Les différentes étapes d’une attaque

Bon nombre d’attaques, qu’elles soient simples ou complexes, suivent le même schéma :

Tout d’abord, il faut connaitre la cible, c’est-à-dire, récolter le plus d’informations possibles dessus. D’une part, on récolte les informations qu’elle rend publiques sur internet (adresse IP). Puis, un scan est effectué pour récupérer toutes les informations supplémentaires, telles que l’OS de l’ordinateur, le masque de sous réseau, les règles de firewall, etc…).

S’en suit une étape d’identification des failles : à partir des informations que l’on a récupéré, on cherche les failles à exploiter. Elles peuvent être au niveau des protocoles, du système d’exploitation, des applications, …

Enfin, bien sûr, l’attaquant passe à l’action pour contrôler l’ordinateur.

Quels sont les types d’attaques ?

http://igm.univ-mlv.fr/~duris/NTREZO/20032004/Baudoin-Karle-IDS-IPS.pdf

Le sniffing

Grâce à un logiciel appelé "sniffer", il est possible d’intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées. Si quelqu’un se connecte par telnet par exemple à ce moment-là, son mot de passe transitant en clair sur le net, il sera aisé de le lire. De même, il est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception. Une restriction de cette technique est de se situer sur le même réseau que la machine ciblée.

L’IP spoofing

Cette attaque est difficile à mettre en œuvre et nécessite une bonne connaissance du protocole TCP. Elle consiste, le plus souvent, à se faire passer pour une autre machine en falsifiant son adresse IP de manière à accéder à un serveur ayant une "relation de confiance" avec la machine "spoofée". Cette attaque n’est intéressante que dans la mesure où la machine de confiance dont l’attaquant à pris l’identité peut accéder au serveur cible en tant que root.

Le DoS (Denial of Service)

Le DoS est une attaque visant à générer des arrêts de service et donc à empêcher le bon fonctionnement d’un système. Cette attaque ne permet pas en elle-même d’avoir accès à des données. En général, le déni de service va exploiter les faiblesses de l’architecture d’un réseau ou d’un protocole. Il en existe de plusieurs types comme le flooding, le TCP-SYN flooding, le smurf ou le débordement de tampon (buffer-overflow).

Les programmes cachés ou virus

Il existe une grande variété de virus. On ne classe cependant pas les virus d’après leurs dégâts mais selon leur mode de propagation et de multiplication. On recense donc les vers (capables de se propager dans le réseau), les troyens (créant des failles dans un système), Les bombes logiques (se lançant suite à un événement du système (appel d’une primitive, date spéciale)).

L’ingénierie sociale (social engineering)

Ce n’est pas vraiment une attaque informatique en soit, mais plutôt une méthode consistant à se faire passer pour quelqu’un que l’on n’est pas afin de recueillir des informations confidentielles.

Le craquage de mots de passe

Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s’effectuer à l’aide d’un dictionnaire des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu’à trouver la bonne). Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l’appui d’un très grand nombre de machines.