Lexique du vocabulaire de la sécurité informatique

A

Attaque active : Attaque se traduisant par une modification illégale d'un état, par exemple la manipulation des fichiers sur un serveur.

AIS (Automated Information System) : Système d'information automatisé . Terme désignant tous les équipements (de nature matérielle, logicielle, ou "firmware") permettant l'acquisition automatique, le stockage, la manipulation, le contrôle, l'affichage, la transmission, ou la réception de données.

Alert : Message décrivant une circonstance se rapportant à la sécurité réseau. Les alertes viennent souvent de systèmes de surveillance actifs sur le réseau.

Ankle-Biter : Personne voulant devenir Hacker ou Cracker mais ayant très peu de connaissances sur les systèmes informatiques. Ce sont la plupart du temps des jeunes adolescents se servant de programmes faciles à utiliser et provenant d'internet .

Anomaly Detection Model : Système de sécurité détectant les intrusions en recherchant les activités sortant du comportement habituel du système et des utilisateurs.

Application Level Gateway (Firewall) : Un firewall est un système ou une application qui gère l'ensemble des connections TCP lors d'une session réseau. Ces "murs de feu" redirigent souvent les paquets sortants afin d'en camoufler l'expéditeur.

APT (Advanced Persistent Threat) : Attaque désignant une typologie d'attaques (généralement un regroupement de plusieurs types d'attaques)

ASIM (Automated Security Incident Measurement) : Evaluation automatique d'un incident de sécurité. Surveille le trafic réseau et collecte des informations sur les éléments du réseau où des activités non autorisées sont détectées.

Assessement : Analyse des vulnérabilités d'un système d'information automatisé consistant en la surveillance et l'inspection du système dans le but d'aider l'administrateur à le sécuriser de la meilleure façon possible.

Attaque : Tentative d'évitement des contrôles de sécurité sur un serveur. Le succès de l'attaque dépend de la vulnérabilité du serveur attaqué, mais si elle réussit, l'attaquant aura un accès illimité au serveur et pourra faire tout ce qu'il veut (vol, destruction de données...)

Audit : Examination des renseignements et activités dans le but de s'assurer qu'ils respectent les contrôles établis et les procédures opérationnelles.

Audit Trail : Enregistrement de l'utilisation des ressources systèmes sur un ordinateur : identification, fichiers accédés, violations des droits...

Authentication Header (AH) : En-tête d'identification . Champs qui suit l'en-tête IP dans un datagramme IP et qui vérifie la provenance et l'intégrité du datagramme.

Automated Security Monitoring : Gestion automatique de la sécurité. Terme désignant tous les services de sécurité assurant un niveau de protection effectif pour l'environnement matériel, l'environnement logiciel, et toute sorte de données.