authentification

⇨ Codes de contrôle

⇨ Chiffrement

⇨ Signature électronique, notarisation

⇨ Serveur de sécurité, pare-feu (*firewall*)

⇨ Journal d’audit