Les attaques informatiques

I) Les spywares :

Les spywares sont des programmes espions qui recueillent :
- Les URL visités
- Les recherches des mots clés.
- Des informations personnelles ou de paiement bancaire.

En général, les spywares s'installent en même temps que d'autres logiciels.

II) Les trojans ou chevaux de troie :

Les trojans sont des programmes qui exécutent des opérations à l'insu de l'utilisateur afin d'ouvrir une porte dérobée (backdoor). Cette dernière permettra à un pirate de prendre le contrôle de la machine

En général, le trojan est caché dans un programme sain.

III) Les vers :

Les vers sont considérés comme des virus réseaux car ils peuvent s'auto reproduire et infecter un réseau en utilisant les mécanismes réseaux (récupération carnet d'adresse, envoi de copie …).

IV) Le spamming :

Le spamming consiste en l'envoi de message non souhaité et dérangeant à plusieurs personnes dans un but promotionnel ou publicitaire.

Le spamming repose sur l'utilisation abusive des systèmes de messagerie électronique ou de traitements automatisés des données (émail, messagerie instantanée, forum, texto …).

V) Le mailbombing :

Le mailbombing est une attaque dont le but est soit la saturation de la boite aux lettres de la victime ou une attaque de deny de service (DoS).

Certains virus pratiquent aussi le mailbombing, et sont ainsi capables de s'envoyer en plusieurs centaines d'exemplaires à la même personne en un temps réduit.

VI) Phising :

Le phishing consiste à récupérer frauduleusement des informations auprès d'internaute. Cette technique d'ingénierie sociale est utilisée par les pirates afin d'exploiter la faille humaine en se faisant passer pour quelqu'un de confiance. En général ce sont des mails semblant provenir de banque ou de commerce.

VII) Scam :

Le scam (qui est une pratique frauduleuse d'origine africaine) consiste à extorquer de l'argent à des internautes en leur faisant miroiter une somme d'argent.

VIII) Hoax :

Un hoax est une information fausse, périmée ou invérifiable propagée spontanément par les internautes. Il peut s'agir d'alerte virus, de disparition d'enfant, de promesse de bonheur, de pétition.

Ils existent avant tout sous forme écrite (courrier électronique, message dans un forum) et contrairement aux rumeurs hors ligne incitent le plus souvent explicitement l'internaute à faire suivre la nouvelle à tous ses contacts, d'où une rapide réaction en chaîne.

IX) Attaque deni de service :

Une attaque par déni de service (DoS) a pour objectif de rendre indisponible des services ou des ressource en envoyant des paquets IP ou des données afin de les saturer ou de les rendre instables.

Un déni de service provoqué par plusieurs machines est appelé déni de service distribué (DDOS : Distributed Denial of Service). Les attaques par déni de service distribué les plus connues sont Tribal Flood Network (TFN) et Trinoo.

Les dénis de service par exploitation de vulnérabilités, consistant à exploiter une faille du système distant afin de le rendre inutilisable.

X) Attaque SMURF (camouflage) :

Attaque malveillante consistant à envoyer un grand nombre de ping spoofés vers des adresses broadcast afin d'amplifier le nombre de paquets par la réponse vers les adresses spoofées. Cette technique offre des possibilités de saturation exponentielles selon le nombre d'hôtes répondant à la requête.

XI) Ping de la mort :

Attaque par interruption de service (DoS) consistant à l'envoi d'un paquet ping de taille surdimensionné, dans le but d'entraîner le blocage de la machine réceptrice lors de la tentative de réassemblage du paquet de données surdimensionné.

XII) Spoofing :

Tentative d'accès à un système réseau par usurpation (utilisateur, système ou programme autorisés).