Glossaire

Acces Denied

Littéralement, Accès refusé. Procédure en vigueur sur les espaces de discussion et permettant aux administrateurs d'interdire l'accès à une personne, en général repérée par son adresse IP.

Adresse IP

IP signifiant Internet Protocol, l'adresse IP est l'identifiant unique d'un équipement connecté au réseau. Chaque ordinateur, routeur, console, téléphone ou autre, connectés à Internet, possède une adresse qui l'identifie. Cette adresse, présente dans chaque transaction entre le client et le serveur, permet de déterminer la destination des paquets de données.

Backdoor

Porte arrière. Il s'agit d'un logiciel apparemment anodin, mais qui ouvre secrètement une connexion pour des ordinateurs tiers. Les actions que pourront alors réaliser les auteurs de l'intrusion dépendront des fonctionnalités proposées par le logiciel.

Batch

Script de commande destiné à faire exécuter à l'ordinateur une série d'instructions de façon séquentielle.

Cache

Il s'agit d'une mémoire résiduelle destinée à optimiser les accès. Sur les moteurs de recherche, le cache conserve les pages consultées un certain temps pour pouvoir les délivrer plus rapidement à la demande d'un utilisateur, agissant ainsi comme un tampon relai. Cependant, lorsqu'une page est supprimée d'un site web, si elle a été placée en cache sur un moteur de recherches, elle peut encore y être consultée.

Chat

Système de discussion en temps réel sur internet.

Cheval de Troie

Logiciel utilisant la stratégie d'Ulysse pour pénétrer un ordinateur. Il se fait passer pour un autre logiciel, soit connu, soit disposant de fonctionnalités attirantes et sans aucun rapport avec la véritable intention de son auteur. Une fois installé sur l'ordinateur, il peut réaliser son véritable dessein, détruire, espionner ou ouvrir une backdoor.

DMZ

De Militarized Zone : zone démilitarisée. Dans une architecture réseau, le firewall a pour objet de filtrer les transactions et de traduire els adresses IP de façon à ce que seules les personnes implicitement autorisées puissent accéder aux ressources du réseau interne. Mais certaines applications, comme les serveurs Web, doivent se situer dans une zone annexe, en partie protégée par le Firewall, en partie ouverte au

public. C’est le rôle de cette zone démilitarisée, la portion accessible au public d'un réseau protégé.

Firewall

Pare-feu. Équipement matériel ou logiciel destiné a assurer la sécurité d'un réseau. Il filtre les transactions et, par principe, détermine au travers de règles le trafic qui est autorisé. Ainsi, il est possible de limiter les services accessibles et les utilisateurs qui y auront accès.
C'est un équipement indispensable à tout réseau connecté à Internet.

GPS

Global Positionning Service. Service public de géopositionnement par satellite. Démocratisé depuis quelques années, le GPS est présent sur de nombreux équipements comme les téléphones portables ou les appareils photo numériques. Il permet d'obtenir la position de l'équipement de façon précise en appelant un satellite géo stationnaire.

Harponnage (voir phising)

Keylogger

Logiciel espion ayant pour fonction de conserver la trace de toutes les touches tapées sur un clavier pour les fournir à un pirate. Sur les formulaires web sécurisés, les mots de passe ne sont pas lisibles et les transactions souvent cryptées. Le Keylogger s'en moque, en conservant les touches tapées au clavier dans un petit fichier qu'il transmet ensuite, il contourne la difficulté.

Nacites

Ce sont les microprogrammes d'Ylian Estevez. Concentrés de technologie, ils cumulent les fonctions de Keyloggers, de Backdoor et fournissent un grand nombre de possibilités à Ylian. Parmi leurs originalités, citons le fait qu'ils contournent les pare-feux en passant leurs flux de données au travers des services autorisés, comme le web ou le mail, et transmettent ces informations en même temps que celles légitimement transmises par l'utilisateur. Ils sont connectés à un système de console centrale permettant à Ylian de les surveiller et d'en prendre le contrôle. Les nacites sont modulaires, Ylian peut ajouter des fonctionnalités à l'un d'entre eux lorsqu'il le souhaite. Dès qu'ils sont repérés, c'est-à-dire que l'on tente d'y accéder par un autre moyen que celui autorisé par Ylian, ils s'autodétruisent de façon irréversible. Les légions de nacites sont les fers de lance de l'activité d'Ylian Estevez.

Nickname

Pseudonyme utilisé sur un forum ou un service de discussion en temps réel.

Patché

Mis à jour. Les patchs sont des correctifs qui rectifient les bugs et vulnérabilités présents sur les logiciels et systèmes d'exploitation. Il est donc important de procéder à ces mises à jour. Mais comme l'a expérimenté Taylor Sylk, une fausse mise à jour peut cacher une tentative d'intrusion.

Playlist

Liste de fichiers. Dans les radios comme dans les lecteurs MP3, il est possible d'utiliser des playlist. Ainsi, c'est de façon informatique et préalable que l'on détermine la programmation musicale d'une station.

Phishing

Hameçonnage. Technique de hacking utilisant une fausse page web, en tout point identique à la vraie, pour obtenir des informations. Ainsi, si vous recevez par courrier électronique un message en provenance de votre banque et vous invitant à accéder à votre compte, cela a de grandes chances d'être un hameçonnage. En vous connectant sur le faux site, identique à celui que vous connaissez, vous taperez sans crainte le numéro de votre compte et votre mot de passe. Mais ceux-ci iront directement chez le pirate vous ayant ainsi piégé.

Proxy

Serveur Passerelle : Le proxy est un serveur qui relaye les transactions à l'identique. Jadis utilisé pour partager des connexions ou pour gérer du cache, il est aujourd'hui très utile pour cacher sa véritable adresse IP. Lorsqu'une connexion est établie avec un serveur via un proxy, le serveur ne connaît que l'adresse du proxy, et ignore tout de celle qui a réellement initié la demande.

Team

Anglicisme couramment employé pour décrire une équipe de pirates signant des exploits.

VPN

Réseau privé virtuel (Virtual Private Network). Technologie visant à établir un tunnel crypté entre deux équipements ou deux réseaux afin d'éviter que les informations qui y transitent soient interceptées. Aujourd'hui très utilisés, ils ont également la faculté de tromper les serveurs sur l'identité réelle de l'auteur d'une demande, un peu comme avec un proxy.