GLOSSAIRE*

Pour vous aider à vous familiariser avec le thème de cette conférence, nous vous proposons quelques définitions de termes liés au domaine abordé cet après-midi.

Cette fiche est aussi disponible en ligne à l'adresse suivante : http://www.forumtelecom.org/pv/021210g.pdf

ADRESSE IP
Numéro unique de la forme XXX.XXX.XXX.XXX (XXX étant un nombre entier compris entre 0 et 255) qui identifie chaque ordinateur connecté à Internet ou à tout autre réseau utilisant le protocole TCP/IP. Indispensable aux échanges d'informations entre les différentes machines, l'adresse IP peut être fixe, c'est-à-dire attribuée pour une durée indéterminée à un même ordinateur, ou bien dynamique, c'est-à-dire attribuée à chaque nouvelle connexion (cas de la majorité des contrats de base d'accès à Internet).

BACKDOOR
Programmes usurpateurs qui détournent des fonctionnalités systèmes dans le but d'ouvrir des accès utiles aux pirates pour contrôler à distance les machines ciblées. Ces programmes, très dangereux, sont la plupart du temps installés par le biais d'un "cheval de Troie". Parmi les plus célèbres, on peut citer BackOrifice (BO) ou encore NetBus.

BUFFER OVERFLOW
Voir **Débordement de zone de tampon**

CHEVAL DE TROIE
Un cheval de Troie est un programme d'aspect anodin, masquant un code exécutable malicieux déclenchant ou servant à déclencher une attaque.
Un cheval de Troie est en général utilisé pour ouvrir une porte dérobée (Backdoor) sur un système et donc permettre l'accès à distance de son ordinateur à un pirate informatique.

DEBORDEMENT DE ZONE DE TAMPON
Attaque consistant à envoyer dans un buffer plus d'informations qu'il ne peut en contenir, occasionnant un dysfonctionnement qui conduit un système à donner "la main" au pirate avec le maximum de droits.

DENI DE SERVICE
Le fait de saturer un serveur au moyen de requêtes généralement mal formées et/ou très nombreuses afin de perturber ou de rendre non opérationnel le service qu'il fournit à ses utilisateurs.

DENI DE SERVICE DISTRIBUE :
Cette technique de déni de service exploite plusieurs machines compromises pour lancer une attaque sur un site dont la bande passante ou les mesures de défense sont juste dimensionnées pour résister à un seul attaquant.

DENIAL OF SERVICE
Voir **déni de service**

FIREWALL
Système logiciel ou serveur dédié situé entre deux réseaux informatiques, dont

la tâche est de contrôler aussi bien les communications entrantes que sortantes, dans le but de sécuriser les échanges d'informations.

HOAX

En français, "canular". Il s'agit de rumeurs et fausses informations qu'une personne cherche à répandre le plus largement possible en utilisant comme support les autres internautes, qui relaieront l'information généralement par E-Mail.

MACRO

Petit programme qui permet l'exécution d'une série de commandes prédéfinies. On l'utilise pour automatiser les tâches répétitives dans les logiciels et notamment dans les applications Microsoft Office (Word, Excel, etc.).

MAILBOMBING

Attaque basique qui consiste à envoyer des centaines, des milliers voire des dizaines de milliers de messages appelés "mailbomb" à un unique destinataire dans un but évidemment malveillant. Ce dernier va du simple encombrement de boîte aux lettres, avec possibilité de perte de données en cas de saturation de la capacité de stockage, jusqu'au crash machine ou déni de service.

MALWARE

Contraction de "malicious software", le terme malware désigne les programmes spécifiquement conçus pour endommager ou entraver le fonctionnement normal d'un système, tels que les virus, les vers, les chevaux de Troie, ainsi que certains javascripts ou applets java hostiles. Cette famille ne doit pas être confondue avec les spywares (espiogiciels), autre famille de logiciels dont le fonctionnement est également contestable mais dont le but premier n'est pas de nuire à l'intégrité d'un système.

PGP (PRETTY GOOD PRIVACY)

Agorithme d'encryption de données garantissant la confidentialité du contenu des messages (notamment des E-Mail) durant le transfert et après la réception.

PORT

Un port est un numéro de 16 bits (ce qui permet un intervalle de 1 à 65535) utilisé par les protocoles de la couche de transport - les protocoles TCP et UDP. Les ports sont utilisés pour adresser des applications (services) s'exécutant sur un ordinateur. Si une seule application réseau était présente sur un ordinateur, les numéros de port ne seraient pas nécessaires. Cependant, plusieurs applications peuvent s'exécuter simultanément sur un PC donné, aussi est-il nécessaire de les différentier. D'où l'utilité des numéros de port. Aussi, on peut assimiler un numéro de port à l'adresse d'une application sur le PC.

PROXY

Logiciel permettant d'accéder à certains services d'Internet à travers un firewall et/ou destiné à jouer le rôle d'un cache partagé par plusieurs utilisateurs afin d'accélérer la consultation de certains fichiers fréquemment accédés.

SNIFFER

Sonde logicielle destinée à analyser le trafic sur un réseau. On l'associe souvent au firewall pour détecter plus efficacement les backdoors. Les pirates les utilisent aussi pour récupérer à la volée (illégalement) des informations sensibles à l'insu des administrateurs réseau.

Spoofing

Méthode de piratage, s'appuyant sur le protocole UDP, et consistant à usurper l'adresse IP d'un ordinateur "ami" du système à attaquer, de manière à pouvoir y pénétrer de manière transparente.

SSL (SECURE SOCKET LAYER)

Protocole développé par Netscape pour la transmission privée de documents au

travers d'Internet. Il utilise une clé privée pour coder (encrypter) les données transférées. Netscape Navigator et Internet Explorer, notamment, supportent ce protocole. De nombreux sites Web utilisent le protocole pour les informations confidentielles des utilisateurs telles que les numéros de carte de crédit. Par convention, les pages Web qui requièrent l'utilisation de ce protocole commencent par https (au lieu de http).

TROJAN OU TROJAN HORSE

voir **Cheval de Troie**

UNIX (UNICS, UNIPLEXED INFORMATION AND COMPUTER SERVICE)

Système d'exploitation multitâches et multi-utilisateurs très performant développé à la fin des années 60. Ce système d'exploitation ouvert a été porté sur la plupart des ordinateurs, de l'ordinateur central au PC à processeur Intel en passant par les stations de travail, ce qui fait qu'il en existe maintenant beaucoup de variantes. Le dérivé le plus connu d'UNIX est Linux.

VER

Un Ver est un programme indépendant, qui se copie d'ordinateur en ordinateur. La différence entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme et donc l'infecter, il va simplement se copier via un réseau ou Internet, d'ordinateur en ordinateur. Ce type de réplication peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances du réseau dans une entreprise. Comme un virus, ce ver peut contenir une action nuisible du type destruction de données ou envoi d'informations confidentielles.

VPN (VIRTUAL PRIVATE NETWORK)

Réseau privé virtuel, permet d'accéder à un réseau privé d'entreprise depuis l'extérieur en garantissant une connexion sécurisée.

WORN

Voir V**er**

Le FORUM TELECOM® est une initiative de la SPI+ bénéficiant du soutien financier de la Région wallonne et du FEDER.

[*] Ce glossaire à été réalisé sur base des sources suivantes :

- Glossaire du FORUM TELECOM
- http://www.secuser.com/glossaire/m.htm
- http://securit.free.fr/glossaire.htm
- http://www.symantec.com/region/fr/avcenter/glossaire.html
- http://www.icbo.ch/index.html?/security/glossaire.html
- http://home.datacomm.ch/oranewatches/winroute/418.htm
- http://www.atrid.fr/opensource/glossaire.html
- http://www.diamss.com/htm/fr/search/glossary/