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.

B

Back Door : Trou de sécurité laissé volontairement dans le système, souvent sous la forme d'un programme dissimulé, par l'administrateur ou par un hacker ayant obtenu un accès root afin de pouvoir conserver cet accès sans forcer la sécurité du système. Voir le film "Wargames".
BCRCI : Brigade Centrale de Répression du Crime Informatique : Service de la police française.
Biba Integrity Model : Modèle formel de sécurité pour l'intégrité des sujets et objets d'un système.
Bomb : Terme désignant tout type de d'attaque visant à crasher le système cible en utilisant des failles logicielles ou protocolaires.
Brèche : Terme employé lors de la réussite d'une attaque sur un serveur, lors de la pénétration d'un système.
Brute Force : Attaque qui permet de trouver un mot de passe
Broadcast : Ping envoyé par l'ordinateur local vers tous les autres ordinateurs du réseau. L'ordinateur local reçois donc les réponses de tout le monde. C'est utile lorsque qu'un ordinateur recemment connecté à un réseau veut connaitre les adresses IP de tout les autres ordinateurs.
Buffer Overflow : Phénomène se produisant lorsque le tampon (buffer) ne peut pas traîter correctement toutes les données qu'il reçoit. Cela arrive quand le taux de transfert de données du destinataire est trop inférieur à celui de l'expéditeur. Un buffer Overflow entraîne très souvent un crash du système cible; c'est pourquoi il peut être utilisé volontairement par un hacker.
Bug : Malfonction d'un programme ou d'un matériel due à une erreur involontaire de programmation ou de construction.

C

C2 : Abréviation de Commandement et Contrôle (Command & Control).
Certifier : Etablir la validité d'un utilisateur ou d'un objet en créant un acompte lui alouant des droits.
Certification : Identification. Vérification de l'identité d'un utilisateur ou de toute autre entité dans un système, le plus souvent par mot de passe, pour lui permettre de gérer les ressources auxquelles il a accès.
CGI : Common Gateway Interface. Le CGI est une méthode permettant de faire interagir des serveurs web et des programmes.
CGI-scripts : Scripts permettant la création de pages web dynamiques et interactives. Les CGI-scripts sont réputés pour être très vulnérables aux attaques.
Clipper Chip : Puce VLSI créée par la NSA pour l'encryption de communications vocales. Ce chip utilise l'ESS (Escrow Encryption Standard) et y ajoute l'algorithme d'encryption Skipjack.
COAST (Computer Operations, Audit, and Security Technology) : Opérations informatiques, surveillance, et technologie de sécurité. C'est un projet multiple, sur lequel travaillent plusieurs laboratoires d'investigation dans la sécurité informatique dans le département des sciences informatiques à la Prude University. Des chercheurs et ingénieurs dans les grandes compagnies et les gouvernements participent également à ce projet. Sa recherche est centrée sur les besoins et limitations du monde réel, avec une focalisation particulière sur la sécurité des systèmes informatiques.
Compromise : Intrusion dans un système ayant pour conséquence la divulgation, la modification, ou la destruction d'informations confidentielles.
Computer Abuse : Activité illégale volontaire qui affecte la disponibilité, la confidentialité, ou l'intégrité des ressources d'un ordinateur. Les "Computer Abuse" comprennent la fraude, le détournement, le vol, l'endommagement, l'utilisation non autorisée, et le refus de service.
Computer Fraud : Crimes informatiques impliquant la modification de données dans le but d'en tirer quelque chose de valeur.

Computer Network Attack : Attaque visant à endommager, dégrader, ou détruire des informations se trouvant dans des ordinateurs ou dans des réseaux informatiques, voire détruire les ordinateurs et les réseaux eux mêmes.
Computer Security : Procédures technologiques de sécurité appliquées à des systèmes informatiques pour assurer la disponibilité, l'intégrité, et la confidentialité des informations contenues dans le système.
Computer Security Incident : Intrusion ou tentative d'intrusion dans un Système d'Information Automatisé (AIS). Ces incidents de sécurité peuvent entraîner de longues investigations sur un grand nombre de systèmes informatiques.
Computer Security Intrusion : Accès non autorisé ou pénétration d'un Système d'Information Automatisé (AIS).
Confidentiality : Confidentialité. Elle assure que les informations resteront secrètes et que seules les personnes autorisées y auront accès.
COPS (Computer Oracle and Password System) : Système de gestion pour les serveurs Unix; c'est un logiciel testant la sécurité de shells scripts et de programmes écrits en C. Il recherche des faiblesses dans leur sécurité et les signale quand il en trouve.
Countermeasures : Contre-mesures. Action, matériel, procédure, technique, ou tout autre mesure réduisant la vulnérabilité d'un système d'information automatisé (AIS). Les contre-mesures destinées à des menaces et vulnérabilités spécifiques nécessitent des techniques plus sophistiquées et peuvent être identifiées à des systèmes de sécurité.
Crack : Outil de Hacking utilisé pour décoder des mots de passe encryptés. Les administrateurs utilisent aussi Crack pour évaluer la faiblesse des mots de passe des utilisateurs inexpérimentés dans le but d'augmenter la sécurité du système.
Cracker : Personne ayant cassé les sécurités d'un système.
Cracking : Action de s'introduire dans un système informatique.
Crash : Faille soudaine et brutale dans un système informatique.
Cryptanalysis :
1) Analyse d'un système de cryptage et/ou de ses entrées/sorties pour en tirer des variables confidentielles et des données sensibles.
2) Action de décrypter des messages sans la connaissance de l'algorithme ou de la clé de cryptage.
Cryptographic Hash Function : Processus qui transforme une valeur d'un ensemble de données de manière que toute manipulation de cet ensemble soit détectable.
Cryptography : Cryptographie . Terme désignant la science, les principes, les moyens, et les méthodes pour rendre un texte incompréhensible et pour convertir les messages cryptés en textes compréhensibles.
Cryptology : Cryptologie. Science se rapportant aux communications camouflées, déguisées, ou cryptées.
Cyberspace: Cyberespace. Terme désignant l'ensemble de tous les ordinateurs connectés et la société assemblée autour d'eux. Le Cyberespace est le plus souvent appelé INTERNET.

D

Datagramme : Packet IP. Cela inclue l'entête IP et les données transportées.
Disponibilité : Elle assure que les informations et les communications seront utilisables quand une requête leur sera formulée.
Dark Side Hacker : Un Hacker criminel ou malveillant.
DARPA (Defense Advenced Reaserch Projects Agency) : Agence de recherche avancée de projets de défense.
Data Driven Attack : Attaque codée en données semblant inoffensives mais pouvant s'avérer dangereuses une fois les défense d'un système dépassées. Le but de ce type d'attaque est le plus souvent de pouvoir passer à travers un Firewall.
Data Encryption Standard :
1) (DES) Algorithme de cryptage adopté par le bureau National des Standards pour une utilisation publique.

2) Algorithme de cryptage pour la protection des données non classées. Le DES, approuvé par l'Institut National des Standards et des Technologies (NIST), est destiné à une utilisation publique et gouvernementale.
Defense Information Operations : Processus qui intègre et coordonne les politiques avec les procédures, les opérations, le personnel, et les technologies pour protéger les informations et défendre les systèmes d'information. Les DIO se servent d'informations, de sécurité physique, d'opérations de sécurité, d'opérations anti-psychologiques et anti-intelligence, de protections électroniques et d'opérations d'information spéciales. Les DIO assurent un accès aux informations précis, rapide, et fiable tout en les protégeant des ennemis voulant les exploiter.
Deamon Dialer : Programme qui appelle systématiquement le même numéro de téléphone. Ces programmes peuvent être autorisés dans la mesure où ils servent a accéder à des BBS, mais ils peuvent aussi être illégaux s'il sont utilisés pour des attaques de type Denial of Service.
Denial of Service (DOS & DDOS) : Attaques volontaires visant à empêcher le fonctionnement d'un système d'Information Automatisé (AIS).
Derf : Action d'exploiter un terminal sur lequel quelqu'un s'est déjà identifié et a oublié de fermer sa session.
DES : Voir Data Encryption Standard
DNS Spoofing : Utilisation du DNS (Domain Name Server) d'un autre système en corrompant le name service cache d'un système victime, ou en faisant passer un DNS pour un domaine valide.

E

Electronic Attack (EA) : Attaque électronique. Division du EW (voir Electronic Warfare) où l'on utilise l'électromagnétique, l'énergétique, ou les armes anti-radiation dans le but d'attaquer du personnel, des aménagements, ou des équipements avec l'intention de dégrader, neutraliser, ou détruire la capacité de combat ennemie. Une EA inclut : les actions exécutées pour prévenir ou réduire une utilisation ennemie du spectre électromagnétique, telle que le Jamming ou l'utilisation d'armes à mécanisme électromagnétique ou énergétique (lasers, fréquences radio, rayons de particules).
Electronic Protection (EP) : Protection électronique. Division du EW qui représente toutes les mesures prises pour protéger le personnel, les aménagements, et les équipements des effets de l'utilisation ennemie du EW dégradant, neutralisant, ou détruisant les capacités de combat alliées.
Electronic Warfare (EW) : Terme désignant toutes les actions militaires impliquant l'utilisation d'électromagnétique et d'énergétique dans le but de contrôler le spectre électromagnétique ou d'attaquer l'ennemi. Les trois divisions principales de l'Electronic Warfare sont les Attaques Electroniques (EA), la Protection Electronique (EP), et le Support de Guerre Electronique (ES).
Electronic Warfare Support (ES) : Support de Guerre Electronique. Division du EW impliquant l'exécution de tâches par , ou sous contrôle direct d'un Commander opérationnel pour chercher, intercepter, identifier, et situer les sources d'énergie électromagnétique émises intentionnellement ou non dans le but de détecter les menaces. Par conséquent, l'ES fournit les informations nécessaires aux décisions concernant les opérations d'EW et autres opérations tactiques telles que les menaces d'évasion. Les données des ES peuvent être utilisées pour produire des signaux de renseignements.
Encapsulating Security Payload (ESA) : Mécanisme fournissant une protection pour la confidentialité et l'intégrité de datagrammes IP.
Ethernet Sniffing : Programme écoutant l'interface ethernet pour des paquets intéressant l'utilisateur. Quand le programme repère un paquet répondant à certains critères, il copie son contenu dans un fichier. Les critères les plus fréquents pour un paquet intéressant sont des mots tels que "login" ou "password".

F

False Negative : Evénement se produisant quand une intrusion est identifiée comme une non intrusion par le système et la laisse se produire.
False Positive : Evénement se produisant quand un système classe une action comme anormale (par exemple une intrusion) quand il s'agit d'une action légitime.
Fault Tolerance : Capacité d'un système ou d'un composant à continuer de fonctionner correctement malgré la présence de problèmes matériels ou logiciels.
Firewall : Système ou combinaison de systèmes qui renforce la limite entre deux réseaux ou plus. C'est un type de passerelle limitant l'accès entre les réseaux conformément à la politique locale de sécurité. Cette limite est basée sur le filtrage des informations transitant entre les deux réseaux. C'est un outil indispensable de sécurisation.
Fishing : Technique pour récupérer des informations personnelles.
Fishbowl : Contenir, isoler, et subordonner un utilisateur non autorisé sur un système dans le but d'obtenir des informations sur cet utilisateur.
Flag : Drapeau en français. C'est un indicateur binaire, généralement codé sur un bit.
Flood : Inondation, déluge en français. Type d'attaque réseau qui consiste à envoyer un flux important de packets ou de messages visant à saturer l'ordinateur victime. Cette attaque n'est vraiment valable que si le débit (bande passante) de l'attaquant est supérieur à celui de la victime. Les récentes attaques contre Yahoo et EBay de Mafiaboy sont de ce type.
Fork Bomb : Aussi connu sous le nom de "logic bomb", code pouvant être écrit en une ligne de code sur un système Unix; basé sur une duplication infinie de lui-même, il peut éventuellement "exploser" en détruisant toutes les entrées dans la table des processus et bloquant efficacement le système.

H

Hacker : Personne aimant explorer les détails des systèmes informatiques et comment étendre leurs capacités. Personne malveillante ou curieuse s'intéressant à tout ce qui touche à l'informatique et qui essaie de découvrir le maximum d'information en recherchant partout. Personne aimant apprendre les détails des systèmes de programmation, par opposition à la plupart des utilisateurs qui préfèrent apprendre le minimum nécessaire.
Hacking : Utilisation non autorisée ou tentative de tromper ou de passer outre les mécanismes de sécurité sur un ordinateur ou un réseau.
Hacking Run : Session de Hacking de durée très supérieure à la normale, en particulier celles durant plus de 12 heures.
Hameconnage : Technique pour récupérer des informations personnelles.
Host : Un ordinateur simple ou une station de travail; il peut être connecté à un réseau.
Host Based : Information, telle que des données livrées par un audit, provenant d'un simple host qui peut être utilisée pour détecter les intrusions.

I

IDEA (International Data Encryption Algorythm) : Algorithme international d'encryption de données. Algorithme d'encryption - décryption par clé qui utilise une clé deux fois plus longue qu'une clé DES.
IDIOT (Intrusion Detection In Our Time) : Système détectant les intrusions en utilisant le

pattern-matching (détection d'opérations inhabituelles).
Information Assurence (IA) : Opérations d'information qui protègent et défendent les informations et les systèmes d'information en assurant leur disponibilité, leur confidentialité, leur intégrité, et leur authenticité. Cela inclut la restauration de systèmes d'information en incorporant protection, détections, et capacités de réaction.
Information Operations (IO) : Opérations d'information. Actions exécutées pour affecter des informations ou systèmes d'information, tout en défendant les siennes.
Information Security : Résultat d'un système de règles et/ou de procédures pour identifier, contrôler, et protéger des informations dont la protection est autorisée par un ordre exécutif.
Information Superiority : Capacité à collecter, traiter, et disséminer un flot ininterrompu d'informations tout en exploitant et en empêchant un ennemi de faire de même.
Information Warfare : Actions effectuées pour achever un "Information Security" en affectant les informations, les processus d'information, et les systèmes d'information ennemis tout en défendant les siens. Action d'exploiter, de corrompre, de détruire ou d'empêcher le fonctionnement des informations ennemies et de leurs fonctions, tout en protégeant les siennes de ces actions.
Information Warfare (IW) : Opérations d'information conduites pendant une crise ou un conflit pour achever ou faire avancer des objectifs spécifiques sur un ou des ennemis spécifiques.
Intégrité : Assure que les informations ne seront pas, accidentellement ou intentionnellement, altérées ou détruites.
Internet Worm : Programme de type vers qui apparut sur Internet en 1988. Il fut codé par Robert T. Morris dans un but expérimental, mais l'expérience échappa à son contrôle.
Intrusion : Série d'actions tentant de compromettre l'intégrité, la confidentialité, ou la disponibilité d'une ressource.
Intrusion Detection (IDS / IPS) : Techniques tentant de détecter une intrusion dans un ordinateur ou un réseau par l'observation d'actions, de logs de sécurité, ou de données d'audits. Détections d'intrusions (ou tentatives d'intrusions) manuellement ou en utilisant des programmes qui se servent des logs ou autres informations disponibles sur le réseau.
IP Splicing/ Hijacking : Action par laquelle une session active établie est interceptée par un utilisateur non autorisé. Les attaques de type IP Splicing se produisent après l'identification, ce qui permet à l'attaquant d'assumer le rôle d'un utilisateur déjà autorisé. Les protections primaires contre l'IP Splicing consistent en une encyption au niveau de la session ou du réseau.
IP Spoofing : Action par laquelle un système tente de se faire passer illicitement pour un autre système en utilisant son adresse IP.

K

Key : Symbole ou séquence de symboles appliqués à un texte pour le crypter ou le décrypter.
Key Escrow : Système consistant à donner un morceau d'une clé à chacun des dépositaires, de manière que, avec la collaboration de chacun d'eux, la clé puisse être reconstituée dans sa totalité.
Keystore Monitoring : Forme spécialisée d'audit trail, ou matériel spécifique qui enregistre chaque clé tapée par un utilisateur et chaque caractère de la réponse que retourne l'AIS à l'utilisateur.

L

LAN (Local Arena Network) : Réseau Local. Système de communications informatiques limité à quelques kilomètres de distance et utilisant une connexion très rapide (de 2 à 10 Mega-octets par seconde). Système de communications sur courtes distances qui connecte des machines ADP dans un immeuble ou un groupe d'immeubles sur quelques kilomètres carrés, incluant des stations de travail, des processeurs, des contrôleurs, des commutateurs et des gateways.

Leapfrog Attack : Utilisation d'informations sur un UserID et un password obtenus illicitement d'un host pour compromettre un autre host. Action d'établir une connexion TELNET à travers un ou

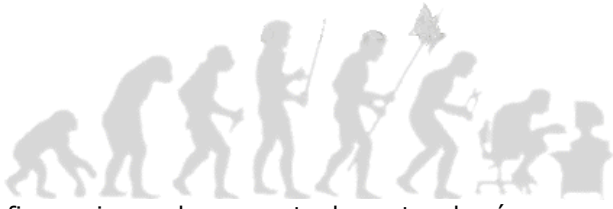
plusieurs hosts dans le but de diminuer les traces laissées.
Letterbomb : Partie d'un e-mail contenant des données ayant pour but d'affecter la machine ou le terminal du receveur. Sous Unix, une Letterbomb peut aussi tenter de faire interpréter son contenu comme une commande shell. Le résultat de ces attaques peut aller d'un simple divertissement à un Denial of Service.
Logic Bomb : Aussi connu sous le nom de Fork Bomb, programme résidant sur un système informatique, qui, quand il est exécuté recherche une condition particulière ou un état particulier du système pour exécuter une action illicite une fois cette condition trouvée.

M

Mailbomb : E-mails envoyés en masse vers un système unique ou une personne unique dans l'intention de Crasher la machine du destinataire. Le Mailbombing est très souvent considéré comme scandaleux.
Malicious code : Matériel, logiciel ou firmware qui est inclus volontairement dans un système dans le but d'y réaliser des opérations illégales (comme par exemple un Cheval de Troie).
Malware : Logiciel pour nuire à un système informatique
Metric : Variable x prise au hasard représentant une mesure quantitative accumulée après une période.
Mimicking : Synonyme de camouflage ou spoofing.
Misuse Detection Model : Le système détecte les intrusions en recherchant les activités qui correspondent à des techniques d'intrusion connues ou à des vulnérabilités systèmes. Aussi connu sous le nom de Rules Based Detection.
Mocking Bird : Programme informatique ou processus qui imite le comportement autorisé (ou tout autre fonction apparemment utile) d'un système normal mais qui exécutes des activités illégales une fois invoqué par l'utilisateur.
Multihost Based Auditing : Système d'audit de hosts multiples pouvant servir à détecter des intrusions.

N

NAK Attack : Technique de pénétration basée sur une faiblesse potentielle d'un système d'exploitation qui ne manipule pas bien les interruptions de désynchronisation et laisse ainsi le système sans protection durant ces interruptions.
National Information Infrastructure (NII) : Interconnections nationales de réseaux de communication, d'ordinateurs, de bases de données, et de consommations électroniques qui forment un grand ensemble d'informations disponible aux utilisateurs. Le NII comprend une large gamme d'équipements tels que des caméras, des scanners, des claviers, des machines fac-similées, des ordinateurs, des CD, des cassettes audio et vidéo, des câbles, des télégrammes, des satellites, des lignes de transmission par fibres optiques, des réseaux, des écrans, des imprimantes… Le personnel allié et ennemi qui prend les décisions et qui manipule les informations transmises constitue une partie critique du NII.
NCSC : voir National Computer Security Center.
Network : Réseau. Deux ou plusieurs machines connectées pour des communications.
Network Based : Trafic de données d'audits provenant de hosts et utilisés pour détecter les intrusions.



Network Level Firewall : Firewall analysant le trafic au niveau des paquets de protocole réseau (IP).
Network Security : Sécurité réseau. Protection des réseaux et de leurs services de modifications illicites, destruction, ou accès non autorisé à des ressources; et mesures de précautions assurant que le réseau exécute correctement ses fonctions critiques et qu'il n'y a pas d'effets nuisibles. La Sécurité Réseau inclut des vérifications d'intégrité des données.
Network Security Officer : Particulier nommé par une autorité désignée pour garantir que les mesures de sécurité et toutes les directives applicables sont implémentées sur le cycle de vie d'un AIS.
Network Weaving : Autre nom du "Leapfrogging".
Non-Discretionnary Security : Aspect de la politique de sécurité du DoD qui limite l'accès aux niveaux de sécurité de base. Un niveau de sécurité est composé d'un niveau de lecture et d'un niveau de réglage des restrictions. Pour un accès en lecture sur une ressource, un utilisateur doit avoir un accès d'un niveau identique ou plus élevé que celui de l'information et doivent avoir aussi accès à toutes les catégories incluses dans les catégories spécifiées pour l'accès à cette ressource.
Non-Repudiation : Méthode par laquelle l'expéditeur de données donne une preuve d'envoi et le receveur est assuré de l'identité de l'expéditeur, pour que personne ne puisse, par la suite, nier avoir traité ces données.

O

Open Security : Environnement ne fournissant pas un niveau de sécurité suffisant pour les applications et les équipements contre des pénétrations sur le système.
Open Systems Security : Réserve d'outils pour un travail Internet sécurisé entre systèmes ouverts.
Operational Data Security : Protection de données contre des modifications accidentelles ou illicites, la destruction, ou la révélation durant des opérations d'entrée ou sortie ou de traitement de ces données.
Operational Security :
1/ Action de renier les informations adverses sur les intentions et capacités alliées en identifiant, contrôlant et protégeant les indications sur les projets ou l'exécution d'opérations militaires ou autres activités.
2/ Processus d'analyse par lequel le gouvernement des Etats-Unis peut renier les informations adverses potentielles sur ses intentions et capacités, en identifiant, contrôlant et protégeant les projets et exécutions d'opérations et activités sensibles.
Operations Security (OPSEC) : Processus d'identification d'informations critiques et d'analyse des actions alliées en rapport avec des opérations militaires et autres activités, dans le but de :
a/ Identifier les actions qui peuvent être observées par les systèmes d'information ennemis.
b/ Déterminer les indications pouvant être obtenues par des systèmes d'information hostiles et pouvant être interprétés ou rassemblées pour en tirer des informations utiles aux ennemis.
c/ Sélectionner et exécuter des mesures éliminant ou réduisant les vulnérabilités d'actions alliées.
Orange Book : Voir Trusted Computer Security Evaluation Criteria.
OSI (Open Systems Interconnection) : Connexion de systèmes ouverts. Ensemble de standards reconnus internationalement et développés ouvertement ayant besoin d'administrer des ressources réseau.

P

Packet : Bloc de données envoyées sur le réseau transmettant : les identités des stations sources et destinations, les informations de contrôle d'erreur, et les messages. Synonyme de "trame".
Packet Filter : Inspecte chaque paquet pour trouver un type de contenu défini par l'utilisateur, tel

que une adresse IP, mais ne trace pas l'état des sessions. C'est un des types de Firewall les moins securisés.
Packet Filtering : Caractéristique incorporée aux routeurs limitant le flux d'informations basées sur les communications prédéfinies telles que la provenance, la destination, ou le type de service

fourni par le réseau. Les filtreurs de paquets permettent aux administrateurs de limiter le trafic de protocoles spécifiques, d'isoler les domaines de mail, et d'exécuter d'autres fonctions de contrôle du trafic.
Packet Sniffer : Appareil ou programme qui gère les échanges de données entre deux ordinateurs d'un réseau.
Passive Attack : Attaque ne résultant pas en un changement d'état illicite; telle qu'une attaque qui observe et enregistre seulement des données.
Passive Threat : Menaces de révélations illicites d'informations sans changement d'état du système. Type de menace impliquant l'interception et non l'altération d'informations.
PEM (Privacy Enhanced Mail) : Standard IETF servant à sécuriser les échange de courrier électronique.
Penetration : Réussite d'un accès non autorisé sur un système automatique.
Penetration signature : Description d'une situation ou d'une série de conditions dans lesquelles une pénétration pourrait se produire, ou d'événements système qui, assemblés, peuvent indiquer une pénétration en cours.
Penetration testing : Partie du Security Testing dans laquelle les évaluateurs tentent de tromper les sécurités d'un système. Les évaluateurs doivent assurer l'utilisation de toute l'architecture du système et de la documentation implémentée; cela peut inclure le listage du code source du système, des manuels, des diagrammes de circuit. Les évaluateurs travaillent sous les mêmes contraintes que celles appliquées aux utilisateurs ordinaires.
Perimeter Based Security : Action de sécuriser un réseau en contrôlant l'accès à toutes les entrées et sorties du réseau. Cette technique est souvent associée avec des firewalls et/ou des filtres.
Perpetrator : Entité de l'environnement externe pouvant représenter un risque. Entité de l'environnement externe exécutant une attaque; par exemple un Hacker.
Personnal Security : Procédures établies dans le but d'assurer que le personnel qui a accès a des informations classées disposes des autorisations requises.
PGP (Prettu Good Privacy) : Programme gratuit (freeware) utilisé principalement pour sécuriser le courrier électronique.
Phage : Programmes modifiant d'autres programmes ou des bases de données de façon illicite; par exemple, un programme propageant un virus ou un cheval de troie.
PHF: Programme de démonstration de fichier d'annuaire (Phone book file) que les Hackers utilisent pour gagner l'accès à un système informatique et pour lire et capturer des fichiers password.
PHF hack : CGI script connu pour sa vulnérabilité qui ne filtre pas les caractères spéciaux (ajout d'une ligne par exemple) tapés par l'utilisateur.
Phishing : Technique pour récupérer des informations personnelles.
Phraker : Personne combinant le phreaking téléphonique et le hacking informatique.
Phreak(er) : Personne fascinée par les systèmes téléphoniques. C'est habituellement une personne utilisant ses connaissances sur les systèmes téléphoniques afin de faire payer ses appels par quelqu'un d'autre.
Phreaking : L'art et la science de pirater le réseau téléphonique.
Physical Security : Mesures utilisées pour fournir des protections physiques aux ressources contre les menaces délibérées et accidentelles.
Piggy Back : Action d'obtenir un accès non autorisé sur un système par la connexion légitime d'un autre utilisateur.
Ping : Requête IP envoyée par l'ordinateur local demandant une réponse à l'ordinateur distant. Sert à connaitre si un ordinateur est connecté à un réseau et qu'il supporte IP.
Ping Of Death : Utilisation d'un ping avec un paquet de taille supérieure a 65507. Ce type d'attaque entraîne un Denial of Service.
Plain Text : Données non cryptées. Synonyme de "en clair".
Port : Interface logique de communication entre deux ordinateurs. Exemple : en TCP/IP, le port 21 est celui de FTP, 80 celui de http, etc...
Private Key Cryptography : Méthode d'encryption où l'encrypteur et le décrypteur utilisent la

même clé qui doit rester secrète. Cette méthode n'est utilisée habituellement que par des petits groupes.
Probe : Effort visant à rassembler des informations sur une machine ou sur ses utilisateurs dans le but évident de gagner plus tard un accès illicite sur le système.
Procedural Security : Voir Administrative Security.
Profile : Modèle d'activité pour un utilisateur pouvant détecter les changements dans les routines habituelles.
Promiscuous Mode : Habituellement, une interface Ethernet lit toutes les informations d'adressage et accepte uniquement les paquets lui étant exclusivement destinés; mais quand l'interface est en Promiscuous Mode, elle lit toutes les informations (sniffer) en portant peu attention à la destination.
Protocol : Méthodes universelles de communication utilisées par les Ordinateurs. Spécification décrivant les règles et les procédures que les produits doivent suivre pour pouvoir effectuer des activités telles que la transmission de données sur un réseau. Si ils utilisent les mêmes protocoles, les produits de constructeurs différents doivent pouvoir communiquer sur le même réseau.
Prowler : Robot effectuant régulièrement des tâches telles que rechercher et effacer des fichiers core, tronquer des logs de fichiers d'administration, détruire des répertoires perdus, et nettoyer le système.
Proxy : Mécanisme de type firewall qui remplace l'adresse IP d'un host sur un réseau interne par sa propre adresse IP pour tout le trafic circulant. Programme agissant selon les directives d'un utilisateur, les proxys caractéristiques acceptent une connexion d'un utilisateur, décident si l'utilisateur ou l'adresse IP du client est autorisée à utiliser le proxy, avec une éventuelle authentification, et complète ensuite une connexion vers la destination demandée par l'utilisateur.
Psycological Operations (PSYP) : Opérations organisées pour transmettre les informations et indication choisies à des gouvernements, groupes, organisations, ou particuliers étrangers dans le but d'influencer leurs émotions, leurs motivations, leurs raisonnements, et leur comportement. Le but de ces opérations psychologiques est d'induire ou de renforcer les attitudes et comportements étrangers en faveur des objectifs de l'initiateur de ces opérations.
Public Key Cryptography : Type de cryptopgraphie dans lequel le processus d'encryption est disponible au public et non protégé; mais dans lequel la clé de décryption est protégée de telle sorte que seul un groupe ayant connaissance des deux parties du processus de décryption puisse décrypter le texte crypté.

R

Ransomware: Logiciel chiffrant vos données et réclamant une rançon pour déchiffrer vos données.
Red Book : Voir Trusted Network Interpretation.
Reference Monitor : Concept de contrôle de sécurité dans lequel une machine virtuelle gère l'accès à des objets. En principe, un Reference Monitor devrait être complet (lorsque il gère tous les accès), isolé des modifications par les entités système, et son état vérifiable. Un centre de sécurité (Security Kernel) est une implémentation d'un Reference Monitor dans une base matérielle donnée.
Replicator : Programme agissant pour produire des copies de lui-même, ça peut être par exemple un programme, un Worm, une ForkBomb, ou un virus. Il est souvent dit que Unix et le C sont les deux moitiés pouvant amener à la création de Replicators très performants.
Retro-Virus : Un retro-virus est un virus qui attend jusqu'à ce que tous les médias disponibles soient aussi infectés pour qu'il ne soit plus possible de restaurer l'état normal du système.
Rexd : Cette commande Unix est celle du server Sun RPC pour l'exécution distante de programmes. Un bot lance les programmes dès qu'une requête est formulée.
Risk Assessement : Etude des vulnérabilités, menaces, probabilités, pertes et de l'efficacité théorique des mesures de sécurité. Procédure d'évaluation des menaces et vulnérabilités connues pour déterminer les pertes attendues et pour établir le degré de sécurité des opérations système.
Risk Management : Procédure visant à identifier, contrôler, et minimiser l'impact d'événements variables. Les objectifs des programmes de Risk Management est de réduire les risques et obtenir

et maintenir la DAA (Designated Approving Authority).
Rootkit : Outils de sécurité utilisés par les Hackers qui capture les mots de passe et le trafic de messages depuis et vers un ordinateur. Ensemble d'outils permettant au Hacker d'introduire une BackDoor dans un système, de collecter des informations sur les autres systèmes du réseau, de masquer les modifications qu'il a apporté au système… Un Rootkit est un des exemples classique des logiciels type Cheval de Troie. Des Rootkit sont disponibles pour un large panel de systèmes d'exploitation.
Router : Connexions d'appareils similaires à des ponts mais transportant des paquets et des

frames contenant certains protocoles. Les routeurs relient les LAN au niveau de la couche réseau.
Routing Control : Application de règles durant l'exécution de tâches de routage dans le but de pouvoir choisir d'éviter des réseaux, liens ou relais spécifiques.
RSA Algorithm : RSA pour Rivest-Shanir-Aldman. Algorithme d'encryption à clé publique simulant un système de cryptage très complexe.
Rules Based Detection : Système de détection d'intrusions recherchant des activités correspondant à des techniques d'intrusion connues (signatures) ou à des vulnérabilités système. Aussi connu sous le nom de Misuse Detection.

S

Samourai : Hacker proposant ses services pour des travaux de cracking légaux ou tout autre travail légitime nécessitant l'intervention d'un serrurier de l'électronique.
SATAN (Security Administration Tool For Analysing Networks) : Outil servant à sonder et identifier à distance les vulnérabilités de systèmes sur des réseaux IP. Programme puissant et gratuit aidant à identifier les faiblesses de sécurité système.
Secure Network Server : Appareil qui agit comme un portail entre une enclave protégée et le monde extérieur.
Secure Shell : Connexion shell entièrement cryptée entre deux machines et protégée par une phrase très longue pour mot de passe.
Sécurité administrative : Gestion limitée et contrôles supplémentaires des données afin de leur fournir un niveau de protection suffisant.
Security : Condition résultant de la mise en place et de la maintenance de mesures de protection assurant un état d'inviolabilité contre les actions ou influences hostiles.
Security Architecture : Description détaillée de tous les aspects du système se rapportant à la sécurité, accompagnée d'une série de principes guidant les projets. Une Architecture de Sécurité décrit la façon dont le système devrait être assemblé pour satisfaire le niveau de sécurité requis.
Security Audit : Recherche effectuée sur un système informatique visant à découvrir des problèmes et vulnérabilités de sécurité.
Security Countermeasures : Contre mesures destinées à des menaces et vulnérabilités spécifiques ou entraînant la mise en place de nouvelles activités de sécurité.
Security Domains : Ensemble d'objets auquel un sujet à la capacité d'accéder.
Security Features : Ensemble de mécanismes, fonctions et caractéristiques matérielles et logicielles d'un AIS relevant de la sécurité.
Security Incident : Action ou circonstance impliquant des informations classées dont les conditions varient de celles décrites par les publications de sécurité des administrateurs. Par exemple des compromis, des révélations de données, des détournements.
Security Kernel : Eléments matériels, logiciels, et firmware d'une Trusted Computing Base qui implémente les références d'un concept de surveillance. Un Security Kernel doit gérer tous les accès, doit être protégé des modifications extérieures, et son état doit être vérifiable.
Security Label : Partie sensible d'une information d'un sujet ou d'un objet, telle que sa classification hiérarchique (confidentiel, secret, top secret) ou une catégorie de sécurité non hiérarchique à laquelle il appartient (par exemple compartiment des informations sensibles, des informations critiques sur la fabrication d'armes nucléaires).
Security Level : Combinaison d'une classification hiérarchique et d'une série de catégories non

hiérarchiques représentant la sensibilité d'une information.
Security Officer : ADP officiel ayant la responsabilité de la sécurité d'un système ADP.
Security Perimeter : Limite à l'intérieur de laquelle les contrôles de sécurité sont effectifs pour protéger le système.
Security Policies : Série de lois, règles et pratiques régulant les moyens utilisés par une organisation pour gérer, protéger et distribuer des informations sensibles.
Security Policy Model : Présentation formelle des politiques de sécurité appliquées par un système. Ce modèle doit identifier la série de règles et pratiques régulant les moyens utilisés pour gérer, protéger et distribuer des informations sensibles.
Security Requirement : Types et niveaux de protection nécessaires aux équipements, aux données, aux informations, aux applications, et aux aménagements.
Security Service : Service, fournit par un ensemble de systèmes ouverts communiquants, qui assure une sécurité adéquate pour les systèmes ou les transferts de données.
Security Violation : Circonstance dans laquelle un utilisateur ou une autre personne trompe ou déjoue les contrôles d'un système pour obtenir un accès non autorisé aux informations contenues sur ce systèmes ou aux ressources système.
SEFTI : Service d'Enquête sur les Fraudes aux Technologies de l'Information : Service de la police française.
Server : Système fournissant de services réseaux tels que le stockage de données et le transfert de fichiers, ou un programme fournissant de tels services. Un bot (qui tourne souvent sur un autre système que celui du serveur) exécute un service pour une personne effectuant une requête.
Signaling System 7 (SS-7) : Protocole utilisé par les compagnies de téléphone. Il a trois fonctions de base : superviser, altérer, et adresser. Superviser consiste à examiner les statuts d'une ligne ou d'un circuit afin de déterminer si ils s'ont occupés, inactifs, ou en requête. Altérer consiste à indiquer la provenance d'un appel entrant. Adresser consiste à transmettre des signaux de routage et de destination sur le réseau sous forme de tonalités ou d'impulsions.
Simple Network Management Protocol (SNMP) : Protocole ou Programme utilisé pour contrôler les communications utilisant TCP/IP.
Skipjack : Algorithme d'encryption développé par la NSA pour le Clipper Chip. Les détails de l'algorithme ne sont pas publiés.
Smurfing : Attaque de type Denial of Service dans laquelle l'attaquant camoufle (spoof) l'adresse source d'un paquet ICMP de requête Echo (ping) au broadcast pour un réseau, ce qui entraîne toutes les machines du réseau à répondre en masse à la victime en encombrant de cette façon le réseau.
Snarf : Action de récupérer un fichier ou document important dans le but de l'utiliser, avec ou sans permission de l'auteur.
Sneaker : Particulier qui tente de pénétrer dans de systèmes dans le but de tester leur sécurité; semblable à une tiger team.
Sniffer : Programme capturant des données à travers un réseau informatique. Utilisé par les Hackers pour capturer des login, et des passwords. Outil logiciel qui surveille et identifie le trafic de paquets réseaux. Un sniffer peut aussi être utilisé légalement par le personnel d'opération et de maintenance du réseau pour résoudre les problèmes liés au réseau.
Spam : Attaque visant à cr asher un programme en faisant déborder un tampon (buffer) de taille fixe avec un trop grand nombre de données entrantes. Peut aussi servir à submerger (flood) une personne ou un newsgroup avec des messages sans rapport avec les autres ou inapropriés.
Special Information Operations (SIO) : Opérations d'information qui par leur nature sensible; a cause de leur effet ou impact potentiel, de leurs besoins en sécurité, ou des risques qu'elles peuvent faire encourir au gouvernement; exigent un examen et un processus d'approbation spéciaux.
SORM : "Echelon" russe.
SPI (Secure Profile Inspector) : Outil de surveillance réseau pour Unix, développé par le Département de l'Energie.
Spoofing : Action de se faire passe pour quelqu'un d'autre. Incitation délibérée à un utilisateur ou à une ressources à effectuer une action incorrecte. Tentative de gagner l'accès a un AIS en se faisant passer pour un utilisateur autorisé. Les personnifications (Impersonating), les actions de se masquer (Masquerading), et les simulations (Mimicking) sont des formes de spoofing.
Spyware : Logiciel espion
SSL (Secure Socket Layer) : Protocole de session par couches fournissant identification et

confidentialité aux applications.
Subversion : Se produit lorsque un intrus modifie les opérations du mécanisme de détection d'intrusions pour forcer un False Negative.
Syn Flood : Quand la SYN queue est submergée (flooded), aucune nouvelle connexion ne peut être ouverte.

T

TCP/IP : Transmission Control Protocol / Internet Protocol. Série de protocoles destinés au réseau sur lesquels est basé le réseau Internet.
Tcpwrapper : Outil logiciel fournissant des formes d'identification réseau supplémentaires, te limitant l'accès aux services aux hosts autorisés.
Term Rule Based Security Policy : Politique de sécurité basée sur des règles globales imposées à tous les utilisateurs. Ces règles consistent habituellement en une comparaison entre la sensibilité des ressources étant accédées, et la possession des attributs correspondants pour un utilisateur, un groupe d'utilisateurs ou des entités agissant selon les requêtes des utilisateurs.
Terminal Hijacking : Technique permettant à un attaquant, sur une certaine machine, de contrôler n'importe quelle session active de type terminal. Un Hacker attaquant ainsi peut envoyer et recevoir les entrées/sorties du terminal pendant qu'un utilisateur est sur le terminal.
Threat : Moyens par lesquels les capacités ou les intentions d'une menace visant à affecter les systèmes, aménagements; et des opérations ennemies peuvent être manifestées.
Threat Agent : Méthodes et objets utilisés pour exploiter une vulnérabilité sur un système d'informations, une opération, ou un aménagement.
Threat Assessement : Processus de routine évaluant le degré de menace pour un système et décrivant la nature de la menace.
Tiger : Outil logiciel qui scanne le système à la recherche de faiblesses.
Tiger Team : Equipes d'experts en informatique sponsorisés par les gouvernements et les grandes industries qui tentent de casser les défenses de systèmes informatiques dans le but de découvrir, et éventuellement de corriger, des trous de sécurité.
Tinkerbell Program : Programme de surveillance utilisé pour scanner les connexions réseau entrantes et pour générer des alertes quand des appels sont reçus d'un site particulier, ou quand des tentatives d'identification avec certains login sont effectuées.
Topology : Carte ou plan du réseau. La topologie physique décrit la façon dont les câbles et les fils sont installés, et la Topologie logique ou électrique décrit la façon dont les informations circulent.
Trace Packet : Dans un réseau de communications par paquets, paquet unique envoyant un rapport à chaque stade de sa progression au centre de contrôle réseau depuis chaque élément visité du système.
Traceroute : Action d'envoyer des paquets de type trace pour obtenir des informations; de tracer le chemin emprunté par les paquets UDP depuis le host local jusqu'à un host distant. Habituellement, un traceroute afficher la durée et la localisation du chemin emprunté pour atteindre la destination.
Tranquillity : Modèle de règle de sécurité correspondant à un état pour un objet actif où le niveau de sécurité ne peut pas être changé durant la période d'activité.
Tripwire : Outil logiciel pour la sécurité. Habituellement, il fonctionne avec une base de données qui maintient des informations sur la taille en octets des fichiers. Si la taille change, il prévient le responsable de sécurité du système.
Trojan Horse : Programme en apparence utile et inoffensif mais contenant du code caché supplémentaire permettant de récolter, d'exploiter, de falsifier ou de détruire des données de façon illicite.
Trusted Computer Systèm Evaluation Center (TCSEC) : Système employant suffisamment de mesures de sécurité logicielles et matérielles pour autoriser son utilisation pour des échanges simultanées d'informations et de données sensibles.
Trusted Computing Base (TCB) : Ensemble des mécanismes de protection d'un système informatique incluant le matériel, l'ensemble des logiciels, et le firmware. Une TCB consiste en un ou plusieurs composant qui mis ensembles, renforcent une politique de sécurité appliquée à un

produit ou un système.
Trusted Network Interpretation : Caractéristiques de sécurité spécifiques, protection suffisante et structures d'évaluation du livre orange (Orange Book) appliquées à des réseaux informatiques isolés de type LAN ou WAN.
TTY Watcher : Outil utilisé par les Hackers leur permettant, même avec de faibles connaissances, de faire du Terminal Hijacking. Les TTY Watchers utilisent une interface GUI.

V

Vaccines : Programme s'injectant dans un fichier exécutable afin d'en vérifier l'authenticité et d'avertir si un changement est effectué.
Virus : Programme pouvant infecter d'autres programmes en les modifiant pour y ajouter, éventuellement, une copie de lui-même.
Vulnerability : Défaut matériel, logiciel, ou firmware laissant un AIS ouvert à une exploitation potentielle. Faiblesse dans les procédures de sécurité, les contrôles d'administration, les contrôles internes, et autres; sur un systèmes informatisé; pouvant être exploité par une attaque visant à gagner un accès illicite aux informations, ou pour interrompre des processus critiques en cours.
Vulnerability Analysis : Examination systématique d'un AIS ou d'un produit dans le but de déterminer les mesures de sécurité adéquates, identifier les déficiences de sécurité, analyser l'efficacité des mesures proposées, et pour confirmer que de telles mesures seront adéquates une fois implémentées.

W

WAIS (Wide Area Information Service) : Service Internet permettant de rechercher parmi un grand nombre de bases de données classées par catégories.
WAN (Wide Area Network) : Réseau physique permettant à un certain nombre de machines indépendantes de communiquer entre elles par des protocoles de transmission communs sur des zones géographiques plus grandes que celle des réseaux locaux.
War Dialer : Programme composant une liste ou une série de numéros de téléphone et enregistre ceux qui répondent avec des tonalités spéciales, pouvant être des points d'entrée d'ordinateurs ou de systèmes de télécommunications.
Worm : Programme se reproduisant de machine en machine à travers les connexions réseau et les systèmes d'information quand il se répand.