CONTEXTE ET INTRODUCTION

Pour des soucis d'efficacité et de rentabilité, une entreprise communique aujourd'hui avec ses filiales, ses partenaires et va jusqu'à offrir des services aux particuliers, ce qui induit une ouverture massive à l'information. Cette entreprise possède certaines informations qui ne doivent être divulguées ni modifiées qu'à un certain nombre de personnes ou encore qui doivent être disponibles de manière transparente à l'utilisateur.

Ces informations feront l'objet d'un détournement si le système abritant ces informations est vulnérable. La sécurité devient alors un facteur décisif du bon fonctionnement de l'entreprise si celle-ci est connectée aux réseaux.

Le principe des réseaux est basé sur celui de l'autoroute : tout le monde y a accès et c'est à chacun de se protéger. L'actualité est également tournée régulièrement vers le partage des ressources peer to peer ou client serveur, qui permet de mettre en relation des utilisateurs via un même réseau interne ou étendu. L'administrateur du réseau doit prévoir en conséquence une politique de sécurité précisant la gestion des services, les droits d'accès, les services réseau disponibles, les précautions à prendre, les procédures à suivre lorsqu'une faille a été décelée dans la protection du réseau et enfin les méthodes de sauvegarde et restauration de données.

En effet, sans une politique de sécurité régulièrement mise à jour contre les menaces et les failles réseaux, un système connecté au réseau ne survit pas assez longtemps. En même temps que l'informatique et Internet ont révolutionné nos gestes et nos habitudes, des menaces qu'il faut connaître et apprendre à gérer ont aussi fait leur apparition en parallèle: Les virus, qui se cachent dans la messagerie ou sur des pages Internet au contenu douteux ou les spams, ces courriers électroniques indésirables qui polluent nos boites aux lettre n'en sont que quelque exemples. Quelles sont les menaces qui pèsent réellement sur nos matériels ? Comment s'en protéger ?

Ce mémoire à donc pour objectif d'identifier les ressources sensibles qu'il faut sécuriser dans un réseau d'entreprise, les risques et menaces potentiels liés au réseau et au système d'information et les solutions qui peuvent être mises en œuvre. Non seulement, la compréhension du fonctionnement des menaces n'est pas un acte de malveillance, mais c'est actuellement un besoin pour tout administrateur de réseaux (réseaux d'entreprise, réseaux informatiques, réseaux de télécommunication……) qui côtoie le monde des ordinateurs, car il aura un jour ou l'autre à les affronter.

CHAPITRE 1: GENERALITES SUR LA SECURITE DES INFORMATIONS ET DES RESEAUX

La notion de sécurité informatique couvre, en pratique, de larges problématiques.

Toutefois, s'il ne faut retenir qu'une seule définition, ce serait sans doute celle-ci : la sécurité consiste à adapter votre outil à l'organisation de votre entreprise et notamment définir qui doit avoir accès à quelles informations. Comme vos locaux, vos informations et votre réseau doivent être protégés.

La sécurité informatique, d'une manière générale doit donc assurer que les ressources sensibles d'une organisation sont disponibles et utilisées dans le cadre où il est prévu qu'elles le soient. Cela signifie que la sécurité informatique devrait être abordée dans un contexte global impliquant

- 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.

1 Les ressources sensibles [1] [3] [5] [10]

1.1 Les ressources humaines

Ce sont paradoxalement les personnes chargées de la sécurité et de l'administration des systèmes qui représente le risque humain le plus courant susceptible d'attenter à la sécurité d'un réseau. Parce que ces responsables ont accès à tout, et qu'ils ne sont pas à l'abri d'une simple erreur, les matériels d'un réseau et donc l'ensemble des utilisateurs, peuvent en subir les conséquences. Par ailleurs, toute personne ayant accès à une machine court un risque, quel que soit son niveau. Son mot de passe par exemple peut fort bien tomber sous le regard d'un pirate sans scrupule et expérimenté.

1.2 Les ressources logicielles

Aucun logiciel un tant soit peu complexe n'est exempt de « bug ». On a coutume de dire qu'un logiciel n'est jamais aussi efficace que le jour ou on n'en a plus besoin, car alors la plupart des erreurs qu'il pouvait comporter ont été corrigées. De ce fait, un logiciel peut fort bien, par erreur ouvrir une porte dans un système informatique en réseau, créant ainsi une faille de sécurité et permettre ainsi au pirate de tout ordre de s'infiltrer dans le système et de nuire à son intégrité.

1.3 Les Ressources physiques et matérielles

1.3.1 Les locaux

Un autre aspect non négligeable de la sécurité réseau est représenté par la sécurité physique. Elle constitue l'une des premières barrières à mettre en place, la sécurité d'un système réseau (informatiques, téléphoniques…) commence par celles des locaux accueillant les matériels. En effet, toute mesure de contrôle du système sera déjà fortement compromise si l'on permet à n'importe qui de pénétrer dans les locaux sensibles.

1.3.2 Les voies d'accès

La porte d'entrée n'est pas le seul moyen d'accès dans un central informatique ou télécommunication, il est, par conséquent très important de faire une liste des divers risques : une cloison ou une vitre peut se briser facilement, une gaine d'aération n'est pas forcément trop petite pour un homme, et enfin, il ne faut surtout pas oublier de protéger les câbles de connexion à des réseaux. Si, malgré tout, une intrusion malveillante est encore possible, le meilleur moyen de protection contre le vol d'un outil de télécommunication ou d'une station consiste à l'attacher à son support, ou à le fixer solidement au mur.

1.4 Les données

La protection des données se justifie en trois points bien distincts :

1.4.1 La disponibilité

On aime en générale avoir accès aux données en quasi-permanence.

1.4.2 Le secret

La notion de secret est très importante dans certaine entreprise. Imaginer un instant que quelqu'un puisse avoir accès aux données du nouveau produit que Microsoft® veut mettre en place, il va sans dire que quel que soit le type d'entreprise le fait de savoir que les secrets de tel ou tel produit est bien gardé est quelque chose de for plaisant. Il nous viendrait à l'esprit de séparer nos données confidentielles des accès réseau, une fois cela réalisé, pourquoi se soucier de l'aspect sécuritaire et tout simplement parce que le secret n'est pas l'unique point qu'il faut prendre en compte.

1.4.3 L’intégrité

Vous devez toujours vous soucier de l’intégrité et de l’accessibilité de votre système. En effet, même si vos données ne sont pas secrètes, vous souffrirez des conséquences de leur modification ou de leur destruction. Lorsque des données sont modifier ou détruits à votre insu, il faut dans la plus part des temps consacrer du temps à la reconstitution des dommages, ce qui bien évidemment nécessite du temps et de l’argent.

Voilà pourquoi, bien sécuriser un réseau est quelque chose de primordial. Il y a aussi un aspect qu’il faut prendre en compte, la perte de confiance de la part de vos clients, investisseurs et autres, qui, lorsqu’ils savent que vous vous êtes fait pirater ne veulent plus vous faire confiance.

1.5 La réputation

La notion de réputation est très importante, en effet, la plus part des entreprises préfèrent ne pas faire savoir que leur entreprise a été piratée tout simplement pour éviter une mauvaise publicité. Dire qu’on a été piraté insinue que votre site n’est pas du tout sécurisé. Le pirate apparaît généralement sur Internet avec votre identité, il se sert de votre identité pour aller créer des dommages à d’autres sites. Les messages provenant d’un intrus ayant eu accès à votre site ressembleront exactement aux vôtres parce que se seront les vôtres. Inutile donc d’imaginé ce que peut être la réputation d’une entreprise ayant l’étiquette gruyère. C’est pourquoi il faut mettre en place une bonne politique de sécurité ; mais avant de faire cela il faut déterminer contre quoi vous essayez de vous protéger.

La question est maintenant de savoir quels sont les risques et vulnérabilités qui sont omniprésents dans les systèmes réseaux ?

2 Risques et vulnérabilités liés aux réseaux [2] [13]

Lorsqu'une organisation telle qu'une entreprise, par exemple, envisage de fonder un réseau, il faut impérativement considérer le facteur sécurité. En effet, une connexion au réseau ne se fait pas sans risque. Un grand nombre d'utilisateurs des réseaux ne sont pas conscients des risques et des vulnérabilités liés à ces réseaux. Ces vulnérabilités viennent surtout d’une mauvaise protection du réseau interne de l’entreprise, le niveau de sécurité du réseau interne est primordial. On distingue plusieurs types de risques qui peuvent être regroupées en plusieurs catégories:

- Les vulnérabilités du réseau interne. L'introduction des services Internet dans un réseau d'entreprise peut ouvrir des trous de sécurité qui permettent à des intrus d'accéder au reste du réseau interne que ce soit physiquement ou logiquement.
- Les vulnérabilités des serveurs. On peut accéder à un serveur du réseau interne à partir de l'Internet pour lire ou même modifier les fichiers qu'il contient. Une société spécialisée dans la vente par correspondance (*on-line)* qui mémorise des numéros de carte de crédit sur un serveur connecté sur l'Internet est particulièrement exposée à ce risque.
- Les vulnérabilités de la transmission des données. La confidentialité et l'intégrité des informations peuvent être violées si un agresseur intercepte les communications du réseau d'entreprise (messagerie, serveur d'information, téléchargement de fichiers, etc.).
- Les risques de la disponibilité. Un agresseur malveillant peut réaliser une attaque qui rend des machines, ou même le réseau tout entier, indisponible pour les utilisateurs légitimes.
- Les risques de répudiation. Un partenaire dans une transaction en ligne peut nier qu'une transaction n'ait jamais eu lieu.

2.1 Les vulnérabilités techniques

2.1.1 Vulnérabilité du service TCP/IP

La vulnérabilité des services TCP/IP est due au fait que beaucoup de ces services ne sont pas surs et peuvent être compromis par des intrus bien informés. Dans un environnement LAN, ce sont surtout les services visant à améliorer l'administration du réseau qui présente le plus de vulnérabilités. Ces vulnérabilités hérité du manque de sécurité de TCP/IP se retrouvent dans un grand nombre d'applications comme celles basées sur les services RPC (Remote Procedure Call) comme NFS (Network File System), NIS (Network Information Service), les serveurs FTP, les serveurs de messageries notamment sendmail, etc...

De plus, le pilote protocolaire TCP/IP de plusieurs systèmes d'exploitations ne vérifie pas correctement certaines allocations de mémoire. Un utilisateur malveillant peut s'appuyer sur cette vulnérabilité pour exécuter du code arbitraire à distance, ou perturber l'accès au système ciblé.

2.1.2 Vulnérabilité des données

La facilité d'espionnage et de trucage des communications résulte du fait que la plupart du trafic qui transitent sur les réseaux, s'effectue "en clair", c'est-à-dire sans procédé de chiffrement. Par conséquent, les lignes de communication et donc les transferts de messages électroniques (*e-mail*), de mots de passe, de fichiers peuvent être surveillé et enregistrer à l'aide de logiciels spécialisés.

2.1.3 Les vulnérabilités dues à l'absence de politique de sécurité

Il n'est pas rare de constater qu'un réseau d'entreprise, par exemple, autorise plus de services entrée/sortie que nécessaire. Or, il est primordial de limiter l'accès à ces services qui peuvent permettre à un intrus connaissant bien le réseau interne d'obtenir des informations précieuses pour sa tâche d'espionnage ou de sabotage. Il est donc nécessaire d'établir une politique de sécurité définissant les restrictions d'accès et d'utilisation des services à appliquer.

2.1.4 Les vulnérabilités liées aux erreurs de configuration :

Le paramétrage de dispositifs de sécurité telles que des routeurs filtres permettant grâce à des listes d'accès (*access-list*) de limiter l'accès à des services, est souvent complexe et peut entraîner des erreurs de configuration accidentelles. De telles erreurs peuvent réduire à néant l'efficacité d'une politique de sécurité.

CHAPITRE 2 : LES ATTAQUES INFORMATIQUES UTILISANT DES TECHNIQUES

1 Chevaux de Troie [5] [7]

La légende veut que les Grecs, n'arrivant pas à pénétrer dans les fortifications de la ville de Troie, aient l'idée de donner en cadeau un énorme cheval de bois en offrande à la ville en abandonnant le siège. Les Troyens (peuple de la ville de Troie), apprécièrent cette offrande à priori inoffensive et la ramenèrent dans les murs de la ville. Cependant le cheval était rempli de soldats cachés qui s'empressèrent d'en sortir à la tombée de la nuit, alors que la ville entière était endormie, pour ouvrir les portes de la cité et en donner l'accès au reste de l'armée

Les chevaux de Troie (« Trojan horse » ou « Trojans » en anglais) tirent leur nom de cette célèbre légende mythologique. Comme cette dernière, ils utilisent une ruse pour agir de façon invisible, le plus souvent en se greffant sur un programme anodin.

Ils font parties des grandes menaces que l'on peut rencontrer sur le web, parmi les virus et autres vers. Pourtant, contrairement à ceux-ci, les chevaux de Troie ne se reproduisent pas (en tout cas, ce n'est pas leur objectif premier). Ce sont à la base de simples programmes destinés à être exécutés à l'insu de l'utilisateur.

1.1 Définition

Un cheval de Troie est un programme informatique simulant de faire quelque chose, mais faisant tout autre chose à la place. A la façon du virus, le cheval de Troie est un code caché dans un programme sain qui exécute des commandes sournoise, et qui généralement donne un accès à la machine sur laquelle il exécuté en ouvrant une porte dérobée (backdoor), le Trojan s'infiltre par la suite sur le disque dur pour y effectuer des actions néfastes une fois à l'intérieur, dès qu'on exécutera son fichier porteur. Un cheval de Troie est donc conçu pour espionner et infiltrer les systèmes. Ils sont furtifs et très difficiles à détecter, surtout tant que l'attaquent ne cherche pas à se manifester. Il est évidemment utilisé par les pirates (Hackers, Crackers, Script kiddyes….) pour prendre le contrôle d'un PC.

1.2 Principes

Le principe des chevaux de Troie étant d'ouvrir un port de votre machine pour permettre à un pirate d'en prendre le contrôle (par exemple voler des données personnelles stockées sur le disque), le but du pirate est dans un premier temps d'infecter votre machine en vous faisant ouvrir

un fichier infecté contenant le troyen et dans un second temps d'accéder à votre machine part le port qu'il à ouvert.

Toutefois pour pouvoir s'infiltrer sur votre machine, le pirate doit généralement en connaître l'adresse IP. Ainsi :

- Soit vous avez une adresse IP fixe (cas d'une entreprise ou bien parfois de particuliers connecté par câble, ...) auquel l'adresse IP peut être facilement récupérée
- Soit votre adresse IP est dynamique (affectée à chaque connexion), c'est le cas pour les connexions par modem ; auquel cas le pirate doit scanner des adresses IP au hasard afin de déceler les adresses IP correspondant à des machines infectées.

1.3 Modes d'action

Leur mode opératoire est souvent le même; ils doivent tout d'abord être introduits dans le système cible le plus discrètement possible. Les moyens sont variés et exploitent le vaste éventail des failles de sécurité, du simple économiseur d'écran piégé (envoyé par mail ou autre, du type cadeau.exe, snow.exe, etc, etc...) jusqu'à l'exploitation plus complexe d'un buffer overflow. Après leur introduction dans le système, ils se cachent dans des répertoires système ou se lient à des exécutables. Ils modifient le système d'exploitation cible (sous Windows, la base des registres) pour pouvoir démarrer en même temps que la machine. De plus, ils sont actifs en permanence (car un cheval de Troie est un véritable serveur, il reste à l'écoute des connections provenant de l'attaquant pour recevoir des instructions) mais ils restent furtifs et sont rarement détectables par l'utilisateur. Ainsi, un listing des tâches courantes ne fournira pas d'indication suffisante : soit le cheval de Troie y sera invisible, soit son nom sera tout ce qu'il y a de plus banal.

1.4 Objectif

Leur objectif est d'ouvrir une porte dérobée(« backdoor ») sur le système cible, permettant par la suite à l'attaquant de revenir à loisir épier, collecter des données, les corrompre, contrôler voir même détruire le système.

1.5 Fonctionnalités

Voici quelques exemples de fonctionnalités des chevaux de Troie :

- Accès Telnet : permet de lancer une application en mode texte « MS-DOS » ou « Invite commande » de façon invisible et de rédiger l'entrée/ sortie standard vers un port parti

culier. L'attaquant n'a plus qu'à s'y connecter (via Telnet) pour communiquer directement avec l'application.

- Accès http avec un navigateur qui supporte le téléchargement et l'envoi de fichier : permet de créer un serveur web basique dont la racine est celle du disque dur (défaut).Ainsi, un simple navigateur web permet de naviguer dans l'arborescence des fichiers, d'en télécharger et même d'en rajouter.
- Information sur le système distant
- Récupère tous les mots de passe : permet d'accéder aux fichiers mots de passe Windows (pwl et autres) et d'en afficher le contenu. A noter que les mots de passe utilisés pour des connections distantes, partager de documents, etc. sont également récupérés.
- Envoi de boite de dialogue (version Windows) avec réponse de l'utilisateur : permet de communiquer avec l'utilisateur.
- Télécharger / Envoyer / Supprimer / Créer des fichiers : permet d'accéder au système de fichiers dans sa totalité.
- Ouverture/Fermeture des fenêtres actives : permet d'interagir avec le système cible.
- Accès a la base de registre
- Augmenter / Diminuer le volume sonore
- Ajouter des plugins
- Démarrage d'application
- Jouer des fichiers. wave
- Afficher des images
- Ouvrir des documents
- Imprimer
- Fonction Keylogger : permet d'enregistrer toute frappe au clavier pour récupération et traitement ultérieur (mots de passe sur le web, mails, etc.….). Cette fonctionnalité existe également en version temps réel : affichage des frappes clavier en directe chez l'attaquant.
- Capture d'écran : permet de visualiser le poste de travail et les actions de l'utilisateur tout en économisant la bande passante (par rapport au streaming vidéo)
- Capture d'image si l'ordinateur est équipé d'une Webcam : opération basée sur l'utilisation détournée des librairies système (COM) qui supportent les webcams. Le résultat est complètement indétectable pour l'utilisateur.
- Capture du son si l'ordinateur / Serveur est équipé d'un microphone

- Eteindre l'ordinateur
- Redémarrer l'ordinateur
- Déconnecter l'ordinateur du réseau
- Dialogue avec l'utilisateur
- Ouverture /Fermeture du CD-ROM
- Inversion des boutons de la souris
- Envoyer l'utilisateur a une URL choisie
- Blocage du clavier

2 Espiogiciels (Spywares) [5] [7]

A chaque connexion Internet, un utilisateur laisse derrière lui très grand nombre d'informations. Ces traces sont généralement intéressantes mais non suffisantes à un public de professionnels ou d'espions cherchant à obtenir d'autres éléments que ces techniques laissés en standard .Les professionnels d'un secteur déterminé cherchent à connaître les habitudes de téléchargement de leurs clients, leurs modes de consommations, leurs centres d'intérêts, ou la périodicité de leurs achats par exemple. Les pirates ou espions seront, eux, plus intéresse par le contenu des machines connectées, la réception de ces informations, etc...

Pour faciliter la récolte de ce type de renseignements, il existe des« espiogiciels ».

2.1 Définition

Un espiogiciel est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel il est installé (on appelle donc parfois mouchard) a fin de les envoyer à la société qui le diffuse pour lui permettre de dresser le profil des internautes (profilage)

Ils se trouvent généralement dans le code d'un programme que l'utilisateur téléchargera innocemment sur Internet. Dans la plupart des cas, ces espiogiciels sont des « petits morceaux de codes parasite » (routines) intègres dans le code principal du programme .Dans un même programme, il peut y avoir plusieurs routines parasites différents, ayant chacune une fonction déterminée.

2.2 Objectif

L'objectif de l'espiogiciel est simple : récolter le maximum d'information possible sur un internaute .Les récoltes d'informations peuvent ainsi être :

- La traçabilité des URL des sites visités,
- Le traquage des mots –clés saisis dans les moteurs de recherche,
- L'analyse des achats réalisés via Internet,
- Voire les informations de paiement bancaire (numéro de carte bleue / VISA) ou bien des informations personnelles

2.3 Les types des Spywares

On distingue généralement deux types de spywares :

- Les spywares internes (ou spywares intégrés) comportant directement des lignes de codes dédiées aux fonctions de collectes données.
- Les spywares externes, programmes de collectes autonomes installées.

3 Keyloggers [5] [7]

3.1 Définition

Keyloggers ou Enregistreurs de frappes sont des portion de codes très dangereux, ils ne sont pourtant pas répertoriés parmi les virus ,vers ,ou chevaux de Troie car n'ont pas pour objectif de modifier quoi que se soit dans la machine cible .Ces programmes ,très furtifs ,sont à l'affût de ce que vous tapez sur votre clavier ,notamment des identifiants et des mots de passe. Les Keylogger se connecte ensuite au Net et envoie les informations ainsi collectées au pirate, qui peut ainsi s'introduire dans votre système sans effort.

3.2 Objectif

L'objectif des Keylogger est d'enregistrer et de restituer tout le travail qui a été réalisé par un utilisateur .Les touches enregistrées permettent effectivement de rétracter non seulement le travail courant ,mais aussi de récupérer tous les identifiants et mots de passes.

Certains Keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute activité de l'ordinateur!

3.3 Modes d'action

Ils sont installés directement par le pirate sur la machine visée, si l'ordinateur n'a pas de connexion Internet permettant une installation à distance via un cheval de Troie. En général, les

Keylogger se lancent directement au démarrage de la machine hôte. Une fois le Keylogger lancé, il enregistre au fur et à mesure tout ce qui est réalisé. Dans la plupart des cas ,si la machine cible est pourvue d'une connexion Internet ,un fichier ,le Keylogger enverra discrètement ,à une adresse mail ou à un serveur Internet ,un fichier ,généralement crypté,contenant tous les renseignements collectés .

3.4 Les Keyloggers logiciels et matériel

Les Keyloggers peuvent être soit logiciels soient matériels. Dans le premier cas il s'agit d'un processus furtif (ou bien portant un nom ressemblant fortement au nom d'un processus système), écrivant les informations captées dans un fichier caché!

Les Keyloggers peuvent également être matériel : il s'agit alors d'un dispositif (câble) intercalé entre la prise clavier de l'ordinateur et le clavier

4 Virus [4] [5] [7] [12]

En 1983, le chercheur Fred Cohen définissait un virus informatique ainsi « un programme qui peut contaminer un autre programme en le modifiant pour inclure une copie de lui-même », en d'autres mots, tous les virus se reproduisent d'eux-mêmes. Pour bien jouer le jeu, la plupart des virus tentent d'échapper aux détections, soit en utilisant des méthodes d'encryptage ou en effectuant de légères mutations chaque fois qu'ils se reproduisent.

Un virus informatique partage bien des traits communs avec son homologue biologique. Comme lui, il ne peut survivre par lui-même : il doit s'associer intimement avec un objet du système afin d'en faire son vecteur, et le détourner pour assurer sa reproduction et, donc, sa survie. Actuellement, plusieurs virus ont une charge utile, c'est-à-dire un ensemble d'instructions conçu pour perturber le cours normal du traitement informatique. La charge utile peut déclencher n'importe quoi, d'un message clignotant inoffensif jusqu'à la réécriture complète de la table d'allocation des fichiers, ce qui implique que vous perdez toutes les données de votre disque dur. Les virus utilisent souvent l'horloge interne de votre ordinateur pour déclencher la charge utile à une date particulière, les vendredis 13 et les anniversaires célèbres sont populaires

4.1 Principes de fonctionnement

4.1.1 Mécanisme de réplication

Ce mécanisme permet au virus de se répliquer. Il y a plusieurs méthodes pour y arriver :

- soit en infectant davantage de fichiers
- soit en utilisant un service réseau pour infecter d'autres ordinateurs

4.1.2 Charge utile

La charge utile est le coeur même du virus, c'est elle qui contient sa capacité de nuisance réelle. Elle peut être l'une de celles-ci :

- Affichage d'un message,
- Altérations mineures de fichiers,
- Destruction du contenu d'un disque dur,
- Détérioration lente du contenu des fichiers avec ou sans possibilité de restauration,
- Vol ou diffusion d'informations confidentielles.

4.1.3 Déclencheur

Le déclencheur peut être réglé pour :

- Une action immédiate
- Une action ponctuelle (un jour particulier)
- Une action répétitive (à chaque démarrage du système)

4.2 Mécanisme de protection

II.4.2.1 Compression

La compression est faite pour limiter la taille du code du virus, pour offrir un plus petit motif pour les anti-virus et pour ne pas attirer l'attention par des pertes de taille de disque.

4.2.2 Polymorphisme

Le polymorphisme permet de limiter la reconnaissance du code par les scanners anti-virus.

4.2.3 Furtivité

Il s'agit ici de rendre plus difficile la détection par l'anti-virus en détournant tous les appels au disque.

4.2.4 Multiples phases

C'est une méthode exotique de création de virus qui consiste à le faire passer par plusieurs modes d'infection. Le virus peut agir comme un virus macro puis comme un virus résident infectant les fichiers par des macros.

4.3 Caractéristiques

II.4.3.1 La résidence :

Dès son exécution, le virus s'extrait de son hôte et va se loger dans la mémoire vive où il prend le contrôle de la machine ;

4.3.2 La cryptographie

A chaque réplication, le virus est chiffré (afin de dissimuler les instructions qui, si elles s'y trouvaient en clair, révéleraient la présence de ce virus ou pourraient indiquer la présence de code suspect);

4.3.3 Le métamorphisme

Contrairement au chiffrement simple et au polymorphisme, où le corps du virus ne change pas et est simplement chiffré, le métamorphisme permet au virus de modifier sa structure même et les instructions qui le composent

4.4 Les catégories de virus :

4.4.1 Virus de Zone d'amorce

Un virus de zone d'amorce utilise la méthode la plus simple existante pour se propager. Il infecte la zone d'amorce des disques durs et des disquettes.

Pour être infecté, il faut avoir démarré sur une disquette, ou un disque amovible contenant le virus. Une fois la zone d'amorce de l'ordinateur infectée, ce virus se transmettra sur toute disquette ou support amovible inséré dans l'ordinateur.

4.4.2 Virus DOS

La plupart des virus fonctionnent sous le système d'exploitation DOS. Il est beaucoup plus simple d'écrire un virus pour DOS, car DOS existe depuis beaucoup plus longtemps que Windows et il y a donc beaucoup plus de gens ayant l'expertise nécessaire à ce genre de pratiques. De plus un virus écrit sous DOS sera beaucoup plus petit en taille que son équivalent écrit sous Windows.

4.4.3 Virus Windows

Les virus Windows fonctionnent sous Windows et vont pouvoir infecter les programmes Windows. Le nombre de virus Windows est beaucoup plus réduit que le nombre de virus DOS, néanmoins ils sont considérés comme une plus grande menace que les virus DOS puisque la plupart des ordinateurs fonctionnent maintenant sous Windows.

4.4.4 Virus Macintosh

La plupart des virus Macintosh connus à ce jour sont bénins et ne détruisent rien, ils se contentent d'afficher des images ou des messages. Les virus Macintosh sont spécifiques au mac et ne peuvent infecter des programmes Windows. Le nombre de virus Macintosh est assez réduit due à la complexité du système d'exploitation MacOS.

4.4.5 Virus Macro

Les virus Macros sont la plus grande menace à ce jour, ils se propagent lorsqu'un document Microsoft Word, Excel ou PowerPoint contaminé est exécuté. Un virus Macro est une série de commandes permettant d'effectuer un certain nombre de tâches automatiquement au sein des applications ci dessus. Le but non nuisible du langage de macro dans ces applications est à l'origine de pouvoir créer des raccourcis pour effectuer des tâches courantes, par exemple en une touche imprimer un document, le sauvegarder et fermer l'application.

Les Virus Macros non supprimés se répandent très rapidement. L'ouverture d'un document infecté va contaminer le document par défaut de l'application, et ensuite tous les documents qui seront ouverts au sein de l'application. Les documents Word, Excel et PowerPoint étant les documents les plus souvent partagés, envoyés par Internet, ceci explique la diffusion rapide de ces virus. De plus le langage de programmation des Macros est beaucoup plus facile à apprendre et moins compliqué qu'un langage de programmation classique.

4.4.6 Virus Polymorphe

Ceci est une sous catégorie, dans le sens ou n'importe lequel des types de virus ci dessus peut en plus être polymorphe. Les virus polymorphes incluent un code spécial permettant de rendre chaque infection différente de la précédente. Ce changement constant rend la détection de ce type de virus compliqué. Souvent le code change, mais l'action pour lequel il a été créé est toujours la

même. Par exemple, le virus peut intervertir l'ordre des instructions de son action en son sein, ou rajouter de fausses instructions afin de tromper la vigilance de l'antivirus, qui lui, recherche une signature précise.
Beaucoup de virus polymorphes sont aussi encryptés. Le virus encryptera son code et ne le décryptera que lorsqu'il doit infecter un nouveau fichier, le rendant encore plus difficile à détecter.

4.4.7 Virus Furtif

Un virus furtif, comme son nom l'indique, va se cacher lorsque l'ordinateur ou l'utilisateur accède au fichier infecté. Si l'utilisateur ou l'antivirus tente de voir si le fichier est infecté, le virus le saura et va se cacher offrant à l'antivirus et à l'utilisateur une version non infectée du fichier.

4.4.8 Virus Multi cibles

Les virus multi cibles utilisent à la fois les techniques d'infection des virus programmes et ceux de zone d'amorce. Ils infecteront donc à la fois les zones d'amorces et les programmes. Ces virus ont tendance à avoir une taille un peu plus élevée que les autres types puisqu'ils doivent contenir les instructions pour effectuer deux types d'infections. En doublant l'infection, le virus double sa chance d'être transmis à un autre ordinateur et de se répandre. Ceci explique qu'ils sont responsables d'un grand nombre d'infections, sans être très nombreux.

4.4.9 Virus résidents

Les virus résidents sont des virus qui se chargent en RAM et qui infectent les fichiers au fil du temps lors de leur ouverture ou exécution. Les plus récents de ces virus prennent souvent la forme d'un pilote virtuel sous Windows (.vxd). Ils sont alors chargés par le système d'exploitation lui même et avant les anti-virus. Ceci les rend plus difficiles à détruire.

4.4.10 Virus de fichiers exécutables

Ces virus disposent d'une fonction d'altération des fichiers exécutables présents sur les disques de la machine infectée. Ces virus utilisent plusieurs techniques d'infection :

- Virus par recouvrement : Ces virus écrasent le début des programmes cibles avec leur propre code machine. Le programme cible est alors inutilisable. Le seul avantage de cette technique est que la taille du code n'est pas modifiée.

- Virus par ajout : Ces virus altèrent le début du programme infecté pour faire exécuter le code viral en premier. Ce code est ajouté à la fin du fichier. La taille du fichier est modifiée.
- Virus par entrelacement : Cette technique est plus fine que les deux précédentes. Il s'agit alors d'insérer le code malicieux dans des zones non utilisées du programme. Ces zones sont typiquement entre les blocs du programme (code, données et pile).

4.4.11 Virus compagnons

Les virus compagnons sont des virus portant le même nom qu'un autre programme et qui utilisent la précédence des extensions. En effet, si l'on veut utiliser un programme prg.exe, qu'il existe dans le chemin un programme prg.com et que l'on appelle prg sans extension, c'est prg.com qui s'exécutera. Le virus compagnon utilise donc un nom de fichier du système ou courant en substituant l'extension .com à .exe. Il s'exécutera donc à la place de l'exécutable réel en .exe lors d'un appel sans précision de l'extension. Le virus compagnon peut, ou non, être dans le même répertoire que sa cible. Il suffit qu'il soit dans un répertoire situé dans la variable PATH. Ces virus sont apparentés aux chevaux de Troie.

4.4.12 Virus défensifs

Ces virus sont capables de désactiver ou détruire certains anti-virus. Ils sont donc capables de se propager sans être détectés.

4.4.13 Virus mailers et mass-mailers

Ces virus sont capables d'utiliser la messagerie électronique pour se propager. Les virus mailers envoient un mail à chaque activation. Les virus mass-mailers envoient plusieurs mails à chaque activation

5 Vers (Worm) [4] [5] [7] [12]

Vers 1988,un étudiant : Robert T.Morris ,de Cornell University avait fabriqué un programme capable de’ se propager sur un réseau , il le lança et,8heures après l’avoir lâché ,celui-ci avait déjà infecté plusieurs milliers d’ordinateurs .C’est ainsi que de nombreux ordinateurs sont tombés en pannes en quelques heures car le programme se reproduisait trop vite pour qu’il puisse être effacé

sur le réseau .De plus ,celui-ci a créer une saturation au niveau de la bande passante ,ce qui a obligé la NSA a arrêté les connexions pendant une journée.

5.1 Définition

Un vers est programme parasite. Il n'est pas forcément autopropageable. Le ver peut se « reproduire » de manière autonome, contrairement à un virus, qui pour fonctionner, nécessite un programme hôte. Le ver n'a pas besoin d'avoir un support physique ou logique (disque dur, programme hôte, fichier …) pour se propager, un ver est donc un virus réseau.

5.2 Buts

Le but d'un Ver est totalement maléfique : grignoter des ressources système : CPU, mémoire, espace disque, bande passante….

5.3 Mode de propagation

Ils se propagent, comme toutes données binaires, par disquettes, CD ROM, réseaux (LAN ou WAN) …Les pièces jointes des mails sont souvent leur mode de diffusion préféré. Ils apparaissent sous des noms des fichiers ayant les extensions * PIF,*EXE, *BAT,*SCR, ou *COM.

5.4 Mode de fonctionnements

Une fois lancés, ils se dupliquent et grâce à des fichiers attachés contenant des instructions permettant de récupérer l'ensemble des adresses de courrier contenues dans le carnet d'adresse, ils envoient des copies d'eux –même à tous ces destinataires.

6 Spam [2] [5] [7]

L'ouverture de nouveaux services par Internet est souvent l'occasion pour des pirates de tester leur sécurité .Dans le cas de la messagerie, la situation est particulièrement délicate en raison de la nature même la messagerie qui utilise des protocoles de transfert Internet (SMTP :
Simple mail transfert protocole).En effet, il est pratiquement impossible d'empêcher l'envoi de contenus subversifs, l'envoi de message collectifs (et la constitution de groupes favorise cela), ou encore l'usurpation d'une identité….

6.1 Définition

On définit le Spam comme une attaque visant à crasher un programme en faisant déborder un tampon (buffer) de taille fixe avec un trop grand nombre de données entrantes .

Peut aussi servir à submerger (flood) une personne ou un newsgroup avec des messages sans rapport avec les autres ou inappropriés.

6.2 Buts

Le but premier du Spam est de faire de la publicité à moindre prix par « envoi massif de courrier électronique non sollicité « (junk mail) ou par « multi postage abusif » (EMP).

6.3 Effets du Spam

Le principal inconvénient du Spam est l'espace qu'il occupe dans les boites aux lettres des victimes et la bande passante qu'il gaspille sur le réseau Internet.

7 Mail-bombing [2] [5] [7]

7.1 Définition

Le Mail-bombing consiste à envoyer un nombre faramineux d'emails (plusieurs milliers par exemple) à un ou des destinataires. En effet les mails sont stockés sur le un serveur de messagerie, jusqu'à ce qu'ils soient relevés par le propriétaire du compte de messagerie. Ainsi lorsque celui –ci relèvera le courrier, ce dernier mettra beaucoup trop de temps et la boite aux lettres deviendra alors inutilisable ….

7.2 Objectif

L'objectif étant de :

- Saturer le serveur de mails
- Saturer la bande passante du serveur et du oui des destinataires,
- Rendre impossible aux destinataires de continuer à utiliser l'adresse électronique.

8 Déni de service (Denial of Service) [2] [5] [7]

Le « Denial – of –service » ou Déni de service est une attaque très évoluée visant à rendre muette une machine en la submergeant de trafic inutile. Il peut y avoir plusieurs machines à l'origine de cette attaque qui vise à anéantir des serveurs, des sous réseaux, etc...

8.1 Définition

D'une manière générale, on parle de déni de service quand une personne ou une organisation est privée d'un service utilisant des ressources qu'elle est en droit d'avoir en temps normal. On trouvera par exemple des déni de service touchant le service de courrier électronique, d'accès à Internet, de ressources partagées (pages web), ou tout autre service à caractère commercial. Les attaques par « Denial of service « consistent à paralyser temporairement (rendre indisponible pendant un temps donné) des serveurs afin qu'ils ne puissent être utilisés et consultés. Les attaques par déni de service sont un fléau pouvant toucher tout serveur d'entreprise ou tout particulier relié à Internet.

8.1 Buts

Le but du « Denial-of-service » n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur Internet et éventuellement de nuire à leur fonctionnement si leurs activités repose sur un système d'information en l'empêchant de fonctionner.

8.2 Mode et techniques d'attaques

Les attaques par déni de service consistent en un envoi de paquets IP de taille ou de constitution inhabituelle, ayant pour cause la saturation de la machine victime. Pour être précis , le Denial of service se fait par le biais de l'envoi d'un datagramme IP de 65536 octets fabriqués grâce à la fragmentation .Une fois le datagramme refragmenté sur l'hôte distant on obtiendra un débordement de mémoire (communément appelé Buffer overflow) provoquant un plantage de la machine.

CHAPITRE 3 : LES AUTRES FORMES DE MENACE

1 Ingénierie Sociale (Social Engineering) [1] [3] [5] [7]

Le terme d'«ingénierie sociale» (social engineering) désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité. Il exploite la « faiblesse humaine » et permet de récupérer plus facilement et plus rapidement des informations que par une attaque « logique » avec technique. Contrairement aux autres attaques, elle ne nécessite pas de logiciel. La seule force de persuasion est la clé de voûte de cette attaque. Il y a quatre grandes méthodes de social engineering : par téléphone, par lettre, par Internet et in « situ ».

1.1 Le social engineering par téléphone

Le cas le plus typique de social engineering est la récupération d'information par téléphone.

Par exemple, l'attaquant commence par se renseigner au préalable sur la société, en recherchant des informations pertinentes via Internet : numéros de téléphone, nom, prénom, fonction des responsables de la société ou encore des informations relatives aux administrateurs du système d'information. L'attaquant va ensuite téléphoner et se substituer à une personne, un administrateur par exemple. Il prendra soin de donner quelques informations faisant penser à la victime qu'il appartient à l'entreprise ou qu'il est bien la personne qu'il prétend être. Ensuite, il va utiliser différentes manoeuvres psychologiques pour soutirer des informations. Il peut, par exemple, commencer à perturber la victime en lui indiquant qu'un virus très dangereux sévit sur sa machine et demander à cette personne d'effectuer des opérations plus ou moins complexes. Une fois que la victime est en disposition psychologique plus faible (stress), l'attaquant peut alors lui proposer qu'elle lui donne le login et le mot de passe pour qu'il fasse les manipulations à sa place. La victime, soulagée, sera alors bien contente de donner son mot de passe, sans forcément s'apercevoir du piège. Les services clients (« help-desk ») sont particulièrement vulnérables, car les employés sont entraînés à être serviables et à dépanner les utilisateurs. Il peut être facile de dire qu'on a oublié son mot de passe et qu'on a un travail très urgent à terminer. La personne du service client sera alors tentée d'effectuer une opération permettant l'accès illégitime. Le « social engineering » par téléphone peut également passer par le piratage du PABX de l'entreprise. L'attaquant pourra ainsi faire croire qu'il appelle de l'intérieur de l'entreprise, ce qui lui apporte un gain de confiance par rapport à sa victime.

1.2 Le social engineering par lettre

Le hacker vous fera une lettre très professionnelle. Au besoin, il n'hésitera pas à voir un imprimeur pour avoir du papier à lettre comportant un logo, un filigrane, téléphone, fax, email... Il utilisera très certainement une boîte postale pour l'adresse de sa société fictive.

1.3 Le social engineering par internet

Le social engineering par Internet est semblable à celui par téléphone. Le hacker se fera facilement passer pour un opérateur système, un responsable informatique ou un ingénieur système.

1.4 Le social engineering « in situ »

Le « social engineering » peut également être pratiqué dans les locaux même de l'entreprise. Le pirate ou l'espion industriel peut pratiquer du social engineering pour accéder aux locaux : un sourire avenant, une forte assurance, une décontraction certaine, costard, cravate, très classe, très propre, attaché-case, agenda rempli, documents divers, carte de visite, badge...Ensuite, il n'a qu'à fureter à droite à gauche, rentrer dans les bureaux vides, aller voir du côté des imprimantes et jeter un oeil dans les poubelles pour trouver des informations intéressantes.

2 Le Reverse Social Engineering (RSE) [1] [3] [5] [7]

Le « reverse social engineering » est une manoeuvre beaucoup plus complexe qui consiste à inverser la situation. Par exemple, ce n'est pas l'attaquant qui appelle pour récupérer des informations, mais la victime qui appelle l'attaquant pour les lui donner !

Un cas typique de « reverse social engineering » consiste pour l'attaquant à saboter une machine à laquelle il a accès par d'autres moyens. La victime qui s'aperçoit que la machine ne marche plus, va vouloir appeler quelqu'un pour l'aider. L'attaquant aura pris soin de faire savoir qu'il était capable de réparer les dégâts (en en parlant autour de lui, en laissant traîner des cartes de visite, en mettant un message d'erreur demandant explicitement de l'appeler en cas de panne, etc.). La victime appellera alors l'attaquant et sera toute disposée à lui confier des informations sensibles : numéro de contrat de support, login, mot de passe ...

3 Phising [1] [3] [5] [7]

Le phishing (contraction des mots anglais «fishing», en français pêche, et «phreaking», désignant le piratage de lignes téléphoniques) est une technique frauduleuse utilisée par les pirates

informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes. La technique du phishing est une technique d'«ingénierie sociale» c'est-à-dire consistant à exploiter non pas une faille informatique mais la «faille humaine» en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance. Le mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et les invite à se connecter en ligne par le biais d'un lien et de mettre à jour des informations les concernant dans un formulaire d'une page web factice aux couleurs du site original en prétextant par exemple une mise à jour du service, une intervention du support technique, etc…

Dans la mesure où les adresses électroniques sont collectées au hasard sur Internet, le message a généralement peu de sens puisque l'internaute n'est pas client de la banque de laquelle le courrier semble provenir. Mais sur la quantité des messages envoyés il arrive que le destinataire soit effectivement client de la banque. Ainsi, par le biais du formulaire, les pirates réussissent à obtenir les identifiants et mots de passe des internautes ou bien des données personnelles ou bancaires (numéro de client, numéro de compte en banque, etc.).

Grâce à ces données les pirates sont capables de transférer directement l'argent sur un autre compte ou bien d'obtenir ultérieurement les données nécessaires en utilisant intelligemment les données personnelles ainsi collectées.

4 Loteries [1] [3] [5] [7]

Vous recevez un courrier électronique indiquant que vous êtes l'heureux gagnant du premier prix d'une grande loterie d'une valeur de plusieurs (centaines de) milliers d'euro. Pour empocher le pactole il suffit de répondre à ce courrier. Après une mise en confiance et quelques échanges de courriers, éventuellement avec des pièces jointes représentant des papiers attestant que vous êtes bien le vainqueur, votre interlocuteur vous expliquera que pour pouvoir toucher la dite somme, il faut s'affranchir de frais administratifs, puis viennent des frais de douane, des taxes diverses et variées, etc. C'est de cette façon que ces cybertruands arrivent à extorquer des milliers d'euros à des internautes dupes de cette supercherie.

5 Hoax ou faux virus [1] [3] [5] [7]

Les virus canulars ne sont pas des virus en tant que tels. Il n'y a aucune technique sous-jacente. Un virus canular consiste simplement à envoyer un message électronique à des personnes, leur demandant d'envoyer ce message au plus grand nombre de personnes.

Ils peuvent donc avoir une capacité de nuisance réelle : saturation des messageries, saturation d'un numéro de téléphone cité dans le message, voire saturation de services administratifs ou hospitaliers évoqués dans le message. Ces canulars sont toujours construits de la même manière. Une introduction très alarmiste, des éléments pseudo techniques qui peuvent être démontés rapidement pour peu qu'on prenne la peine d'y réfléchir, des sources officielles citées à leur dépend, et la sempiternelle conclusion qui demande, pour sauver l'humanité toute entière de faire suivre le message au plus grand nombre de personnes. Certains de ces canulars sont d'ordre technique et évoquent le danger d'un hypothétique virus qu'il est facile d'éradiquer en détruisant certains fichiers sur l'ordinateur de l'internaute (fichiers nécessaires bien entendu au bon fonctionnement de l'ordinateur et qui l'empêcheront de démarrer ou de fonctionner s'ils sont détruits). Certains de ces canulars sont d'ordre littéraire. Ils racontent des histoires abracadabrantes particulièrement alarmistes et participent en plus à la création de rumeurs. Ces virus n'ont pas de capacité de nuisance au sein d'eux-mêmes. Ils ont besoin de la crédulité des utilisateurs pour se répandre.

6 Scam [1] [3] [5] [7]

Le «scam» («ruse» en anglais), est une pratique frauduleuse d'origine africaine, consistant à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage. Cette arnaque est issue du Nigeria, ce qui lui vaut également l'appellation «419» en référence à l'article du code pénal nigérian réprimant ce type de pratique. L'arnaque est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche africain décédé il y a peu. Ce dernier a déposé plusieurs millions de dollars dans une compagnie de sécurité financière et votre interlocuteur a besoin d'un associé à l'étranger pour l'aider à transférer les fonds. Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les fonds. En répondant à ce type de message l'internaute s'enferme dans un cercle vicieux pouvant lui coûter de quelques centaines d'euro s'il mord à l'hameçon et même la vie dans certains cas. En effet, deux cas de figures se présentent :

- Soit les échanges avec l'escroc se font virtuellement auquel cas celui-ci va envoyer quelques "documents officiels" pour rassurer sa victime et petit à petit lui demander d'avancer des frais pour des honoraires d'avocats, puis des frais de douanes, des frais de banque, etc.

- Soit la victime accepte, sous pression du cyberbandit, de se rendre dans le pays avec la somme en liquide auquel cas elle devra payer des frais pour pouvoir rester dans le pays, payer des frais de banque, soudoyer des hommes d'affaires, et ainsi de suite.

Dans le meilleur des cas la victime rentre chez elle en avion délestée d'une somme d'argent non négligeable, dans le pire scénario plus personne ne la revoit jamais...

7 Les intrusions systèmes [1] [2] [3] [10] [11] [13]

On peut regroupé les attaques par intrusion en 2 types :

- ❖ Les intrusions directes.
- ❖ Les attaques « man in the middle. »

7.1 Les intrusions directes.

C'est la plus simple des attaques. Le hacker s'introduit directement vers sa victime à partir de son ordinateur

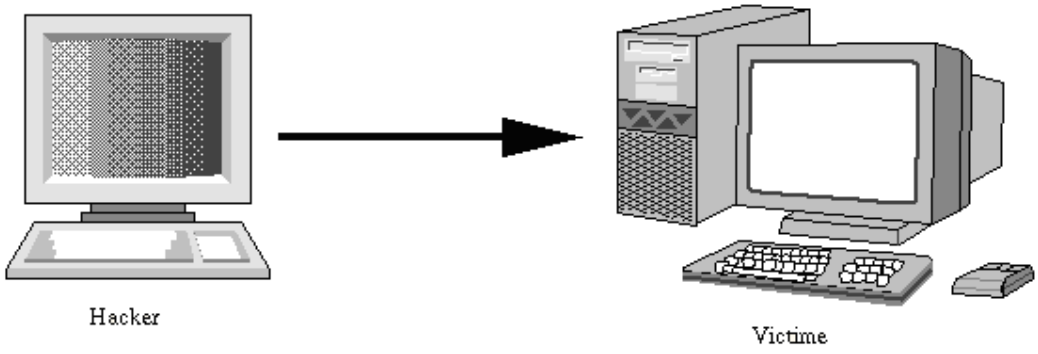


Figure 3.01: Intrusion directe

7.2 Les attaques « man in the middle. »

L'attaque "Man In The Middle" ou « Attaque de l'homme au milieu » s'agit d'un type d'attaque où une tierce personne s'interpose de manière transparente dans une connexion pour écouter ou s'introduire dans un système sans se faire remarquer.

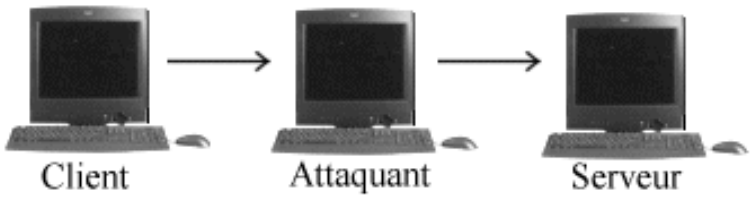


Figure 3.02: Attaque de l'homme au milieu

Il existe plusieurs méthodes pour cela :

7.2.1 Le Hijacking

Ce type d'attaque est fondé sur une faiblesse de TCP/IP, il consiste à désynchroniser une connexion entre deux machines à partir d'une troisième machine. Une fois cette manoeuvre réussie, l'intrus a usurpé l'identité de la machine désynchronisée.

7.2.2 Le TCP-SYN flooding

Cette technique d'attaque exploite la particularité du mode d'établissement des connexions de TCP. Lors de l'établissement d'une connexion, serveur et client échangent des informations, en même temps. Au cours de cette phase d'établissement des connexions restent semi-ouvertes sur le serveur dans l'attente d'accusé de réception du client. C'est la porte que recherche le pirate pour pénétrer sur le réseau. Pour obtenir cette situation, il va susciter l'ouverture de session sur le serveur, en utilisant souvent le relais d'une machine faiblement protégée.

7.2.3 Le spoofing IP

Le « spoofing » (mystification) est une technique permettant à un pirate d'envoyer à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate .Le spoofing IP n'est pas pour autant un changement d'adresse IP .Plus exactement il s'agit d'une mascarade de l'adresse IP au niveau des paquets émis, c'est-à-dire une modification des paquets envoyés afin de faire croire au destinataire qu'ils proviennent d'une autre machine. La technique du spoofing peut permettre à un pirate de faire passer des paquets sur un réseau sans que ceux –ci ne soient interceptés par le système de filtrage de paquets (firewall). Donc, le spoofing IP est par extension le fait de voler l'adresse IP d'une autre personne.

7.2.4 Les intrusions 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.

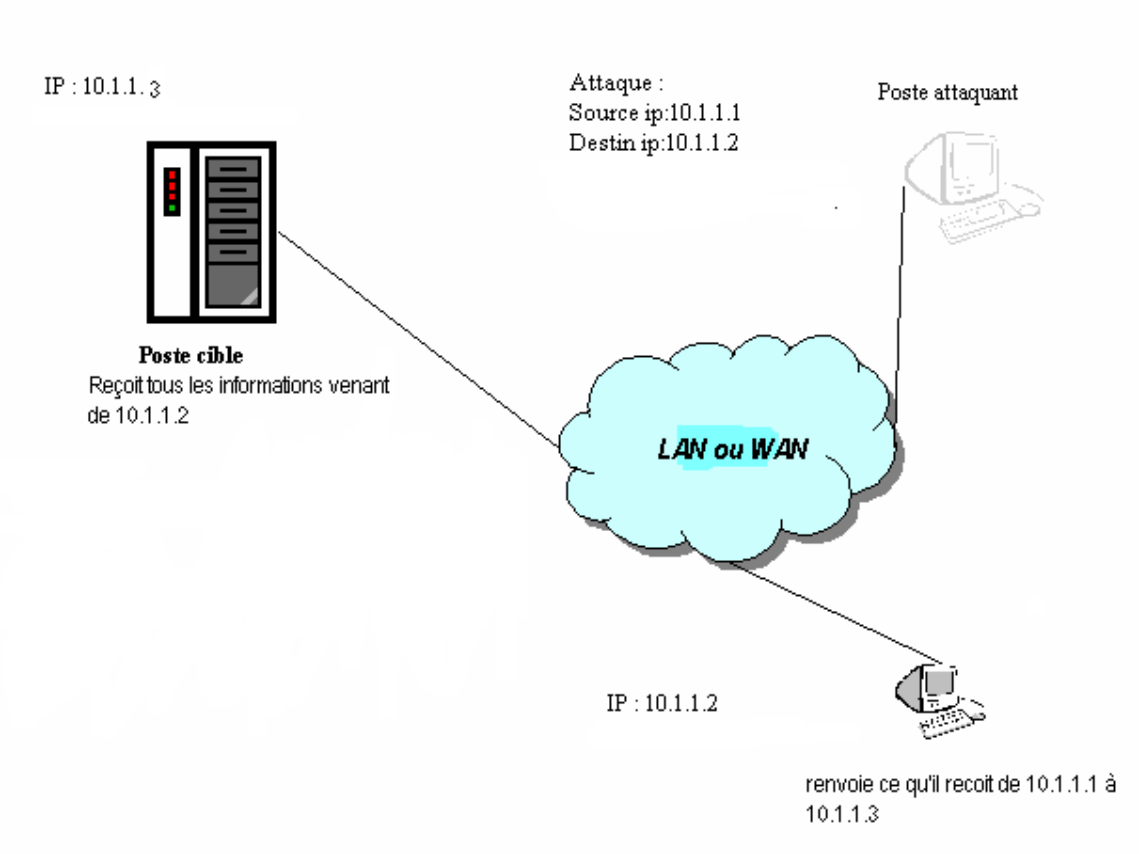


Figure 3.03: Intrusion indirecte par rebond

7.3 L'observation du réseau.

7.3.1 L'examen des paquets (sniffing)

Un réseau à support partagé est un réseau dans lequel les paquets sont transmis partout sur le réseau quand ils circulent de l'origine vers les points de destination. La capture de ces paquets est appelée "observation de réseau" ou "reniflement de paquets" ou encore "interception illégale". Si un renifleur *(sniffer)* ou encore analyseur de protocoles est installé n'importe où le long du chemin entre une machine origine et une machine destination, les informations de connexion peuvent être saisies et utilisées ensuite pour attaquer la machine de destination. L'observation du réseau est une des menaces les plus sérieuses pour les entreprises.

7.3.2 Le détournement de session

Le détournement de session est une variante du spoofing IP. Un intrus cherche une communication réelle entre deux stations et essaie de prendre le pouvoir. Après avoir pris le contrôle d'une station (un firewall ou un composant dans un réseau de prestataire de service) par laquelle passe la communication ou une autre machine sur le même réseau local que celui d'une des deux machines, l'intrus observe la communication comme il veut. Ainsi il peut déterminer les numéros de séquence utilisés. Ensuite il génère le trafic qui semble venir de l'une ou l'autre des deux machines en volant effectivement la session de l'un des deux correspondants pour avoir les mêmes privilèges d'accès que l'utilisateur légitime. Après avoir éliminer l'utilisateur légitime de la communication, il peut maintenant continuer ce que l'utilisateur original a commencé.

CHAPITRE 4 : LES CONTRES MESURES

La création d'une stratégie de sécurité du site consiste à établir une liste de tous les éléments à protéger. Cette liste doit pouvoir être mise à jour facilement et régulièrement. Les éléments à considérer comprennent :

- Matériel : unités centrales, cartes, claviers, terminaux, stations de travail, ordinateurs personnels, imprimantes, lecteur de disquette, lignes de transmission, serveurs de terminaux, routeurs.
- Logiciel : programmes applications, utilitaires, programmes de diagnostic, systèmes d'exploitation, programmes de communication.
- Données : pendant l'exécution, stockées en ligne, archivées hors ligne, sous forme de sauvegardes, listes de contrôle et bases de données, en transit sur supports de communication.
- Personnes : utilisateurs, personnel nécessaire à l'exploitation des systèmes. Documentation: sur les programmes, le matériel, les systèmes, les procédures administratives locales.
- Fournitures : papiers, formulaires, rubans, supports magnétiques.

Puis vient ensuite la protection proprement dite :

1 Réduire l'accès au réseau par l'utilisation d'un firewall [1] [2] [3] [6] [10] [11] [13]

Les systèmes "Firewall" protègent et facilitent l'utilisation de réseau à plusieurs niveaux.

- Ils permettent la mise en place d'un courrier électronique et d'autres applications telles que le système ftp et la connexion à distance, même s'ils limitent l'accès au réseau interne.
- Ils constituent un dispositif d'autorisation, garantissant un niveau de sécurité, dans la mesure où seuls des utilisateurs ou des applications spécifiées peuvent se connecter via le système "Firewall".
- Ils possèdent généralement une fonction de journalisation et d'alarme, permettant le suivi d'une utilisation identifiée et de signaux lors d'événements précis.
- Ils permettent la traduction d'adresses, qui masquent l'adresse et le nom réels de toute machine transmettant des données par le dispositif "Firewall". Par exemple, pour tous les messages adressés à une personne appartenant au service d'assistance technique, les

adresses se transformeront en techsupp@company.com, afin de cacher efficacement le nom d'un utilisateur réel et d'une adresse de réseau.

- Ils permettent d'ajouter de nouvelles fonctions, telles que le chiffrement et les capacités de réseau privé virtuel. Le chiffrement consiste à coder ou à verrouiller les données et à empêcher la lecture d'informations par des utilisateurs non autorisés. Les réseaux privés virtuels (VPN) utilisent le chiffrement pour permettre des transmissions fiables sur les réseaux publics (comme le réseau Internet).
- Les systèmes "Firewall" peuvent également être développés au sein du réseau d'une entreprise afin de compartimenter différents serveurs et différents réseaux, et ainsi de contrôler les accès au sein du réseau. Une entreprise peut souhaiter, par exemple, séparer le "serveur comptabilité et fiches de salaire" du reste du réseau, pour n'autoriser que certains individus à accéder à ces informations.

2 Installer et mettre à jour régulièrement un logiciel d'antivirus [1] [2] [3][10] [11] [13]

2.1 Automatisation

Plusieurs antivirus existent sur le marché : les antivirus professionnels et les antivirus personnel. Mais le meilleur antivirus du monde n'a de sens que si l'organisation assure sa mise à jour régulière. En effet de nouveaux virus voient le jour quotidiennement. Alors il serait préférable d'utiliser des antivirus qui assurent leur mise à jour automatique.

2.2 Vérification

De manière périodique, l'administrateur réseau doit procéder à la vérification de la date de dernière mise à jour sur les postes de travail. En effet, il suffit parfois de peu de chose pour bloquer la fonction de mise à jour automatique et les utilisateurs ne s'en rendront souvent pas compte.

3 Surveiller les flux d'informations

Les flux d'informations dans votre système réseau doivent êtres connus et surveiller pour des raisons de sécurité, de disponibilité et de coût. Un trafic anormal peut révéler une intrusion ou un système défectueux. Généralement ce sont des logiciels spécialisés installés sur les serveurs qui peuvent visualiser ces flux que ce soit local ou en réseaux.

4 Contrôler les documents provenant de l’extérieur [1] [2] [3][13]

Toute pièce jointe doit faire l’objet d’une analyse par un antivirus récent avant d’être ouverte par un utilisateur. L’antivirus peut être centralisé (sur le serveur) ou local (sur les postes de travail).

5 Définir une politique de sécurité interne :

5.1 Nécessité d'authentification et d’identification

Ces procédés permettent de savoir si un interlocuteur est bien celui qu'il prétend être. Les demandes de nom et de mot de passe utilisés pour filtrer l'accès à un site ou un document sont une forme d'authentification mais d’autres sont encore plus poussées, comme l’identification du PC ou de la carte réseau, du numéro de ligne téléphonique, …

Tous les utilisateurs d’un réseau devraient ainsi avoir un identifiant et un mot de passe unique et secret leur permettant, en entrant une seule fois leur code, un accès à toutes les informations auxquelles ils ont le droit.

L'authentification sert alors à :

- La protection contre les accès illicites,
- S'assurer de l'identité du demandeur,
- Garantir le bon destinataire,

5.2.1 Mots de passe

Les mots de passe permettent d'authentifier les utilisateurs lorsqu'ils se connectent au système informatique. Généralement, ils permettent de vérifier l'identité de l'utilisateur. Malheureusement, il existe certains moyens pour neutraliser un système de mots de passe :

- Un individu, désireux de se connecter, peut "écouter" un nom d'utilisateur et un mot de passe pendant qu'un utilisateur autorisé se connecte sur un réseau public.
- Un individu désireux de se connecter, peut s'attaquer à votre système d'accès en tapant un dictionnaire entier de mots (ou de plaques d'immatriculation ou toutes autres listes) dans un champ de mot de passe.
- Des utilisateurs risquent de communiquer leur mot de passe à un collaborateur ou risquent de laisser dans un endroit public une liste de mots de passe système.

Heureusement, il existe une technologie de mots de passe et d'outils permettant de rendre votre réseau plus fiable :

- La génération des mots de passe valables "une fois" est efficace dans des situations spécifiques de connexion à distance, car elles supposent qu'un mot de passe peut être neutralisé. Avant de quitter le réseau interne, le système génère une liste de mots de passe qui fonctionneront seulement une fois pour un nom d'utilisateur donné. Pour se connecter au système à distance, l'utilisateur ne peut utiliser son mot de passe qu'une seule fois, celui-ci cessant alors d'être valide.
- Les fonctions de système d'exploitation, telles que l'expiration des mots de passe et l'application d'une stratégie de mots de passe. L'expiration du mot de passe est une fonction obligeant l'utilisateur à créer régulièrement de nouveaux mots de passe. Une bonne stratégie de mots de passe consiste à définir un nombre minimal de caractères et un mélange des lettres et numéros. Le système d'exploitation ne pourra accepter un mot de passe s'il ne respecte pas ces règles.
- Les cartes à puce garantissent une protection particulièrement fiable des mots de passe. Le principe consiste à créer des mots de passe uniques sur un petit dispositif de type carte de crédit, ledit système étant basé sur un principe "d'interrogations - réponses". Le mot de passe est ensuite tapé (procédure de connexion) et validé sur un serveur de mots de passe, qui gère tous les accès au système. Logiquement, ces systèmes sont souvent onéreux dans leur application.
- La signature unique est peut-être la dernière ironie en matière de système de sécurité : plus un utilisateur possède de mots de passe, moins ces derniers sont fiables (et non le contraire). Le système s'ouvre ainsi à des connexions non autorisées. De nombreux réseaux informatiques d'entreprise sont conçus sur un principe de mots de passe multiples en fonction de la partie du système à laquelle vous voulez vous connecter. Lorsque des utilisateurs se voient attribuer plusieurs mots de passe (certains en manient plus de 50), ils sont plus ou moins contraints de les écrire ou de créer des mots de passe facilement mémorisables. Un système à signature unique se compose essentiellement d'une liste de contrôle d'accès centralisée, déterminant l'identité des personnes autorisées à se connecter sur différents secteurs du réseau informatique. Ce système inclut également un mécanisme permettant de communiquer le mot de passe correct. Un utilisateur n'a besoin que d'un seul mot de passe pour se connecter au système.

5.2.2 Biométrie

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques (empreinte digital, empreinte rétinien…) .Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu.

La technique de biométrie est utilisée de préférence pour les opérations d'identification plutôt que d'authentification.

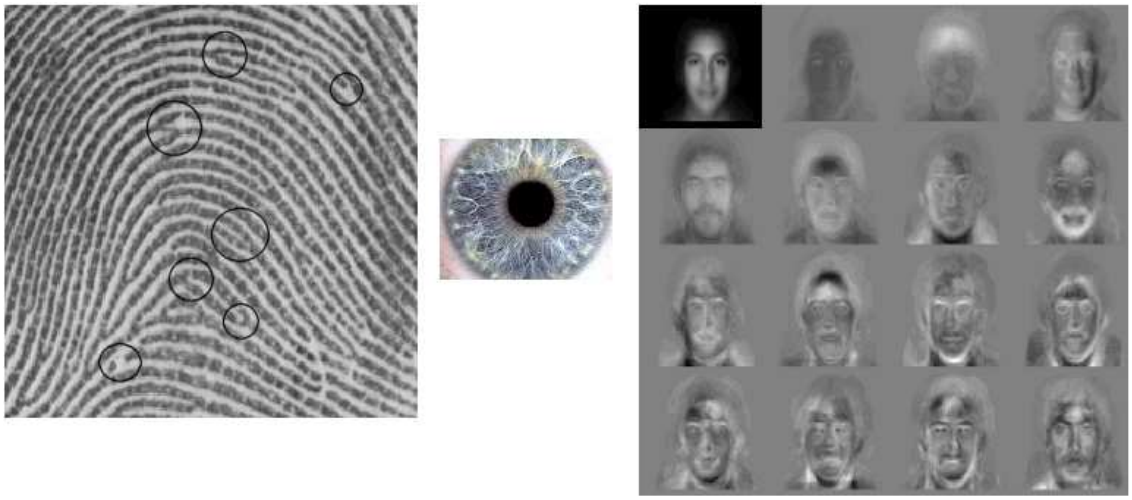


Figure 4.01 : Techniques d'identifications avancées (empreinte digital, empreinte rétinien, identification faciale)

6 Crypter les données [1] [3] [10]

Que se soit en liaison directe par modem, via un VPN, ou dans un échange e-mail, les communications entre le réseau et un PC distant peuvent être cryptées, c'est à dire chiffrées. Ainsi l'émetteur est clairement identifié et son message est garanti intègre (non modifié depuis l'émission), de même que le récepteur. Cette méthode s'améliore chaque jour, avec des clés de cryptage de plus en plus longue, donc plus difficiles à percer.

7 Sécuriser les données [1] [3] [10]

7.1 Accès physique

7.1.1 Serveur

Au-delà de la configuration des accès aux serveurs, l'accès physique à la machine est également crucial. Idéalement les serveurs se trouveront dans une pièce ignifugée et refroidie, fermée à clé et munie d'une alarme.

7.1.2 Réseau

Si les câbles du réseau sont apparents, il est assez simple d'en détourner un ou de récupérer les informations qui y circulent avec de petits appareils électroniques bon marché. C'est encore plus vrai dans les réseaux sans fils. On veillera donc à protéger les câbles dans des goulottes ou dans les murs et à disposer les panneaux techniques dans des endroits non accessibles au public.

7.1.3 Poste de travail

Lorsqu'un utilisateur est amené à sortir de son bureau, il est utile qu'il se déconnecte du réseau. En effet, n'importe qui peut s'asseoir derrière le PC toujours connecté et avoir accès aux mêmes informations que l'utilisateur. De même tous les postes de travail seront recensés, numéroté et peut être attachés physiquement aux murs ou aux bureaux dans le cas des PC portables, en particulier dans les lieux faciles d'accès (intrusion nocturne par exemple).

7.2 Postes distants

7.2.1 VPN

Dès lors que l'accès est autorisé depuis l'extérieur (Internet…) il est intéressant de mettre en oeuvre un système de VPN (Virtual Private Networking). Ce système permet d'isoler une communication entre un poste client et un serveur, via Internet, pour rendre la communication la plus sécurisée possible. Un réseau privé virtuel est une sorte de tunnel privé qui traverse le réseau public, comme Internet, et qui permet de connecter les télétravailleurs à votre réseau ou vos sites distants entre eux. Les utilisateurs du réseau peuvent se connecter en toute confidentialité et partager les applications et les informations. Couplés aux firewalls ils permettent de restreindre l'accès à certaines ressources du réseau.

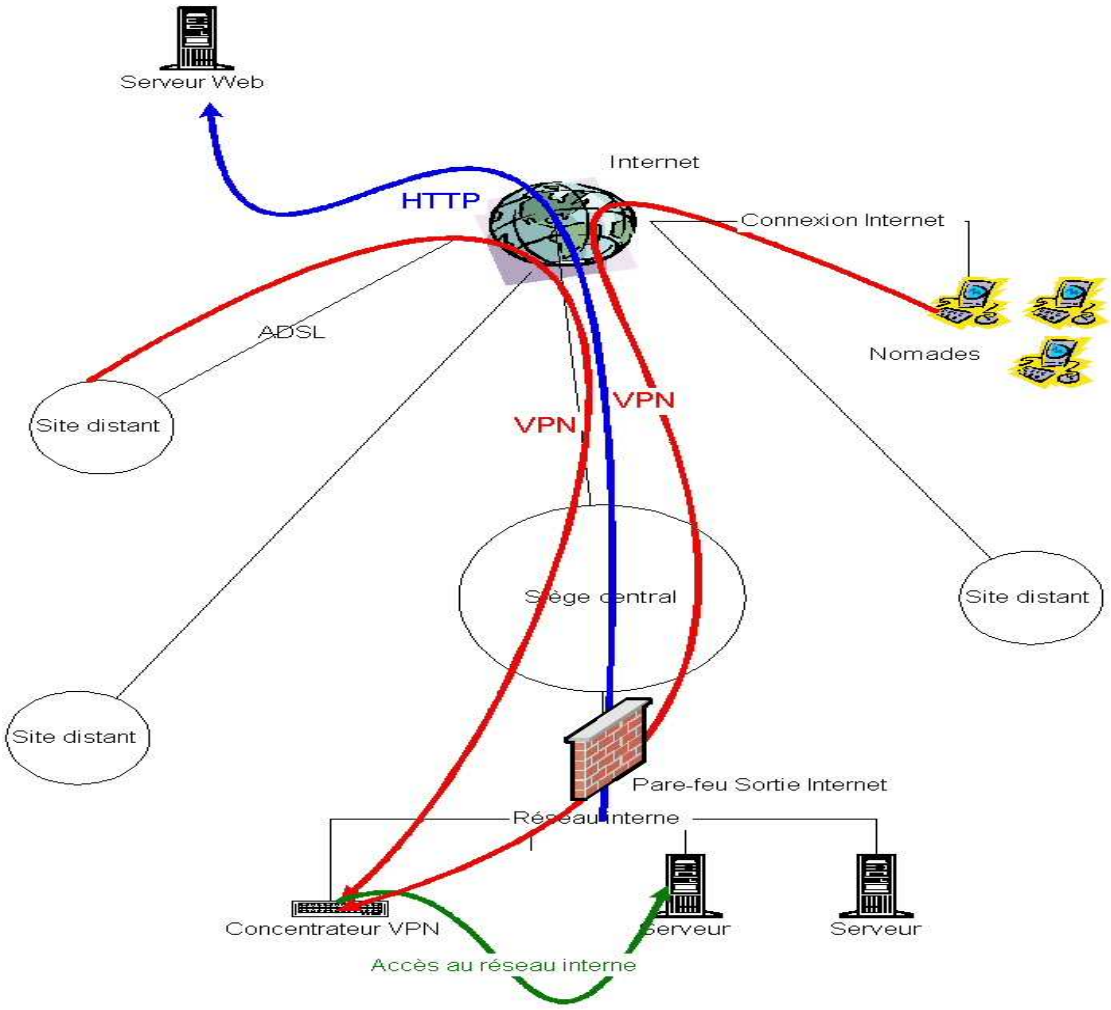


Figure 4.02 : VPN et Firewall

8 Sauvegarder les données [1] [3] [10]

Les données sont installées en principe (qu'elles soient réparties ou non) sur des mémoires de masses (disques durs, bandes magnétiques, CD-RW, DVD-W). Des sauvegardes méthodiques (dépendant du service exploitation), l'utilisation de dispositifs spéciaux tels que disques miroirs permettent dans un large mesure d'éviter la perte (toujours réjudiciable) de données. Une des méthodes les plus efficaces consiste à sauvegarder sur bandes magnétiques selon une procédure définie :

par exemple :

-sauvegarde journalière (fichiers modifiés uniquement)

-sauvegarde hebdomadaire (tous les fichiers utilisateur)

- sauvegarde système journalière (fichiers système modifiés uniquement)
- sauvegarde système hebdomadaire (tous les fichiers système)
- sauvegarde mensuelle (tous les fichiers système et utilisateur)

Cette procédure est valable quel que soit le système utilisé (Mainframe, Mini, Micro-ordinateur).

Figure 4.03 : Moyen de sauvegarde

9 Analyser les journaux d'activité [1] [2] [3] [6] [10] [11] [13]

Afin de détecter les intrusions – internes et externes – dans votre système d'information, il est bon de connaître quel est le comportement « normal » de votre système. Ainsi, vous pourrez mettre en évidence tout changement suspect. La communication avec le monde extérieur se fait de plus en plus par Email. Il est possible de garder un journal d'entrée et sortie de tous les e-mails transitant par votre serveur. Si les informations sont dites « sensibles », il est aussi possible d'archiver en temps réel tout le flux de courrier.

Les accès à vos serveurs de fichiers peuvent aussi être enregistrés dans les journaux de votre système, les « event logs ».

Enfin, il est parfois souhaitable de tracer l'utilisation d'un logiciel ou d'un fichier particulier.

En plus des rapports fournis par votre système d'exploitation, certains logiciels gardent une liste des accès enregistrant le nom de l'utilisateur et l'heure d'accès.

10 Tester les intrusions [2] [13]

Votre système une fois sécurisé doit être testé. Pour ce, vous devez « jouer » au hacker afin de vérifier que touts les accès sont bien contrôlé. Ce travail demande beaucoup d'imagination car le point faible de votre système est précisément celui auquel vous n'avez pas pensé. Ces tests doivent se réaliser de l'extérieur et de l'intérieur de votre système. Ces tests doivent être menés régulièrement.

CHAPITRE 5: CONCEPTION ET SIMULATION DE QUELQUES MENACES INFORMATIQUES EN RESEAUX (TROJAN, KEYLOGGER, DENIAL OF SERVICE…)

1 Les ressources utilisées pour la conception et la simulation de l'application [4] [8] [9] [12]

1.1 Les ressources logicielles

1.1.1 Le langage C++

C++ est un langage de haut niveau très puissant qui simplifie la manipulation :

- des entrées et sorties sous Windows®
- des traitements de fichiers
- des interfaces graphiques (IHM) sous Windows® 32bits
- de la programmation réseau utilisant les sockets
- de la gestion des processus et threads
- de l'intégration d'un langage de bas niveau comme l'assembleur

1.1.2 Le langage Assembleur

Le langage assembleur est un langage de bas niveau très souple qui est utile pour le compactage des codes afin que les données acheminées sur les réseaux aient un débit réduit.

1.1.3 Le Système d'exploitation Microsoft® Windows® XP

Actuellement c'est le système d'exploitation le plus utilisé, alors que les services du protocole TCP/IP en est le plus vulnérable aux chevaux de Troie et aux autres menaces informatiques.

1.2 Les ressources matérielles

Au moins deux ordinateurs ayant chacun un carte réseau (Ethernet) et connectés au réseau local (L.A.N); Ou deux ordinateurs possédant chacun un modem d'accès à distance et connectés a l'Internet.

2 L'application serveur

2.1 Présentation

Le serveur est une application qui contient en même temps le code d'un troyen et d'un Keylogger (cf. chapitre 2). Il simule un programme banale qui soi-disant « vous permet de se connecter gratuitement a l'Internet ». Il s'installe sur l'environnement Windows® comme toute installation

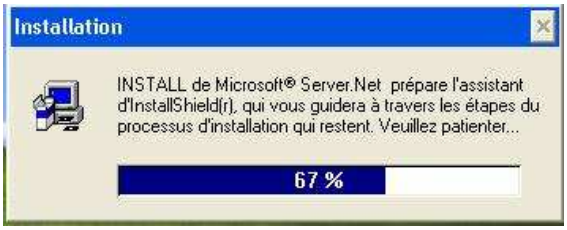
de logiciel sous Windows®. Après installation, l'application s'affiche une seule fois et au moindre déplacement de la souris il se cache et travaille en mémoire comme étant un processus Windows® ; de ce fait, il :

-Ouvre automatiquement un port de communication TCP/IP : arbitrairement 12345 (fonction cheval de Troie)

-Attend les commandes provenant de l'application cliente

-Enregistre toute frappe au clavier (fonction Keylogger), à la demande de l'application cliente,

-Démarre automatiquement avec Windows® sous le nom de processus : « InternetServer » au cas ou la victime ferme sa session ou redémarre l'ordinateur.



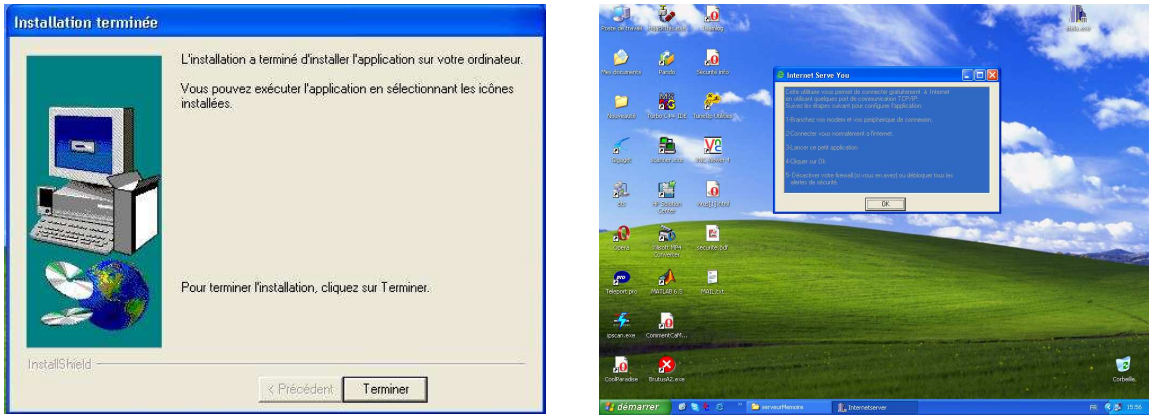


Figure 5.01 : Les étapes de l'installation de l'application Serveur et affichage de son interface graphique après l'installation

2.2 Caractéristiques techniques de l'application serveur

- Établissement d'une connexion (circuit virtuel) entre le client et le serveur via l'adresse IP et le numéro de port (arbitrairement 12345) du PC contenant le serveur
- Connexion assurée par le protocole TCP
- Mode d'échange par flot d'octets : le récepteur n'a pas connaissance du découpage des données effectué par l'émetteur
- Le serveur est "passif" : il n'est activé que lors de l'arrivée d'une demande de connexion du client ou d'une commande du client
- Le serveur répond aux demandes de service de plusieurs clients : les requêtes arrivées et non traitées sont stockées dans une file d'attente
- Utilisation du mode itératif pour la gestion des requêtes : le processus traite les requêtes les unes après les autres

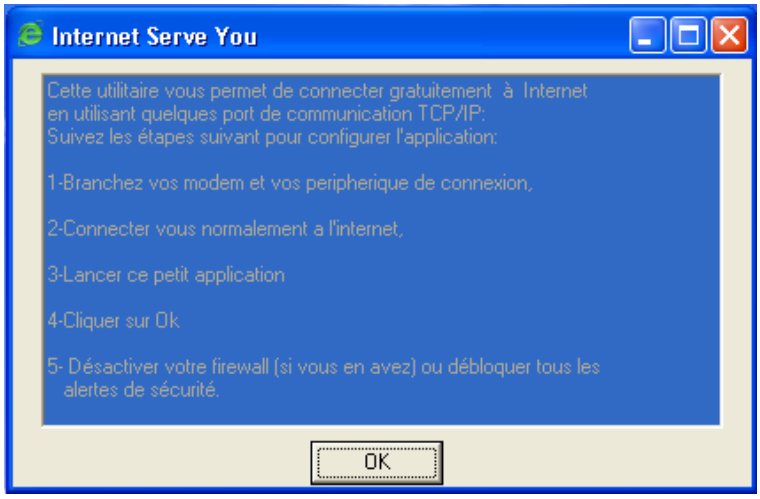


*Figure 5.02:*L'interface graphique de l'application serveur

3 L'application cliente

3.1 Présentation

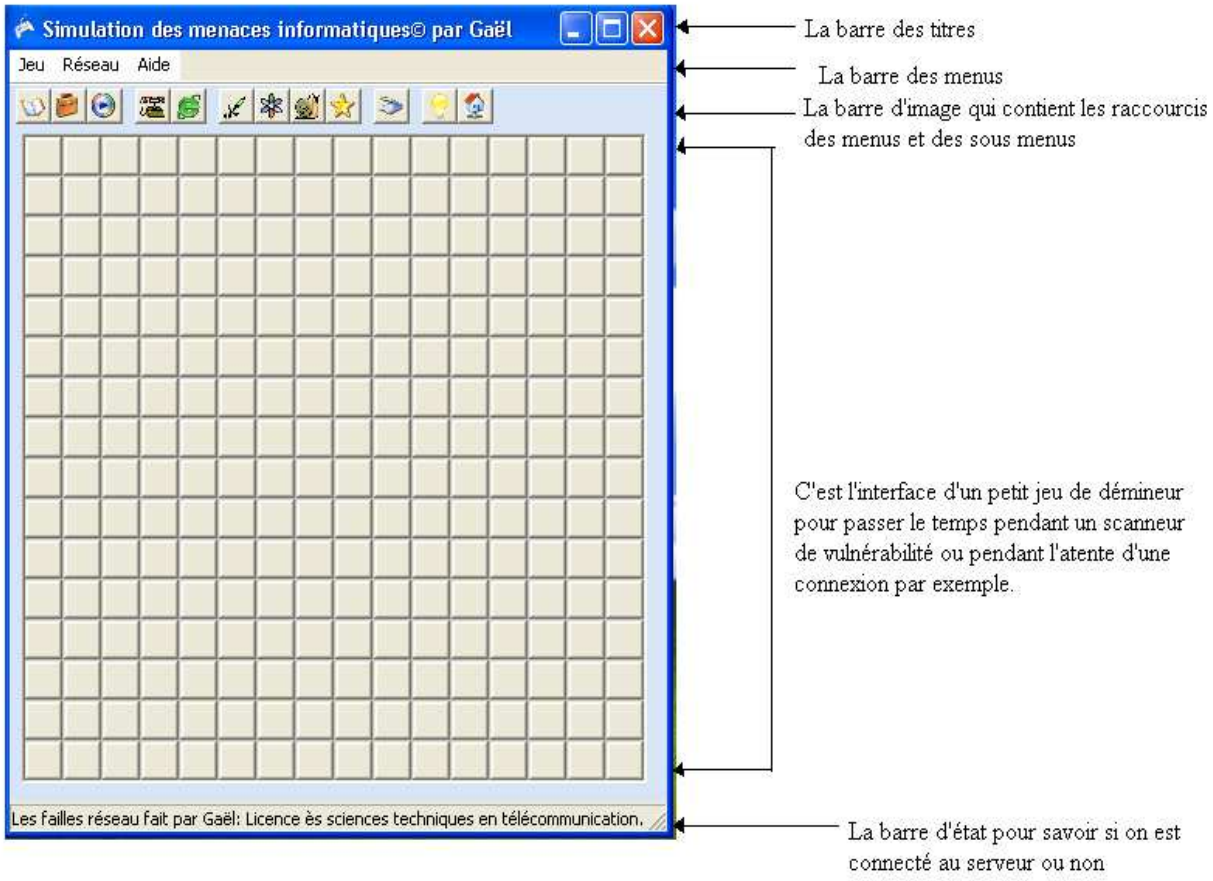


*Figure 5.03:*L'interface graphique de l'application cliente

Une fois que le serveur a ouvert le port 12345, le client peut se connecter sur l'ordinateur distant (sur le même port, c'est-à-dire 12345) contenant l'application serveur si et seulement si le client connaît son adresse IP.

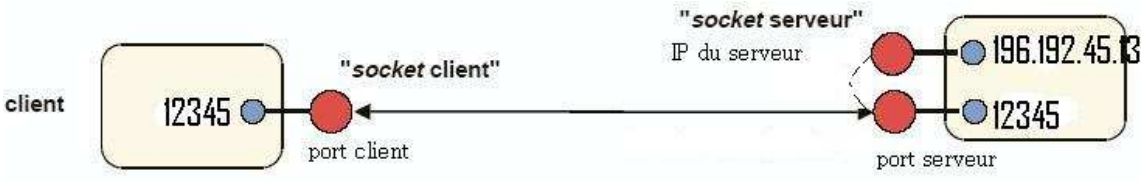


Figure 5.04: communication client-serveur par socket

3.2 Configuration de la connexion

Pour configurer la connexion du client vers serveur, il faut d'abord choisir le menu réseau, puis cliquer sur l'option configuration et ainsi paramétrer le port de communication et l'adresse ip du pc contenant le troyen.

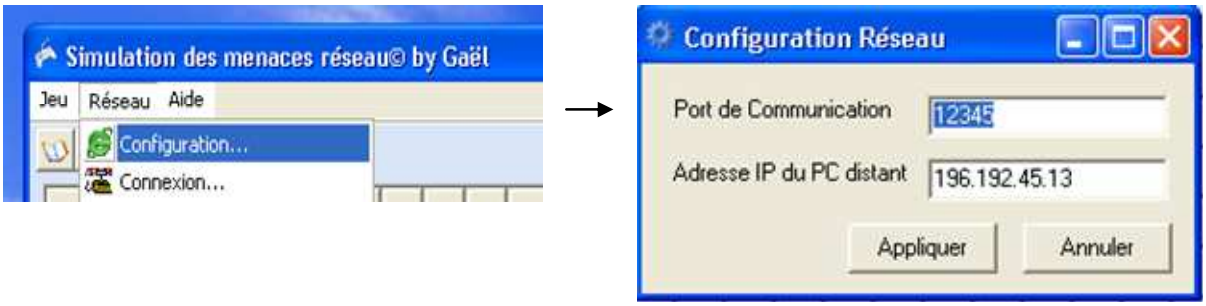


Figure 5.05 : Configuration de la connexion

Après l'établissement de la connexion, l'application cliente est en mesure de tout faire, de tout contrôler sur la machine distante.

3.3 Fonction Keylogger

Le serveur enregistre en même temps toute frappe au clavier et créer automatique un fichier nommé « FichierLog .txt » sur son disque dur local, Il transfert ensuite ce fichier vers l'application cliente a travers le réseau via le socket.

Le client reçoit le fichier lit son contenu et l'affiche dans la zone de texte de la fenêtre Keylogger. Ainsi le client peut ensuite enregistrer le log sur son disque dur locale, effacer le log de la machine distante ou même désactiver ou activer la fonction écoute du serveur distant.

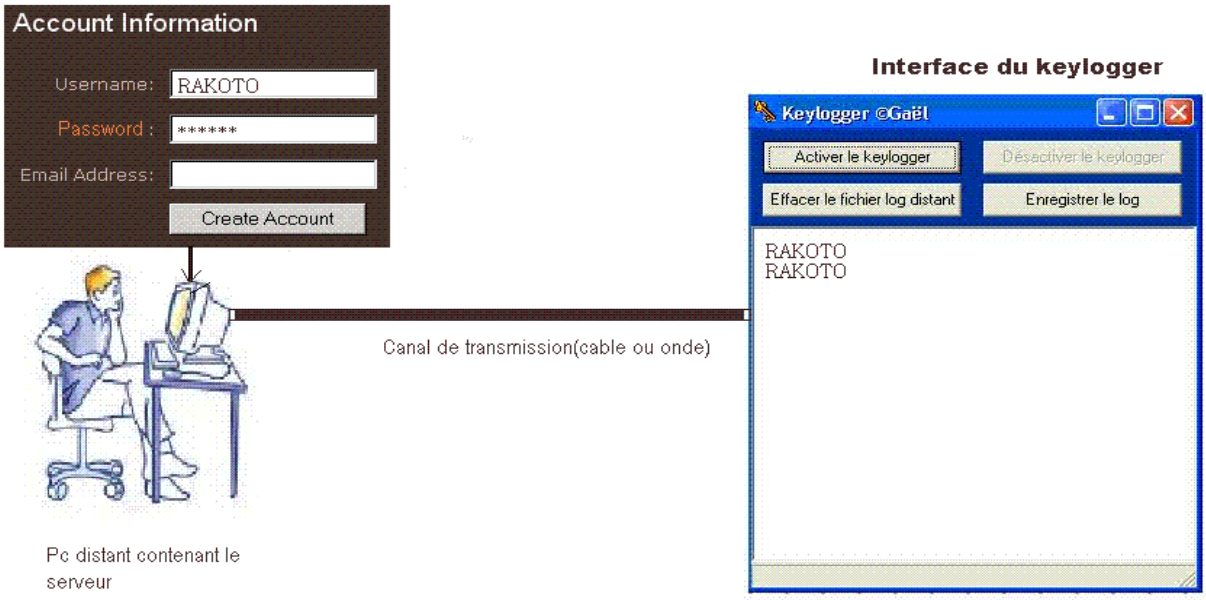


Figure 5.06 : Action du Keylogger

3.4 Fonction déni de service

Le déni de service vise à saturer la bande passante de la machine distante contenant le serveur en envoyant une multitude d'octet sur le canal par le socket. Le but en est de démontrer la vulnérabilité du protocole TCP en déconnectant le serveur du réseau Ce type de déni de service n'est valable que si plus de 3 machines reproduisent en même temps la même attaque car chaque machine ne saturera que 40% du débit du serveur

3.5 Le scanneur de port ou scanneur de sécurité

Le scanneur de port n'est pas une menace proprement dite (ça dépend de quel camp on est) car il est utilisé par les administrateurs réseaux pour identifier les ports ouverts de leur système, mail c'est aussi l'outil fétiche des pirates pour déterminer les vulnérabilités d'un ordinateur.

Pour accéder au scanneur de port sur l'application cliente, cliquer sur le menu réseau, puis sur le sous-menu Outils de scan et enfin lancer le Scanneur de port.

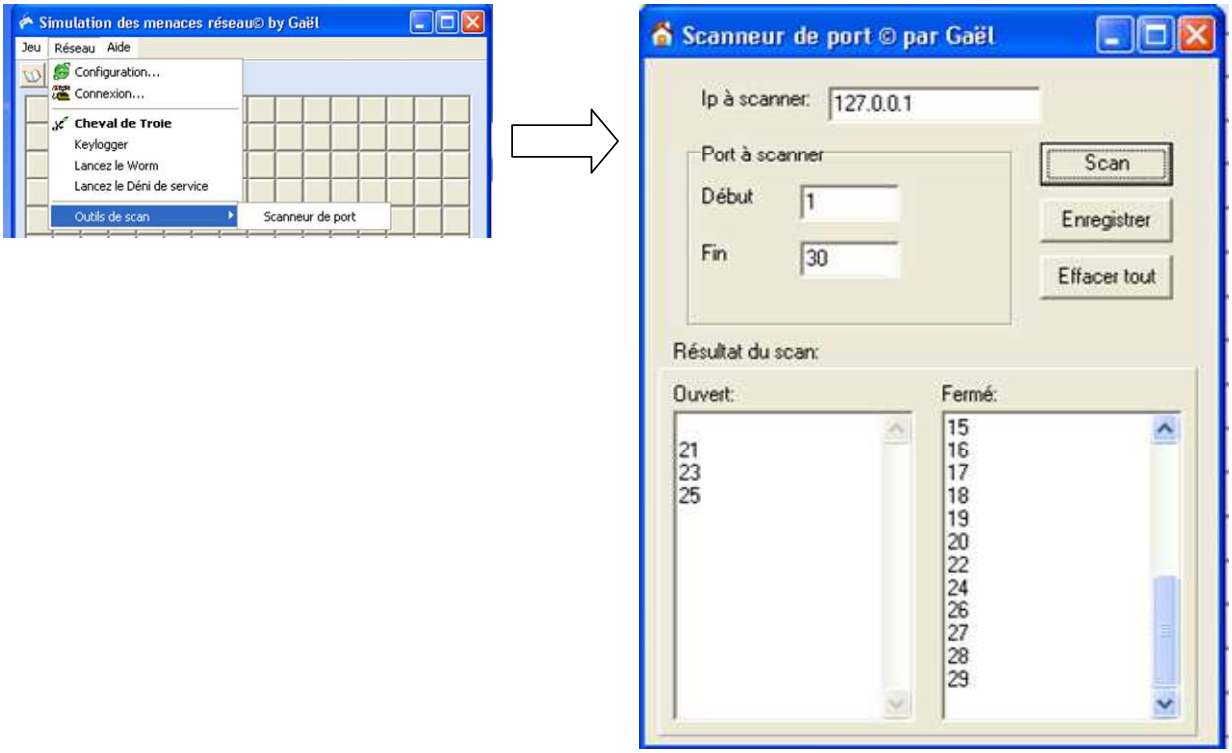


Figure 5.07 : Le scanneur de sécurité

3.6 Fonction Cheval de Troie

Le cheval de Troie établit une interaction complète sans autorisation avec le PC distant, il englobe beaucoup de fonctionnalité.

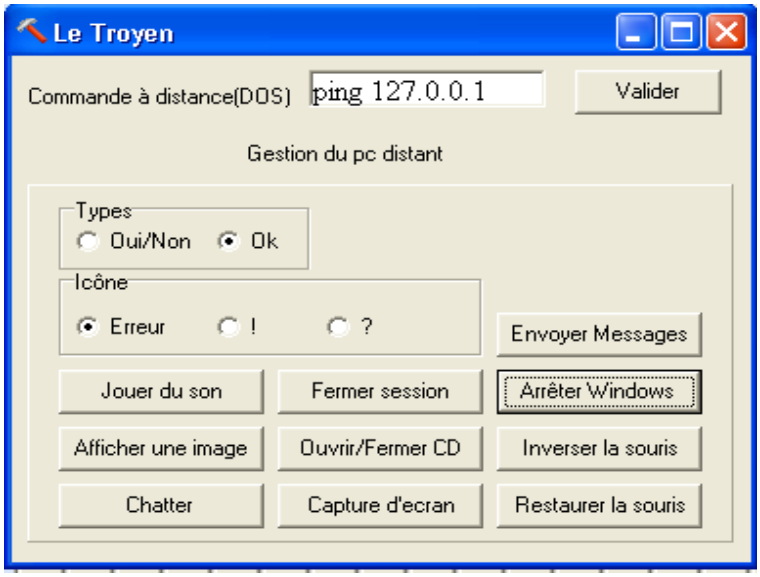


Figure 5.08 : La fiche Cheval de Troie

Ce cheval de Troie permet entre autre de :

- Fermer la session utilisateur distant et déconnecter celui-ci du réseau,
- Arrêter et mettre hors tension l'ordinateur distant,
- Jouer du son au format wave et midi.
- Afficher des images sur le poste distant,
- Inverser et Restaurer les boutons de la souris
- Ouvrir et fermer le lecteur de CD-ROM
- Envoyer des messages de type erreur avec des boutons ok, oui/non.
- Dialoguer avec la victime en affichant un logiciel de « chat »
- Faire une capture d'écran en temps réel.
- Envoyer des commande DOS (exemple : dir ou ping 127.0.0.1 –w 1 –t) idéal pour les attaques « man in the middle ».

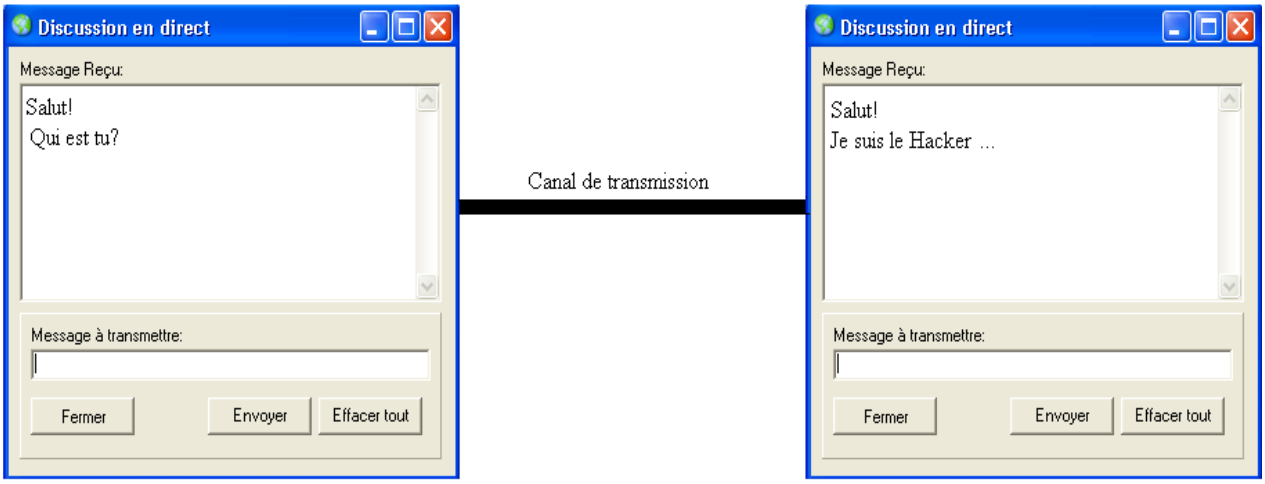


Figure 5.09 : Le logiciel de discussion : « chat »

3.7 Le menu aide

Comme tout bon logiciel, l'application cliente contient un menu qui comprend le manuel d'utilisation du logiciel et une boîte à propos.

Figure 5.10 : Accéder à la rubrique d'aide

3.7.1 Le manuel d'utilisation ou rubrique d'aide

C'est un fichier d'aide qui explique à l'utilisateur comment utiliser l'application. Dans l'application principale, l'utilisateur peut choisir le menu aide puis cliquer sur la commande « rubrique d'aide » afin d'afficher celle-ci!

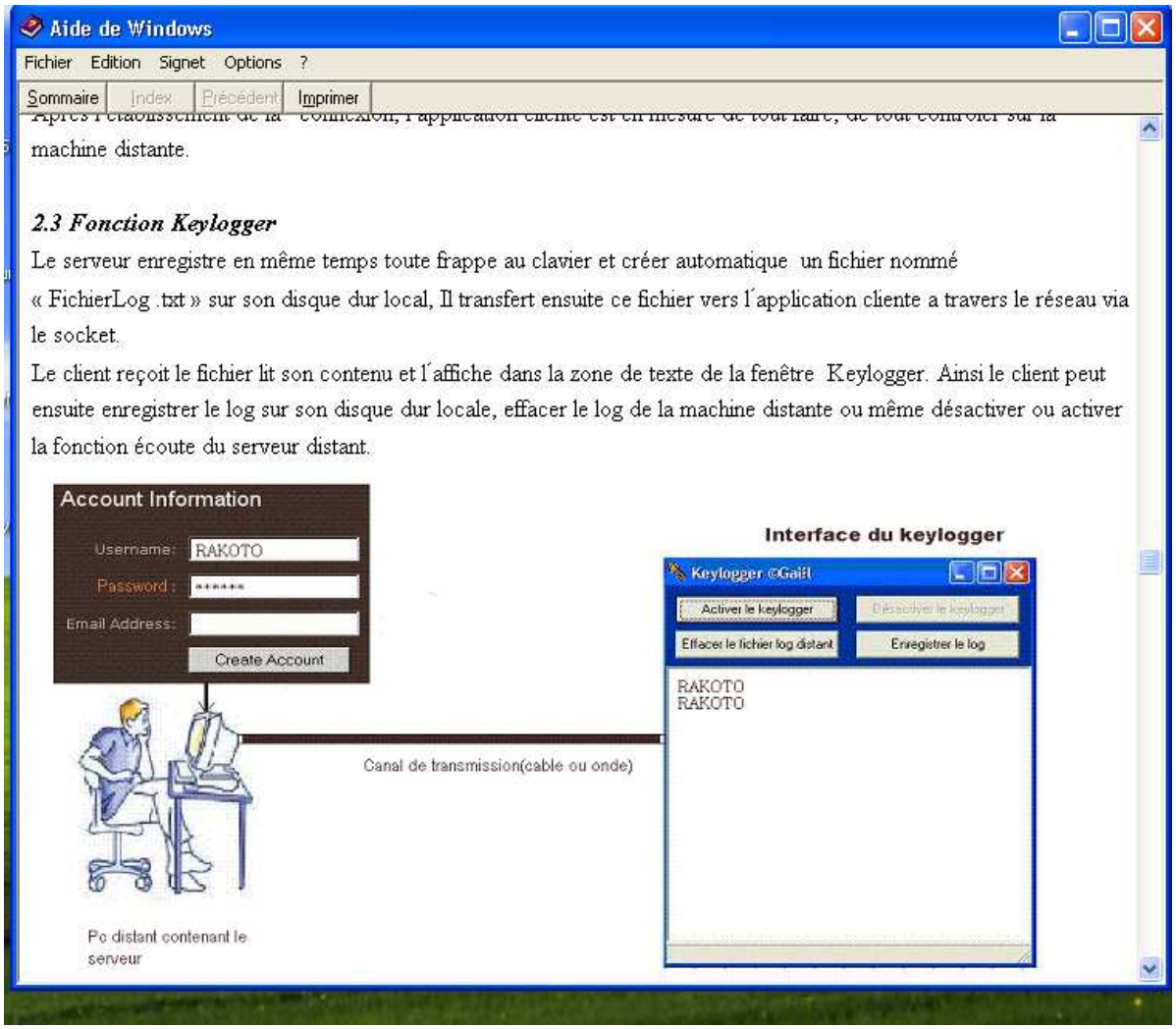


Figure 5.11 : La rubrique d'aide.

3.7.2 La boîte à propos

La boîte à propos affiche des informations sur le produit : son nom, la date, un logo, le copyright et le nom du concepteur de l'application

Figure 5.12 : La boite à propos

CONCLUSION GENERALE

Nos systèmes sont interconnectés aux réseaux depuis longtemps. Lors du choix de l'architecture des points d'accès de ces systèmes aux réseaux, la sécurité n'était pas un critère prioritaire. Le but principal était alors la connectivité totale (full connectivity).On pensait qu'il pourrait y avoir des problèmes de sécurité dans le futur mais ce n'était pas prioritaire dans les choix techniques. Les réseaux n'étaient qu'un ensemble de moyen de recherche où « tout le monde se connaissait ». On n'avait pas d'attaque de spam, Trojan, virus, flood, spoofing, sniffer.

Maintenant les réseaux sont devenus des outils de communication mondiale, utilisés par des bons et mauvais citoyens et toutes les déviances courantes y sont présentes. On a pu voir rapidement que cette connectivité totale était une aubaine pour les personnes mal intentionnées qui pouvaient ainsi essayer très facilement de tester toutes les machines d'un site et découvrir rapidement un maillon faible afin de s'introduire facilement dans le système.

Lorsqu'une intrusion est constatée, les dégâts sont souvent importants et nécessitent un travail long et fastidieux pour remonter le système et supprimer les failles de sécurité. Tout cela affecte lourdement la continuité du réseau et du système d'information. Les méthodes et les outils qu'utilisent les pirates sont bien rodés et d'un accès malheureusement très facile ; des kits entiers de piratage circulent sur le réseau.

C'est pour cela que la sécurité des informations et des réseaux est alors devenu un concept primordial pour tout administrateur car je répète toujours et jamais assez:nul n'est à l'abri des menaces.

ANNEXES

1 Vocabulaires :

1.1 Code malveillant :

Protocole de représentation de données, d'information, d'instruction qui recourt à une notation spécifique et qui possède une volonté de nuire et de détruire.

1.2 Communication client-serveur

- Client = toute application, sur une machine donnée qui va initier une connexion et faire une requête.
- Serveur = toute application, sur une machine donnée, qui va être à l'écoute des connexions entrantes, et répondra aux requêtes qui lui sont destinées

1.3 Connexions distantes :

Il existe 2 types :

- Connexions interactives : permet de se connecter sur une machine distante afin de travailler dessus utilisant des applications tels que telnet, netmeeting, netbus.
- Connexions non-interactives : transferts de fichiers ou lancement de commandes non interactives

1.4 Failles

Points faibles d'un système.

1.5 Internet Protocol (IP) :

Protocole décrit dans la RFC 791, Protocole de communication utilisé par les ordinateurs reliés à l'Internet. Un paquet IP contient en en-tête quelques informations, dont les adresses source et destination. L'IP est le protocole en-tête de base dans un paquet et se trouve toujours là, Il assure le format des paquets et la bonne transmission sur le réseau.

L'adresse IP est à la base de tout; elle est attribuée par le FAI à chaque connexion.

C'est une sorte de numéro de série. Cette IP est dynamique, elle change à chaque connexion.

1.6 Ports TCP :

La communication vers un service donné s'effectue sur un port. La combinaison {Adresse IP, numéro de port} correspond à un processus sur le client ou le serveur.

Les serveurs écoutent généralement sur un port connu.

Port :	Protocole:	Description:
1	Tcp	Port Service Multiplexer
5		Remote Job Entry
7		Echo
13		Daytime
15		netstat
21		FTP : File Transfert Protocole
22		SSH Remote Login Protocol
23	Tcp	Telnet
25		SMTP
29		MSG ICP
79		Finger
80	Tcp	Http
110		POP3

Port :	Protocole:	Description:
119		nntp
139	Tcp	NetBIOS
143		IMAP
529	Tcp	IRC-SERV
614		SSL shell
767		phone
1025	Tcp	network blackjack
1243		SubSeven
1359		FTSRV
1367		DCS
5800		VNC
6346		Utilisé par GNUtella
8080		Standart Http

Tableau : Liste des ports les plus utilisés (liste non exhaustive)

1.7 Système d'exploitation :

Logiciel gérant un ordinateur, indépendant des programmes d'applications mais indispensable à leur mise en œuvre.

1.8 Transmission Control Protocol (TCP) :

Le protocole TCP (Transmission Control Protocol) est l'un des principaux protocoles employés sur Internet. Il facilite les tâches critiques telles que le transfert de fichiers et les sessions distantes. Il accomplit ces opérations par l'intermédiaire d'une méthode de transfert fiable orientée connexion, fondée sur la transmission d'un flux. Ce flux garantit quel les données arriveront dans un ordre et un état identiques à ceux d'émission.

C'est un Protocole décrit dans la RFC 793 :

- Fonctionne en mode connecté,
- Établit une connexion,
- Transfert des données
- Utilisation des numéros de port (entre 1 et 65535)
- Utilisation de drapeaux (SYN, ACK, FIN, RST, etc.)

BIBLIOGRAPHIE

[1] H. Brunel, *Sécurité des systèmes d'information*, Novembre 2004

[2] J.L. Archimbaud, *Recommandations d'architecture de réseau avec filtrages pour améliorer la sécurité en particulier pour mieux se protéger des attaques venant de l'Internet*, CNRS/UREC : Janvier 2000

[3] G Florin et S Natkin, *La sécurité*, 2003

[4] D. Manso, *Les virus et leurs méthodes sous DOS*, ENSIMAG Année Spéciale Informatique, Juin 1996

[5] http://www.securiteinfo.com

[6] F. Borderies, O. Chatel, J.C. Denis, D. Reis. , *Administration réseau*, ENSIMAG Année Spéciale Informatique, 1993

[7] http://www.commentcamarche.net

[8] *Le guide du développeur en C++ builder sous windows 95,98,NT* ,Edition 2000

[9] C. Berthet, *Aide mémoire d'informatique*, Dunod Informatique : Paris, 1982

[10] J.L. Archimbaud, *Sécurité Réseaux*, CNRS/UREC : Octobre 1995

[11] O. Tharan, *Architecture réseaux*, Institut Pasteur, 2004

[12] H.McBungus, ''The Virus Writer's Handbook: The Complete Guide'', 1992

[13] J.L Archimbaud, *Conseil de Sécurité sur l'Administration de Machines Unix sur un Réseau TCP/IP*, 2003