ATTAQUE et DEFENSE dans un réseau

Intrusions au sein d'un réseau.

❖ SECURITE, UNE PREOCCUPATION A LA HAUSSE ET NON SANS RAISON

A - ETAT DES LIEUX : LES CHIFFRES DE LA SECURITE

B - LES PRINCIPAUX RISQUES POUR UN RESEAU INFORMATIQUE

1 - LES ATTAQUES VENANT DE L'EXTERIEUR

a - TECHNIQUES D'ATTAQUES
- **a - 1 - Les attaques directes**
- **a - 2 - Les attaques indirectes par rebond**
- **a - 3 - Les attaques indirectes par reponse**

b - AUTRES TECHNIQUES D'ATTAQUES :
- **b - 1 - Les sniffers**
- **b - 2 - Les scanners**
- **b - 3 - Les intrusions**
- **b - 4 - Les virus**

2 - LES RISQUES VENANT DE L'INTERIEUR
- **a - LES ERREURS D'UTILISATION**
- **b - ACCIDENTS "NATURELS"**
- **c - VOL, VANDALISME**
- **d - LES COUPURES DE SERVICES ESSENTIELS**
- **e - LE SOCIAL ENGINEERING**

❖ CONCLUSION ET LIENS

Sécuriser un réseau informatique

VULNERABILITE DES SYSTEMES ET SECURITE.

❖ SECURITE PASSIVE

- **1-LA SECURITE MINIMUM**
- **2-STRUCTURE DU RESEAU**
- **3-LA SEPARATION DES TRAFICS**
  - **Brins physiques et brins logiques**
  - **Installer les services réseau sur des machines dédiées**
- **4- METTRE DES FILTRES ET DES ALARMES SUR LE ROUTEUR D'ENTREE**
- **5- FIREWALL ET PROXY**
  - **Qu'est-ce qu'un firewall ?**
  - **De quoi protège un firewall ?**
  - **Qu'est-ce qu'un proxy ?**
  - **Structurez vos réseaux**

❖ LA SECURITE ACTIVE.

DETECTION.

- **1-LOGICIEL DE DETECTION SYSTEMATIQUE D'ERREURS.**
- **2-LES SYSTEMES DE DETECTION D'INTRUSIONS.**
- **3-UTILISATION DES AGENTS MOBILES DANS LES SYSTEMES DE DETECTION D'INTRUSIONS**
  - **a.Qu'est-ce qu'un agent mobile ?**
  - **b.Avantages et inconvénients des agents mobiles**
- **4.PERSPECTIVES POUR LA RECHERCHE**

SURVEILLANCE.

- **1-L'AUDIT DE SECURITE.**
- **2-LE TABLEAU DE BORD**.

ACTIONS CORRECTIVES

- **En cas d'incident, savoir que faire et le faire savoir !**

LA SECURITE, DEMAIN UN ENJEU POUR TOUS ?

ANNEXE

Intrusions au sein d'un réseau.

❖ SECURITE, UNE PREOCCUPATION A LA HAUSSE ET NON SANS RAISON

Qu'est ce que la sécurité informatique, que recouvre exactement cette notion ? La réponse est large et complexe si l'on prend en compte tout ce qui peut porter atteinte au bon fonctionnement d'un système d'information. Avant de tenter une définition, le mieux est encore de raisonner par défaut sur l'insécurité informatique.

Commençons par évaluer toutes les menaces que celle-ci peut faire peser sur l'entreprise. Un sinistre informatique entraîne le plus couramment la détérioration, voire la destruction de ressources. Lesquelles ? Il peut s'agir prioritairement de données plus ou moins sensibles. Dans ce cas, c'est le capital d'information de l'entreprise qui est atteint. Les matériels ou les systèmes d'exploitation peuvent aussi être touchés ou rendus inopérants. Il y a alors perte des immobilisations. Ces conséquences techniques directes ont pour les entreprises des implications financières très lourdes que le Computer Security Institute évalue au niveau mondial à 265,6 millions de dollars. Et le bilan n'est pas clos pour autant ! Ce serait sans compter avec les pertes indirectes liées à l'impact du sinistre sur l'exploitation de l'entreprise : perte d'image, de chiffre d'affaires, de clients…
Des propos alarmistes qu'il convient de relativiser en fonction du niveau de dépendance des entreprises vis-à-vis de leur informatique. Rappelons tout de même à cet égard que selon certaines études, 67 % des entreprises françaises déclarent dépendre fortement de leur système d'information.

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

$$\text{Risque} = \frac{\text{Menace x Vulnérabilité}}{\text{Contre-mesure}}$$

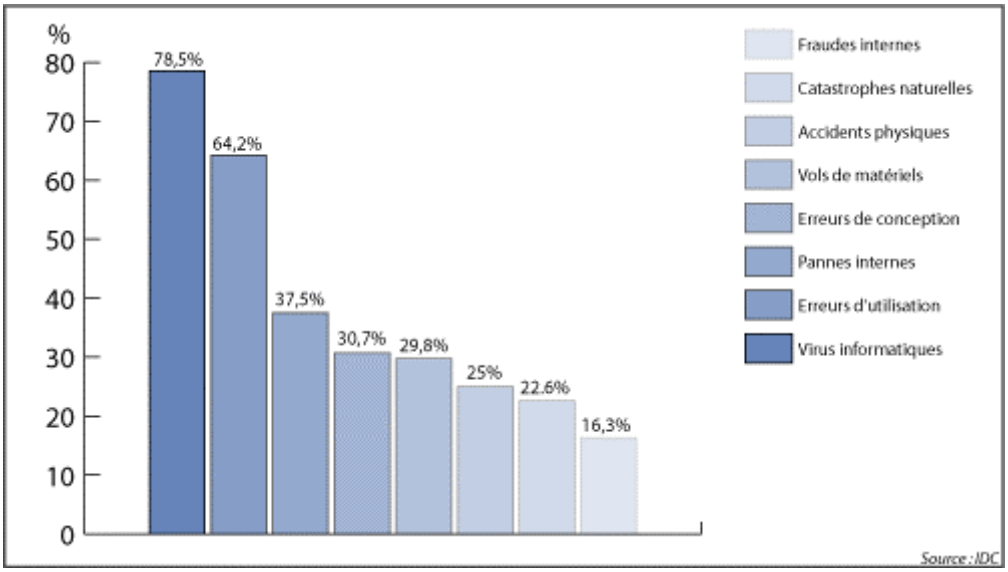
La sécurité informatique couvre généralement trois principaux objectifs :

- 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

A - ETAT DES LIEUX : LES CHIFFRES DE LA SECURITE

Quelle est la situation des PME/PMI sur le plan de la sécurité ? Seraient-elles plus à l'abri que les grandes entreprises et les institutions ? Leur consommation Internet a décuplé en cinq ans, portée par les messageries, l'achat en ligne et l'utilisation de services externalisés en mode ASP (Application Services Provider ou Fournisseur d'Applications Hébergées). Sensibilisées, elles le sont, mais sans pour autant engager une politique volontariste dans ce domaine. La sécurité n'est pas encore jugée comme un investissement à part entière et les moyens alloués ne sont pas toujours à la hauteur des risques encourus.

Une étude IDC réalisée auprès de 350 entreprises européennes révèle les principales attaques répertoriées :



35,2% des sociétés interrogées auraient été **victimes au moins une fois d'une attaque venue de l'extérieur**.

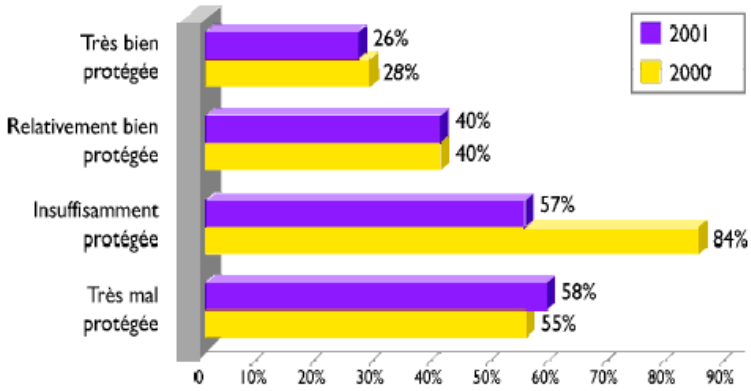
Cette étude nous apprend également que si 56,9% des entreprises considèrent que la sécurité est une affaire de spécialistes, 54,5% d'entre elles reconnaissent cependant ne pas avoir de ressource interne dédiée à cette tâche. En moyenne, en France, ce n'est que 1,6% du budget informatique des entreprises qui est consacré à la sécurité. Bien que 78,8% des entreprises interrogées estiment avoir suffisamment sécurisé leur système pour assurer la continuité de service en cas de problème, 8,4% des responsables informatiques reconnaissent tout de même ne pas savoir si leur entreprise dispose ou non d'un plan de sécurité.

Enfin, suite à cette étude, 48,1% des entreprises ont indiqué que leur direction générale avait l'intention de s'impliquer davantage dans la stratégie de sécurité en 2002.

Cette étude a été réalisée entre novembre et décembre 2001 auprès de 350 entreprises européennes dans 6 pays (France ; Allemagne ; Angleterre ; Italie ; Espagne ; Afrique du Sud).

Le "Rapport 2001 sur les crimes informatiques et la sécurité" réalisé par l'Institut sur la sécurité informatique et la police fédérale américaine (FBI) montre que les attaques au moyen de virus et d'autres infractions à la sécurité informatique sont en augmentation aux Etats-Unis. Seulement 35% des personnes interrogées ont accepté de divulguer les chiffres de leurs pertes, mais celles-ci s'élevaient à plus de 377,8 millions de dollars en 2001, soit une augmentation de près de 265,6 millions de dollars par rapport aux pertes enregistrées dans une étude identique en 2000.

L'analyse entre le sentiment de protection des entreprises et la prévision de renforcement des dispositifs de sécurité pour les deux ans à venir donne le graphe suivant :



Pour analyser ce comparatif 2001/2000 le plus justement possible, il est important de ne pas perdre de vue dans la comparaison le sentiment de confiance en très nette augmentation énoncé précédemment.

B - LES PRINCIPAUX RISQUES POUR UN RESEAU INFORMATIQUE

1 - LES ATTAQUES VENANT DE L'EXTERIEUR

a - TECHNIQUES D'ATTAQUES

Une attaque à distance est une agression contre une machine par une personne non autorisée. Une machine distante est : toute machine autre que la sienne pouvant être jointe grâce à un protocole à travers un réseau. De nombreuses méthodes existent, avec différents buts, en voilà quelques unes des plus répandues.

Les hackers utilisent plusieurs techniques d'attaques. Ces attaques peuvent être regroupées en trois familles différentes :

- Les attaques directes.
- Les attaques indirectes par rebond.
- Les attaques indirectes par réponses.

Nous allons voir en détail ces trois familles.

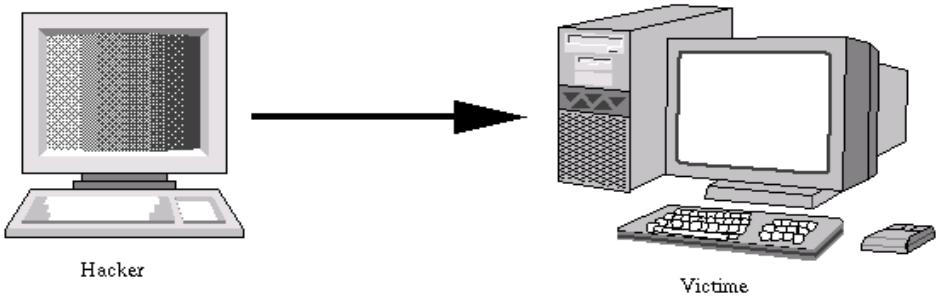
a - 1 - Les attaques directes

C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur. La plupart des "script kiddies" utilisent cette technique. En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

Il est à noter que le « script kiddies » n'en reste pas moins la forme la moins avancée des intrusions sur ordinateur.

En effet, les « Script Kiddies » utilisent des programmes existants (souvent créés par des crackers) pour accéder aux ordinateurs qui sont vulnérables. Cela n'exige qu'une faible connaissance, voir pas de connaissance du tout de la sécurité des ordinateurs puisque le « Script Kiddie » exécute seulement un programme. Néanmoins, ces individus aussi peu compétent qu'ils soient, constituent une menace pour

votre réseau au même titre que les crackers, non pas à cause de leur compétence, mais à cause de leur nombre. Il y a beaucoup plus « Script Kiddies » explorant Internet qu'il n'y a de crackers. Tôt ou tard, l'un d'entre eux doit nécessairement trouver un ordinateur vulnérable. Et, si vous n'êtes pas protégé, ce sera le votre.



Attaque directe

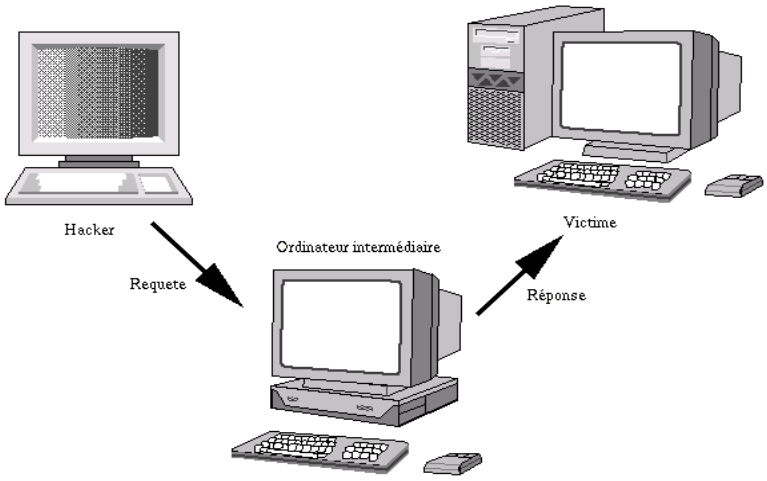
Si vous vous faites attaqués de la sorte, il y a de grandes chances pour que vous puissiez remonter à l'origine de l'attaque, identifiant par la même occasion l'identité de l'attaquant.

a - 2 - Les attaques indirectes par rebond

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

- Masquer l'identité (l'adresse IP) du hacker.
- Eventuellement, utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante...) pour attaquer.

Le principe en lui même, est simple : Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où le terme de rebond.



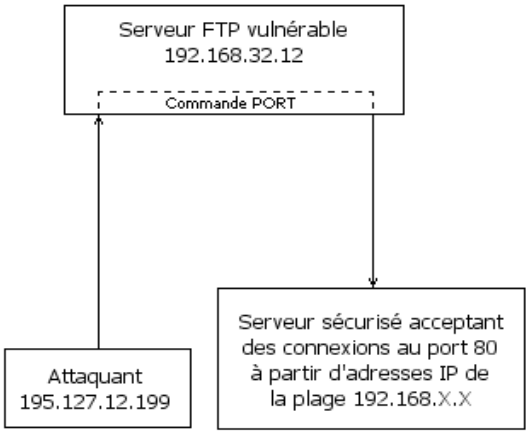
Attaque indirecte par rebond

L'attaque FTP Bounce fait partie de cette famille d'attaque.
Si vous êtes victime de ce genre d'attaque, il n'est pas facile de remonter à la source. Au plus simple, vous remontrez à l'ordinateur intermédiaire. Cette technique est basée sur une utilisation de la commande PORT du protocole FTP lorsque le serveur FTP est en mode actif. En effet, cette

commande permet de se connecter à n'importe quel autre serveur distant, et à un port donné. Dans ce cas, il est possible que la sécurité du serveur cible soit compromis, dans le cas ou il effectue une vérification des adresses IP d'origine. En effet, l'adresse IP que le serveur cible verra sera l'adresse IP du serveur FTP, et non l'adresse IP de l'attaquant.

Ce petit schéma explique la technique utilisée

:



a - 3 - Les attaques indirectes par reponse

Cette attaque est un dérivé de l'attaque par rebond. Elle offre les même avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.
Là aussi, il n'est pas aisé de remonter à la source...

b - AUTRES TECHNIQUES D'ATTAQUES

b - 1 - Les sniffers

Un sniffer est un dispositif, logiciel ou matériel, qui permet de capturer les informations qui transite sur la machine où il se trouve. Les sniffers ne sont pas des dispositif illégaux, ils servent par exemple à détecter des failles de sécurité ou à régler des conflits. Cependant, leur utilisation se révèle illégale quand la personne concernée n'a pas donné son accord. Ils peuvent ainsi, capturer le texte saisi sur la machine mais aussi toutes informations provenant des machines du réseau passant par la machine en question.
Les sniffers sont généralement utilisés pour récupérer les mots de passe d'un réseau. Pour cela, les sniffers enregistrent les entêtes de paquets émis et reçus.
Il existe quantité de logiciels permettant de « sniffer ». Pour n'en citer que deux, il y a par exemple : Sniffer Pro 3, NetXRay.

b - 2 - Les scanners

Un scanner est un programme qui permet de savoir quels ports sont ouverts sur une machine donnée. Les scanners servent pour les hackers à savoir comment ils vont procéder pour attaquer une machine. Leur utilisation n'est heureusement pas seulement malsaine, car les scanners peuvent aussi vous permettre de déterminer quels ports sont ouverts sur votre machine pour prévenir une attaque.
Sur le principe de fonctionnement, TCP et UDP utilisent les numéros de ports pour identifier les services des couches supérieures du réseau. Les scanners (ou scrutateurs) de ports permettent aux

administrateurs systèmes de déterminer les services TCP/UDP disponibles sur un serveur. L'une des règles fondamentales de la sécurité des serveurs est de désactiver tout service non utilisé par le système, car tout service TCP/UDP actif offre aux hackers une possibilité de pénétrer dans le système. Le scanner de ports vous permettra de vérifier que seuls les services TCP/UDP nécessaires sont exécutés.

Il existe plusieurs outils pour scanner les ports, combinant diverses méthodes pour détecter les attaques. NMAP est un des scanners de port qui fait parler le plus de lui en ce moment. Et cela pour 3 raisons, il fait parti des nouvelles générations de scanners qui analyse un réseau sans se faire repérer, il implémente l'option TCP/IP fingerprinting (empreinte de la pile TCP), qui permet à un hacker d'identifier près de 200 systèmes d'exploitation, et enfin parce qu'il est gratuit et que ces sources sont également disponibles (GNU).

D’autres logiciels de scan existent tel que : Netsnoop, Super Scan….

b - 3 - Les intrusions

Intrusion au moyen d'un "trojan"

Aujourd'hui les trojans (ou "chevaux de Troie") prolifèrent sous de nombreuses formes sur l'Internet et menacent toutes les machines connectées au réseau.
Ce genre de programmes tire son nom de la fameuse ruse grecque, ce qui dans notre cas consiste à le faire passer pour un logiciel alléchant (jeux, utilitaire performant ou encore logiciel XX...).
Sur le principe de fonctionnement, après avoir exécuter le fichier infecté, le trojan s'installe dans la base de registre pour faire en sorte de s'exécuter à chaque démarrage de votre PC. Certains troyens, plus vicieux, agissent comme un virus en infectant tous les programmes exécutables et ils n'augmentent leurs tailles que de quelques Ko (100 à 200 Ko).
Ensuite leur fonctionnement est calqué sur celui des logiciels de prise de contrôle à distance d'un PC, c'est à dire qu'il laisse en permanence une porte ouverte sur votre machine (un port)
Ensuite il ne reste plus qu'à ce que la personne malveillante vous "retrouve" et utilise la partie complémentaire du trojans, située sur sa machine, pour prendre le contrôle total de la votre.

LISTE NON EXHAUSTIVE DES PORTS UTILISES PAR DIFFERENTS TROJANS

Numéro du port	Type d'attaque possible
0	Troyen
19	Troyen
21	port FTP
23	port telnet
53	Troyen
59	Nuke, Flood
129	??
137	??
138	??
139	Nuke, Flood
666	??
1027	??
1029	??
1032	??
5000	Troyen : Socket 23
5001	Troyen : Socket 23
12345	Troyen : Netbus
12346	Troyen : Netbus
30303	Troyen
31337	Troyen : Back Orifice

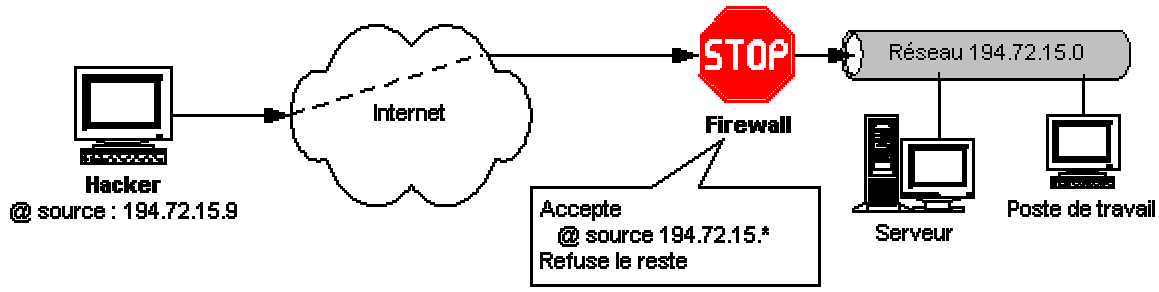
Intrusion au moyen des ressources partagées

Comme son nom l'indique, le partage de fichiers vous permet de partager des fichiers avec d'autres utilisateurs, donc de laisser ceux-ci venir lire, modifier, créer voire supprimer des fichiers sur votre disque dur.
Cette fonctionnalité peut s'avérer très utile lorsque vous êtes en réseau local (quelques machines connues reliées ensemble), mais devient très dangereuse si vous donnez - en le sachant ou non - ces permissions à n'importe qui sur internet.

L'IP spoofing

Est un mécanisme qui consiste à se faire passer pour une personne ayant une adresse IP attribuée, on falsifie donc l'adresse IP.

L'IP spoofing nécessite plusieurs étapes. Premièrement, l'attaquant doit choisir sa victime (un serveur). Ensuite, il doit trouver une configuration pour laquelle la victime autorise une connexion avec une machine de confiance. L'intérêt réside alors dans le but de se faire passer pour cette machine autorisée. Pour cela, la machine autorisée est rendue invalide (pour ne pas pouvoir réagir), les numéros de séquence du serveur sont analysés. Une connexion simulée avec des paquets falsifiés de l'attaquant est alors demandée au serveur avec des numéros de séquence devinés. Si la connexion est établie, l'attaquant modifie alors des informations pour permettre de revenir plus facilement ultérieurement.



Quelques exemples de logiciels pour le spoofing : Winspoof 97, Spewfy…

b - 4 - Les virus

Un virus est un programme capable de se reproduire dans un ordinateur, pouvant infecter d'autres programmes et ainsi se transmettre d'un ordinateur à l'autre, si l'on copie le programme infecté sur un ordinateur sain. S'ils ne faisaient que se reproduire, les virus n'inquiéteraient personne. Seulement voilà, ils peuvent être programmés pour être nuisibles, par exemple en effaçant les données de la machine sur laquelle ils s'exécuteront à une date précise.

2 - LES RISQUES VENANT DE L'INTERIEUR

Si les risques externes comme la fraude informatique et les attaques logiques ciblées ont été fortement médiatisés, il ne faudrait pas que l'arbre des virus et autres hackers cache la forêt des problèmes les plus courants dont la cause est souvent interne à l'entreprise !

a - LES ERREURS D'UTILISATION

L'erreur est humaine et peut affecter tous les stades de l'activité informatique : analyse, conception, réalisation, mise en oeuvre, utilisation. Les conséquences des erreurs peuvent être désastreuses, surtout si elles sont restées longtemps inaperçues et qu'elles ont provoqué de graves pertes. Il peut également arriver que l'on se trouve fort démuni face aux erreurs venant de l'amont : le bug de l'"An 2000".

b - ACCIDENTS "NATURELS"

Cette catégorie regroupe tous les sinistres comme les incendies, dégâts des eaux, explosions, catastrophes naturelles, etc. Certains de ces risques ne peuvent être raisonnablement pris en compte (ex. effondrement causé par la présence d'une ancienne carrière souterraine), d'autres peuvent être prévenus ou combattus (ex. incendie), l'informatique n'étant alors qu'un des aspects du problème.

c - VOL, VANDALISME

Ces problèmes sont la plupart du temps marginaux, sauf dans les grandes entreprises, l'administration et les établissements d'enseignement où les vols ou dégradations sont généralement commis par les personnes fréquentant habituellement les lieux (personnel, étudiants).

d - LES COUPURES DE SERVICES ESSENTIELS

Il s'agit de l'ensemble des causes pouvant entraîner l'indisponibilité ou le disfonctionnement total ou partiel du système. Ces causes sont multiples et l'on peut citer par exemple : l'électricité, télécommunications …Mais cela peut être aussi le fait de panne matériel.

e - LE SOCIAL ENGINEERING

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.

Au final, toujours selon les sources Clusif, les accidents et les erreurs d'utilisation représentent près de 80 % des causes de sinistres informatiques. Sans que l'on puisse imputer les 20 % restant à la seule malveillance d'intervenants extérieurs.
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.

❖ CONCLUSION ET LIENS

Alors que les individus et les organisations partagent de plus en plus d'informations, communiquent de plus en plus par Internet, la vulnérabilité aux attaques ou aux intrusions augmente. Autorisations, contrôles d'accès, exigences de confidentialité sont quelques exemples des composants technologiques disponibles dans une politique de sécurité multi-niveau. D'autres composants importants sont la formation à la confidentialité des mots de passe, une politique de sécurité d'entreprise et une sécurité système physique.

http://www.securityfocus.com
http://www.secuser.com/index.htm
http://www.microsoft.com/france/internet/securite.asp.
http://www.commentcamarche.com
http://www.snifferpro.co.uk
http://www.secusys.com/index.htm
http://www.guill.net/index.php3?cat
http://jmsylv.free.fr/hacking.h

VULNERABILITE DES SYSTEMES ET SECURITE.

❖ SECURITE PASSIVE

- **1-LA SECURITE MINIMUM**
- **2-STRUCTURE DU RESEAU**
- **3-LA SEPARATION DES TRAFICS**
  - **Brins physiques et brins logiques**
  - **Installer les services réseau sur des machines dédiées**
- **4- METTRE DES FILTRES ET DES ALARMES SUR LE ROUTEUR D'ENTREE**
- **5- FIREWALL ET PROXY**
  - **Qu'est-ce qu'un firewall ?**
  - **De quoi protège un firewall ?**
  - **Qu'est-ce qu'un proxy ?**
  - **Structurez vos réseaux**

❖ LA SECURITE ACTIVE.

DETECTION.

- **1-LOGICIEL DE DETECTION SYSTEMATIQUE D'ERREURS.**
- **2-LES SYSTEMES DE DETECTION D'INTRUSIONS.**
- **3-UTILISATION DES AGENTS MOBILES DANS LES SYSTEMES DE DETECTION D'INTRUSIONS**
  - **a.Qu'est-ce qu'un agent mobile ?**
  - **b.Avantages et inconvénients des agents mobiles**
- **4.PERSPECTIVES POUR LA RECHERCHE**

SURVEILLANCE.

- **1-L'AUDIT DE SECURITE.**
- **2-LE TABLEAU DE BORD**.

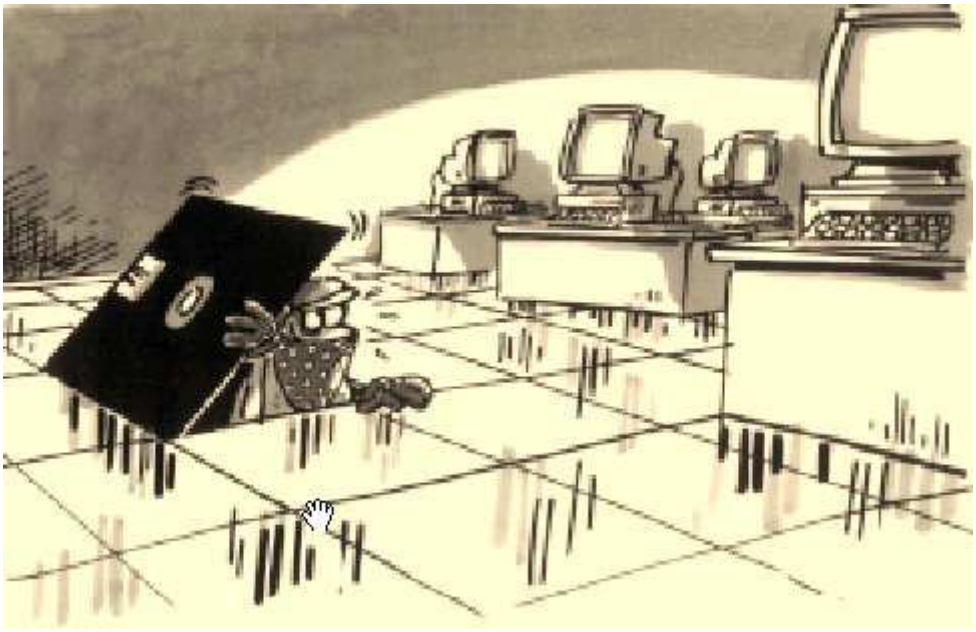
ACTIONS CORRECTIVES

- **En cas d'incident, savoir que faire et le faire savoir !**

LA SECURITE, DEMAIN UN ENJEU POUR TOUS ?

ANNEXE

Securiser un réseau informatique



VULNERABILITE DES SYSTEMES ET SECURITE.

La politique de sécurité est complexe et est basée sur des jugements humains, et on trouve notamment des faiblesses dues à la gestion et à la configuration des systèmes.
Il y a aussi en permanence de nouvelles technologies qui émergent, et par là, même de nouveaux points d'attaques.
Les bugs dans les programmes sont courants et seront toujours exploitables par les attaquants.
De plus, les mots de passe, par exemple, peuvent être cassés.
Enfin, même un système fiable peut être attaqué par des personnes abusant de leurs droits légitimes.
En dernier point, les organisations sont peu ou pas protégées contre les attaques sur leur réseau ou les hôtes du réseau et acceptent de courir des risques, car la sécurité n'est pas leur principale priorité, et représente une démarche coûteuse.

Faire de la sécurité sur des systèmes d'informations consiste à s'assurer que celui qui modifie ou consulte des données du système en a l'autorisation et qu'il peut le faire correctement car le service est disponible.
La sécurité ne doit pas rester statique car toute défense peut être contournée ; c'est pourquoi une bonne politique de sécurité comprend toujours deux volets :
-la sécurité passive
-la sécurité active

❖ SECURITE PASSIVE

La sécurité « passive » : c'est le blindage du système.
Elle se concentre trop souvent sur le point d'entrée du réseau interne et se caractérise par l'élaboration d'une politique de sécurité explicite, une organisation adaptée à cette politique, des procédures des méthodes de travail, des techniques et des outils…

▪ 1-LA SECURITE MINIMUM

- Protéger physiquement les machines contenant des informations sensibles (locaux à accès sécurisé : clef, reconnaissance vocale, digitale, iris, alarmé).

- Supprimer les informations confidentielles des machines reliées au réseau si elles n'ont pas besoin d'y être.

- Authentification des utilisateurs
-Proscrire les accès banalisés (guest, visiteur, invité…).
-Mettre en service une procédure d'entrée: signature d'une charte, attribution d'espace disque, machine, compte, ressources allouées.
-Vérifier régulièrement que tous les comptes ouverts sont encore d'actualité. Les comptes inutilisés depuis plus de trois mois doivent être désactivés.

-

-Vérifier régulièrement la solidité des mots de passe (avec un logiciel tel que « crack » ,ou LC4).

-Sensibiliser les utilisateurs aux problèmes de sécurité.

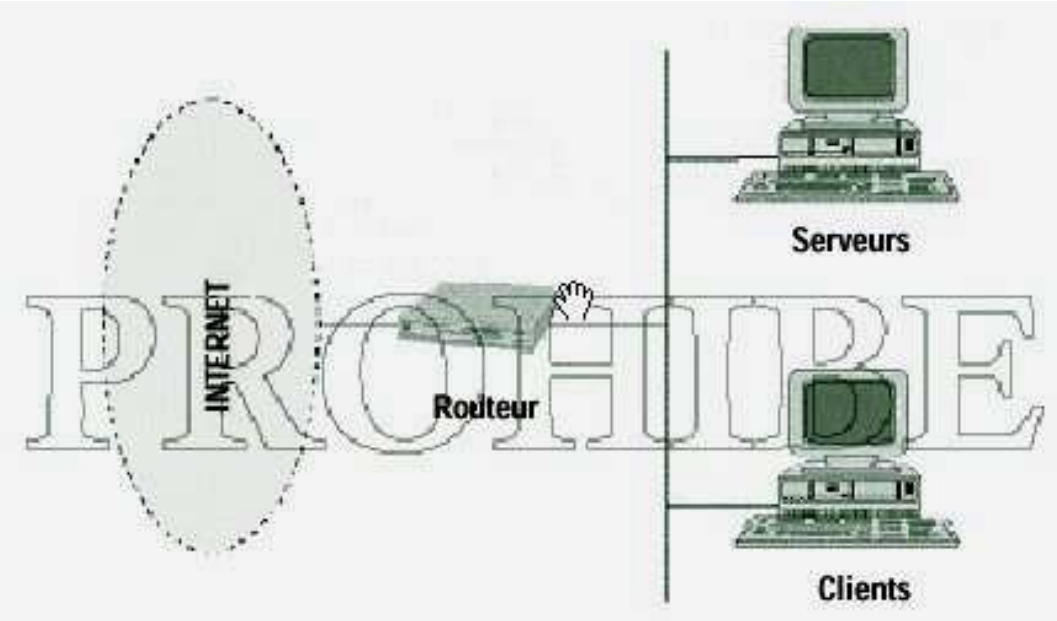
-Installer un logiciel anti-virus à jour sur chaque poste.

- **Toujours mettre à jour les systèmes avec les correctifs sécurité** (patchs, téléchargés sur les sites officiels !).

- Sauvegarder régulièrement les données (quoi, quand, comment ?) : les vérifier régulièrement !

2-STRUCTURE DU RESEAU

Les réseaux dits « Ethernet à plat » où toutes les stations sont connectées sur un même réseau de diffusion, présente plusieurs inconvénients majeurs :
– Il est possible d'écouter (ou sniffer), depuis n'importe quelle station, toutes les transactions sur le réseau. Un utilisateur malveillant peut ainsi découvrir très rapidement les mots de passe de tous les utilisateurs.
– Il n'est pas possible d'effectuer un quelconque tri en fonction du niveau de protection ou d'ouverture que l'on veut donner à une station. Certains serveurs nécessitent plus de protection que d'autres, certaines stations n'ont pas besoin d'être accessibles depuis l'Internet, …



Il faut ainsi préférer la commutation (éventuellement les concentrateurs sécurisés) qui limite les possibilités de l'écoute et le partitionnement (un sous-réseau par service, ou type d'activité, ou type de serveurs, ou…) qui est le début de la structuration.
Puisqu'on peut pénétrer également par le réseau, il va falloir mettre, là aussi, « une porte d'entrée ». Pour être utile, cette porte doit être pourvue de « serrures » permettant de restreindre les accès à ceux qui y sont autorisés, et il peut y avoir également un concierge qui veille sur « les entrées et les sorties », note les noms des visiteurs étrangers et vérifie que les demandes de services sont bien conformes aux instructions qu'il a reçues. Les concepts d'architecture réseau suivent l'offre commerciale qui est, elle-même, dépendante de l'évolution de la technique.

– le filtrage des accès et des services (le concierge vérifie les entrées) ;
– la journalisation de l'activité (le concierge tient un registre) ;
– l'authentification forte (la serrure de la porte).

▪ 3-LA SEPARATION DES TRAFICS

♦ Brins physiques et brins logiques

Une architecture réseau de sécurité est une architecture dans laquelle on a su séparer les différents flux d'information, au moins un sous-réseau physique (un brin ou un réseau virtuel) par type d'utilisation de machines : machines de services, machines de comptabilité, machines de direction, machines de gestion. L'idéal est d'organiser les sous-réseaux en groupes de travail cohérents qui constituent autant de compartiments étanches en cas de piratage. Il faut associer ces sous-réseaux physiques à des sous-réseaux logiques IP.

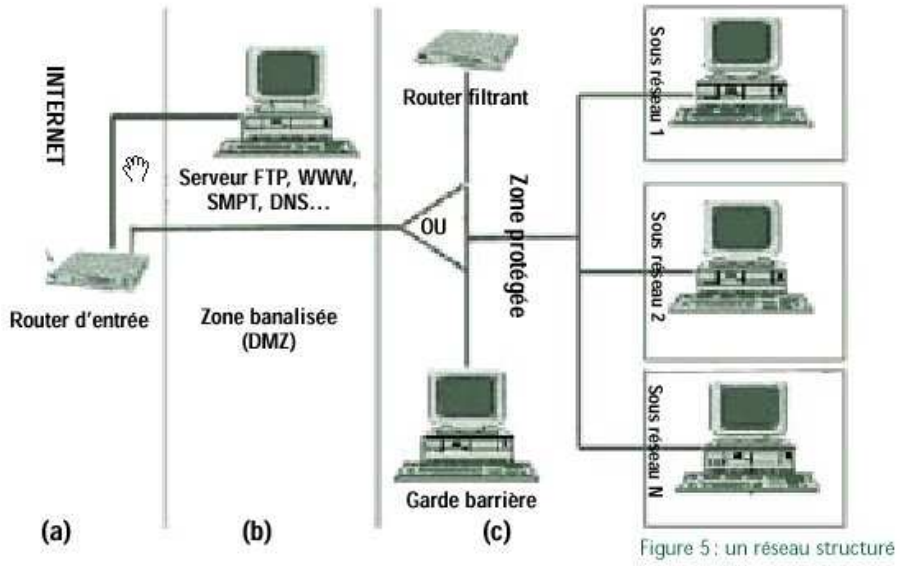


Figure 5 : un réseau structuré

♦ Installer les services réseau sur des machines dédiées

Les services comme le DNS, la messagerie, le web, le FTP anonyme… sont les services les plus utilisés depuis l'extérieur. Il est plus prudent de les installer sur des machines dédiées, sur lesquelles il n'y a pas (ou très peu) de connexion interactive possible et surtout ne pas y installer de répertoires utilisateur. Regrouper ces machines dans un sous-réseau particulier (appelé parfois DMZ) isolé du réseau interne par un élément filtrant, routeur ou garde-barrière.

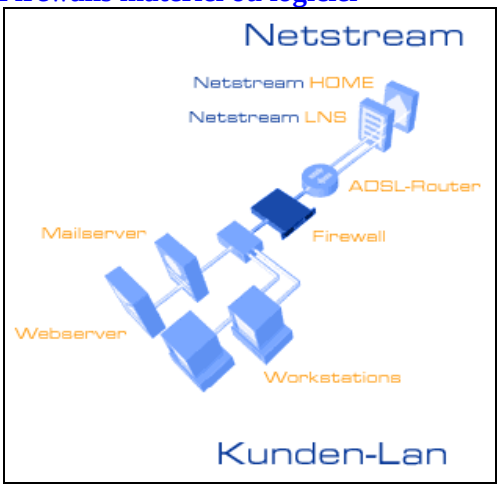
▪ 4- METTRE DES FILTRES ET DES ALARMES SUR LE ROUTEUR D'ENTREE

Un routeur, équipement qui initialement avait pour seule fonction l'interconnexion de réseaux, intègre maintenant de plus en plus les fonctions de sécurité qui sont devenues indispensables. Il est recommandé d'installer un équipement de ce type à la porte Internet et d'en faire assurer l'administration par son propre personnel afin de toujours rester maître de sa sécurité.
Sur ce routeur d'entrée, il vaut mieux interdire (sauf pour des besoins spécifiques) les services suivants:
Bootp, tftp, syslog, sunrpc, snmp, xdmcp, rlogin, rsh, lpr, openwin, imap, nfs, x11, irc, netbios, sqlserver, ipx, wins, ica et ica browser, rdp, back orifice, netbus.
Ce sont actuellement des services à problème potentiel : certains ont des versions boguées, d'autres sont très dangereux quand ils sont mal configurés sur les stations. Mais cette liste ne sera jamais à jour. Le mieux est donc d'avoir une politique de filtrage où « tout ce qui n'est pas explicitement autorisé est interdit ». On ne laisse alors passer que les services que l'on utilise (exemple : SMTP, protocole de messagerie, entrant uniquement vers le serveur de messagerie). L'installation d'un système de journalisation sur le routeur d'entrée, transmettant à une station protégée toutes les alarmes qu'il génère, en particulier l'activation d'un filtre, est le complément indispensable pour surveiller l'activité réseau.

5- FIREWALL ET PROXY

Afin d'éviter que des attaques puissent venir d'internet par le routeur, il convient d'isoler le réseau interne de l'entreprise. La méthode la plus connue est le firewall et le serveur proxy, mais il n'y a pas que ça... Par exemple, sur les routeurs, il est possible de faire du filtrage de paquets ou de la translation d'adresse pour qu'une personne de l'extérieur ne puisse ni accéder, ni voir ce qu'il y a à l'intérieur.
Un firewall est une entité qui fait cette opération de filtrage. On va pouvoir analyser les données qui rentrent et les interdirent si elles ne proviennent pas de quelqu'un de connu ou si elles ne répondent pas à une requête interne. Le firewall, placé à l'entrée du réseau, constitue ainsi un unique point d'accès par où chacun est obligé de passer...Le serveur Proxy, lui, permet de faire le relais au niveau des applications pour rendre les machines internes invisibles à l'extérieur. Si personne à l'extérieur ne peut voir les machines internes, l'attaque est beaucoup plus difficile, car l'attaquant est aveugle! N'oubliez quand même pas que 80% des attaques proviennent de l'intérieur du réseau et non de l'extérieur...

Firewalls matériel ou logiciel



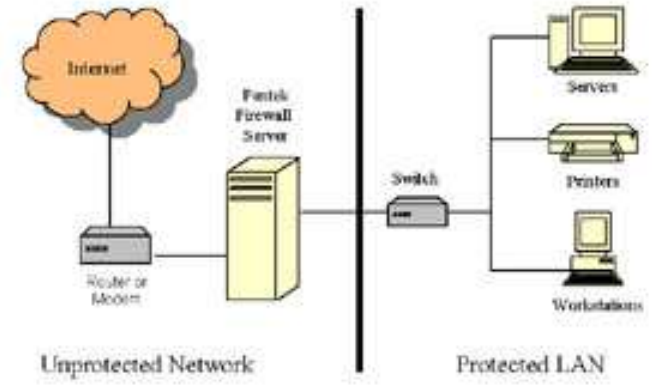


Figure 1 – Example Firewall

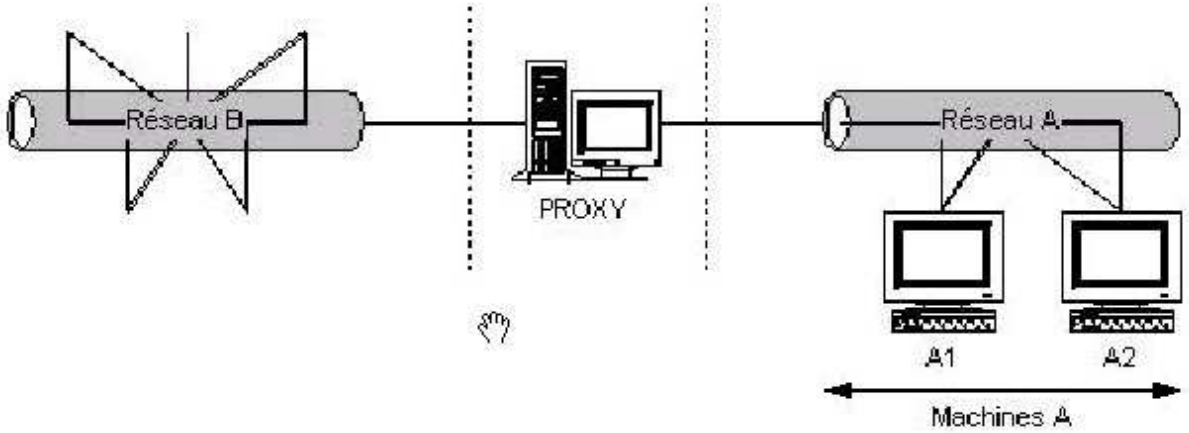
♦ Qu'est-ce qu'un firewall ?

Un firewall est un système ou un groupe de système qui gère les contrôles d'accès entre deux réseaux. Plusieurs méthodes sont utilisées à l'heure actuelle. Deux mécanismes sont utilisés : le premier consiste à interdire le trafic, et le deuxième à l'autoriser.
Certains firewalls mettent beaucoup d'énergie à empêcher quiconque de passer alors que d'autres tendent à tout laisser passer. La chose la plus importante à comprendre est qu'il représente une politique de contrôle d'accès.
Vous devez avoir une idée précise de cette politique dans son ensemble pour savoir ce que vous devez autoriser ou interdire.

♦ De quoi protège un firewall ?

Certains firewalls laissent uniquement passer le courrier électronique. De cette manière, ils interdisent toute autre attaque qu'une attaque basé sur le service de courrier. D'autres firewalls, moins stricts, bloquent uniquement les services reconnus comme étant des services dangereux.
Généralement, les firewalls sont configurés pour protéger contre les accès non authentifiés du réseau externe.
Ceci, plus qu'autre chose, empêche les vandales de se logger sur des machines de votre réseau interne, mais autorise les utilisateurs de communiquer librement avec l'extérieur.
Les firewalls sont également intéressants dans le sens où ils constituent un point unique où l'audit et la sécurité peuvent être imposés. Tous les échanges passeront par lui. Il pourra donner des résumés de trafic, des statistiques sur ce trafic, ou encore toutes les connexions entre les deux réseaux.

♦ Qu'est-ce qu'un proxy ?



Le but d'un serveur proxy est d'isoler une ou plusieurs machines pour les protéger :
Les machines A doivent se connecter au réseau par l'intermédiaire du serveur Proxy. Ce dernier sert de relais entre le réseau et les machines à cacher. Ainsi, les machines du réseau B auront l'impression de communiquer avec le proxy, et non les machines A.
Pour les applications du réseau B, l'adresse IP du client sera celle du serveur Proxy. Par exemple, lors d'une connexion à un serveur HTTP, le navigateur se connecte au serveur proxy et demande l'affichage d'une URL. C'est le serveur proxy qui gère la requête et qui renvoie le résultat à votre navigateur.
Ainsi, en utilisant un numéro de port différent, le proxy oblige toutes les requête à passer par lui en supprimant les trames dont le numéro de port ne lui correspond pas.
De plus, le proxy possède un avantage supplémentaire en termes de performances. Si deux utilisateurs demandent à peu de temps d'intervalle la même page, celle-ci sera mémorisée dans le proxy, et apparaîtra donc beaucoup plus rapidement par la suite.
Ce procédé est très intéressant en termes de sécurité sur Internet, les machines sont protégées. Le serveur proxy peut filtrer les requêtes, en fonctions de certaines règles (adresse IP, utilisateur, groupe, etc…).
Il convient aussi de ne pas faire les installations de programmes dans les dossiers proposés par défaut.

♦ Structurez vos réseaux

Les gardes-barrières et routeurs filtrants permettent de partitionner le réseau. Le garde-barrière (*firewal*l) permet de concentrer la sécurité en un point (normalement le point d'entrée dans un réseau ou un sous-réseau) et de contrôler tout le trafic. Le routeur filtrant permet de filtrer les paquets, les demandes de service réseau, et d'enregistrer les traces dans un but de vérifications, de diagnostics des incidents et éventuellement d'établissement de preuves en cas de piratage. Plus complets, les gardes-barrières applicatifs, qui intègrent des fonctions de relayage d'applications, permettent d'authentifier les utilisateurs, de contrôler tous les accès, de journaliser l'activité d'un sous-réseau et, éventuellement, d'intégrer des systèmes de chiffrement ou de faire un contrôle antivirus du flux entrant. En revanche, le routeur filtrant permet d'absorber des débits beaucoup plus importants que les gardes-barrières qui constituent très rapidement un goulet d'étranglement. Il faut être très attentif dans le choix des solutions : avant d'acheter un matériel, il faut faire une étude technique, organisationnelle et financière.

❖ LA SECURITE ACTIVE.

La sécurité « active » : c'est la défense « en profondeur »…qui est une surveillance permanente ou régulière des systèmes et qui complète la sécurité passive.
Elle consiste par exemple à :
– surveiller les moyens de protection pour contrôler leur efficacité (mais aussi l'efficacité de la politique de sécurité) ;
– détecter les attaques et les mauvaises configurations en enregistrant les accès aux services sensibles, en mettant en place des automatismes de détection d'intrusion, etc...
– répondre par des actions correctives : arrêt de session, reconfiguration dynamique des systèmes de contrôle d'accès, enregistrement des sessions.
– mettre en place des leurres.

DETECTION

▪ 1-LOGICIEL DE DETECTION SYSTEMATIQUE D'ERREURS.

Les pirates utilisent des logiciel de test de la configuration pour repérer les failles du système qu'ils attaquent (Cops, Satan,…). Ces logiciels permettent de façon automatique de chercher les erreurs de configuration ou les vulnérabilités du système. Si vous les utilisez avant le pirate et que vous réparez ces failles, ce sera moins facile pour lui!

Utiliser les logiciels des pirates pour repérer les vulnérabilités avant eux !

Comportement en cas d'attaque détectée
Déclenchement d'une alarme (passif) ou mesures correctives (actif). La plupart des systèmes actuels se contentent d'une alarme à l'administrateur du réseau.

Sources des données à analyser
- Sources d'information système (historique des commandes systèmes, accounting (usage des ressources partagées), système d'audit de sécurité)
- Sources d'information applicatives : fichier de log pour les applications
- Sources d'information réseau : dispositifs d'écoute du réseau

▪ 2-LES SYSTEMES DE DETECTION D'INTRUSIONS.

Vous pouvez utiliser un logiciel de détection d'intrusions. Comme pour une alarme dans une maison, ce logiciel émet une alarme lorsqu'il détecte que quelqu'un de non-autorisé est entré sur le réseau.

Tout comme les outils de monitoring, les IDS sont aussi des outils de monitoring. Sauf que ceux-ci ce focalisent sur les intrusions possibles en cours ou ayant eu lieu, sur votre réseau ou votre machine. Attention, en aucun cas un IDS ne peut remplacer un firewall, mais par contre ces deux outils peuvent se combiner.

Les trois principales fonctions d'un IDS sont :

-Le monitoring des intrusions.

-La détection des intrusions en cours.

-La réponse aux intrusions en cours.

La détection des intrusions est basée sur un principe de règles évènementielles qui correspondent à un comportement de tentative d'intrusion. Ces règles sont de part la suite regroupée en catégories (OS, Virus, SCAN, etc.). Si une de ces règles correspond à un comportement suspects, une alerte peut-être remontée à l'administrateur par SMS, Courrier électronique, etc. L'on peut aussi, enregistrer l'adresse

IP ou le nom d'utilisateur de la source de tentative d'intrusion et fermer le compte par exemple.

Deux types de IDS existent :

Les IDS hôte d'une seule machine (HIDS)
Ce type de IDS ne fait l'analyse que de ce qui se passe en source ou en destination de cette machine.

Les IDS réseau (NIDS)
Ce type de IDS font l'analyse de tous ce qui se passe sur votre réseau à tous niveau de protocole.

Il est possible bien sûr de combiner ces deux sortes de IDS.

Liste d'exemples de IDS :

NIDS : Snort, OpenSnort, Shadow, etc.

HIDS : Logsurfer, Swatch, Scanlogd, Nocol, Tripwire, etc.

- **Liens : SecurityFocus :** http://www.securityfocus.com/ , **Snort :** http://www.snort.org/

3-UTILISATION DES AGENTS MOBILES DANS LES SYSTEMES DE DETECTION D'INTRUSIONS

Une alternative à l'utilisation d'un module monolithique pour la détection d'intrusions est la mise en oeuvre de processus indépendants.

a.Qu'est-ce qu'un agent mobile ?

Un agent mobile est un programme autonome qui peut se déplacer de son propre chef, de machine en machine sur un réseau hétérogène dans le but de détecter et combattre les intrusions.
Chaque agent est un programme léger, insuffisant pour faire un système de détection d'intrusions entier car il n'a qu'une vision restreinte du système.

b.Avantages et inconvénients des agents mobiles

analogie entre le système immunitaire humain et cette approche : chaque cellule ou agent doit combattre les intrus avant que ça ne deviennent une menace pour le système.

Il y a des inconvénients : quand les agents se déplacent, un noeud dépourvu d'agent est vulnérable pendant un moment.
Ils imposent une utilisation des ressources et ce, quelque soit le système. Enfin, certains attaquants réussiront toujours à obtenir des droits pendant quelques temps avant d'être détectés.

Les agents risquent de demander d'assez gros programmes et le temps d'adaptation des agents à un système, car il y aura un manque de connaissance de base étant donné que beaucoup de plates-formes et de configurations sont différentes.

4.PERSPECTIVES POUR LA RECHERCHE

Les tendances vont de la machine vers le réseau, d'un système centralisé vers un système distribué, vers une plus grande interopérabilité des systèmes et vers une plus grande résistance aux attaques. Les constantes de la recherche sont l'utilisation d'un système hybride (approche comportementale et par scénarios) permettant de la détection en temps réel.

SURVEILLANCE.

1-L'AUDIT DE SECURITE.

L'audit de sécurité permet d'enregistrer tout ou partie des actions effectuées sur le système. L'analyse de ses informations permet de détecter d'éventuelles intrusions. Les systèmes d'exploitation disposent généralement de systèmes d'audit intégrés, certaines applications aussi. Les différents évènements du systèmes sont enregistrés dans un journal d'audit qui devra être analysé fréquemment, voire en permanence.
Les outils doivent être choisi en fonction de la politique de sécurité, et cet outils (en audit) ne doit pas perturber le travail des utilisateurs.

Spécification des activités systèmes à auditer
- Informations sur les accès au système (qui a accédé au système, quand, où et comment).
- Informations sur l'usage fait du système (commandes, utilisation des E/S, du CPU et de la mémoire).
- Informations sur l'usage fait des fichiers (quand, type et source de l'accès, volume d'info échangé).
- Information relatives à chaque application (lancements, arrêts, modules exécutés, E/S, commandes).
- Informations sur les violations éventuelles de la sécurité (tentatives de commandes non autorisés…)
- Informations statistiques sur le système (refus d'accès au système, usage de certaines commandes).

Analyse du journal d'audit
On cherche dans le journal d'audit les comportements portant atteintes à la confidentialité, à l'intégrité, ou à la disponibilité de service. Sur les réseaux, il est impératif d'avoir une base de temps commune pour estampiller les évènements.

Méthodes de détection d'intrusions

L'approche comportementale : détection d'une attaque exploitant une vulnérabilité inconnue :
- *Méthodes statistiques* : le modèle de Denning recoupant 6 éléments du systèmes et plusieurs modèles pour détecter une déviation de comportement.
- *Systèmes experts* : utiliser un ensemble de règles pour définir un comportement normal.
- *Les réseaux de neurones* peuvent être appliqués de plusieurs manières.

L'approche par scénarios : détection d'une attaque exploitant une vulnérabilité connue :
- *Systèmes experts* : ensemble de règles précisant la politique de sécurité et les failles du système.
- *Pattern Matching* (reconnaissance de forme) : représentation de l'attaque comme une suite de lettres d'un alphabet, chaque lettre étant un événement.
- *Algorithmes génétiques* : algorithme basé sur le système biologique permettant une analyse efficace.

Approche comportementale ou par scénarios ?
Avec l'approche comportementale, on a la possibilité de détecter une intrusion par une attaque inconnue jusqu'alors. Par contre, le choix des paramètres est délicat, ce système de mesures n'est pas prouvé exact, et on obtient beaucoup de faux positifs. Qui plus est, un utilisateur peut apprendre à la machine un comportement qu'il souhaite, notamment un comportement totalement anarchique.
Avec l'approche par scénarios, on peut prendre en compte les comportements exacts des attaquants potentiels. Par contre, la base de règle doit être bien construite et les performances sont limités par l'esprit humain qui les a conçues.
Quelques outils de détection d'intrusions

NIDES (Next Generation Expert System de l'US Navy)
Il s'appuie sur une approche statistique (modèle de Denning) et une approche " système expert ".
NIDES fonctionne sur une machine dédié indépendante du système surveillé. Le système cible transmet l'audit par le réseau de façon chiffrée. NIDES apprend les habitudes du système cible en étudiant les évènements d'accès aux fichiers et répertoires, de connexions, de consommation de ressources, d'exécution de commande, d'activité réseau et d'activité des programmes.
L'approche statistique de NIDES s'appuie sur deux types de mesures : les mesures continues quantifiables et les mesures catégorielles (nom de fichier…)

Le système expert de NIDES s'appuie sur une base de règles décrivant des comportements anormaux. Chaque règle déclenchée accroît un " taux de suspicion ".

LEURRE

Qu'est ce qu'un leurre honey pots (pot de miel)?

L'idée du leurre est d'installer un système d'exploitation non sécurisé ou présentant de nombreuses vulnérabilités permettant un accès facile à ses ressources. Le système leurre doit être installé de manière similaire à un serveur de production classique de l'organisation et doit comporter de nombreux faux fichiers, répertoires et autres données ressemblant aux vraies. Ce faisant, le honey pot ressemblera à une machine légitime avec des fichiers légitimes, laissant le hacker croire qu'il a obtenu un accès à des informations importantes. Avec un petit peu de chance, l'intrus restera dans les alentours pour rassembler des données pendant que l'honey pot collectera des informations sur l'intrus et la source de son attaque. Idéalement, les honey pots fournissent un environnement où les intrus peuvent être surveillé ou/et les vulnérabilités décelée avant qu'elle soient utilisées sur les vrais serveurs. Les leurres ne sont pas installés pour capturer les intrus mais pour surveiller et apprendre leurs mouvements, trouver comment ils sondent et exploitent le système et comment prévenir l'utilisation de ses vulnérabilités sur des serveurs de production sans que tout ceci ne soit remarqué par le hacker.

Quelques honey pots commerciaux et logiciels utiles

CyberCop Sting par Network Associates (Linux, Solaris, Cisco IOS et NT)

BackOfficer Friendly par NFR (émuler un serveur Back Orifice).

- **2-LE TABLEAU DE BORD**.

Il faut concevoir des indices statistiques afin de constituer des « tableaux de bord» qui permettent d'évaluer l'impact de la politique de sécurité sur la qualité de la recherche, l'organisation et le management. Ces tableaux de bord constituent une véritable métrique de la sécurité.
– Ils mesurent la vulnérabilité résiduelle d'un système d'information et permettent d'apprécier son évolution.
– Ils évaluent l'efficacité de la politique de sécurité.
– Ils indiquent les modifications de l'environnement.
- Ils alertent sur l'apparition de nouvelles faiblesses.

ACTIONS CORRECTIVES

- **En cas d'incident, savoir que faire et le faire savoir !**

Un incident de sécurité est toujours, un événement grave. Si un utilisateur découvre des traces permettant de suspecter une malveillance quelconque sur une machine, il doit d'abord, et avant toute chose, en informer le directeur. Mais ce n'est pas tout. Il faut aussi empêcher que le mal s'étende en prévenant ceux dont la charge est d'essayer de garder la sécurité du réseau. Il faut également isoler les systèmes d'information systèmes qui ont été violés, faire le bilan des dégâts et enregistrer tout ce qui peut permettre de retrouver l'origine de l'agression. Ce n'est qu'après tout cela que, finalement, on peut commencer à réparer. En résumé, lors d'un incident, il faut :

Déconnecter du réseau, la ou les machines suspectées, ou mettre un filtre qui empêche tout accès de l'extérieur.

Effectuer une sauvegarde du système pour conserver les traces de l'incident.
En particulier il faut vérifier toutes les machines du réseau et contrôler s'il y a un **sniffeur** installé. Si c'est le cas, changer les mots de passe de tous les utilisateurs sur toutes les stations.

Réinstaller le système et les comptes utilisateurs.

Ne donner aucune information sur l'incident à des tiers non habilités.

annexe « suis-je contaminé ? »

LA SECURITE, DEMAIN UN ENJEU POUR TOUS ?

Les systèmes informatiques et les réseaux, sont maintenant au coeur de tous les systèmes. Ce développement technique a permis d'accroître considérablement nos capacités de traitement, de stockage et de transmission de l'information ; mais il a rendu en même temps les systèmes d'information beaucoup plus fragiles. La gravité des accidents, des maladresses, des erreurs ou des malveillances est bien plus grande qu'auparavant : c'est souvent la perte de plusieurs jours, parfois de plusieurs semaines de travail. Ces pertes peuvent être même irréparables. Parallèlement, les techniques et les savoir-faire se sont généralisés. Il y a vingt ans, attaquer un système informatique centralisé demandait une certaine « technicité » qu'il n'est plus nécessaire de posséder aujourd'hui. On trouve sur Internet les « boîtes à outils » toutes prêtes permettant d'attaquer n'importe quel site, surtout s'il est mal administré.
Quoi qu'il en soit, l'utilisateur d'un réseau est un des maillons de la chaîne en ce qui concerne la sécurité puisqu'il a la charge de l'exécution de tous les actes élémentaires.

S'il ne voit ces mesures que comme une somme de contraintes mises en place pour lui gâcher la vie, la partie est perdue d'avance. D'où l'importance des recommandations de sécurité et des chartes informatiques qui, accompagnées des explications nécessaires, sont avant tout un moyen de sensibilisation.
Bien présentées, elles deviennent le « règlement intérieur du club des utilisateurs » ; elles sont alors facilement acceptées et la vie collective y gagne en qualité.

A l'inverse, le rigorisme est une autre déviance des conceptions de la sécurité. Opposé en apparence, cet autre excès aboutit au même résultat : le blocage du système d'information.

Il faut donc déterminer un seuil de vulnérabilité acceptable en fonction de contraintes et d'objectifs, et en contrôler les défaillances par des alarmes, des audits, et l'enregistrement des accès réseau.

De toute façon la sécurité est un enjeu fort pour demain et surtout l'affaire de tous ceux qui s'inscrivent dans la logique d'entreprise.

ANNEXE

Comment savoir si je suis contaminé ?

Lorsque 500 Mo en trop sont utilisés sur votre disque dur, vous pouvez penser qu'il s'agit d'un comportement normal de Windows. Certains logiciels peuvent en avoir besoin ou alors vous avez peut-être oublié de désinstaller un jeu. Toutes ces raisons peuvent cacher la vraie raison. Voici quelques comportements suspects qu'il faut à tout prix prendre au sérieux et chercher à en déterminer la cause, même si votre logiciel anti-virus vous affirme que vous n'êtes pas contaminé. En connaissant certaines des fonctions des chevaux de Troie, vous serez plus apte à réagir lorsque vous serez confrontés à de telles activités sur votre ordinateur. J'ai rajouté dans cet article des liens vers diverses bases de données relatives aux chevaux de Troie que vous devriez visiter si vous voulez approfondir vos connaissances.

- Lorsque vous visiter un site Internet, des fenêtres (pop-up) peuvent s'ouvrir automatiquement. Cela est tout à fait normal. Mais si jamais, alors que vous ne faîtes rien, votre navigateur vous emmène sur un site Internet que vous ne connaissez pas, alors vous devez vous inquiéter.

- Un message étrange peut apparaître sur votre écran, vous demandant de répondre à des questions personnelles.

- La configuration de Windows peut se modifier automatiquement, en changeant votre économiseur d'écran, la date et l'heure, le volume du son. La souris peut bouger toute seule et le lecteur de CD-Rom peut s'ouvrir.

Evidemment les attaquants les plus expérimentés se contenteront de vous espionner et d'utiliser votre ordinateur pour une raison particulière. Ils ne s'amuseront pas avec les astuces citées ci-dessus. Ils s'arrangeront pour ne pas éveiller la suspicion sur l'ordinateur cible évitant de se faire facilement remarquer.

Logiciels Anti-Virus

Les vieux logiciels anti-virus ne détectaient que les virus et seulement quelques rares chevaux de Troie très connus. Depuis, réalisant la gravité de la situation, la plupart des anti-virus détectent la majorité des chevaux de Troie. Mais, comme toujours, les gens pensent être en sécurité lorsqu'ils utilisent un logiciel anti-virus. Ils n'ont de réelle conscience sécuritaire.
Ces logiciels se basent sur la "signature" de chacun de ces chevaux de Troie et sur les méthodes connues d'exécution automatique. Mais il ne s'agit pas là de la solution parfaite. Les chevaux de Troie peuvent utiliser d'autres méthodes pour se cacher, de méthodes qui sont indétectables par les logiciels anti-virus. Lorsque les premiers logiciels anti-troyen sont sortis, les logiciels anti-virus, pour s'assurer leur clientèle, ont dû développer des modules anti-troyen, certains étant même très efficaces. Pour votre sécurité optimale, il est tout de même recommandé d'utiliser la combinaison d'un logiciel anti-virus et logiciel d'un anti-troyen.

De nouveaux chevaux de Troie apparaissent tous les jours et les logiciels de détection sont remis à jour quotidiennement pour la protection maximale de leurs clients. Mais souvent les utilisateurs ne mettent pas à jour leur fichier

de signatures aussi souvent qu'ils le devraient. Leur logiciel de détection est donc incapable de reconnaître certains virii et chevaux de Troie. Vous devez mettre à jour quotidiennement votre logiciel. Cela ne vous prendra que quelques minutes. Chaque fois que vous téléchargez un nouveau fichier, il doit être systématiquement analysé par vos logiciels avant d'être exécuté. Si, pour une raison quelconque, le fichier vous paraît suspect, ne l'exécutez sous aucun prétexte, mais envoyez le plutôt à votre laboratoire d'analyse de fichiers pour analyse.

.Logiciels Anti-Troyen

Voici une liste des logiciels anti-troyen les plus connus. Cette liste comprend aussi des logiciels, gratuiciel, divers qui vous aideront à analyser votre ordinateur à la recherche d'activités pouvant résulter de la présence d'un cheval de Troie. Je vous propose de visiter chaque site. Vous pourrez choisir vous-même le logiciel qui correspond au mieux à vos besoins. Dans la section des liens, vous trouverez des sites Internet vous proposant des analyses et des critiques des logiciels présents dans cette section.

-- TDS-3 --

Trojan Defence Suite (TDS) est un logiciel indispensable en matière de protection contre les chevaux de Troie. Il contient des fonctions encore jamais rencontrées dans d'autres logiciels. Ces fonctions sont très avancées et cela vous prendra certainement un peu de temps avant de pouvoir utiliser pleinement le logiciel. Lisez les excellent fichiers d'aide.

Vous pouvez télécharger TDS à http://tds.diamondcs.com.au/

-- LockDown2000 --

Il s'agit d'un très bon logiciel anti-troyen qui détecte une majorité des chevaux de Troie et autres logiciels de piratage. Il vous aidera à surveiller vos fichiers systèmes, les processus, la base de registre, ainsi que toute modification qui y sera apportée. Vous aurez plus d'informations sur le site Internet.

Vous pouvez télécharger LockDown2000 à http://www.lockdown2000.com

-- TFAK5 --

Trojans First Aid Kit (trousse de secours) est un scanneur de chevaux de Troie développé par SnakeByte. Il dispose de fonctions uniques. Il pourrait aussi être utilisé comme logiciel client pour certains chevaux de Troie.

Vous pouvez télécharger TFAK5 à http://www.snake-basket.de/tfak/TFAK5.zip

-- Trojan Remover --

Ce logiciel de détection reconnaît, le 15 août 2002, 5468 chevaux de Troie et vers, ainsi que leurs variantes. Des fonctions de surveillance des fichiers systèmes et de la base de registre sont incluses. Vous aurez plus d'informations sur le site Internet:

http://www.simplysup.com/tremover/details.html

-- Pest Patrol --

Cet utilitaire scanne votre ordinateur à la recherche de chevaux de Troie de certains logiciels de piratage connus ainsi que des logiciels espions. Vous aurez plus d'informations sur le site Internet officiel:

http://www.safersite.com/

-- Anti-Trojan 5.5 --

Ce logiciel est capable de supprimer la plupart des chevaux de Troie connus. Vous aurez plus d'informations sur le site Internet officiel:

http://www.anti-trojan.net

-- Tauscan --

Ce scanneur indispensable de chevaux de Troie dispose de fonctions uniques. Il est capable de détecter de nouveaux chevaux de Troie encore jamais distribués publiquement. Vous aurez plus d'informations sur le site Internet officiel:

http://www.agnitum.com/products/tauscan/

-- The Cleaner --

Logiciel anti-troyen très populaire, connu de tous. Visitez le site Internet:

http://www.moosoft.com/

-- PC Door Guard --

Logiciel de détection de chevaux de Troie. Il en détecte un nombre important et comprend aussi une fonction de surveillance des fichiers et des répertoires. Pour plus d'informations:

http://www.trojanclinic.com/pdg.html

-- Trojan Hunter --

Logiciel très pratique de détection de chevaux de Troie disposant de nombreuses fonctions.

Vous aurez plus d'information à http://www.mischel.dhs.org/trojanhunter.jsp

-- LogMonitor --

Cet un outil de surveillance des fichiers et des répertoires. Le logiciel s'exécute périodiquement et surveille la date de modification de fichiers sélectionnés. Il permet d'exécuter un logiciel externe. Il surveille aussi les répertoires à la recherche d'ajout, suppression et modification de fichier. Je recommande cet outil pratique et qui vous sera très utile.

Site Internet: http://logmon.bitrix.ru/logmon/eng/

-- PrcView --

PrcView est un gratuiciel permettant de surveiller les processus en cours,

montrant des informations détaillées sur chacun d'entre eux. Ces informations comprennent la date de création, la version, le chemin complet d'accès aux DLL utilisés par chaque processus, la liste complète des threads, blocs mémoire et des heaps. PrcView permet aussi de terminer ou d'ajouter un débuggeur un processus sélectionné. PrcView fonctionne sur les systèmes d'exploitation Windows 95/98 et Windows NT. Il comprend une interface graphique et en ligne de commande.

Pour obtenir PrcView: http://www.xmlsp.com/pview/prcview.htm

-- XNetStat --

Outil de surveillance réseau pour Windows avec une interface graphique. Il vous aidera à surveiller les ports ouverts sur votre ordinateur. Vous pouvez le télécharger à:

http://packetstormsecurity.org/Win/netstat.zip

-- ConSeal PC FIREWALL --

Un très bon pare-feu pour des utilisateurs avancés de Windows ayant des connaissance basique du TCP/IP et d'autres protocoles. Ce logiciel vous aidera à sécuriser votre ordinateur. Il possède de nombreux avantages sur d'autre pare-feu pour Windows. Pour obtenir le détail des fonctionnalités, visitez le site officiel:

http://www.consealfirewall.com/

Après Le Nettoyage

La sécurité de votre ordinateur a été compromise, des données sensibles ont pu être volées, des fichiers ont pu être modifiés et votre ordinateur a peut-être été utilisé dans le cadre d'activités illégales. Voici ce que vous devez faire après avoir nettoyé votre ordinateur de tout cheval de Troie.

- Le pirate connaît désormais les données de connexion à votre FAI (Fournisseur d'Accès Internet) comme vos mots de passe, ceux d'ICQ, de mIRC, de sites FTP ou de certains services web. Vous devez contacter votre FAI pour qu'il modifie votre mot de passe. Modifier aussi vos mots de passe ICQ et mIRC. Modifiez les même si, apparemment, ils n'ont pas été changés. Un pirate peut vous faire croire que tout va bien en prenant le soin de ne rien modifier. Il vous sera d'autant plus facile de récupérer vos données. Changez les mots de passe de vos comptes de courrier électronique, notamment ceux de compte en-ligne comme Yahoo! et Hotmail. Les pirates peuvent uniquement modifier la "question secrète" ce qui leur permettra de se connecter à votre compte que vous ayez modifié votre mot de passe ou non.

- Si vous utilisez la fonction carnet d'adresse de votre logiciel de courrier, vous y avez certainement entré la liste complète des adresses électroniques de vos amis ou collègues. L'attaquant peut utiliser cette liste et tenter de contaminer vos contacts. Informez-les de la situation et conseillez-les de vérifier à leur tour l'intégrité des fichiers que vous leur avez envoyés et la présence de chevaux de Troie dans leurs ordinateurs. Faites de même pour vos contacts ICQ. Ces derniers sont aussi des cibles potentielles.

- Rechercher sur votre disque dur la présence de d'espace libre manquant pouvant être occupé par des fichiers pirates ou par des images pédophiles pornographiques.

- Pensez aussi à toute donnée sensible que vous possédiez avant que la sécurité de votre ordinateur soit compromise. Si vous êtes persuadés que le pirate a pu y avoir accès, prenez les décisions nécessaire, comme contacter les propriétaires des données.

- Exécutez une analyse complète de votre ordinateur avec un logiciel anti-virus. Le pirate aura pu contaminer votre ordinateur avec des virus pouvant détruire vos données au cas où il n'aurait plus accès.

- Surveillez les processus du système d'exploitation, AVANT et APRES que vous vous soyez connecté à l'Internet. Pour vous tromper, certains chevaux de Troie peuvent s'exécuter une fois qu'ils ont détecté une connexion réseau. Soyez donc très vigilant.

Scanneurs En-Ligne

Ces services sont, de nos jours, devenus très pratique pour tout utilisateur n'ayant que peu de connaissance en matière de sécurité mais soucieux de se protéger. Si cette section se trouve à la fin de l'article, c'est qu'il y a une raison. Si vous avez lu l'article, vous êtes sensés avoir maintenant une bonne connaissance des chevaux de Troie, de leur fonctionnement et des techniques permettant de les détecter. Vous êtes alors capable de juger de l'utilité de ces scanneurs en-ligne ou s'ils vous procurent un faux sentiment de sécurité.

Il existe différents types de scanneurs en-ligne: Les scanneurs anti-troyen, les scanneurs de ports et les analyseurs de failles.

- Les scanneurs anti-troyen
  Ils utilisent une liste, avec des ports prédéfinis associés avec le nom du cheval de Troie utilisant son port par défaut, par exemple Girl Friend=21544. Si ce port en mode "écoute" est détecté sur votre ordinateur, le logiciel vous informera que vous êtes contaminé par le cheval de Troie Girl Friend. Mais, comme vous le savez maintenant, le cheval de Troie peut être modifié, selon le choix de l'attaquant, pour utiliser n'importe quel port. Ces scanneurs deviennent alors inutiles. Des attaquants sérieux n'oublieront pas de modifier le port.

- Les scanneurs de ports
  Ce service vous permettra de scanner les ports connus ainsi que la totalité des ports disponibles. Encore une fois, les ports connus sont ceux associés à des protocoles définis, par exemple 21-FTP, 23-Telnet, 25-SMTP. Le scannage total des 65.535 ports disponibles ne sera généralement pas proposé gratuitement à cause de la charge que représente l'opération en terme de bande passante. Une association avec les ports connus sera faite, mais dans le cas où le scannage découvrirait un port non-associé, il le mentionnera de la manière suivante: Port 34525 Etat:en écoute. Cela veut dire que ce port est prêt à recevoir une tentative de connexion de l'extérieur.

- Les analyseurs de failles
  Le but est d'analyser votre navigateur ou logiciel de courrier électronique à la recherche de failles. Si des failles sont découvertes, il vous sera proposé des liens vers des sites disposant de mises à jour ou de la dernière

version les corrigeant.

Il est conseillé de fermer tout logiciel utilisant l'Internet avant d'être scanné par de tels services. Vous pourrez décider quel service, capable de détecté une contamination, correspond le mieux à vos besoins. J'espère que vous connaissez maintenant les principes généraux ainsi que les réponses qui peuvent être apportées. Des liens vers certains de ces services ont été inclus dans la section des liens.

Conseils

Voici une section utile qui vous présente des astuces et des conseils pour se protéger des chevaux de Troie. Elle rassemble différentes techniques déjà expliquées auparavant mais résumées ici pour vous permettre les lire et de les comprendre plus facilement.

[01] N'acceptez de fichiers de personne, même d'un ami. Vous ne pouvez jamais être certain de l'identité réelle de l'expéditeur. Si vous avez besoin, par exemple, d'un document de travail, assurez-vous par d'autres moyens, comme le téléphone, que ce fichier provient bien de votre correspondant. Cela prendra certainement du temps, mais cet excès de précautions vous évitera une contamination.

[02] Avant d'exécuter un fichier, vérifier son extension. S'agit-il vraiment d'un .doc ou d'un exécutable avec l'icône d'un .doc.

[03] Mettez régulièrement à jour les bibliothèques de vos logiciels anti-virus et anti-troyen. Pour une sécurité optimale, faites-le quotidiennement. De nouveaux virus et chevaux de Troie sont découverts tous les jours. La plupart de ces logiciel ont une fonction de scannage automatique. Programmez cette fonction pour qu'elle se déclenche la nuit, alors que votre ordinateur est peut-être allumé. Cela renforcera encore l'efficacité de votre système de sécurité.

[04] Soyez toujours en possession de la dernière version de vos logiciels. Des nouvelles failles apparaissent fréquemment. Vérifiez aussi l'existence de tout problème de sécurité liés à vos logiciels et modifiez les ou mettez les à jour si nécessaire. Certains logiciels disposent d'une fonction de recherche automatique des mises à jour. Utilisez cette fonction.

[05] Prenez le temps de surveiller régulièrement les tâches exécutées par votre ordinateur avec certain des logiciels mentionnés. Vous serez surpris de ce que vous pourrez y trouver.

[06] Soyez conscient du risque que vous prenez en acceptant un logiciel envoyé par quelqu'un que vous venez de rencontrer sur ICQ ou IRC.

[07] Considérez les gratuiciels comme dangereux. Avant d'en télécharger un, recherchez les analyses dont ils ont fait l'objet.

[08] Lisez attentivement les fichiers d'aide des logiciels de détection pour être sûr de les utiliser le plus efficacement possible.

[09] Téléchargez un logiciel uniquement sur le site Internet officiel ou un à partir d'un site miroir référencé. Ne téléchargez jamais la dernière

version d'ICQ ou de mIRC d'un site hébergé chez un fournisseur d'espace gratuit comme Geocities. Considérez ce site comme sensible.

[10] Si vous voulez jouer avec des chevaux de Troie, vous pouvez aussi être contaminé. Certains auront pris le soin d'infecter des chevaux de Troie avec un autre cheval de Troie. Ils n'auront plus qu'a attendre qu'un apprenti moins expérimenté tente de les utiliser.

[11] Ne croyez pas tout ce que vous lisez sur l'Internet, et ne téléchargez pas des logiciels sur lesquels vous n'avez jamais rien lu.