



Liste des risques :

- 1- Programmes malveillants
- 2- Techniques d'attaques par messagerie
- 3- Attaques sur le réseau
- 4- Attaque sur les mots de passe



1-Programmes malveillants

Un logiciel malveillant (*malware* en anglais) est un logiciel développé dans le but de nuire à un système informatique. Voici les principaux types de programmes malveillants :

- Le **virus** : programme se dupliquant sur d'autres ordinateurs ;
- Le **ver** (*worm* en anglais) : exploite les ressources d'un ordinateur afin d'assurer sa reproduction ;
- Le **wabbit** : programme qui se réplique par lui-même (mais qui n'est ni un virus, ni un ver) ;
- Le **cheval de Troie** (*trojan* en anglais) : programme à apparence légitime (voulue) qui exécute des routines nuisibles sans l'autorisation de l'utilisateur ;
- La **porte dérobée** (*backdoor* en anglais) : ouvreur d'un accès frauduleux sur un système informatique, à distance ;
- Le **logiciel espion** (*spyware* en anglais) : collecteur d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation, et en envoyant celles-ci à un organisme tiers ;
- **L'enregistreur de frappe** (*keylogger* en anglais) : programme généralement invisible installé sur le poste d'un utilisateur et chargé d'enregistrer à son insu ses frappes clavier ;
- **L'exploit** : programme permettant d'exploiter une faille de sécurité d'un logiciel ;
- Le **rootkit** : ensemble de logiciels permettant généralement d'obtenir les droits d'administrateur sur une machine, d'installer une **porte dérobée**, de truquer les informations susceptibles de révéler la compromission, et d'effacer les traces laissées par l'opération dans les journaux système.

Virus informatique

Un **virus informatique** est un **programme informatique** écrit dans le but de se dupliquer sur d'autres **ordinateurs**. Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme **l'Internet**, mais aussi les **disquettes**, les **céderoms**, les clefs **USB**, etc.

Son appellation provient d'une analogie avec le **virus biologique** puisqu'il présente des similitudes dans sa manière de se propager et de se reproduire. On attribue le terme de « virus informatique » à l'informaticien et spécialiste en **biologie moléculaire Leonard Adleman** (Fred Cohen, *Experiments with Computer Viruses*, 1984).

Le nombre total de virus couverts par **Sophos** s'élevait à 93 875 (tous types confondus, en août **2004**) d'après *Mag-securs* ([1]). Ce chiffre n'est qu'une approximation grossière du nombre réel de virus en circulation, chaque éditeur d'antivirus ayant intérêt à « gonfler » la réalité, d'autant plus que très peu de virus identifiés atteignent le stade de la diffusion massive

sur les réseaux. La très grande majorité concerne la **plate-forme Windows**. Le reste est essentiellement destiné à des systèmes d'exploitation qui ne sont plus distribués depuis quelques années, comme les 27 virus — aucun n'étant dangereux — frappant **Mac OS 9** et ses prédécesseurs (recensés par John Norstad, auteur de l'antivirus *Disinfectant*).

Les virus font souvent l'objet de fausses alertes que la rumeur propage, encombrant les messageries. Certaines d'entre elles, jouant sur l'ignorance en informatique des utilisateurs, leur font parfois détruire des éléments de système d'exploitation totalement sains.

Ver informatique

Un **ver informatique** est un logiciel malveillant qui se reproduit sur des ordinateurs à l'aide d'un réseau informatique comme l'Internet.

Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources afin d'assurer sa reproduction. La définition d'un *ver* s'arrête à la manière dont il se propage de machine en machine, mais le véritable but de tels programmes peut aller au delà du simple fait de se reproduire : espionner, offrir un point d'accès caché (porte dérobée), détruire des données, faire des dégâts, envoi de multiples requêtes vers un site internet dans le but de le saturer, etc. Les effets secondaires peuvent être aussi un ralentissement de la machine infectée, ralentissement du réseau, plantage de services ou du système, etc.

Des vers écrits sous forme de script peuvent être intégrés dans un courriel ou sur une page HTML sur internet. Ils sont activés par les actions de l'utilisateur qui croit accéder à des informations lui étant destinées.

Un ver peut tout aussi bien être programmé en C, C++, Delphi, assembleur, etc. Il utilise la plupart du temps des bugs de logiciels pour se propager.

Wabbit

Un **wabbit** est un type de logiciel malveillant qui s'auto réplique. Contrairement aux virus, il n'infecte pas les programmes ni les documents. Contrairement aux vers, il ne se propage pas par les réseaux.

En plus de s'autorépliquer rapidement, les wabbits peuvent avoir d'autres effets malveillants. Un exemple de wabbit est la bombe fork, du nom de la commande Unix exploitée : fork.

L'origine probable du terme est la prononciation du personnage de bande dessinée Elmer Fudd (de l'univers de Bugs Bunny) du mot « rabbit » (en anglais : *lapin*). Ce personnage est un chasseur (entre autres de lapins, comme Bugs Bunny) dont les capacités intellectuelles sont

ridiculisées, entre autres, par son incapacité à prononcer les « r » : « rabbit » devient donc « wabbit ». Par ailleurs, il est connu que les lapins se reproduisent à une très grande vitesse.

Cheval de Troie (informatique)

Un **cheval de Troie** (*trojan* en anglais) est un type de logiciel malveillant, c'est-à-dire un logiciel d'apparence légitime, mais conçu pour subrepticement exécuter des actions nuisibles à l'utilisateur ; un cheval de Troie, dans un programme, tente d'utiliser les droits appartenant à son environnement d'appel pour détourner, diffuser ou détruire des informations. Le partage des programmes introduit la problématique des chevaux de Troie. Les trojans auraient été créés dans les années 80, par un jeune hacker allemand du nom de Karl Koch.

Fonctionnement

Un cheval de Troie n'est pas un virus informatique dans le sens où il ne se duplique pas par lui-même, fonction essentielle pour qu'un logiciel puisse être considéré comme un virus. Un cheval de Troie est conçu pour être dupliqué par des utilisateurs naïfs, attirés par les fonctionnalités vantées.

Les chevaux de Troie servent très fréquemment à introduire une porte dérobée sur un ordinateur. L'action nuisible à l'utilisateur est alors le fait qu'un pirate informatique peut à tout moment prendre à distance (par Internet) le contrôle de l'ordinateur.

Il est difficile, voire impossible de définir exactement ce qu'est un cheval de Troie, car la légitimité d'un logiciel dépend aussi du contexte dans lequel il est employé. Les portes dérobées par exemple peuvent s'avérer utiles pour un administrateur réseau ; en revanche, dans les mains d'un pirate elles sont clairement illégitimes.

Le cheval de troie est un logiciel que nous pouvons recevoir par e-mail ou même télécharger sur un site qui ressemble à 2 gouttes d'eau d'un site officiel.

Une fois téléchargé, puis installé, il ira ouvrir des portes dans votre ordinateur.

Le logiciel prendra alors l'aspect d'un vrais logiciel et il fera probablement ce que vous désirez!

Rendu là, le logiciel recevra une demande du serveur de son créateur pour envoyer une centaine de paquets défectués à un serveur. Après 200 paquets, habituellement les serveurs commencent à devenir lent puis si le logiciel a été installé sur plusieurs ordinateurs il va y avoir des milliers de paquets envoyer sur le serveur, il va peut-être se fermer lui-même. Si cela arrive, tout les sites internet qui se trouvent sur ce serveur ne fonctionneront pas.

Protections

Pour éviter les infections de chevaux de Troie, la règle la plus simple est d'installer un minimum de logiciels, de provenance sûre. Après infection, on peut détecter un cheval de Troie avec un logiciel antivirus à jour. Enfin, on peut utiliser un pare-feu pour limiter et surveiller les connexions au réseau que pourrait utiliser le pirate. Toutefois, une fois installé, le cheval de Troie peut désactiver les antivirus et pare-feu existants.

Dans les structures à fort besoin de sécurité, les solutions généralement proposée consistent à :

- confiner le programme dans des domaines dans lequel il possède les droits pour réaliser sa tâche et pas davantage ;
- interdire la diffusion des données passées en paramètre.

Ce dernier problème est difficile à résoudre car le programme peut utiliser de nombreux moyens détournés pour transmettre des informations : les canaux cachés (*covert channels*).

Porte dérobée

(Redirigé depuis Backdoor)

Dans un logiciel une **porte dérobée** (de l'anglais *backdoor*, littéralement *porte de derrière*) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel. En sécurité informatique, la porte dérobée peut être considérée comme un type de cheval de Troie.

Technique

Une porte dérobée peut être introduite soit par le développeur du logiciel, soit par un tiers, typiquement un pirate informatique. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle (par exemple, par contournement de l'authentification). Enfin, selon l'étendue des droits que le système d'exploitation donne au logiciel contenant la porte dérobée, le contrôle peut s'étendre à l'ensemble des opérations de l'ordinateur.

La généralisation de la mise en réseau des ordinateurs rend les portes dérobées nettement plus utiles que du temps où un accès physique à l'ordinateur était la règle.

Parmi les motivations amenant les développeurs de logiciel à créer des portes dérobées, il y a :

1. L'intérêt pratique d'un accès facile et toujours ouvert au logiciel pour pouvoir mener efficacement les actions de maintenance.
2. La possibilité de désactiver subrepticement le logiciel en cas de désaccord avec son client (non-paiement de licence).

Parmi les motivations amenant les pirates informatiques à installer une porte dérobée :

1. La possibilité de surveiller ce que fait l'utilisateur légitime et de copier ou détruire des données ayant une valeur (mots de passe, clé privée pour déchiffrer des messages privés, coordonnées bancaires, secrets commerciaux).
2. La possibilité de prendre le contrôle d'un ordinateur et de pouvoir l'utiliser pour mener des actions malveillantes (envoi de pourriels notamment pour l'hameçonnage, de virus informatiques, déni de service).
3. Le contrôle d'un vaste réseau d'ordinateurs (voir *botnet*), qui peut être utilisé pour du chantage au déni de service distribué (DDoS), ou revendu à des criminels.

Pour installer des portes dérobées en masse, les pirates informatiques utilisent des virus. Ceux-ci se répandent automatiquement et installent un serveur informatique sur chaque ordinateur infecté. Ensuite le pirate peut se connecter à travers Internet au serveur.

Une porte dérobée peut aussi être insérée par voie d'Easter egg, de compilateur (voir la section plus bas *Le cas du compilateur C Unix: Trusting Trust*), ou peut prendre la forme d'un programme, comme Back Orifice.

Logiciel espion

Un **logiciel espion** (**espioniciel**, **mouchard** ou en anglais *spyware*) est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur n'en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet, qui lui sert de moyen de transmission de données.

Enregistreur de frappe

Un **enregistreur de frappe** ou **keylogger** peut être assimilé à un matériel ou à un logiciel espion qui a la particularité d'enregistrer les touches frappées sur le clavier sous certaines conditions et de les transmettre via les réseaux. Par exemple, certains enregistreur de frappe analysent les sites visités et enregistrent les codes secrets et mots de passe lors de la saisie.

Exploit (informatique)

Dans le domaine de la sécurité informatique, un **exploit** est un programme permettant à un individu d'exploiter une faille de sécurité informatique dans un système d'exploitation ou un logiciel que ce soit à distance (*remote exploit*) ou sur la machine sur laquelle cet exploit est exécuté (*local exploit*).

Prononcer comme en anglais « *explo-ï-te* » et non « *exploï* », le mot provenant de *exploitation* (de faille informatique) et non pas du fait de réaliser un quelconque exploit extraordinaire.

Rootkit

On nomme **rootkit** un programme ou ensemble de programmes permettant à un Pirate informatique de maintenir - dans le temps - un accès frauduleux à un système informatique. Le pré-requis du rootkit est une machine *déjà* compromise.

Principe d'un rootkit

Un rootkit s'utilise après une intrusion et l'installation d'une porte dérobée afin de camoufler tous les changements effectués lors de l'intrusion. Ainsi l'on peut préserver l'accès à la machine un maximum de temps, en effet les rootkits sont difficilement détectables et seule une analyse forensique approfondie peut en révéler la présence.

Rôle du rootkit

La fonction principale du « rootkit » est de camoufler la mise en place d'une ou plusieurs « portes dérobées ». Ces portes dérobées (utilisables en local ou à distance) permettent au pirate de s'introduire à nouveau au cœur de la machine sans pour autant exploiter une nouvelle fois la faille avec laquelle il a pu obtenir l'accès frauduleux initial, qui serait tôt ou tard comblée.

Les « rootkit » opèrent une suite de modifications, notamment au niveau des commandes système, voire du noyau (kernel).

A la différence d'un virus informatique ou un ver de nouvelle génération, un « rootkit » ne se réplique pas.

L'installation d'un « rootkit » nécessite des droits administrateur sur la machine, notamment à cause des modifications profondes du système qu'il engendre. Cela signifie que le pirate doit initialement disposer d'un accès frauduleux, avec les droits du « root » sous linux par exemple, afin de mettre en place son « rootkit ».

Un « rootkit » ne permet pas en tant que tel de s'introduire de manière frauduleuse sur une machine saine. En revanche, certains « rootkit » permettent la collecte des mots de passe qui transitent par la machine « corrompue ». Ainsi, un « rootkit » peut indirectement donner l'accès à d'autres machines.

Certains « rootkit » sont également livrés avec des collections d'« exploits », ces petits bouts de code dédiés à l'exploitation d'une faille bien déterminée. Le but est d'aider les pirates dans leur conquête de machines encore vierges.

Un «rootkit» a pour but principal la furtivité, il permet par exemple de cacher certains processus, certains fichiers et clef de registre... Il opère au niveau du noyau (la plupart du

temps chargé en tant que driver) et peut donc tromper à sa guise les programmes qui sont exécutés en mode utilisateur (antivirus, firewalls). Le rootkit est souvent couplé à d'autres programmes tel qu'un sniffeur de frappe, de paquets...

Le « rootkit » n'a de raison d'être que si une faille est présente, si les conditions sont réunies pour que son exploitation soit réussie et si elle permet un accès avec les droits administrateur. Donc pas de faille, pas de rootkit.

Le meilleur moyen de se protéger des rootkit est de se prémunir contre les failles.

Pour finir, les « rootkit » existent depuis plusieurs années. Le projet Chkrootkit dédié au développement d'un outil de détection de « rootkit » pour les plateformes Linux, *BSD, Solaris et HP-UX a été démarré en 1997. Le phénomène n'est donc pas nouveau. En 2002, Securityfocus faisait état des avancements en matière de « rootkit » pour les plateformes Microsoft Windows..

2-Techniques d'attaque par messagerie

En dehors des nombreux programmes malveillants qui se propagent par la messagerie électronique, il existe des attaques spécifiques à celle-ci :

Le **pourriel** (*spam* en anglais) : un courrier électronique non sollicité, la plupart du temps de la publicité. Ils encombrant le réseau, et font perdre du temps à leurs destinataires

L'**hameçonnage** (*phishing* en anglais) : un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles

Le **canular informatique** (*hoax* en anglais) : un courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes. Ils encombrant le réseau, et font perdre du temps à leurs destinataires. Dans certains cas, ils incitent l'utilisateur à effectuer des manipulations dangereuses sur son poste (suppression d'un fichier prétendument lié à un virus par exemple).

Pourriel

Boîte de réception infestée

Le **pourriel** ou *spam* en anglais, désigne les communications électroniques massives, notamment de courriers électroniques, non sollicitées par les destinataires, à des fins publicitaires ou malhonnêtes.

Origine du mot anglais

L'association de *spam* et de *indésirable* provient d'un sketch comique des Monty Python dans lequel le même mot, désignant un jambon en boîte de basse qualité, envahit la conversation et

le menu d'un petit restaurant. *SPAM* est la contraction de **SP**iced **hAM** (jambon épicé) et est une marque créée et déposée par Hormel Foods en 1937 (cf. **(en)** "[SPAM In Time](#)" sur le [site officiel](#)). Ce sketch parodiait d'ailleurs une des premières formes de message indésirable. En effet c'est une publicité radiophonique pour *SPAM*, pendant laquelle la marque était répétée de nombreuses fois, qui est à l'origine du sketch des [Monty Python](#).

Ce « pâté » a largement été utilisé par l'intendance des forces armées US pour la nourriture des soldats. Un dessin dû à la plume du sergent George Baker montre tout le cas que les soldats faisaient de cette nourriture considérée comme une cochonnerie lassante et décourageante. Incidemment George Baker est le créateur d'un personnage devenu célèbre : the Sad Sack paru pour la première fois en 1942 dans *Yank* dont les dessins ont été réunis par l'éditeur Simon & Schuster en 1944. Dans cet ouvrage vers la fin du volume (non paginé) figure un ensemble de sept dessins dont le titre générique est « SPAM ». Le copyright est de 1944. Il s'agirait de la première émergence publique du mot pour désigner un objet repoussant dont on aimerait bien ne pas être le destinataire.

Hameçonnage

L'**hameçonnage**, appelé en anglais *phishing*, est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. L'hameçonnage peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques.

Étymologie de *phishing*

Le terme *phishing* s'inspire du terme *phreaking* : mot-valise de « phone » et « freak ». Originellement, le *phreaking* était un type d'arnaque utilisé afin de profiter de services téléphoniques gratuits surtout présent à l'époque des appareils analogiques (années '70).

Le terme *phishing* aurait été inventé par les pirates qui essayaient de voler des comptes AOL. Il serait construit sur l'expression anglaise *password harvesting fishing*, soit « pêche aux mots de passe ». Un attaquant se faisait passer pour un membre de l'équipe AOL et envoyait un message instantané à une victime potentielle. Ce message demandait à la victime d'indiquer son mot de passe, afin de, par exemple, « vérifier son compte AOL » ou « confirmer ses informations bancaires ». Une fois que la victime avait révélé son mot de passe, l'attaquant pouvait accéder au compte et l'utiliser à des fins malveillantes, comme l'envoi de pourriel.

Canular informatique

En informatique, les canulars (appelés **hoax** en anglais) se trouvent souvent sous la forme de courriel ou de simple lettre-chaîne. Dans ce dernier cas, internet ne fait qu'amplifier un phénomène qui existait déjà à travers le courrier traditionnel.

A la différence des pourriels qui sont la plupart du temps envoyés de manière automatisée à une liste de destinataires, les canulars sont, eux, relayés manuellement par des personnes de bonne foi.

Les canulars sont souvent bâtis sur les mêmes modèles que les légendes urbaines. Dans ce cas ils en exploitent les caractéristiques de diffusion par colportage, ce qui renforce à la fois leur impact et leur audience.

Très souvent on peut s'apercevoir que :

- les fausses alertes au virus qui circulent par courriel sont destinées à faire paniquer les utilisateurs novices, parfois à leur faire commettre des manipulations dangereuses de leur système informatique et souvent à congestionner le réseau par leur diffusion hors de tout contrôle ;
- des quantités d'adresses e-mail sont aussi exposées, car souvent les utilisateurs ne savent pas les mettre en mode invisible ;
- on essaie de vous prendre par les sentiments de manière assez grossière (sauvez Brian !)
- les faits relatés sont généralement très flous (*au Brésil*, par exemple, sans plus de détail, ou *dans 3 mois*, sans donner la date de départ) ;
- les références sont généralement inexistantes ou au contraire trop énormes (le Pentagone, Microsoft, ...)
- parfois, on vous fait des promesses disproportionnées (devenir milliardaire vite et aisément, gagner un bateau, ...)
- parfois on vous assure à maintes reprises que ce n'est pas un canular, parfois en disant qu'un de ses amis a été convaincu par le message alors que c'est -évidemment- totalement faux ;
- on vous demande de renvoyer le message à toutes vos connaissances, ou à une adresse de courrier électronique bien précise
- enfin une variante appelée le **viroax** associe le virus et le hoax. Elle profite de la crédulité du destinataire, le pousse à effacer un fichier de son ordinateur, en lui faisant penser que c'est un virus, fichier parfois utile au fonctionnement de son système d'exploitation, son antivirus ou son pare-feu.

3-Attaques sur le réseau

Voici les principales techniques d'attaques sur le réseau :

- Le **sniffing** : technique permettant de récupérer toutes les informations transitant sur un réseau (on utilise pour cela un logiciel *sniffer*). Elle est généralement utilisée pour récupérer les mots de passe des applications qui ne chiffrent pas leurs communications, et pour identifier les machines qui communiquent sur le réseau.
- La **mystification** (en anglais *spoofing*) : technique consistant à prendre l'identité d'une autre personne ou d'une autre machine. Elle est généralement utilisée pour récupérer des informations sensibles, que l'on ne pourrait pas avoir autrement.
- Le **déni de service** (en anglais *denial of service*) : technique visant à générer des arrêts de service, et ainsi d'empêcher le bon fonctionnement d'un système.

Packet sniffer

Les **packet sniffers** (littéralement « renifleurs de paquets », aussi connus sous le nom de **renifleurs** ou **sniffeurs**) sont des logiciels qui peuvent récupérer les données transitant par le biais d'un réseau local. Ils permettent une consultation aisée des données non-chiffrées et peuvent ainsi servir à intercepter des mots de passes qui transitent en clair ou toute autre information non-chiffrée, à résoudre des problèmes réseaux en visualisant ce qui passe à travers l'interface réseau, ou à effectuer de la rétro-ingénierie réseau à des buts d'interopérabilité, de sécurité ou de résolution de problème.

Ce sont des sortes de sondes que l'on place sur un réseau pour l'écouter et en particulier parfois récupérer à la volée des informations sensibles lorsqu'elles ne sont pas chiffrées, comme des mots de passe (parfois sans que les utilisateurs ou les administrateurs du réseau ne s'en rendent compte).

Le renifleur peut être un équipement matériel ou un logiciel : le premier est bien plus puissant et efficace que le second, encore que, la puissance des machines augmentant sans cesse, l'écart se resserre. Mais le premier est surtout beaucoup plus cher que le second.

Lorsqu'une machine veut communiquer avec une autre sur un réseau non-switché (relié par un hub ou câblé en câble coaxial, techniques obsolètes), elle envoie ses messages sur le réseau à l'ensemble des machines et normalement seule la machine destinataire intercepte le message pour le lire, alors que les autres l'ignorent. Ainsi en utilisant la méthode du sniffing, il est possible d'écouter le trafic passant par un adaptateur réseau (carte réseau, carte réseau sans fil, etc.).

Pour pouvoir écouter tout le trafic sur une interface réseau, celle-ci doit être configurée dans un mode spécifique, le « mode promiscuous ». Ce mode permet d'écouter tous les paquets passant par l'interface, alors que dans le mode normal, le matériel servant d'interface réseau élimine les paquets n'étant pas à destination de l'hôte. Par exemple, il

n'est pas nécessaire de mettre la carte en mode « promiscuous » pour avoir accès aux mots de passe transitant sur un serveur FTP, vu que tous les mots de passe sont à destination dudit serveur.

La solution à ce problème d'indiscrétion est d'utiliser des protocoles de communication chiffrés, comme SSH (SFTP, scp), SSL (HTTPS ou FTPS) (et non des protocoles en clair comme HTTP, FTP, Telnet).

Le « **packet sniffer** » décompose ces messages et les rassemble, ainsi les informations peuvent être analysées à des fins frauduleuses (détecter des logins, des mots de passe, des emails), analyser un problème réseau, superviser un trafic ou encore faire de la rétro-ingénierie.

« **Sniffer** », c'est effectuer un sniffing. C'est une technique qui peut être ressentie comme profondément malhonnête et indélicate, mais bien pratique et nécessaire lorsque l'on est à la recherche d'une panne.

Usurpation d'adresse IP

L'**usurpation d'adresse IP** (en anglais : *IP spoofing*) est une technique de hacking consistant à utiliser l'adresse IP d'une machine, ou d'un équipement, afin d'en usurper l'identité. Elle permet de récupérer l'accès à des informations en se faisant passer pour la machine dont on spoofe l'adresse IP. De manière plus précise, cette technique permet la création de paquets IP avec une adresse IP source appartenant à quelqu'un d'autre.

Déni de service

Effets

D'une manière générale, l'attaque par **déni de service** ou *Denial of Service* (DoS) vise à rendre une application informatique incapable de répondre aux requêtes de ses utilisateurs.

Une machine serveur offrant des services à ses clients (par exemple un serveur web) doit traiter des requêtes provenant de plusieurs clients. Lorsque ces derniers ne peuvent en bénéficier pour des raisons délibérément provoquées par un tiers il y a *déni de service*.

Types d'attaques

De nombreux types d'attaques par déni de service existent (le simple fait de débrancher la prise d'un serveur peut être qualifiée d'attaque par déni de service) mais l'attaquant procède souvent par saturation d'au moins un des éléments chargés d'animer l'application.

4-Attaques sur les mots de passe

Les attaques sur les mots de passe peuvent consister à faire de nombreux essais jusqu'à trouver le bon mot de passe.

Dans ce cadre, notons les deux méthodes suivantes:

- **L'attaque par dictionnaire** : le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants et aussi des variantes de ceux-ci (à l'envers, avec un chiffre à la fin, *etc.*). Ces listes sont généralement dans toutes les langues les plus utilisées, contiennent des mots existants, ou des diminutifs (comme par exemple "powa" pour "power", ou "G0d" pour "god").
- **L'attaque par force brute** : toutes les possibilités sont faites dans l'ordre jusqu'à trouver la bonne solution (par exemple de "aaaaa" jusqu'à "ZZZZZ" pour un mot de passe composé strictement de six caractères alphabétiques).

Attaque par dictionnaire

L'**attaque par dictionnaire** est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Elle consiste à tester une série de mots de passe potentiels, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire. Si tel n'est pas le cas, l'attaque échouera.

Cette méthode repose sur le fait que de nombreuses personnes utilisent des mots de passe courants (*par ex* : un prénom, une couleur, le nom d'un animal...). C'est pour cette raison qu'il est toujours conseillé de **bien réfléchir avant de choisir un mot de passe**.

L'attaque par dictionnaire est souvent une méthode utilisée en complément de l'attaque par force brute qui consiste à tester de manière exhaustive les différentes possibilités de mots de passe. Cette dernière est particulièrement efficace pour des mots de passe n'excédant pas 5 ou 6 caractères.

Contenu du dictionnaire et règles

Outre le contenu habituel d'un dictionnaire qui renferme un ensemble de mots, le dictionnaire peut être fortement amélioré en combinant les mots ou en appliquant certaines règles. Par exemple, pour chaque mot, on peut essayer de changer la casse de certaines lettres. Une autre astuce consiste à répéter deux fois le mot (par exemple « secretsecret »), dans l'espoir que

l'utilisateur fasse appel à cette méthode **peu sûre** pour renforcer son mot de passe. On peut aussi générer des dictionnaires, par exemple pour des numéros de plaque, des numéros de sécurité sociale, des dates de naissance, etc.

Attaque par force brute

Deep Crack, circuit dédié à l'attaque par force brute de DES.

L'**attaque par force brute** est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles. Cette méthode de recherche exhaustive ne réussit que dans les cas où le mot de passe cherché est constitué de peu de caractères.

Pour contrer cette attaque, il suffit simplement de choisir des mots de passe d'une grande longueur ou des clés suffisamment grandes. Ainsi, l'attaquant devra mettre beaucoup de temps pour trouver le bon mot de passe.

Cette méthode est souvent combinée avec l'attaque par dictionnaire pour obtenir de meilleurs résultats.